ПРАКТИКУМ

АЛГЕБРА І ТЕОРІЯ ЧИСЕЛ

С. Т. ЗАВАЛО, С. С. ЛЕВІЩЕНКО,
В. В. ПИЛАЄВ, І. О. РОКИЦЬКИЙ

ПРАКТИКУМ

АЛГЕБРА І ТЕОРІЯ ЧИСЕЛ

Частина 2

Допущено Міністерством освіти УРСР як навчальний посібник для студентів фізико-математичних факультетів педагогічних інститутів

КИЇВ
ГОЛОВНЕ ВИДАВНИЦТВО
ВИДАВНИЧОГО ОБ'ЄДНАННЯ
«ВИЩА ШКОЛА»
1986

УДК 512+511 (076.5)

Алгебра и теория чисел: Практикум. Часть 2 / Завало С. Т., Левищенко С. С., Пылаев В. В., Рокицкий И. А. — К.: Вища шк. Головное изд-во, 1986. — 264 с. — Яз. укр.

Практикум составлен в соответствии с действующей программой курса «Алгебра и теория чисел» для физико-математических факультетов педагогических институтов.

Каждый параграф пособия имеет следующую структуру: сначала помещен список рекомендованной литературы с ссылкой на соответствующие параграфы и страницы, затем даны основные теоретические сведения и приведены подробные решения нескольких типичных задач. В конце параграфа имеются задачи для самостоятельного решения. К этим задачам даны ответы, указания, а иногда и полные решения.

Приложение содержит таблицу квадратов натуральных чисел от 1 до 99, таблицу простых чисел от 2 до 4057 и их наименьшие первообразные корни, таблицу первообразных корней и индексов по простому модулю от 2 до 97.

Предназначен для студентов физико-математических факультетов педагогических институтов.

Табл. 66. Ил. 2. Библиогр.: 44 назв.

Рецензенти: доценти *В. Г. Тарнопольський, М. М. Мурач* (Чернігівський педагогічний інститут), доцент *І. І. Мельник* (Херсонський педагогічний інститут)

Редакція літератури з математики і фізики
Зав. редакцією *Є. Л. Корженевич*

А 1702030000—20 / М211(04)—86 — 125—86

Розділ І. ТЕОРІЯ ПОДІЛЬНОСТІ В КІЛЬЦІ ЦІЛИХ ЧИСЕЛ

§ 1. Відношення подільності, його найпростіші властивості. Теорема про ділення з остачею

Література

[1] — § 5, с. 70—72;
[2] — § 5, с. 66—69;
[3] — гл. 4, § 4, с. 141—146;
[4] — гл. II, § 2, 4, с. 83—84, с. 104—105;
[8] — гл. 1, § 8, с. 59—60;
[10] — гл. 1, § 1, с. 7—9;
[11] — гл. 1, § 2, с. 18—20;
[12] — гл. I, § 1, с. 23—25;
[14] — § 1, с. 17—19.

ТЕОРЕТИЧНІ ВІДОМОСТІ

Якщо для цілих чисел a і b в кільці цілих чисел $\mathbf{Z}$ існує таке ціле число q, що $a = bq$, то кажуть, що «a ділиться на b» або «b ділить a» і пишуть відповідно $a \vdots b$, $b \mid a$. Число a при цьому називають **кратним** числа b, а b — **дільником** числа a. Якщо в кільці $\mathbf{Z}$ не існує числа q такого, що $a = bq$, то кажуть, що «a не ділиться на b», або «b не ділить a» і пишуть відповідно a не $\vdots b$, b не $\mid a$.

Нехай a, b, c, d, m, n — довільні цілі числа. Тоді:

1°. $a \vdots a$;
2°. $0 \vdots a$;
3°. $a \vdots \pm 1$;
4°. Якщо $a \vdots 0$, то $a = 0$;
5°. Якщо $a \vdots b$ і $b \vdots c$, то $a \vdots c$;
6°. Якщо $a \vdots c$, то $ab \vdots c$;
7°. Якщо $a \vdots c$ і $b \vdots c$, то $(a \pm b) \vdots c$;
8°. Якщо $a \vdots c$, $(a \pm b) \vdots c$, то $b \vdots c$;
9°. Якщо $a \vdots c$, b не $\vdots c$, то $(a \pm b)$ не $\vdots c$;
10°. Якщо $a \vdots b$, то $ac \vdots bc$;
11°. Якщо $ac \vdots bc$ і $c \neq 0$, то $a \vdots b$;
12°. Якщо $c \vdots a$, $d \vdots b$, то $cd \vdots ab$;
13°. Якщо $a \vdots c$, $b \vdots c$, то $(ma \pm nb) \vdots c$;
14°. Якщо $a \vdots b$ і $b \vdots a$, то $a = \pm b$;
15°. Якщо $a \vdots b$ і $|b| > |a|$, то $a = 0$.

Для будь-яких цілих чисел a і b, де $b \neq 0$, існує єдина пара цілих чисел q і r така, що $a = bq + r$, $0 \leqslant r < |b|$ (узагальнення теореми про ділення з остачею). Число q називають **неповною часткою**, а r — **остачею** від ділення a на b. Ціле число a тоді і тільки тоді кратне цілому числу $b \neq 0$, коли остача від ділення a на b дорівнює нулю.

ПРИКЛАДИ РОЗВ'ЯЗУВАННЯ ЗАДАЧ

1. При діленні цілого числа a на 17 неповна частка дорівнює 13. Знайти найбільше значення a.

Розв'язання. Маємо $a = 17 \cdot 13 + r$, де $0 \leqslant r < 17$. Отже, найбільше значення для a дорівнює $17 \cdot 13 + 16 = 237$.

2. При діленні числа $a = 50$ на число b остача $r = 6$. Знайти b і неповну частку q.

Розв'язання. Маємо $50 = bq + 6$, де $6 < b$. Тоді $bq = 44 = 44 \cdot 1 = 1 \cdot 44 = 22 \cdot 2 = 2 \cdot 22 = 11 \cdot 4 = 4 \cdot 11$. Оскільки $b > 6$, то b є одним з чисел 44, 22 або 11. Тоді q відповідно дорівнює 1, 2 або 4.

3. Знайти неповну частку q і остачу r від ділення цілого числа a на ціле число b, якщо: а) $a=37$, $b=8$; б) $a=8$, $b=37$; в) $a=37$, $b=-8$; г) $a=-37$, $b=8$; д) $a=8$, $b=-37$; е) $a=-8$, $b=-37$; є) $a=-8$, $b=37$; ж) $a=-37$, $b=-8$.

Розв'язання. Щоб знайти неповну частку q і остачу r при діленні цілого числа a на ціле число b, треба знайти найбільше ціле число k, яке кратне b і не перевищує a. Тоді неповну частку q дістають як частку від ділення k на b, а остачу r — як різницю між a та k. а) $k=32=8\cdot 4$. Отже, $q=4$, $r=5$; б) $k=0=37\cdot 0$, $q=0$, $r=8$; в) $k=32=(-8)\cdot(-4)$, $q=-4$ $r=5$; г) $k=-40=8\cdot(-5)$, $q=-5$, $r=3$; д) $k=0=(-37)\cdot 0$, $q=0$, $r=8$; е) $k=-37=(-37)\cdot 1$, $q=1$, $r=29$; є) $k=-37=37\cdot(-1)$, $q=-1$, $r=29$; ж) $k=-40=(-8)\cdot 5$, $q=5$, $r=3$.

Зауваження. Згідно з теорією, існує єдина пара чисел q і r для довільних цілих чисел a і b, $b\neq 0$, така, що $a=bq+r$, $0\leqslant r<|b|$. Тому аналогічну задачу можна розв'язувати у загальному випадку для довільних a і b, $b\neq 0$.

Наприклад, а) $a>0$, $b>0$, $a>b$; тут діленням a на b знаходимо q і r; б) $a>0$, $b>0$, $a<b$; тут $q=0$, $r=a$; в) $a>0$, $b<0$, $a>|b|$; діленням a на $|b|$ знаходимо q_1 і r, тоді $q=-q_1$; г) $a<0$, $b>0$, $|a|>b$; діленням $|a|$ на b знаходимо q_1 і r, тоді $q=-(q_1+1)$; д) $a>0$, $b<0$, $a<|b|$; тут $q=0$, $r=a$; е) $a<0$, $b<0$, $|a|<|b|$; тут $q=1$, $r=|b|-|a|$; є) $a<0$, $b>0$, $|a|<b$; тут $q=-1$, $r=b+a$; ж) $a<0$, $b<0$, $|a|>|b|$; діленням $|a|$ на $|b|$ знаходимо q_1 і r, тоді $q=q_1+1$.

4. Довести, що $n(n+1)(2n+1)\ \vdots\ 6$ при довільному натуральному n.

Розв'язання. *І спосіб (за методом математичної індукції).* При $n=1$ маємо $n(n+1)(2n+1)=6\ \vdots\ 6$. Припустимо, що при $n=k$ $k(k+1)(2k+1)\ \vdots\ 6$, і доведемо, що твердження справедливе й при $n=k+1$, тобто $(k+1)\cdot(k+2)(2k+3)\ \vdots\ 6$. Оскільки

$$(k+1)(k+2)(2k+3)=k(k+1)(2k+1)+6(k+1)^2,$$

то твердження очевидне, бо перший доданок ділиться на 6 за припущенням, а другий має своїм множником 6, тобто теж ділиться на 6. Тоді твердження $n(n+1)(2n+1)\ \vdots\ 6$ справедливе для довільного натурального числа n.

ІІ спосіб (за методом повної індукції). Оскільки $n(n+1)$ є добуток двох послідовних натуральних чисел, то $n(n+1)\ \vdots\ 2$ і тому $n(n+1)(2n+1)\ \vdots\ 2$. Оскільки $6=2\cdot 3$, а числа 2 і 3 не мають спільних дільників, то для того щоб $n(n+1)(2n+1)\ \vdots\ 6$, треба показати, що $n(n+1)(2n+1)\ \vdots\ 3$. Згідно з теоремою про ділення з остачею, можливі такі випадки: а) $n=3k$; б) $n=3k+1$; в) $n=3k+2$, де k — деяке ціле невід'ємне число. У випадку а) на 3 ділиться число $n=3k$, у випадку б) — число $2n+1=6k+3$, а у випадку в) — число $n+1=3k+3$. Цим доведено, що $n(n+1)(2n+1)$ завжди ділиться на 3. Твердження доведено.

ІІІ спосіб (штучний). Оскільки

$$n(n+1)(2n+1)=n(n+1)[(n-1)+(n+2)]=$$
$$=(n-1)n(n+1)+n(n+1)(n+2),$$

то доводжуване твердження випливає з того, що кожен доданок утвореної суми є добуток трьох послідовних чисел, а отже, він ділиться на 6.

Зауваження

1. При розв'язуванні аналогічних задач не можна віддати перевагу жодному з розглянутих способів. Так, для задачі 4 найраціональнішим є третій спосіб. Твердження, аналогічні розглянутим, завжди можна довести першим способом, хоч процес використання кроку індукції (кроку припущення) не завжди простий (при цьому часто використовується й узагальнена форма математичної індукції). Зрозуміло, що тільки вдале комбінування наведених та інших способів може зробити процес доведення ефективним і економним.

2. Доведення другим і третім способами свідчить про те, що твердження $n(n+1(2n+1)\ \vdots\ 6$ справедливе для будь-якого цілого числа n.

Задачі

1.1. Знайти неповну частку і остачу при діленні цілого числа a на ціле число b, якщо: а) $a=131$, $b=31$; б) $a=31$, $b=131$; в) $a=-131$, $b=31$; г) $a=-31$, $b=131$; д) $a=131$, $b=-31$; е) $a=31$, $b=-131$; є) $a=-31$, $b=-131$; ж) $a=-131$, $b=-31$.

1.2. При діленні цілого числа a на ціле число b дістають неповну частку q і остачу r. Знайти b і q, якщо: а) $a=100$, $r=6$; б) $a=148$, $r=37$; в) $a=298$, $r=10$; г) $a=497$, $r=16$; д) $a=28$, $r=2$; е) $a=14$, $r=14$.

1.3. При діленні цілого числа a на ціле число b утворюється неповна частка q і остача r. Знайти b і r, якщо: а) $a=371$, $q=14$; б) $a=826$, $q=83$; в) $a=441$, $q=25$; г) $a=57$, $q=0$; д) $a=13\,127$, $q=121$; е) $a=100$, $q=100$.

1.4. Знайти загальний вид усіх тих цілих чисел, які: а) діляться на 2; б) діляться на 3; в) діляться на 8; г) при діленні на 7 дають остачу 3; д) при діленні на -4 дають остачу 1; е) не діляться на 2; є) не діляться на -3; ж) не діляться на 2 і на 3.

1.5. Довести, що: а) з трьох послідових цілих чисел одне і тільки одне ділиться на 3; б) з двох послідовних парних цілих чисел одне і тільки одне ділиться на 4; в) з п'яти послідових цілих чисел одне і тільки одне ділиться на 5; г) з n послідовних цілих чисел одне і тільки одне ділиться на n.

1.6. Довести, що: а) добуток двох послідовних цілих чисел ділиться на 2; б) добуток трьох послідовних цілих чисел ділиться на 6; в) добуток чотирьох послідовних цілих чисел ділиться на 24; г) добуток n послідовних цілих чисел ділиться на $n!$.

1.7. Нехай m, n, p, q — цілі числа і $(mn+pq)\ \vdots\ (m-p)$. Довести, що $(mq+np)\ \vdots\ (m-p)$.

1.8. Довести, що:

а) квадрат непарного цілого числа при діленні на 8 дає остачу 1;

б) сума квадратів двох послідовних цілих чисел при діленні на 4 дає остачу 1;

в) числа виду $3k+2$, $k\in Z$ не можуть бути квадратами цілих чисел;

г) сума квадратів двох непарних цілих чисел не може бути квадратом цілого числа;

д) $(n^3-1)\ \vdots\ 7$, або $(n^3+1)\ \vdots\ 7$, якщо n не $\vdots\ 7$, $n\in Z$;

е) сума квадратів п'яти послідовних цілих чисел не може бути квадратом цілого числа;

є) якщо остача від ділення деякого цілого числа на 9 є одне з чисел 2, 3, 5, 6, 8, то це число не може бути квадратом цілого числа;

ж) якщо чисельник дробу є різниця квадратів двох непарних цілих чисел, а знаменник — сума квадратів цих чисел, то такий дріб можна завжди скоротити на 2, але не на 4.

1.9. Довести, що:

а) $(8\cdot 23^{23}-71\cdot 32^{32})\ \vdots\ 10$;

б) $(11^{10}-1)\ \vdots\ 100$;

в) $(2222^{5555} + 5555^{2222}) \vdots 7$.

1.10. Довести, що для довільних цілих чисел m і n:

а) $(n^3 - n) \vdots 6$;
б) $(n^5 - n) \vdots 30$;
в) $(n(n^2 + 5)) \vdots 6$;
г) $(n^7 - n) \vdots 42$;
д) $mn(m^4 - n^4) \vdots 30$;
е) $(n^5 - 5n^3 + 4n) \vdots 120$;
є) $(n^4 + 6n^3 + 11n^2 + 6n) \vdots 24$;
ж) $(n^3 + 11n) \vdots 6$;
з) $(n^2 + 3n + 5)$ не $\vdots 121$.

1.11. Довести, що для довільного натурального числа n:

а) $(2^{4n} - 6) \vdots 10$;
б) $(4^{2n} - 3^{2n} - 7) \vdots 84$;
в) $(6^{2n-1} + 1) \vdots 7$;
г) $(n+1)(n+2)\ldots(n+n) \vdots 2^n$;
д) $(3^{2n} + 5)$ не $\vdots 8$.

1.12. Довести, що для довільного цілого невід'ємного числа n:

а) $(5^{2n} - 1) \vdots 24$;
б) $(10^{3n} - 1) \vdots 27$;
в) $(15^n - 1) \vdots 7$;
г) $(3^{6n} - 2^{6n}) \vdots 35$;
д) $(11^{n+2} + 12^{2n+1}) \vdots 133$;
е) $(10^n + 18n - 1) \vdots 27$;
є) $(3^{2n+3} + 40n - 27) \vdots 64$;
ж) $(4^n + 6n - 1) \vdots 9$;
з) $(10^{n+1} - 9n - 10) \vdots 81$;
к) $(9^{n+1} - 8n - 9) \vdots 16$.

1.13. Довести, що $(2^{2n} - 6) \vdots 10$ для будь-якого натурального числа $n \geqslant 2$.

1.14. Довести, що числа 48, 4488, 444888, ... можна подати у вигляді добутку двох послідовних парних натуральних чисел.

1.15. Довести, що сума $2n+1$ послідовних натуральних чисел ділиться на $2^n + 1$.

1.16. Довести, що в піфагоровому трикутнику (прямокутному трикутнику, довжини сторін якого натуральні числа):

а) довжина, принаймні, одного катета ділиться на 3;
б) довжина, принаймні, однієї із сторін ділиться на 5.

1.17. Довести, що коли довжини сторін і діагоналей прямокутника є натуральні числа, то його площа ділиться на 12.

1.18. Довести, що корені квадратного рівняння $ax^2+bx+c=0$ з цілими непарними коефіцієнтами a, b, c не можуть бути раціональними.

1.19. Довести, що сума кубів трьох послідовних цілих чисел ділиться на 9.

§ 2. Означення і властивості простих та складених чисел. Решето Ератосфена. Канонічна форма натурального числа. Розподіл простих чисел серед чисел натурального ряду

Література

[1] — § 7, с. 89—92; § 8, с. 95—99;
[2] — § 7, с. 86—91; § 8, с. 93—98;
[3] — гл. II, § 1, с. 365—372;
[4] — гл. II, § 7, с. 124—134;

[8] — гл. I, § 8, с. 57—58;
[10] — гл. I, § 4, 5, с. 13—16;
[11] — гл. 2, § 1, 2, с. 28—38;
[12] — гл. I, § 4, с. 31—35.

ТЕОРЕТИЧНІ ВІДОМОСТІ

Натуральне число a, яке більше від 1 і дільниками якого є тільки 1 і a, називають **простим**. Натуральне число a, яке більше від 1 і в якого є дільники, відмінні від 1 і a, називають **складеним**. Число 1 має тільки один натуральний дільник — одиницю, тому воно не належить ні до простих, ні до складених чисел.

Найменший натуральний дільник складеного числа a, відмінний від 1, є число просте і не перевищує $\sqrt{a}$.

Теорема Евкліда. *Множина простих чисел нескінченна.*

Основна теорема арифметики. *Кожне відмінне від 1 натуральне число можна записати у вигляді добутку простих чисел і притому єдиним способом, якщо не брати до уваги порядок розміщення множників.*

Для складання таблиці простих чисел, які не перевищують даного натурального числа a, існує загальний спосіб, який називається **решетом Ератосфена**. Він полягає у послідовному викреслюванні з ряду 1, 2, ..., a числа 1, потім всіх чисел, кратних числу 2 (крім 2), потім — кратних числу 3 (крім 3) і т. д. Отже, слід викреслити всі числа, кратні простим числам: $p_1 = 2$, $p_2 = 3$, $p_3 = 5$, ..., $p_k \leqslant \sqrt{a}$ (удосконалення решета Ератосфена).

Усі невикреслені числа і складають таблицю простих чисел, які не перевищують числа a.

Якщо в розкладі натурального числа $a > 1$ на прості множники об'єднати однакові множники, то дістанемо так зване **канонічне зображення числа**

$$a = p_1^{k_1} p_2^{k_2} \ldots p_m^{k_m},$$

де p_i, p_j — різні прості числа, $i, j = 1, 2, \ldots, m$, $i \neq j$; k_i — натуральні числа.

Зрозуміло, що довільний дільник d числа a має такий вид: $d = p_1^{l_1} p_2^{l_2} \ldots p_m^{l_m}$, $0 \leqslant l_i \leqslant k_i$, $i = 1, 2, \ldots, m$ (це узагальнена канонічна форма числа d).

Через $\pi(x)$ позначають число простих чисел, які не перевищують натурального числа x.

Відомо, що $\lim\limits_{x \to \infty} \left[\pi(x) : \frac{x}{\ln x} \right] = 1$ **(асимптотичний закон розподілу простих чисел)**.

Відомо також, що

$$0{,}92129 \cdot \frac{x}{\ln x} < \pi(x) < 1{,}10555 \cdot \frac{x}{\ln x}$$

(нерівності Чебишова).

Теорема Діріхле. *У кожній арифметичній прогресії, перший член і різниця якої є взаємно прості числа, тобто не мають ніяких спільних дільників, крім 1, міститься нескінченна множина простих чисел.*

ПРИКЛАДИ РОЗВ'ЯЗУВАННЯ ЗАДАЧ

1. Просте чи складене число 323?

Розв'язання. Відомо, що натуральне число n, $n > 1$, є простим тоді і тільки тоді, коли воно не ділиться на жодне з простих чисел, які не перевищують $\sqrt{n}$. Знаходимо з надвишком $\sqrt{323} \approx 18$ і виписуємо всі прості числа, які не перевищують числа 18:

2, 3, 5, 7, 11, 13, 17.

Перевіряємо, чи ділиться число 323 на виписані числа. За ознаками подільності це число не ділиться на 2, 3, 5. Подільність на решту чисел перевіряємо безпосередньо.

В результаті дістаємо, що 323 не ділиться на 7, 11, 13, а ділиться на 17.

Відповідь. Число 323 є складеним.

Зауваження. Якщо існує точне значення $\sqrt{n}$, тобто $\sqrt{n} = k$, $k \in \mathbf{N}$, то n є складеним числом, бо $n \vdots k$.

Процес безпосередньої перевірки подільності числа n на виписані прості числа $p_1 = 2$, $p_2 = 3$, ..., p_k, $p_k \leqslant \sqrt{n}$ припиняється тільки у двох випадках: а) коли знайдеться таке число p_i, на яке ділиться n; б) коли перевірено подільність числа n на всі числа p_i, $i = 1, 2, \ldots, k$.

2. Знайти всі значення простого числа p, якщо $4p^2 + 1$ і $6p^2 + 1$ прості числа.

Розв'язання. Усі натуральні числа містяться серед чисел виду: $5n$, $5n \pm 1$, $5n \pm 2$, де $n \in \mathbf{Z}$. Числа виду $5n$ є простими тільки при $n = 1$; тоді $p = 5$, $4p^2 + 1 = 101$, $6p^2 + 1 = 151$. Оскільки числа 101 і 151 прості, то значення $p = 5$ задовольняє умову.

Покажемо тепер, що інших значень p немає. Справді, якщо $p = 5n \pm 1$, то $4p^2 + 1 = 5(20n^2 \pm 8n + 1)$ є складене число; якщо $p = 5n \pm 2$, то $6p^2 + 1 = 5(30n^2 \pm 24n + 1)$ теж складене число.

3. Знайти канонічний розклад числа 4725.

Розв'язання. Оскільки $4725 = 3 \cdot 1575$, а $1575 = 3 \cdot 525$, $525 = 3 \cdot 175$, $175 = 5 \cdot 35$, $35 = 5 \cdot 7$, то $4725 = 3 \cdot 3 \cdot 3 \cdot 5 \cdot 5 \cdot 7 = 3^3 \cdot 5^2 \cdot 7$.

Скорочено цей процес записують так:

4725	3
1575	3
525	3
175	5
35	5
7	7
1	

Зауваження

1. Якщо треба знайти канонічний розклад числа виду $k \cdot 10^s$, то слід знайти канонічний розклад числа k і здобутий результат домножити на число $2^s \cdot 5^s$.

2. Зрозуміло, що не завжди процес розкладу на прості множники є простим. Для непарних чисел існує спеціальний спосіб розкладу на прості множники. Розглянемо його у наступному прикладі.

4. Довести, що коли непарне натуральне число k, $k > 1$, можна подати у вигляді різниці квадратів двох цілих невід'ємних чисел єдиним способом, то воно просте. У противному разі k складене.

Доведення. Нехай k — деяке непарне натуральне число і $k = 2s + 1$, де s — деяке натуральне число. Припустимо, що k розкладається на множники $k = mn$. Не порушуючи загальності, можна вважати, що $m \geqslant n$. Тоді існують такі невід'ємні цілі числа x і y, що має місце система

$$\begin{cases} x + y = m, \\ x - y = n, \end{cases}$$

в якої

$$x = \frac{m+n}{2}, \quad y = \frac{m-n}{2}.$$

Отже, якщо k складене, то

$$k = mn = (x+y)(x-y) = x^2 - y^2 = \left(\frac{m+n}{2}\right)^2 - \left(\frac{m-n}{2}\right)^2.$$

Якщо k просте, то його можна єдиним способом подати у вигляді добутку $k = (2s+1) \cdot 1$. Тоді $m = 2s + 1 = k$ і $n = 1$.

$$k = \left(\frac{m+n}{2}\right)^2 - \left(\frac{m-n}{2}\right)^2 = \left(\frac{k+1}{2}\right)^2 - \left(\frac{k-1}{2}\right)^2.$$

Таким чином, якщо зображення

$$k = \left(\frac{k+1}{2}\right)^2 - \left(\frac{k-1}{2}\right)^2$$

(воно завжди існує, бо k непарне) є єдине, то k — просте.

Якщо, крім того,

$$k = \left(\frac{m+n}{2}\right)^2 - \left(\frac{m-n}{2}\right)^2,$$

де $n \neq 1$, то k — складене. Зазначимо, що коли k є квадрат числа m, то $x = m$, $y = 0$.

Зауваження

1. З доведення цього твердження випливає спосіб розкладання непарних чисел k, $k > 1$, на множники $(x+y)(x-y)$. Справді, з рівності $k = x^2 - y^2$ дістаємо $k + y^2 = x^2$. Отже, щоб знайти x і y, досить для числа k підібрати квадрат такого цілого невід'ємного числа y, щоб $y \leqslant \frac{k-1}{2}$ і сума $k + y^2$ була повним квадратом, тобто $k + y^2 = x^2$. Знайшовши таким способом x і y, маємо $k = (x+y)(x-y) = mn$.

2. Застосовуючи цей спосіб до розв'язування задач, доцільно користуватися таблицями квадратів натуральних чисел.

3. Для знаходження числа y іноді доводиться випробовувати кілька найближчих квадратів до числа k.

5. Знайти канонічний розклад чисел 4725 і 1769.

Розв'язання. Найближчий квадрат до числа 4725 є число 4761. Знаходимо різницю $4761 - 4725 = 36 = 6^2$. Отже, $4725 + 36 = 4761$, або $4725 + 6^2 = 69^2$. Тоді $4725 = 69^2 - 6^2 = (69+6) \cdot (69-6) = 75 \cdot 63 = 3 \cdot 5 \cdot 5 \cdot 3 \cdot 3 \cdot 7 = 3^3 \cdot 5^2 \cdot 7$. Остаточно маємо $4725 = 3^3 \cdot 5^2 \cdot 7$. Результат, зрозуміло, збігається з результатом прикладу 3.

За таблицею квадратів знаходимо найближчий квадрат до числа 1769. Це число 1849. Потім знаходимо різницю $1849 - 1769 = 80$. Оскільки число 80 не є квадратом, то беремо наступний квадрат — число 1936. Тоді $1936 - 1769 = 167$. Число 167 знову не є квадратом. Випробуємо наступний квадрат — число $2025 = 45^2$. Оскільки $2025 - 1769 = 256 = 16^2$, то $y = 4$. Отже, $1769 + 16^2 = 45^2$. Тоді $1769 = 45^2 - 16^2 = (45+16)(45-16) = 61 \cdot 29 = 29 \cdot 61$. Остаточно маємо $1769 = 29 \cdot 61$.

Задачі

2.1. Чи є числа 127, 919, 1033, 1643, 1657, 2647, 2773, 3163, 3621, 3623, 3631, 3763, 3767, 3769, 7429 простими?

2.2. Знайти всі прості числа, які містяться між числами:

а) 1 і 100;
б) 100 і 150;
в) 150 і 200;
г) 550 і 600;
д) 1250 і 1300;
е) 2300 і 2350;
є) 2550 і 2600;
ж) 4300 і 4350.

2.3. Знайти канонічний розклад числа n, якщо:

а) $n = 160$;
б) $n = 494$;
в) $n = 1001$;
г) $n = 1009$;
д) $n = 1769$;
е) $n = 1800$;
є) $n = 3551$;
ж) $n = 82798848$;
з) $n = 81057226635000$.

2.4. Довести, що дане число a є складеним, якщо:

а) $a = 2^{30} - 1$;
б) $a = n^4 + 4$, $n \neq \pm 1$ (теорема Софії Жермен);
в) $a = n^4 + n^2 + 1$, $n > 1$;

г) $a = n^8 + 4$, $n \neq \pm 1$;
д) $a = n^8 + n^4 + 1$, $n > 1$.

2.5. Знайти канонічний розклад числа a, якщо:
а) $a = 2^6 + 3^6$;
б) $a = 5^4 + 5^3 - 6$;
в) $a = 5^6 + 5^3 - 2$;
г) $a = 7^8 + 7^4 - 6$;
д) $a = 2^{18} + 3^{18}$;
е) $a = 235^2 + 972^2$;
є) $a = 3^{10} + 3^5 + 1$.

2.6. Знайти таке просте число p, щоб простими були також числа:

а) $p + 5$;
б) $2p^2 + 1$;
в) $p^2 + 8$;
г) $p + 10$ і $p + 14$;
д) $p + 4$ і $p + 14$;
е) $p + 2$ і $p + 4$;
є) $8p^2 + 1$ і $8p^2 + 2p + 1$;
ж) $2p + 1$ і $4p + 1$.

2.7. Довести, що три числа p, $p + m$, $p + n$ не можуть бути одночасно простими, якщо $p > 3$ і натуральні числа m і n дають при діленні на 3 відповідно остачі 1 і 2.

2.8. Довести, що з усіх цілих чисел виду $2p + 1$, де p — просте число, тільки одне є точним кубом.

2.9. Довести, що одночасно простими не можуть бути такі числа:

а) $p + 5$ і $p + 10$;
б) p, $p + 2$, $p + 5$;
в) $2^n - 1$ і $2^n + 1$, де $n > 2$.

2.10. Нехай p — просте число і $p > 5$. Довести, що p^2 при діленні на 30 дає остачу 1 або 19.

2.11. Нехай p_k є k-те просте число ($p_1 = 2$, $p_2 = 3$, $p_3 = 5$, $p_4 = 7$ і т. д.). Довести, що:
а) $p_k \leqslant 2^{2^{k-1}}$, причому рівність виконується тільки при $k = 1$;
б) $p_k > 2k$, де $k \geqslant 5$;
в) $p_{k+1} < p_1 p_2 \ldots p_k$, $k > 1$,
г) $p_1 p_2 \ldots p_k > n$, де $p_k \leqslant n$ і $n > 2$.

2.12. Довести, що коли пронумерувати всі прості числа, починаючи з 5, тобто $p_1 = 5$, $p_2 = 7$, $p_3 = 11$ і т. д., то $p_n > 3n$.

2.13. Нехай $M_n = 2^n - 1$, $n \in \mathbf{N}$. Показати, що коли M_n є просте число, то простим є також число n.

Примітка. Прості числа виду $M_n = 2^n - 1$ називаються **числами Мерсенна**. (Мерсенн Марен (1588—1648) — французький математик, фізик і філософ.) Нині відомо 27 чисел Мерсенна, причому 27-е число дістали при $n = 44497$. Скінченною чи нескінченною є множина чисел Мерсенна, невідомо.

2.14. Нехай $F_n = 2^n + 1$, $n \in \mathbf{N}$. Довести, що коли F_n просте число, то $n = 2^k$, де k — деяке ціле невід'ємне число.

Примітка. Прості числа виду $F_k = 2^{2^k} + 1$ називаються **числами Ферма**. (Ферма П'єр (1601—1665) — французький математик і юрист.) Досі не знайдено жодного простого числа виду $2^{2^k} + 1$ при $k \geqslant 5$ (при $k = 0, 1, 2, 3, 4$ числа F_k є простими), а також невідомо, скінченною чи нескінченною є множина чисел Ферма.

2.15. Довести, що $(p^2 - q^2) \vdots 24$, якщо p і q — прості числа, більші від 3.

2.16. Знайти всі прості числа, які є одночасно сумами і різницями простих чисел.

2.17. Нехай p — просте число і $p \geqslant 5$. Довести, що $(p^2 - 1) \vdots 24$.

2.18. Довести, що для будь-якого $n \in \mathbf{N}$ знайдеться таке $x \in \mathbf{N}$, що $nx + 1$ є складене.

2.19. Знайти натуральне число n, якщо:
а) $n = 2^\alpha$, $n + 1 = 3^\beta$, де α, β — деякі натуральні числа;
б) $n = 3^\alpha$, $n + 1 = 2^\beta$, де α, β — деякі натуральні числа.

2.20. Довести, що між натуральними числами n і $n!$, де $n > 2$, міститься, принаймні, одне просте число.

2.21. Знайти n послідовних складених натуральних чисел, якщо:
а) $n = 10$; б) $n = 12$; в) $n = 100$; г) $n = 1000$; д) $n = k$.

2.22. Довести нескінченність множини простих чисел виду:

а) $p = 3k + 2$, $k \in \mathbf{N}$;
б) $p = 3k + 1$, $k \in \mathbf{N}$;
в) $p = 4k + 1$, $k \in \mathbf{N}$;
г) $p = 4k + 3$, $k \in \mathbf{N}$;
д) $p = 6k + 1$, $k \in \mathbf{N}$;
е) $p = 6k + 5$, $k \in \mathbf{N}$.

§ 3. Найбільший спільний дільник і найменше спільне кратне та способи знаходження їх. Взаємно прості числа

Література

[1] — § 5, с. 72—79;
[2] — § 5, с. 69—76;
[3] — гл. 11, § 2—3, с. 372—379;
[4] — гл. 11, § 5, с. 109—119;
[8] — гл. 1, § 8, с. 59;
[10] — гл. 1, § 2, 3, с. 9—13;
[11] — гл. 3, с. 38—48;
[12] — гл. 1, § 2, 3, с. 25—31;
[14] — § 2, 3, 5, 6, с. 19—22, с. 24—28.

ТЕОРЕТИЧНІ ВІДОМОСТІ

Якщо кожне з цілих чисел $a_1, a_2, \ldots, a_n$ ділиться на ціле число d, то число d називають **спільним дільником** чисел $a_1, a_2, \ldots, a_n$. Найбільший із спільних дільників чисел $a_1, a_2, \ldots, a_n$ називається **найбільшим спільним дільником (НСД)** цих чисел і позначається символом $(a_1, a_2, \ldots, a_n)$.

Якщо найбільший спільний дільник чисел $a_1, a_2, \ldots, a_n$ дорівнює 1, то ці числа називають **взаємно простими**. Якщо кожне з чисел $a_1, a_2, \ldots, a_n$ взаємно просте з кожним з решти з них, то числа $a_1, a_2, \ldots, a_n$ називають **попарно взаємно простими**. Зрозуміло, що попарно взаємно прості числа завжди і взаємно прості (але не завжди навпаки). Для двох чисел поняття «попарно взаємно прості» збігається з поняттям «взаємно прості».

Нехай $a_1, a_2, \ldots, a_{n-1}, a_n$ — будь-які цілі числа, серед яких хоч одне відмінне від 0. Нехай $(a_1, a_2) = d_2$, $(d_2, a_3) = d_3, \ldots, (d_{n-2}, a_{n-1}) = d_{n-1}$, $(d_{n-1}, a_n) = d_n$. Тоді $(a_1, a_2, \ldots, a_n) = ((a_1, a_2), a_3), \ldots)$. На основі цього факту можна дати інше означення найбільшого спільного дільника.

Найбільшим спільним дільником чисел $a_1, a_2, \ldots, a_n$ називають невід'ємний спільний дільник цих чисел, який ділиться на будь-який їхній спільний дільник.

Якщо $a \mid b$, то $(a, b) = |b|$.

Якщо $a = bq + r$, де a, b, q, r — цілі числа, то $(a, b) = (b, r)$.

Якщо a, b, m — цілі числа, то $(am, bm) = (a, b) \cdot |m|$.

Якщо a, b — цілі числа, а k — який-небудь їхній спільний дільник, то $\left(\frac{a}{k}, \frac{b}{k}\right) = \frac{(a, b)}{|k|}$ (при цьому хоч одне з чисел a чи b відмінне від нуля).

Якщо $(a, b) = d$, то $\left(\frac{a}{d}, \frac{b}{d}\right) = 1$.

Якщо $d \mid a$, $d \mid b$ і $\left(\frac{a}{d}, \frac{b}{d}\right) = 1$, то $|d| = (a, b)$.

Для знаходження найбільшого спільного дільника двох чисел користуються способом послідовного ділення, який називають **алгоритмом Евкліда**. Розглянемо цей спосіб. Якщо a і b натуральні числа, то за теоремою про ділення з остачею послідовно дістаємо:

$$a = bq_1 + r_1, \quad \text{де} \quad 0 < r_1 < b,$$

$$b = r_1q_2 + r_2, \quad \text{де} \quad 0 < r_2 < r_1,$$

$$r_1 = r_2q_3 + r_3, \quad \text{де} \quad 0 < r_3 < r_2,$$

$$\cdots\cdots\cdots\cdots\cdots\cdots$$

$$r_{n-2} = r_{n-1}q_n + r_n, \quad \text{де} \quad 0 < r_n < r_{n-1},$$

$$r_{n-1} = r_nq_{n+1}, \quad \text{де} \quad r_{n+1} = 0.$$

Остання відмінна від нуля остача r_n і є найбільшим спільним дільником чисел a і b.

Згідно з алгоритмом Евкліда, якщо $(a, b) = d$, то існують такі цілі числа x і y, що $d = ax + by$, і навпаки (лінійне зображення найбільшого спільного дільника).

Для взаємно простих чисел справедливі такі властивості:

1°. Цілі числа a і b взаємно прості тоді і тільки тоді, коли існують цілі числа u та v такі, що $au + bv = 1$;

2°. Якщо $(a, b) = 1$, то $(ac, b) = (c, b)$;

3°. Якщо $(a, b) = (a, c) = 1$, то $(a, bc) = 1$;

4°. Якщо $ab \vdots c$, причому $(b, c) = 1$, то $a \vdots c$;

5°. Якщо $a \vdots b$ і $a \vdots c$, причому $(b, c) = 1$, то $a \vdots bc$;

6°. Якщо $(a, b) = 1$, то $(a^n, b^m) = 1$ для будь-яких цілих невід'ємних чисел n і m;

7°. Якщо для деяких двох натуральних чисел n і m $(a^n, b^m) = 1$, то $(a, b) = 1$;

8°. Якщо p_1, p_2 — різні прості числа, то $(p_1^n, p_2^m) = 1$ для будь-яких цілих невід'ємних n і m.

Нехай $a_1, a_2, \ldots, a_n$ — відмінні від нуля цілі числа. Ціле число k, яке ділиться на всі ці числа $a_1, a_2, \ldots, a_n$, називають **спільним кратним** цих чисел. Найменше з додатних спільних кратних чисел $a_1, a_2, \ldots, a_n$ називають **найменшим спільним кратним (НСК)** цих чисел і позначають символом $[a_1, a_2, \ldots, a_n]$.

Відомо, що $[a, b] = \frac{ab}{(a, b)}$, де a, b — довільні цілі числа, з яких хоча б одне відмінне від нуля. Ця формула лежить в основі першого способу знаходження найменшого спільного кратного двох чисел. Зокрема, найменше спільне кратне взаємно простих чисел дорівнює їхньому добутку.

Нехай $[a_1, a_2] = m_2$, $[m_2, a_3] = m_3$, $\ldots$, $[m_{n-2}, a_{n-1}] = m_{n-1}$, $[m_{n-1}, a_n] = m_n$. Тоді $[a_1, a_2, \ldots, a_n] = m_n$. Це дає змогу звести питання знаходження НСК кількох чисел до питання знаходження НСК двох чисел: $[a_1, a_2, \ldots, a_n] = [\ldots[[a_1, a_2], a_3], \ldots]$.

Наведемо інше означення найменшого спільного кратного.

Найменшим спільним кратним цілих чисел $a_1, a_2, \ldots, a_n$ називають невід'ємне спільне кратне цих чисел, на яке ділиться будь-яке їхнє спільне кратне.

Другий спосіб знаходження НСД і НСК цілих чисел $a_1, a_2, \ldots, a_n$ грунтується на канонічному зображенні цих чисел. Нехай числа a і b мають такі канонічні розклади:

$$a = r_1^{l_1} r_2^{l_2} \ldots r_m^{l_m}, \quad b = q_1^{s_1} q_2^{s_2} \ldots q_t^{s_t}.$$

Позначимо символами $p_1, p_2, \ldots, p_n$ усі різні прості множники, кожен з яких входить до розкладу хоч одного з чисел a і b. Якщо при цьому простий множник p_i не міститься в розкладі якого-небудь з чисел a і b, то вважатимемо, що він входить до цього розкладу в нульовому степені. За цієї умови канонічні розклади a і b можна записати так: $a = p_1^{k_1} p_2^{k_2} \ldots p_n^{k_n}$, $b = p_1^{m_1} p_2^{m_2} \ldots p_n^{m_n}$ (це узагальнені канонічні форми запису чисел a і b), де кожен з показників k_i і m_i, $i = 1, 2, \ldots, n$, є ціле невід'ємне число. Тоді справедливі такі рівності:

$$(a, b) = p_1^{d_1} p_2^{d_2} \ldots p_n^{d_n}, \quad \text{де} \quad d_i = \min(k_i, m_i), \quad i = 1, 2, \ldots, n.$$

$$[a, b] = p_1^{t_1} p_2^{t_2} \ldots p_n^{t_n}, \quad \text{де} \quad t_i = \max(k_i, m_i), \quad i = 1, 2, \ldots, n.$$

ПРИКЛАДИ РОЗВ'ЯЗУВАННЯ ЗАДАЧ

1. Знайти найбільший спільний дільник і найменше спільне кратне чисел 1917 і 1985.

Розв'язання. I *спосіб*. Скористаємося алгоритмом Евкліда для знаходження найбільшого спільного дільника.

1) Ділимо 1985 на 1917, дістаємо частку 1 і першу остачу 68;
2) ділимо 1917 на 68, дістаємо частку 28 і другу остачу 13;
3) ділимо 68 на 13, дістаємо частку 5 і третю остачу 3;
4) ділимо 13 на 3, дістаємо частку 4 і четверту остачу 1;
5) ділимо 3 на 1, дістаємо частку 3 і п'яту остачу 0.

Остання відмінна від нуля остача 1. Отже, $(1985, 1917) = 1$.

Наведені обчислення записують так:

$$\begin{array}{r|l} 1985 & 1917 \\ \hline 1917 & 1 \end{array} \qquad \begin{array}{r|l} 1917 & 68 \\ \hline 136 & 28 \end{array} \qquad \begin{array}{r|l} 557 & \\ \hline 544 & \end{array}$$

$$\begin{array}{r|l} 68 & 13 \\ \hline 65 & 5 \end{array} \qquad \begin{array}{r|l} 13 & 3 \\ \hline 12 & 4 \end{array} \qquad \begin{array}{r|l} 3 & 1 \\ \hline 3 & 3 \end{array} \qquad 0$$

Отже, числа 1985 і 1917 взаємно прості. Найменше спільне кратне цих чисел дорівнює їхньому добутку, тобто $[1985, 1917] = 1985 \cdot 1917 = 3805245$.

II *спосіб*. Знайдемо канонічні розклади чисел 1917 і 1985:

$$1917 = 3^3 \cdot 71, \quad 1985 = 5 \cdot 397.$$

Запишемо ці числа в узагальнених канонічних формах:

$$1917 = 3^3 \cdot 5^0 \cdot 71^1 \cdot 397^0, \quad 1985 = 3^0 \cdot 5^1 \cdot 71^0 \cdot 397^1.$$

Тоді $(1917, 1985) = 3^0 \cdot 5^0 \cdot 71^0 \cdot 397^0 = 1$, а

$$[1917, 1985] = 3^3 \cdot 5^1 \cdot 71^1 \cdot 397^1 = 3805245.$$

Зауваження. Цей спосіб доцільно застосовувати в тих задачах, де треба знайти НСД і НСК в канонічній формі.

2. Знайти найбільший спільний дільник d чисел 1917 і 1985, а також цілі числа x і y, за допомогою яких число d лінійно виражається через числа 1917 і 1985, тобто $d = 1917x + 1985y$.

Розв'язання. Скористаємося попереднім прикладом. Маємо:

$$1985 = 1 \cdot 1917 + 68,$$
$$1917 = 28 \cdot 68 + 13,$$
$$68 = 5 \cdot 13 + 3,$$
$$13 = 4 \cdot 3 + 1,$$
$$3 = 3 \cdot 1 + 0.$$

Починаючи з передостанньої рівності, знаходимо остачі:

$$d = 1 = 13 - 4 \cdot 3, \quad (1)$$
$$3 = 68 - 5 \cdot 13, \quad (2)$$
$$13 = 1917 - 28 \cdot 68, \quad (3)$$
$$68 = 1985 - 1 \cdot 1917. \quad (4)$$

Замінюватимемо послідовно остачі в цих рівностях, поки не залишаться числа 1917 і 1985. Остачу 3 у виразі (1) замінюємо виразом (2) і зводимо подібні члени (13 і 68):

$$1 = 13 - 4 \cdot 3 = 13 - 4 \cdot (68 - 5 \cdot 13) = 21 \cdot 13 - 4 \cdot 68.$$

У цій рівності замість множника 13 підставляємо вираз (3) і знову зводимо подібні члени (68 і 1917):

$$1 = 21 \cdot 13 - 4 \cdot 68 = 21 (1917 - 28 \cdot 68) - 4 \cdot 68 = -592 \cdot 68 + 21 \cdot 1917.$$

У знайденому виразі замість множника 68 підставляємо вираз (4) і знову зводимо подібні члени (1917 і 1985):

$$1 = -592 \cdot 68 + 21 \cdot 1917 = -592 (1985 - 1 \cdot 1917) + 21 \cdot 1917 =$$
$$= 613 \cdot 1917 - 592 \cdot 1985.$$

Отже, $1 = 613 \cdot 1917 - 592 \cdot 1985$, звідси $x = 613$, $y = -592$.

Зауваження

1. Може трапитись, що у виразах для остач (особливо на проміжних етапах, в процесі знаходження лінійного виразу для НСД) деякі неповні частки збігаються з якоюсь остачею. Тоді слід пильно стежити, щоб замість таких частот не було підставлено вираз для остачі.

2. Часто лінійне зображення НСД чисел a і b є громіздким і тому, щоб не робити повну перевірку, можна обмежитися тим, що ліва і права частини рівності $ax + by = d$ повинні мати однакові останні цифри. Так, у розглянутому прикладі права частина виразу $1 = 613 \cdot 1917 - 592 \cdot 1985$ закінчується цифрою 1, а ліва частина є 1.

3. Довести, що $(a, b) = (5a + 3b, 13a + 8b)$ для довільних цілих чисел a і b.

Розв'язання. Введемо позначення $(a, b) = d_1$, $(5a + 3b, 13a + 8b) = d_2$. Доведемо, що $d_1 = d_2$. Оскільки d_1 і d_2 — натуральні числа, то досить показати, що $d_1 \mid d_2$ і $d_2 \mid d_1$.

З означення d_1 маємо: $d_1 \mid a$ і $d_1 \mid b$. Тоді $d_1 \mid 5a + 3b$ і $d_1 \mid 13a + 8b$. Згідно з означенням числа d_2, $d_1 \mid d_2$.

Покажемо, що $d_2 \mid d_1$. Виразимо числа $5a + 3b$ і $13a + 8b$ через d_2. Дістанемо $5a + 3b = d_2x$, $13a + 8b = d_2y$, де x і y — деякі цілі числа. Домноживши першу рівність на 8, а другу на 3 і віднявши від першої рівності другу, знайдемо $a = d_2 (8x - 3y)$. Аналогічно дістаємо $b = d_2 (5y - 13x)$. Отже, $d_2 \mid a$ і $d_2 \mid b$. З означення числа d_1 випливає, що $d_2 \mid d_1$, що й треба було довести.

Зауваження. З доведення цього твердження випливає, що $(a, b) = (m_1a + m_2b, n_1a + n_2b)$, якщо $|m_1n_2 - m_2n_1| = 1$, де m_1, m_2, n_1, n_2 — цілі числа.

4. Знайти натуральні числа m і n, якщо їхня сума дорівнює 168, а найбільший спільний дільник 24.

Розв'язання. Використаємо факт: якщо $(a, b) = d$ і $a = da_1$, $b = db_1$, то $(a_1, b_1) = 1$.

У цьому разі $(m, n) = 24$. Тоді $m = 24m_1$, $n = 24n_1$, де $(m_1, n_1) = 1$. Оскільки $m + n = 168$, то $24m_1 + 24n_1 = 168$, тобто $m_1 + n_1 = 7$. Оскільки натуральні числа m_1 і n_1 взаємно прості, то розглядаючи всі можливі випадки, дістаємо, що m_1 і n_1 набувають таких значень: 1 і 6, 2 і 5, 3 і 4, і навпаки. Отже, числа m і n дорівнюють 24 і 144, 48 і 120, 72 і 96, і навпаки.

Задачі

3.1. Знайти найбільший спільний дільник чисел:

а) 0 і 0;
б) 0 і —7;
в) —231 і 546;
г) 1001 і 6253;
д) 1066 і 1970;
е) 1173 і 323;
є) 2585 і 7975;
ж) 2091 і 1681;
з) 3763 і 3337;
к) 6791400 і 178500;
л) I та H, де I — ваш поштовий індекс, а H — ваш рік народження;
м) T та H, де T — номер телефону деканату, а H — рік заснування факультету;
н) двох послідовних цілих чисел n і $n+1$.

3.2. Знайти найбільший спільний дільник таких чисел:

а) 819, 702 і 689;
б) 3059, 2737 і 943;
в) 2737, 9163 і 9639;
г) 299, 391 і 667;
д) 588, 2058 і 2849;
е) 31605, 13524, 12915 і 11067;
є) 42598, 2324 і 498;
ж) 1023, 1518 і 14883;
з) 3655, 2516, 731 і 663;
к) 91476, 3960 і 3360;
л) років народження всіх членів вашої сім'ї;
м) трьох послідовних цілих чисел n, $n+1$ і $n+2$.

3.3. Знайти найменше спільне кратне чисел:

а) 0 і 0;
б) 0 і 1;
в) 360 і 504;
г) 187 і 533;
д) —2520 і 6600;
е) 252 і 468;
є) 279 і 372;
ж) 178 і —381;
з) двох послідовних цілих чисел n і $n+1$.

3.4. Знайти найменше спільне кратне чисел:

а) 126, 420 і 525;
б) 91, 252 і 462;
в) 84, 147 і 245;
г) n, $n+1$ і $n+2$, де $n \in Z$;
д) 1058, 1403 і 3266;
е) 356, 1068 і 1424.

3.5. Знайти лінійне зображення найбільшого спільного дільника чисел:

а) 21 і 51;
б) —26 і 174;
в) 899 і 493;
г) 1445 і 629;
д) 903 і 731;
е) 1786 і 705;
є) 822 і 1734;
ж) 4373 і —826;
з) —3791 і 3281.

3.6. Довести, що для довільних натуральних чисел a і b:

а) $(a, b) = (a+b, a+2b)$;
б) $(a, b) = (2a+3b, 3a+4b)$;
в) $(a, b) = (7a+5b, 4a+3b)$;
г) $(a, b) = (3a+5b, 8a+13b)$;

д) $(a, b) = (4a+3b, 5a+4b)$;

е) $(a, b) = (ma+nb, ka+lb)$, де m, n, k, l — натуральні числа, причому $|ml-nk| = 1$.

3.7. Знайти натуральні числа a і b, якщо:

а) $\begin{cases} a+b = 150, \\ (a, b) = 30; \end{cases}$

б) $\begin{cases} a+b = 144, \\ (a, b) = 24; \end{cases}$

в) $\begin{cases} ab = 20, \\ [a, b] = 10; \end{cases}$

г) $\begin{cases} ab = 8400, \\ (a, b) = 20; \end{cases}$

д) $\begin{cases} ab = 720, \\ (a, b) = 4; \end{cases}$

е) $\begin{cases} \frac{a}{b} = \frac{11}{7}, \\ (a, b) = 45; \end{cases}$

є) $\begin{cases} \frac{a}{b} = \frac{5}{9}; \\ (a, b) = 28; \end{cases}$

ж) $\begin{cases} (a, b) = 4, \\ [a, b] = 24; \end{cases}$

з) $\begin{cases} (a, b) = 4, \\ [a, b] = 12; \end{cases}$

к) $\begin{cases} (a, b) = 24, \\ [a, b] = 2496; \end{cases}$

л) $\begin{cases} a+b = 667, \\ [a, b] = 120\,(a, b); \end{cases}$

м) $\begin{cases} \frac{a}{(a, b)} + \frac{b}{(a, b)} = 18, \\ [a, b] = 975; \end{cases}$

н) $\begin{cases} ab = 168, \\ (a, b) = 14. \end{cases}$

3.8. Довести, що для довільних натуральних чисел a, b, c:

а) $(a, b) = (-a, b) = (a, a \pm b) = (a \pm b, b)$;

б) $(ab, bc, ca) \vdots (a, b, c)^2$;

в) $(a, b) = (a+b, [a, b])$, якщо $(a, b) \neq 0$;

г) $(a, b, c) = \left(\frac{a+b}{2}, \frac{a+c}{2}, \frac{b+c}{2}\right)$, якщо a, b, c — непарні числа;

д) $[a, b, c] = \frac{abc\,(a, b, c)}{(a, b)(a, c)(b, c)}$;

е) $(a, b)(a, c)(b, c)[a, b][a, c][b, c] = a^2b^2c^2$;

є) $abc = [a, b, c] \cdot (ab, ac, bc)$;

ж) $(a, [b, c]) = [(a, b), (a, c)]$;

з) $[a, (b, c)] = ([a, b], (a, c])$;

к) $(aa_1, bb_1, ab_1, a_1b) = dd_1$, якщо $d = (a, b)$, $d_1 = (a_1, b_1)$;

л) $([a, b], (a, b)) = (a, b)$;

м) $([a, b], ab) = [a, b]$.

3.9. Довести, що для довільних натуральних чисел a, b, c:

а) $(a, a+1) = (a+1, 2a+1) = (a, 2a+1) = 1$;

б) $(a, 2a+1) = (a, 2a-1) = 1$;

в) $\left(2a+1, \frac{a(a+1)}{2}\right) = 1$;

г) $(14a+3, 21a+4) = 1$;

д) $(b-a, b) = 1$, якщо $(a, b) = 1$;

е) $(a+b, ab) = 1$, якщо $(a, b) = 1$;

є) $(a, a+b) = (a+b, 2a+b) = (a, 2a+b) = 1$, якщо $(a, b) = 1$;

ж) $(ac, b) = (c, b)$, зокрема, $c : (ac, b)$, якщо $(a, b) = 1$;

з) $(a+b, a-b) = 1$ або 2, якщо $(a, b) = 1$;

к) $(2^a-1, 2^b-1) = 1$, якщо $(a, b) = 1$;

л) $(11a+2b, 18a+5b) = 1$ або 19, якщо $(a, b) = 1$;

м) $\left(\frac{[a, b]}{a}, \frac{[a, b]}{b}\right) = 1$;

н) $(a^3+2a, a^4+3a^2+1) = 1$.

3.10. Знайти найбільший спільний дільник чисел:

а) a^n-1 і a^m-1, якщо a — ціле, а m і n — натуральні числа;

б) a^2+1 і $2a+3$, якщо a — ціле число;

в) 2^6-1 і $2^{15}-1$.

3.11. Довести, що з п'яти послідовних цілих чисел завжди можна вибрати одне, взаємно просте з усіма іншими.

3.12. Довести, що:

а) $2903^n - 803^n - 464^n + 261^n \vdots 1897$, якщо n — натуральне число;

б) $n(n+1)(n+2) \vdots 504$, якщо $n+1$ є кубом деякого натурального числа;

в) $a^{4n+1} - a \vdots 30$, якщо a — ціле, а n — невід'ємне ціле число;

г) $a^3 - b^3 \vdots 2^n$ тоді і тільки тоді, коли $a-b \vdots 2^n$, де a, b — цілі непарні числа, n — натуральне число;

д) $(a+1, a^{2k}+1) = 1$, якщо a — парне натуральне число, а k — довільне натуральне число.

§ 4. Числові функції. Число і сума натуральних дільників. Ціла і дробова частини дійсного числа. Функція Ейлера

Література

[1] — § 7, с. 93—95, § 16, с. 169—174;
[2] — § 7, с. 92—93, § 16, с. 173—178;
[3] — гл. 11, § 1, с. 368—369, гл. 12, § 3, с. 406—408;
[4] — гл. II, § 8, с. 134—146;
[10] — гл. II, с. 25—32;
[11] — гл. 10, с. 92—95; гл. 33, с. 315—322;
[12] — гл. II, § 4, с. 52—56; гл. VIII, с. 229—246;
[14] — § 11—14, с. 49—63.

ТЕОРЕТИЧНІ ВІДОМОСТІ

Функцію $f(x)$ називають числовою, якщо вона визначена при всіх натуральних значеннях аргументу x.

Через $\tau(n)$ позначають числову функцію, значення якої для будь-якого натурального числа n дорівнює числу всіх його натуральних дільників.

Через $\sigma(n)$ позначають числову функцію, значення якої для будь-якого натурального числа n дорівнює сумі всіх його натуральних дільників.

Через $\varphi(n)$ позначають числову функцію, значення якої для будь-якого натурального числа n дорівнює кількості натуральних (цілих невід'ємних) чисел, взаємно простих з n, які не перевищують (відповідно менших) n. Функцію $\varphi(n)$ називають **функцією Ейлера**.

Через $[x]$ (читається «антьє від x») позначають числову функцію, значення якої для будь-якого дійсного числа x дорівнює найбільшому цілому числу, яке не перевищує x. Функцію $[x]$ називають **цілою частиною від x**.

Через $\{x\}$ позначають числову функцію, значення якої для будь-якого дійсного числа x дорівнює різниці $x - [x]$. Функція $\{x\}$ називається **дробовою частиною** від x.

Числова функція $f(n)$ називається **мультиплікативною**, якщо для кожного n функція $f(n) \neq 0$ і для будь-яких взаємно простих натуральних чисел n і m виконується рівність $f(m \cdot n) = f(m) \cdot f(n)$.

Мультиплікативні функції мають такі **властивості**:

1°. $f(1) = 1$;

2°. Добуток мультиплікативних функцій є мультиплікативна функція;

3°. Якщо числа $n_1, n_2, \ldots, n_k$ попарно взаємно прості, то $f(n_1 \cdot n_2 \ldots n_k) = f(n_1) f(n_2) \ldots f(n_k)$.

Числові функції $\tau(n)$, $\sigma(n)$, $\varphi(n)$ мультиплікативні. Якщо $n = p_1^{k_1} p_2^{k_2} \ldots p_m^{k_m}$ — канонічний розклад натурального числа n, то

$$\tau(n) = (k_1 + 1)(k_2 + 1) \ldots (k_m + 1),$$

$$\sigma(n) = \frac{p_1^{k_1+1} - 1}{p_1 - 1} \cdot \frac{p_2^{k_2+1} - 1}{p_2 - 1} \cdot \ldots \cdot \frac{p_m^{k_m+1} - 1}{p_m - 1},$$

$$\varphi(n) = n\left(1 - \frac{1}{p_1}\right)\left(1 - \frac{1}{p_2}\right) \ldots \left(1 - \frac{1}{p_m}\right).$$

Зрозуміло, що $\tau(1) = \sigma(1) = \varphi(1) = 1$, згідно з означенням цих функцій.

Сума значень функції Ейлера для всіх дільників d_j числа n дорівнює n:

$$\sum_j \varphi(d_j) = n \qquad \text{(формула Гаусса)}.$$

Якщо x — дійсне додатне число, а n — натуральне число, то $\left[\frac{[x]}{n}\right] = \left[\frac{x}{n}\right]$.

Показник α простого числа p, яке входить до канонічного розкладу натурального числа $n!$, обчислюється за формулою

$$\alpha = \left[\frac{n}{p}\right] + \left[\frac{n}{p^2}\right] + \ldots + \left[\frac{n}{p^s}\right], \quad \text{де } p^s \leqslant n < p^{s+1}.$$

ПРИКЛАДИ РОЗВ'ЯЗУВАННЯ ЗАДАЧ

1. Знайти суму дільників, число дільників і дільники числа 680.

Розв'язання. Знаходимо канонічний розклад числа 680: $680 = 2^3 \cdot 5 \cdot 17$. Тоді

$$\tau(680) = (3 + 1)(1 + 1)(1 + 1) = 16,$$

$$\sigma(680) = \frac{2^{3+1} - 1}{2 - 1} \cdot \frac{5^{1+1} - 1}{5 - 1} \cdot \frac{17^{1+1} - 1}{17 - 1} = 1620.$$

Дільники числа 680 дістанемо, коли розкриємо дужки у виразі

$$(1 + 2 + 4 + 8) \cdot (1 + 5) \cdot (1 + 17).$$

Матимемо:

1, 2, 4, 8, 5, 10, 20, 40, 17, 34, 68, 136, 85, 170, 340, 680.

2. Знайти натуральне число x, якщо воно має тільки два різних простих дільники і $\tau(x) = 6$, $\sigma(x) = 28$.

Розв'язання. Оскільки число x має тільки два різних простих дільники (нехай це числа p і q), то канонічний розклад числа x має вид: $x = p^y q^z$, де y і z — деякі натуральні числа. Тоді

$$\tau(x) = (y + 1)(z + 1), \quad \sigma(x) = \frac{p^{y+1} - 1}{p - 1} \cdot \frac{q^{z+1} - 1}{q - 1}.$$

Оскільки $\tau(x) = 6$, то $(y + 1)(z + 1) = 6$. Внаслідок того що числа y і z натуральні, $y = 1$, $z = 2$ або навпаки. Тоді $x = pq^2$ і $\sigma(x) = (p + 1)(q^2 + q + 1)$. Оскільки $\sigma(x) = 28$, то $(p + 1)(q^2 + q + 1) = 28$.

Через те що p і q — різні прості числа, слід розглянути такі можливі випадки: $p + 1 = 4$, $q^2 + q + 1 = 7$ або навпаки. Якщо $p + 1 = 4$, $q^2 + q + 1 = 7$, то $p = 3$, а $q = 2$. Тоді $x = 3^1 \cdot 2^2 = 12$. Якщо $p + 1 = 7$, $q^2 + q + 1 = 4$, то $p = -6$, що суперечить вибору числа p. Отже, єдиним числом, яке задовольняє умову задачі, є число $x = 12$.

3. Знайти натуральне число n, якщо $\varphi(n) = 600$ і $n = 3^\alpha \cdot 5^\beta$, де α, β — натуральні числа.

Розв'язання. Оскільки

$$\varphi(n) = \varphi(3^\alpha 5^\beta) = 3^\alpha 5^\beta \left(1 - \frac{1}{3}\right)\left(1 - \frac{1}{5}\right) = 3^\alpha 5^\beta \cdot \frac{2}{3} \cdot \frac{4}{5},$$

то

$$600 = 3^\alpha 5^\beta \cdot \frac{2}{3} \cdot \frac{4}{5}.$$

Звідси

$$3^2 5^3 = 3^\alpha 5^\beta.$$

Ця рівність можлива тільки при $\alpha = 2$ і $\beta = 3$. Тоді $n = 3^2 \cdot 5^3 = 1125$.

4. Знайти кількість нулів, якими закінчується число 295!

Розв'язання. Щоб розв'язати цю задачу, треба знайти канонічний розклад заданого числа. Справді, якщо $n! = p^\alpha q^\beta \ldots r^\gamma$, то кількість нулів, якими закінчується число, збігатиметься з числом m, де m — менше з чисел k і s, а k і s — показники чисел 2 і 5 відповідно в канонічному розкладі числа $n!$. Оскільки до канонічного розкладу числа $n!$ просте число 5 входить з меншим показником, ніж просте число 2, то для розв'язання задачі досить знайти показник s, з яким просте число 5 входить до добутку $n!$. Як відомо, s знаходять за формулою

$$s = \left[\frac{n}{p}\right] + \left[\frac{n}{p^2}\right] + \left[\frac{n}{p^3}\right] + \ldots$$

Оскільки $\left[\frac{n}{p^{i+1}}\right] = \left[\frac{\left[\frac{n}{p^i}\right]}{p}\right]$, то для нашого прикладу маємо

$$s = \left[\frac{295}{5}\right] + \left[\frac{59}{5}\right] + \left[\frac{11}{5}\right] = 59 + 11 + 2 = 72.$$

Отже, число 295! закінчується 72-ма нулями.

Задачі

4.1. Знайти число і суму всіх натуральних дільників таких чисел: а) 60; б) 100; в) 360; г) 375; д) 720; е) 957; є) 988; ж) 990; з) 1000; к) 1200; л) 1542; м) 3500.

4.2. Знайти всі натуральні дільники чисел: а) 24; б) 50; в) 100; г) 360; д) 375.

4.3. Знайти натуральне число n, якщо:

а) n ділиться тільки на два простих числа і $\tau(n) = 6$, а $\sigma(n) = 42$;

б) $\tau(n) = 1, 2, 3, 4, 5$ або 6 відповідно;

в) n має тільки два простих дільники, $\tau(n) = 12$, $\sigma(n) = 1240$;

г) n має тільки два простих дільники, $\tau(n) = 12$, $\sigma(n) = 465$;

д) $n : 12$ і $\tau(n) = 14$;

е) n — найменше натуральне число, для якого $\tau(n) = 14$;

є) n — найменше натуральне число, для якого $\tau(n)=18$;
ж) n — найменше натуральне число, для якого $\tau(n)=100$;
з) добуток усіх його натуральних дільників дорівнює 5832;
к) $n=2^x3^y5^z$, $\tau\left(\frac{1}{2}n\right)=\tau(n)-30$, $\tau\left(\frac{1}{3}n\right)=\tau(n)-35$,
$\tau\left(\frac{1}{5}n\right)=\tau(n)-42$;
л) n — найменше натуральне число виду $2^xp_1p_2$, де p_1 і p_2 — різні непарні прості числа і $\sigma(n)=3n$ (задача Ферма);
м) добуток усіх його натуральних дільників дорівнює $3^{30}\cdot5^{40}$;
н) $n=2^x\cdot3^y\cdot5^z$, $\tau(5n)=\tau(n)+8$, $\tau(7n)=\tau(n)+12$, $\tau(8n)=\tau(n)+18$.

4.4. Довести, що:
а) існує нескінченна множина натуральних чисел m, для яких $\sigma(m)=2m-1$;
б) множина всіх натуральних чисел, більших від одиниці, кожне з яких дорівнює добутку всіх своїх натуральних дільників, збігається з множиною всіх простих чисел;
в) $\tau(n)$ непарне тоді і тільки тоді, коли n — квадрат натурального числа;
г) добуток усіх дільників числа n дорівнює $n^{\frac{\tau(n)}{2}}$;
д) $(n,\ \tau(m^n))=1$, де n, m — натуральні числа;
е) $\tau(m)\tau(n)>\tau(mn)$, якщо $(m,\ n)>1$;
є) $\sigma(m)\sigma(n)>\sigma(mn)$, якщо $(m,\ n)>1$;
ж) $n=\dfrac{d_1+d_2+\ldots+d_k}{\frac{1}{d_1}+\frac{1}{d_2}+\ldots+\frac{1}{d_k}}$, де $d_1,\ d_2,\ \ldots,\ d_k$ — усі дільники числа n.

4.5. Нехай n — натуральне число. Знайти $\tau(n^3)$, якщо:
а) $\tau(n^2)=15$ і n має тільки два простих дільники;
б) $\tau(n^2)=81$ і n має тільки два простих дільники;
в) $\tau(n^2)=105$ і n має тільки три простих дільники.

4.6. Натуральне число n називається **досконалим**[1], якщо $\sigma(n)=2n$. Довести, що:
а) 6, 28, 496, 8128 — досконалі числа;
б) парне число n є досконалим тоді і тільки тоді, коли $n=2^{k-1}\cdot(2^k-1)$, де $k\geqslant2$, а $p=2^k-1$ — просте число[2] (теорема Евкліда — Ейлера);
в) довільне натуральне число з одним простим дільником не є досконалим;
г) непарне натуральне число з двома простими дільниками не є досконалим.

4.7. Два натуральних числа m і n називаються **дружніми**[3], якщо $\sigma(m)=m+n$. Довести, що дружніми є такі пари чисел:
а) 220 і 284; б) 1184 і 1210; в) 2620 і 2924.

4.8. Побудувати графіки функцій $y=\tau(x)$ і $y=\sigma(x)$, де $1\leqslant x\leqslant20$.

4.9. Знайти функцію Ейлера для чисел: а) 17; б) 31; в) 100; г) 200; д) 375; е) 625; є) 720; ж) 1000; з) 1200.

4.10. Знайти кількість натуральних чисел, які менші від числа n і мають з ним найбільший спільний дільник d, якщо:
а) $n=300$, $d=20$;
б) $n=1476$, $d=41$;
в) $n=1665$, $d=37$;
г) $n=975$, $d=13$;
д) $n=1072$, $d=8$;
е) $n=2500$, $d=50$;
е) $n=2476$, $d=619$.

4.11. Довести, що:
а) $\varphi(n)$ — парне число при $n\geqslant3$;
б) $\varphi(4n)=2\varphi(2n)$, $n\in\mathbf{N}$;
в) $\varphi(4n+2)=\varphi(2n+1)$, $n\in\mathbf{N}$;
г) $S=\frac{1}{2}n\varphi(n)$, де S — сума натуральних чисел, які взаємно прості з числом n і менші від n;
д) $\varphi(5n)\neq\varphi(7n)$ для всіх $n\in\mathbf{N}$;
е) якщо рівняння $\varphi(x)=a$ має корінь $x=m$, де m не : 2, то воно має також корінь $x=2m$;
є) $\varphi(mn)=\varphi(m)\cdot\varphi(n)\cdot\frac{(m,\ n)}{\varphi((m,\ n))}$, $m,\ n\in\mathbf{N}$;
ж) $\varphi(mn)=\varphi((m,\ n))\,\varphi([m,\ n])$, $m,\ n\in\mathbf{N}$;
з) $\varphi(mn)>\varphi(m)\varphi(n)$, якщо $(m,\ n)>1$.

4.12. Розв'язати рівняння:
а) $\varphi(x)=8$;
б) $\varphi(x)=12$;
в) $\varphi(x)=14$;
г) $\varphi(x)=p-1$, p — просте число;
д) $\varphi(x)=2^k$, $k\in\mathbf{N}$;
е) $\varphi(x)=\frac{x}{2}$;
є) $\varphi(x)=\frac{x}{3}$;
ж) $\varphi(x)=\frac{x}{4}$;
з) $\varphi(x)=\frac{4x}{5}$;
к) $\varphi(x)=\frac{2}{3}x$;
л) $\varphi(2x)=\varphi(3x)$;
м) $\varphi(6^x)=72$.

4.13. Знайти натуральне число n, якщо:
а) $n=3^k5^l7^s$, $k,\ l,\ s\in\mathbf{N}$ і $\varphi(n)=3600$;
б) $n=pq$, де p і q — різні прості числа такі, що $p-q=2$ і $\varphi(n)=120$;
в) $n=p^2q^2$, де p і q — різні прості числа і $\varphi(n)=11424$;
г) $n=p^kq^l\ldots s^m$, де $p,\ q,\ \ldots,\ s$ — різні прості числа, $k,\ l,\ \ldots,\ m$ — натуральні числа, більші від 1 і $\varphi(n)=462000$;
д) $n=7^k$, $k\in\mathbf{N}$ і $\varphi(n)=294$;
е) $n=5^k7^l11$, $k,\ l\in\mathbf{N}$ і $\varphi(n)=42\,000$;
є) $n=p^kq^l$, де $p,\ q$ — різні прості числа, $k,\ l\in\mathbf{N}$ і $\varphi(n)=120$;
ж) $n=p^k$, де p — просте число, $k\in\mathbf{N}$, $\varphi(n)=6p^{k-2}$.

4.14. Побудувати графік функції $y=\varphi(x)$, де $1\leqslant x\leqslant20$.

---

[1] Нині відомо 27 досконалих чисел. Усі вони — парні числа. Ще невідомо, чи існують непарні досконалі числа і чи скінченна множина досконалих чисел.
[2] Так зване *просте число Мерсенна* (див. § 2). Зрозуміло, що кожне просте число Мерсенна дає нам деяке досконале число.
[3] Найбільшої пари дружніх чисел ще не знайдено.

4.15. Знайти:

а) $[e]$;
б) $[-e]$;
в) $[1-\sqrt{2}]$;
г) $[|\lg 128|]$;
д) $\left[\frac{1+\sqrt{52}}{2}\right]$;
е) $\left[\sqrt[4]{200}\right]$;
є) $\left[\sqrt[4]{580}+1\right]$;
ж) $\left[4+\cos\frac{101\pi}{204}\right]$;
з) $[2-|\lg 2512|]$;
к) $[1-\ln 50|]$;
л) $\left[\frac{10}{3+\sqrt{3}}\right]$.

4.16. Знайти:

а) $\{\pi\}$;
б) $\{-\pi\}$;
в) $\left\{1+\sin\frac{\pi}{6}\right\}$;
г) $\left\{2{,}1+\cos\frac{\pi}{3}\right\}$;
д) $\left\{1{,}5-\operatorname{tg}\frac{\pi}{4}\right\}$;
е) $\left\{1{,}3+\cos\frac{\pi}{6}\right\}$;
є) $\{-2{,}6\}$;
ж) $\left\{-\frac{23}{7}\right\}$.

4.17. Розв'язати рівняння:

а) $[2{,}3x]=3$;
б) $[3{,}2x]-3=2$;
в) $[ax]=m$,
де $a\neq 0$ і x — дійсне число;
г) $[12{,}4x]=86$;
д) $[x^2]=2$;
е) $[3x^2-x]=x+1$;
є) $[x]=\frac{3}{4}x$;
ж) $[x^2|=x$;
з) $|12{,}4x|=87$;
к) $\left|\frac{x}{m}\right|=\left|\frac{x}{m-1}\right|$, $m\geqslant 2$.

4.18. Довести, що:

а) $[x+y]\geqslant[x]+[y]$, $x, y\in\mathbf{R}$, узагальнити цей результат для більшої кількості доданків;

б) $[r]+\left[r+\frac{1}{2}\right]=[2r]$, де $r\in\mathbf{R}$ і $0\leqslant r<1$;

в) $[\pi]^{[e]}+[e]=[e]^{[\pi]}+[\pi]$;

г) $\left[\frac{p}{4}\right]=\frac{p-1}{4}$ або $\frac{p-3}{4}$, де p — просте непарне число;

д) $\left[\frac{a}{m}\right]=\frac{a-r}{m}$, де r — остача від ділення цілого числа a на натуральне число m;

е) $\frac{[nx]}{n}\leqslant x<\frac{[nx]}{n}+\frac{1}{n}$, $n\in\mathbf{N}$;

є) $\left[\frac{x+y}{n}\right]=\left[\frac{x}{n}\right]+\left[\frac{y}{n}\right]$ або $\left[\frac{x}{n}\right]+\left[\frac{y}{n}\right]+1$;

ж) $\left[\frac{m}{2}\right]=\frac{m-1}{2}$, якщо m — непарне натуральне число;

в) $[nx]\geqslant n[x]$, $n\in\mathbf{N}$, $x\in\mathbf{R}$;

к) $\left[\frac{m}{4}\right]+\left[\frac{2m}{4}\right]+\left[\frac{3m}{4}\right]=\frac{3(m-1)}{2}$, якщо $(m, 4)=1$;

л) $\left[\frac{m}{k}\right]+\left[\frac{2m}{k}\right]+\ldots+\left[\frac{(k-1)m}{k}\right]=\frac{(k-1)(m-1)}{2}$, якщо $(m, k)=1$, $m\geqslant 2$ і $k\geqslant 2$;

м) $[x]+\left[x+\frac{1}{n}\right]+\ldots+\left[x+\frac{n-1}{n}\right]=[nx]$ для будь-якого дійсного x і $n\geqslant 2$;

н) $[x]-2\left[\frac{x}{2}\right]=0$ або 1, $x\in\mathbf{R}$.

4.19. Знайти показник степеня простого числа p, яке міститься в добутку $n!$, якщо:

а) $p=3$, $n=100$;
б) $p=11$, $n=1000$;
в) $p=13$, $n=10\,000$;
г) $p=7$, $n=81\,561$.

4.20. Знайти канонічний розклад чисел: а) 11!; б) 18!; в) 40!; г) 75!; д) $\frac{20!}{10!10!}$.

4.21. Скількома нулями закінчується число $n!$, якщо: а) $n=50$; б) $n=123$; в) $n=1985$.

4.22. Побудувати графіки функцій:

а) $y=[x]$;
б) $y=2[x]$;
в) $y=[2x]$;
г) $y=\left[\frac{1}{2}x\right]$;
д) $y=\frac{1}{2}[x]$;
е) $y=2\left[\frac{1}{2}x\right]$;
є) $y=\frac{1}{2}[2x]$;
ж) $y=[x]+x$;
з) $y=\frac{1}{[x]}$;
к) $y=\frac{x^2}{[x]}$;
л) $y=\frac{x}{[x]}$;
м) $y=\frac{[x]}{x}$;
н) $y=\{x\}$.

4.23. Довести, що:

а) $288!\ \vdots\ (16!)^{18}$;
б) $288!\ \vdots\ (18!)^{16}$;
в) $C_{10000}^{5000}\ \vdots\ 7$;
г) $n!\ \vdots\ (a!\,b!\ldots k!)$, якщо $a+b+\ldots+k\leqslant n$;
д) $(k+1)(k+2)\ldots(k+n)\ \vdots\ n!$, $k, n\in\mathbf{N}$;
е) $(n!)!\ \vdots\ (n!)^{(n-1)!}$;
є) $(k+d)(k+2d)\ldots(k+nd)\ \vdots\ n!$, якщо $(d, n!)=1$;
ж) $\left[\frac{n+1}{2}\right]+\left[\frac{n+2}{4}\right]+\ldots+\left[\frac{n+2^k}{2^{k+1}}\right]+\ldots=n$.

4.24. Скільки є натуральних чисел, які:

а) кратні 786 і містяться між 10^6 і 10^7;
б) менші від числа 1000 і не діляться ні на 5, ні на 7;
в) не більші від 100 і взаємно прості з 36;

г) не більші від 2311 і не діляться на жодне з чисел 5, 7, 13, 17;
д) не більші від 12 317 і взаємно прості з 1575;
е) не більші від 1000 і не взаємно прості з 363?

4.25. Турист перебував у дорозі ціле число днів і проїжджав кожен день стільки кілометрів, скільки днів він подорожував. Якби він проїжджав щодня по 20 км і зупинявся на один день через кожні 40 км, то час його подорожування збільшився б на 37 днів. Скільки днів подорожував турист?

§ 5. Ланцюгові дроби. Підхідні дроби ланцюгового дробу

Література

[1] — § 9, с. 99—111;
[2] — § 9, с. 98—111;
[3] — гл. 11, § 3, с. 379—385;
[4] — гл. IV, § 14, 15, с. 260—278;
[10] — гл. I, § 6, с. 18—22;
[11] — гл. 5, § 1, 2, с. 58—66;
[12] — гл. III, § 3, с. 69—79;
[14] — § 7—9, с. 31—41.

ТЕОРЕТИЧНІ ВІДОМОСТІ

Нехай α — довільне дійсне число. Позначимо через q_1 найбільше ціле число, яке не перевищує α. При дробовому α маємо $\alpha = q_0 + \frac{1}{\alpha_1}$, де $\alpha_1 > 1$. Аналогічно при дробових $\alpha_1, \ldots, \alpha_{s-1}$ маємо

$$\alpha_1 = q_1 + \frac{1}{\alpha_2}, \quad \alpha_2 > 1,$$
$$\ldots\ldots\ldots\ldots$$
$$\alpha_{s-1} = q_{s-1} + \frac{1}{\alpha_s}, \quad \alpha_s > 1,$$

і тому дістаємо розклад в елементарний ланцюговий, або елементарний неперервний, дріб:

$$\alpha = q_0 + \cfrac{1}{q_1 + \cfrac{1}{q_2 + \ddots + \cfrac{1}{q_{s-1} + \cfrac{1}{\alpha_s}}}}. \qquad (1)$$

Якщо α — ірраціональне, то $\alpha_1, \alpha_2, \ldots, \alpha_s$ — ірраціональні (якщо α_s — раціональне, то згідно з розкладом (1) число α теж раціональне), і через це зазначений процес можна нескінченно продовжити, і в результаті дістанемо нескінченний ланцюговий дріб.

Якщо α — раціональне, то існує такий раціональний нескоротний дріб $\frac{a}{b}$, що $\alpha = \frac{a}{b}$, $b > 0$. Тоді зазначений процес скінченний і його можна здійснити за допомогою алгоритму Евкліда. Справді, для чисел a і b маємо:

$$a = bq_0 + r_1, \qquad \frac{a}{b} = q_0 + \frac{1}{\frac{b}{r_1}},$$
$$b = r_1 q_1 + r_2, \qquad \frac{b}{r_1} = q_1 + \frac{1}{\frac{r_1}{r_2}},$$
$$\ldots\ldots\ldots\ldots\ldots\ldots$$
$$r_{n-2} = r_{n-1}q_{n-1} + r_n, \qquad \frac{r_{n-2}}{r_{n-1}} = q_{n-1} + \frac{1}{\frac{r_{n-1}}{r_n}},$$
$$r_{n-1} = r_n q_n, \qquad \frac{r_{n-1}}{r_n} = q_n,$$

$$\frac{a}{b} = q_0 + \cfrac{1}{q_1 + \cfrac{1}{q_2 + \ddots + \cfrac{1}{q_{n-1} + \cfrac{1}{q_n}}}}. \qquad (2)$$

Числа $q_0, q_1, \ldots$, які містяться в розкладі числа α в ланцюговий дріб, називають **неповними частками** або **елементами** цього **ланцюгового дробу**. Скорочено довільний ланцюговий дріб записують так:

$$\alpha = [q_0; q_1, q_2, \ldots, q_n, \ldots].$$

Число q_0 є цілою частиною числа α, а $[0; q_1, q_2, \ldots]$ — дробовою частиною числа α. Правильні дроби $\frac{1}{q_1}, \frac{1}{q_2}, \ldots$ називаються відповідно **першою, другою** і т. д. **ланкою ланцюгового дробу**.

Будь-яке раціональне число α можна подати у вигляді деякого скінченного ланцюгового дробу:

$$\alpha = [q_0; q_1, q_2, \ldots, q_n].$$

Якщо $q_n > 1$ при $n > 0$, то такий розклад єдиний.

Будь-яке ірраціональне число можна подати у вигляді деякого нескінченного ланцюгового дробу, причому цей розклад єдиний.

Нескінченний ланцюговий дріб називається **чистим періодичним**, якщо його неповні частки періодично повторюються в тій самій послідовності, починаючи з q_0, тобто, якщо дріб має вигляд

$$[q_0; q_1, q_2, \ldots, q_n, q_0, q_1, q_2, \ldots, q_n, \ldots]$$

або

$$[(q_0; q_1, q_2, \ldots, q_n)].$$

Ланцюговий дріб називається **мішаним періодичним**, якщо період ланцюгового дробу розпочинається не з q_0, тобто якщо дріб має вигляд $[q_0; q_1, \ldots, q_m, p_0, p_1, \ldots, p_n, p_0, \ldots, p_n, \ldots]$, або $[q_0; q_1, \ldots, q_m, (p_0, \ldots, p_n)]$.

Будь-який нескінченний періодичний ланцюговий дріб (чистий чи мішаний) є дійсним коренем квадратного рівняння з цілими коефіцієнтами, тобто є так званою **квадратичною ірраціональністю**.

Будь-який ірраціональний корінь довільного квадратного рівняння з цілими коефіцієнтами розкладається в нескінченний періодичний ланцюговий дріб (чистий чи мішаний).

Дроби

$$\frac{P_0}{Q_0}=\frac{q_0}{1},\quad \frac{P_1}{Q_1}=q_0+\frac{1}{q_1},\quad \frac{P_2}{Q_2}=q_0+\frac{1}{q_1+\frac{1}{q_2}},\ \ldots,$$

$$\frac{P_k}{Q_k}=q_0+\cfrac{1}{q_1+\cfrac{1}{\ddots+\cfrac{1}{q_k}}},\ \ldots \qquad (3)$$

називаються **підхідними дробами**. При цьому $\frac{P_k}{Q_k}$ називається **підхідним дробом k-го порядку**. Якщо k — парне (непарне), то дріб $\frac{P_k}{Q_k}$ називається **підхідним дробом парного (непарного) порядку**. Зрозуміло, що для скінченного ланцюгового дробу порядку n виконується рівність

$$\frac{P_n}{Q_n}=\frac{a}{b},$$

звідси $\frac{a}{b}=\alpha$, а α — раціональне число, для якого будувався ланцюговий дріб.

Правило утворення підхідних дробів (скінченних і нескінченних):

$$P_s=q_sP_{s-1}+P_{s-2},\quad Q_s=q_sQ_{s-1}+Q_{s-2},\quad s\geqslant 1. \qquad (4)$$

Звідси $P_0=q_0$, $Q_0=1$. Щоб формула (4) виконувалася і при $s=1$, покладають $P_{-1}=1$, $Q_{-1}=0$. Усі обчислення зручно виконувати за такою схемою (табл. 1).

Таблиця 1

k	-1	0	1	2	. . .	n
q_k	—	q_0	q_1	q_2		q_n
P_k	1	q_0	$P_1=q_1P_0+P_{-1}$	$P_2=q_2P_1+P_0$		$P_n=q_nP_{n-1}+P_{n-2}$
Q_k	0	1	$Q_1=q_1Q_0+Q_{-1}$	$Q_2=q_2Q_1+Q_0$		$Q_n=q_nQ_{n-1}+Q_{n-2}$

Щоб обчислити P_s, $s=1, 2, \ldots, n$, треба число q_s, яке стоїть над P_s, помножити на число P_{s-1}, яке передує P_s з цього самого ряду, і до добутку додати число P_{s-2}, яке стоїть в тому самому рядку і передує P_{s-1}. Аналогічно обчислюють і Q_s.

Справедливі такі **властивості підхідних дробів** для скінченного ланцюгового дробу:

1°. $P_sQ_{s-1}-P_{s-1}Q_s=(-1)^{s-1}$, $s\geqslant 1$;

2°. Кожен підхідний дріб нескоротний;

3°. $P_sQ_{s-2}-P_{s-2}Q_s=(-1)^s q_s$, $s\geqslant 2$;

4°. Підхідні дроби парного порядку даного ланцюгового дробу утворюють зростаючу послідовність, а підхідні дроби непарного порядку — спадну послідовність;

5°. Кожен підхідний дріб парного порядку даного ланцюгового дробу менший за будь-який підхідний дріб непарного порядку цього ланцюгового дробу.

Якщо дійсне число α розкладено в ланцюговий дріб (скінченний чи нескінченний)

$$\alpha=[q_0;\ q_1,\ q_2,\ \ldots]$$

і $\frac{P_k}{Q_k}$ є значенням k-го підхідного дробу, то

$$\left|\alpha-\frac{P_k}{Q_k}\right|<\frac{1}{Q_kQ_{k+1}}<\frac{1}{Q_k^2}$$

(оцінка похибки наближення числа α підхідним дробом $\frac{P_k}{Q_k}$).

Якщо α — дійсне число, $\frac{P_k}{Q_k}$ — k-й підхідний дріб розкладу α у ланцюговий дріб, $\frac{x}{y}$ — довільний раціональний дріб із знаменником y, меншим від Q_k, то виконується нерівність $\left|\alpha-\frac{P_k}{Q_k}\right|<\left|\alpha-\frac{x}{y}\right|$ (теорема про найкраще наближення).

Ланцюгові дроби знаходять широке застосування. Сформулюємо теорему, за якою знаходять загальний розв'язок у цілих числах лінійного рівняння з двома невідомими, коефіцієнти і вільний член якого є цілі числа (так звані **невизначені рівняння**).

Загальний розв'язок у цілих числах рівняння $ax+by=c$, де a, b, c — цілі числа, а $(a, b)=1$, можна подати у вигляді

$$x=(-1)^{n-1}cQ_{n-1}+bt,\quad y=(-1)^n cP_{n-1}-at,$$

де t — довільне ціле число, а P_{n-1} і Q_{n-1} — чисельник і знаменник передостаннього підхідного дробу розкладу числа $\frac{a}{b}$ у ланцюговий дріб. Оскільки тут t — довільне ціле число, то можна користуватися формулами $x=(-1)^{n-1}cQ_{n-1}-bt$, $y=(-1)^n cP_{n-1}+at$.

ПРИКЛАДИ РОЗВ'ЯЗУВАННЯ ЗАДАЧ

1. Розкласти в ланцюговий дріб число $-\frac{602}{367}$ і знайти всі підхідні дроби.

Розв'язання. Якщо $\frac{a}{b}$ — додатний дріб, то застосовуємо алгоритм Евкліда. Якщо $\frac{a}{b}<0$, то спочатку подаємо його у вигляді $\frac{a}{b}=-k+\frac{a_1}{b_1}$, де k — натуральне число, а $\frac{a_1}{b_1}$ — правильний дріб. Отже, маємо

$$-\frac{602}{367}=-2+\frac{132}{367}.$$

Далі, за алгоритмом Евкліда дістаємо

$$\begin{array}{r|l} 367 & 132 \\ \hline -264 & 2 \\ \hline 103 & \end{array}$$

$$\begin{array}{r|l} 132 & 103 \\ \hline -103 & 1 \\ \hline 29 & \end{array}$$

$$\begin{array}{r|l} 103 & 29 \\ \hline -87 & 3 \\ \hline 16 & \end{array}$$

$$\begin{array}{r|l} 29 & 16 \\ \hline -16 & 1 \\ \hline 13 & \end{array}$$

$$\begin{array}{r|l} 16 & 13 \\ \hline -13 & 1 \\ \hline 3 & \end{array}$$

$$\begin{array}{r|l} 13 & 3 \\ \hline -12 & 4 \\ \hline 1 & \end{array}$$

$$\begin{array}{r|l} 3 & 1 \\ \hline -3 & 3 \\ \hline 0 & \end{array}$$

Отже, $-\frac{602}{367} = [-2; 2, 1,3, 1,1, 4,3]$, зокрема, $q_0 = -2$, $q_1 = 2$, $q_2 = 1$, $q_3 = 3$, $q_4 = 1$, $q_5 = 1$, $q_6 = 4$, $q_7 = 3$. Для обчислення підхідних дробів складаємо таблицю (табл. 2).

Таблиця 2

k	-1	0	1	2	3	4	5	6	7
q_k	—	-2	2	1	3	1	1	4	3
P_k	1	-2	-3	-5	-18	-23	-41	-187	-602
Q_k	0	1	2	3	11	14	25	114	367

Звідси

$$\frac{P_0}{Q_0} = -2; \quad \frac{P_1}{Q_1} = -\frac{3}{2}; \quad \frac{P_2}{Q_2} = -\frac{5}{3}; \quad \frac{P_3}{Q_3} = -\frac{18}{11};$$

$$\frac{P_4}{Q_4} = -\frac{23}{14}; \quad \frac{P_5}{Q_5} = -\frac{41}{25}; \quad \frac{P_6}{Q_6} = -\frac{187}{114}; \quad \frac{P_7}{Q_7} = -\frac{602}{367}.$$

Зауваження

1. Оскільки $\frac{P_n}{Q_n} = \frac{a}{b}$, то нижні дві клітинки останнього стовпчика в таблиці для обчислення підхідних дробів є своєрідною перевіркою правильності виконання всіх обчислень.

2. Якщо звичайний дріб $\frac{a}{b}$ розкласти в ланцюговий, то останній підхідний дріб $\frac{P_n}{Q_n}$ буде нескоротний, ланцюговий дріб дає змогу водночас скорочувати дріб $\frac{a}{b}$.

3. Обчисливши всі підхідні дроби за даним ланцюговим дробом $[q_0; q_1, q_2, \ldots, q_n]$, можна дістати нескоротний дріб $\frac{a}{b}$, що відповідає йому.

2. Ірраціональне число $\sqrt{14}$ розкласти в ланцюговий дріб і обчислити з точністю до 0,0001 значення $\sqrt{14}$.

Розв'язання. Щоб розкласти дійсне число α в ланцюговий дріб, використовують алгоритм Ейлера — алгоритм виділення цілої частини.

$$\alpha = q_0 + \frac{1}{\alpha_1}, \text{ де } q_0 = [\alpha] \text{ і } \alpha_1 > 1;$$

$$\alpha_1 = q_1 + \frac{1}{\alpha_2}, \text{ де } q_1 = [\alpha_1] \text{ і } \alpha_2 > 1;$$

$$\alpha_2 = q_2 + \frac{1}{\alpha_3}, \text{ де } q_2 = [\alpha_2] \text{ і } \alpha_3 > 1;$$

. . . . . .

Про послідовність $q_0, q_1, q_2, \ldots$, кажуть, що її побудовано з числа α за допомогою алгоритму виділення цілої частини. Всі члени цієї послідовності — цілі числа, причому $q_i \geqslant 1$ для $i = 1, 2, \ldots$.

Процес побудови цієї послідовності закінчується тоді, коли деяке α_n буде цілим числом (тобто тоді, коли $\alpha_{n+1} = 1$).

Якщо α — раціональне число, тобто $\alpha = \frac{a}{b}$, де $a \in \mathbf{Z}$, $b \in \mathbf{N}$, то, застосовуючи алгоритм Евкліда до α і до чисел a і b, дістанемо ту саму послідовність. Тоді матимемо скінченну послідовність $q_0, q_1, q_2, \ldots, q_n$ і розклад числа $\alpha = \frac{a}{b}$ в скінченний ланцюговий дріб: $\alpha = \frac{a}{b} = [q_0; q_1, \ldots, q_n]$.

Якщо α — ірраціональне число, то, очевидно, послідовність $q_0, q_1, q_2, \ldots$ нескінченна (тоді всі $\alpha_i > 1$, $i = 1, 2, \ldots$).

Використовуючи алгоритм виділення цілої частини для числа $\sqrt{14}$, маємо:

$$\sqrt{14} = 3 + \frac{1}{\alpha_1},$$

$$\alpha_1 = \frac{1}{\sqrt{14} - 3} = \frac{\sqrt{14} + 3}{5} = 1 + \frac{1}{\alpha_2},$$

$$\alpha_2 = \frac{1}{\frac{\sqrt{14} + 3}{5} - 1} = \frac{5}{\sqrt{14} - 2} = \frac{\sqrt{14} + 2}{2} = 2 + \frac{1}{\alpha_3},$$

$$\alpha_3 = \frac{1}{\frac{\sqrt{14} + 2}{2} - 2} = \frac{2}{\sqrt{14} - 2} = \frac{\sqrt{14} + 2}{5} = 1 + \frac{1}{\alpha_4},$$

$$\alpha_4 = \frac{1}{\frac{\sqrt{14} + 2}{5} - 1} = \frac{5}{\sqrt{14} - 3} = \sqrt{14} + 3 = 6 + \frac{1}{\alpha_5},$$

$$\alpha_5 = \frac{1}{\sqrt{14} + 3 - 6} = \frac{1}{\sqrt{14} - 3}.$$

Оскільки $\alpha_5 = \alpha_1$, то

$$\sqrt{14} = [3; (1,2, 1,6)].$$

За наближене значення $\sqrt{14}$ можна взяти один з підхідних дробів побудованого ланцюгового дробу. Для обчислення підхідних дробів складемо таблицю (табл. 3).

Таблиця 3

k	-1	0	1	2	3	4	5	6	7	. . .
q_k	—	3	1	2	1	6	1	2	1	. . .
P_k	1	3	4	11	15	101	116	333	449	. . .
Q_k	0	1	1	3	4	27	31	89	120	. . .

Як відомо, похибка наближення числа α підхідним дробом $\frac{P_k}{Q_k}$ не перевищує $\frac{1}{Q_k Q_{k+1}}$ або $\frac{1}{Q_k^2}$.

Оскільки в даному разі $\frac{1}{Q_6 Q_7} = \frac{1}{89 \cdot 120} < 0{,}0001$, то за наближене значення $\sqrt{14}$ з точністю до 0,0001 можна взяти підхідний дріб $\frac{P_6}{Q_6}$, тобто $\frac{333}{89} \approx 3{,}7416$.

Зауваження. Будь-який наступний за $\frac{P_6}{Q_6}$ підхідний дріб буде точнішим раціональним наближенням до $\sqrt{14}$. Проте краще вибирати за наближення той з підхідних дробів, в якого знаменник найменший.

3. Знайти квадратичну ірраціональність α, якщо $\alpha = [4; 3, (2,1)]$.

Розв'язання. Перетворимо спочатку нескінченний чистий періодичний ланцюговий дріб, який дістаємо із заданого ланцюгового дробу після того, як відкинемо цифри, що стоять до періоду:

$$y = [(2,1)] = 2 + \cfrac{1}{1 + \cfrac{1}{2 + \cfrac{1}{1 + \dots}}}\Bigg\}y.$$

Маємо

$$y = 2 + \cfrac{1}{1 + \cfrac{1}{y}},$$

звідки

$$y^2 - 2y - 2 = 0, \quad y_1 = 1 + \sqrt{3}, \quad y_2 = 1 - \sqrt{3}.$$

Оскільки y — додатна квадратична ірраціональність, то $y = 1 + \sqrt{3}$.
Тепер перетворимо в квадратичну ірраціональність заданий нескінченний мішаний періодичний ланцюговий дріб:

$$[4; 3, (2, 1)] = [4; 3, y] = 4 + \cfrac{1}{3 + \cfrac{1}{1 + \sqrt{3}}} =$$

$$= 4 + \frac{1 + \sqrt{3}}{4 + 3\sqrt{3}} = \frac{17 + 13\sqrt{3}}{4 + 3\sqrt{3}} = \frac{49 - \sqrt{3}}{11}.$$

Отже,

$$[4; 3, (2, 1)] = \frac{49 - \sqrt{3}}{11}.$$

4. Розв'язати в цілих числах рівняння $-117x + 343y = 119$.

Розв'язання. Запишемо це рівняння так:

$$117(-x) + 343y = 119. \tag{1}$$

Визначимо невідомі $-x$ та y. Загальний розв'язок у цілих числах рівняння $ax + by = c$, де a, b, c — цілі числа й $(a, b) = 1$, подамо у вигляді

$$\begin{aligned} x &= (-1)^{n-1} c Q_{n-1} + bt, \\ y &= (-1)^n c P_{n-1} - at, \end{aligned} \tag{2}$$

де t — довільне ціле число, а P_{n-1} і Q_{n-1} — чисельник і знаменник передостаннього підхідного дробу розкладу $\frac{a}{b}$ у ланцюговий дріб.

У цьому разі $a = 117$, $b = 343$, $(117, 343) = 1$.

Розкладемо дріб $\frac{117}{343}$ в ланцюговий: $a = [0; 2, 1, 13, 1, 1, 1, 2]$.

Отже, $n = 7$. Обчислимо $P_{n-1} = P_6$ і $Q_{n-1} = Q_6$. Маємо $P_6 = 44$, $Q_6 = 129$. Тоді одним з окремих розв'язків є

$$-x_0 = (-1)^6 \cdot 119 \cdot 129 = 15\,351, \quad y_0 = (-1)^7 \cdot 119 \cdot 44 = -5236.$$

Згідно з формулами (2), загальний розв'язок запишемо як

$$-x = 15\,351 + 343t, \quad y = -5236 - 117t,$$

або

$$x = -15\,351 - 343t, \quad y = -5236 - 117t.$$

Маємо порівняно великі за абсолютною величиною окремі значення для x_0 і y_0, проте із загального розв'язку можна дістати інші окремі значення для x і y, які будуть найменші за абсолютною величиною. Нехай $t = -45$. Тоді $x_1 = 84$, $y_1 = 29$ і загальний розв'язок рівняння (1) є

$$x = 84 + 343k, \quad y = 29 + 117k \quad \text{(тут замінено } -t \text{ на } k\text{)}.$$

Зауваження.

1. У розглянутому прикладі значення x і y можна було визначити відразу. Справді, розкладаючи $-\frac{117}{343}$ в ланцюговий дріб, дістаємо

$$-\frac{117}{343} = [-1; 1, 1, 1, 13, 1, 1, 1, 2].$$

Тоді $n = 8$, $a = -117$, $b = 343$, $c = 119$, $P_{n-1} = P_7 = -44$, $Q_{n-1} = Q_7 = 129$. Згідно з формулами (2), $x_0 = (-1)^7 \cdot 119 \cdot 129 = -15\,351$, $y_0 = (-1)^8 \cdot 119 \cdot (-44) = -44 \cdot 119 = -5236$.

Отже, $x = -15\,351 + 343t$, $y = 5236 + 117t$.

При $t = 45$ маємо той самий результат, що й раніше:

$$x = 84 + 343t, \quad y = 29 + 117t.$$

2. Часто при розв'язуванні аналогічних задач треба обчислити тільки підхідний дріб $\frac{P_{n-1}}{Q_{n-1}}$. Проте доцільно заповнювати всю таблицю для підхідних дробів, оскільки, обчисливши дріб $\frac{P_n}{Q_n}$, можна перевірити розв'язання.

Задачі

5.1. Розкласти в ланцюгові дроби і обчислити їхні підхідні дроби для раціональних чисел:

а) $\frac{23}{18}$;
б) $\frac{36}{19}$;
в) 2,55;
г) −1,425;
д) $-\frac{602}{367}$;
е) $-5\frac{28}{57}$;
є) $\frac{521}{143}$;
ж) $-\frac{83}{217}$;
з) $-\frac{99}{170}$;
к) 0,375;
л) −0,4 (51).

5.2. За допомогою розкладу в ланцюгові дроби скоротити дроби:

а) $\frac{1180}{1829}$; д) $\frac{1241}{6059}$; з) $-\frac{1872}{1560}$;
б) $\frac{2227}{9911}$; е) $\frac{6821}{2147}$; к) $-\frac{3523}{1300}$;
в) $\frac{1043}{3427}$; є) $\frac{32\,671}{10\,027}$; л) $\frac{309\,672}{464\,508}$.
г) $\frac{1857}{9153}$; ж) $\frac{70\,757}{491\,209}$;

5.3. Знайти звичайні нескоротні дроби, що відповідають ланцюговим дробам:

а) [2; 1, 3, 4, 2];
б) [2; 1, 19, 1, 3];
в) [2; 1, 1, 3, 1, 2];
г) [1; 1, 2, 3, 4];
д) [0; 4, 1, 2, 5, 6];
е) [−2; 1, 3, 1, 1, 5];
є) [−3; 1, 2, 1, 1, 5];
ж) [−5; 2, 1, 1, 3, 2];
з) [1; 3, 2, 4, 3, 1, 1, 1, 5];
к) [a; a, a, a, a];
л) [a; b, a, b, a].

5.4. Нехай $\frac{P_{n-1}}{Q_{n-1}}$ — передостанній підхідний дріб у розкладі раціонального числа $\frac{a}{b}$ в ланцюговий дріб. Довести, що $(a, b) = (-1)^n Q_{n-1} a + (-1)^{n-1} P_{n-1} b$.

5.5. Користуючись результатом задачі 5.4, розв'язати задачу 5.3.

5.6. Розкласти звичайний дріб $\frac{a}{b}$ в ланцюговий, замінити його підхідним дробом $\frac{P_k}{Q_k}$, знайти похибку заміни, замінити наближену рівність із зазначенням похибки, якщо:

а) $\frac{a}{b} = \frac{29}{37}$, $k = 4$; б) $\frac{a}{b} = \frac{648}{385}$, $k = 4$;
в) $\frac{a}{b} = \frac{571}{359}$, $k = 5$.

5.7. За допомогою підхідних дробів знайти наближення до дробу $\frac{13\,891}{5065}$ з точністю до: а) 0,001; б) 0,0001.

5.8. Розв'язати рівняння:

а) $[x; 2, 3, 4] = \frac{73}{30}$; б) $[2; 1, 2, x] = \frac{19}{7}$.

5.9. Знайти ланцюговий дріб $[q_0; q_1, \ldots, q_n]$, якщо $q_n = 3$, $\frac{P_{n-1}}{Q_{n-1}} = \frac{14}{9}$.

5.10. Нехай для деякого скінченного ланцюгового дробу $[q_0; q_1, \ldots, q_n]$ маємо $\frac{P_0}{Q_0} = \frac{3}{1}$, $\frac{P_1}{Q_1} = \frac{10}{3}$, $\frac{P_2}{Q_2} = \frac{33}{10}$. Знайти q_2.

5.11. Треба побудувати зубчасту передачу за допомогою двох валів з кількістю зубців, що дорівнює відношенню 587 : 113. Чи можна замінити це відношення відношенням з меншими чисельниками і знаменниками, але похибкою, яка не перевищує 0,001? Як зміниться відповідь, коли: а) початкове відношення 355 : 113, а похибка 0,002; б) початкове відношення 12 532 : 3921, а похибка 0,00005?

5.12. Розв'язати в цілих числах рівняння:

а) $38x + 117y = 209$;
б) $119x - 68y = 34$;
в) $41x + 114y = 5$;
г) $49x + 9y = 400$;
д) $12x + 31y = 170$;
е) $37x + 23y = 15$;
є) $53x + 17y = 25$;
ж) $64x - 39y = 15$;
з) $3827x + 3293y = 1869$;
к) $571x + 359y = -10$.

5.13. Розв'язати в натуральних числах рівняння:

а) $8x + 13y = 15$;
б) $23x - 42y = 72$;
в) $15x + 28y = 185$.

5.14. Розкласти число 100 на суму таких двох натуральних чисел, щоб одне з них ділилось на 7, а друге — на 11.

5.15. Для настилання підлоги завширшки 3 м є дошки завширшки 11 і 13 см. Скільки треба взяти дощок різної ширини, якщо довжина кімнати і довжина дощок однакові, а дошки кладуть вздовж кімнати?

5.16. Для перевезення зерна є мішки по 60 і 80 кг. Скільки треба таких мішків для перевезення 440 кг зерна?

5.17. Скільки білетів вартістю 30 і 50 коп. можна купити на 14 крб. 90 коп?

5.18. Купили 30 птахів за 30 монет однієї вартості; причому за кожних трьох горобців заплатили 1 монету, за кожні дві

горлиці також 1 монету і за кожного голуба — по 2 монети. Скільки купили птахів кожного виду?

5.19. 26 студентів посадили разом 88 дерев, причому кожен студент I, II і III курсу повинен був посадити відповідно 6, 4 і 2 дерева. Скільки було студентів I, II і III курсу?

5.20. Розкласти в ланцюгові дроби такі квадратичні ірраціональності: а) $\sqrt{2}$; б) $\sqrt{3}$; в) $\sqrt{5}$; г) $\sqrt{6}$; д) $\sqrt{7}$; е) $\sqrt{8}$; є) $\sqrt{10}$; ж) $\sqrt{11}$; з) $\sqrt{12}$; к) $\sqrt{13}$; л) $\sqrt{28}$; м) $\sqrt{30}$; н) $\sqrt{59}$.

5.21. Розкласти в ланцюгові дроби такі квадратичні ірраціональності:

а) $1+\sqrt{2}$;
б) $\frac{1+\sqrt{3}}{2}$;
в) $\frac{2+\sqrt{5}}{3}$;
г) $\frac{3+\sqrt{5}}{2}$;
д) $\frac{2+\sqrt{7}}{2}$;
е) $\frac{3+\sqrt{10}}{3}$;
є) $5-\sqrt{15}$;
ж) $1-\sqrt{31}$;
з) $\frac{1+\sqrt{31}}{2}$;
к) $\frac{6-\sqrt{3}}{2}$;
л) $\frac{3-\sqrt{7}}{3}$;
м) $\frac{7-\sqrt{5}}{3}$;
н) $\frac{76+\sqrt{285}}{94}$.

5.22. Знайти квадратичні ірраціональності, якщо відомі їхні розклади у нескінченні періодичні ланцюгові дроби:

а) $[(1, 2)]$;
б) $[1; (3)]$;
в) $[2; (5)]$;
г) $[0; (4)]$;
д) $[0; (7)]$;
е) $[(2, 3)]$;
є) $[3; (4, 11)]$;
ж) $[0; (1, 3)]$;
з) $[0; (2, 1)]$;
к) $[0; (1,4)]$;
л) $[2; (1, 2)]$;
м) $[1; (3, 2)]$;
н) $[1; (3, 1)]$.

5.23. Знайти квадратичні ірраціональності, якщо відомі їхні розклади у нескінченні періодичні ланцюгові дроби:

а) $[0; (1, 3, 2)]$;
б) $[1; (2, 3, 12)]$;
в) $[1; (1, 2, 11)]$;
г) $[2; (3, 1, 4)]$;
д) $[1; (1, 2, 3)]$;
е) $[2; (3, 1, 2)]$;
є) $[3; (1, 1, 6]$;
ж) $[2; (3, 2, 1, 2)]$;
з) $[4; 3, (2, 1, 3, 1)]$;
к) $[3; 2; 1, (3, 1)]$;
л) $[1; 1, 2, 1, 1, (4)]$;
м) $[(1, 2, 4, 6)]$;
н) $[1; (1, 1, 1, 1, 2, 5)]$.

5.24. Знайти квадратні рівняння з цілими коефіцієнтами, корені яких розкладаються в такі нескінченні періодичні ланцюгові дроби:

а) $[10; (10, 20)]$;
б) $[9; (1, 1, 2, 4, 2, 1, 1, 18)]$;
в) $[2; (1, 1, 3)]$;
г) $[1; (1, 2, 2, 1)]$;
д) $[(2, 4, 1, 3)]$;
е) $[2; 1, 2, (1, 1, 3)]$;
є) $[1; 2, (3, 4)]$.

5.25. Знайти квадратичну ірраціональність x, якщо:

а) $x = [q; (2q)]$, $q \in \mathbf{N}$;
б) $x = [q; [q; (q, 2q)]$, $q \in \mathbf{N}$.

5.26. Розкласти в ланцюговий дріб:

а) $\sqrt{q^2+1}$, $q \in \mathbf{N}$;
б) $\sqrt{q^4+2q}$, $q \in \mathbf{N}$;
в) $\sqrt{(q+1)^2-2}$, $q \in \mathbf{N}$;
г) $\sqrt{q^6+2q}$, $q \in \mathbf{N}$.

5.27. Замінити числа підхідними дробами третього порядку і оцінити похибку:

а) $\frac{587}{103}$; б) 3, 14159; в) $\frac{-1+\sqrt{5}}{2}$; г) $\frac{2-\sqrt{3}}{5}$.

5.28. За допомогою ланцюгових дробів обчислити з точністю до 0,0001 обидва корені квадратних рівнянь з цілими коефіцієнтами:

а) $2x^2-15x+26=0$;
б) $x^2+9x+6=0$;
в) $2x^2-3x-6=0$;
г) $x^2-5x+2=0$;
д) $4x^2+20x+23=0$.

5.29. Знайти підхідні дроби $\frac{P_k}{Q_k}$ у розкладі $\sqrt[3]{2}$, якщо $0 \leqslant k \leqslant 3$.

5.30. Знайти другий підхідний дріб у розкладі кореня рівняння $2^x = 5$.

5.31. Розкласти в нескінченний ланцюговий дріб і обчислити з точністю до 0,0001:

а) $\sqrt{30}$; б) $\sqrt{59}$; в) $\frac{3+\sqrt{7}}{2}$; г) $\frac{1+\sqrt{11}}{4}$.

5.32. Довести, що:

а) $[(a, b)] \cdot \frac{1}{[(b, a)]} = \frac{a}{b}$;

б) $\frac{P_2}{Q_2} = \frac{2a+1}{2}$ при розкладі ірраціональності $\sqrt{a^2+a+1}$ в ланцюговий дріб;

в) дріб $\frac{a^4+3a^2+1}{a^3+2a}$, $a \in \mathbf{N}$ є нескоротним;

г) $(P_n, P_{n-1}) = (Q_n, Q_{n-1}) = 1$;

д) $P_{n-1} = Q_n$ для дробу $[q_0; q_1, q_2, \ldots, q_n]$, в якому $q_0 = q_n$, $q_1 = q_{n-1}$, $q_2 = q_{n-2}$, $\ldots$;

е) $\left(\frac{P_{n+2}}{P_n}\right)\left(1-\frac{P_{n-1}}{P_{n+1}}\right) = \left(\frac{Q_{n+2}}{Q_n}-1\right)\left(1-\frac{Q_{n-1}}{Q_{n+1}}\right)$;

є) $\underbrace{[2; 2, 2, \ldots, 2]}_{n} = \frac{(1+\sqrt{2})^{n+1}-(1-\sqrt{2})^{n+1}}{(1+\sqrt{2})^n-(1-\sqrt{2})^n}$;

ж) $Q_n \geqslant 2^{\frac{n-1}{2}}$, якщо $n \geqslant 2$;

з) $\left|\alpha-\frac{P_k}{Q_k}\right| < \frac{1}{2Q_k^2}$ або $\left|\alpha-\frac{P_{k-1}}{Q_{k-1}}\right| < \frac{1}{2Q_{k-1}^2}$

для заданого дійсного додатного числа α і натурального числа k, $k \geqslant 1$;

к) $\frac{p}{q}$ є підхідним дробом розкладу дійсного додатного числа α у ланцюговий дріб, якщо $p,\ q \in \mathbf{N},\ (p, q) = 1$ і $\alpha \neq \frac{p}{q}$, $\left|\alpha - \frac{p}{q}\right| < \frac{1}{2q^2}$;

л) $\left|\alpha - \frac{P_n}{Q_n}\right| > \frac{1}{Q_n(Q_n + Q_{n-1})}$, довівши, що $\frac{P_n}{Q_n}$ і $\frac{P_n + P_{n-1}}{Q_n + Q_{n-1}}$ лежать по один бік від α;

м) підхідний дріб n-го порядку збільшиться (зменшиться), якщо неповну частку q_n збільшити на кілька одиниць, де n — парне (непарне) натуральне число.

5.33. Довести, що:

а) додатний корінь тричлена $bx^2 - abx - a$, де a, b — натуральні числа, розкладається в нескінченний чистий періодичний ланцюговий дріб, довжина періоду якого дорівнює 2;

б) квадратне рівняння з цілими коефіцієнтами має другий корінь $-\frac{1}{[(b, a)]}$, якщо перший його корінь є число $[(a, b)]$;

в) квадратне рівняння з цілими коефіцієнтами має корінь $a - [(c, b)]$, якщо перший його корінь є $x = [(a, b, c)]$;

г) числа $\alpha = [a; b, c]$ і $\beta = [c; b, a]$ пропорційні числам $x = [(a, b, c)]$ і $y = [(c, b, a)]$;

д) ірраціональність виду $\sqrt{m}$, $m \in \mathbf{N}$ розкладається в ланцюговий дріб, період якого починається з другої неповної частки.

5.34. Знайти ірраціональність α, якщо:

а) $\frac{P_k}{Q_k} = \frac{10}{3}$, $\alpha_{k+1} = \sqrt{2}$;

б) $\frac{P_k}{Q_k} = \frac{37}{13}$, $\alpha_{k+1} = \frac{1 + \sqrt{3}}{2}$.

5.35. Знайти загальний вигляд квадратичних ірраціональностей, які розкладаються в ланцюговий дріб з однаковими неповними частками.

§ 6. Системні числа, операції над ними; переведення з однієї системи в іншу

Література

[1] — § 6, с. 79—88;
[2] — § 6, с. 76—86;
[3] — гл. II, § 4, с. 385—389;
[4] — гл. II, § 3, с. 88—104.

ТЕОРЕТИЧНІ ВІДОМОСТІ

Той чи інший спосіб найменування та записування чисел називають **нумерацією** (від лат. numeres — лічба) або **системою числення**.

Розрізняють **усну й письмову нумерації**. *Усна нумерація — це спосіб називання чисел за допомогою слів. Письмовою нумерацією називають спосіб записування чисел за допомогою знаків (символів), які називаються* **цифрами**.

Розрізняють **позиційні і непозиційні системи числення**.

Під позиційною системою числення розуміють систему, в якій значення кожної цифри визначається не тільки цифрою, а й позицією, яку вона займає в запису числа.

Під непозиційною системою числення розуміють систему, в якій кожна цифра завжди позначає те саме число незалежно від її місця (позиції) в запису числа. Прикладом непозиційної системи числення є римська система, яка дійшла до нас із Стародавнього Риму. В ній для запису чисел використовують сім цифр: цифра I означає одиницю, цифра V — п'ять, цифра X — десять, L — п'ятдесят, C — сто, D — п'ятсот, M — тисячу. За допомогою цих цифр можна записати будь-яке число, використовуючи принцип додавання і віднімання. Якщо менша цифра стоїть справа від більшої, то вона додається до неї (причому вона може повторюватися не більш як 3 рази), якщо зліва — то віднімається (повторення меншої цифри не дозволяється). Наприклад, 1985 — MCMLXXXV.

Хоч символу для зображення нуля у римській системі числення немає, проте можна записувати числа, які містять нуль. Наприклад, 1809 — MDCCCIX.

Записи чисел у римській нумерації громіздкі, до того ж множення і ділення на письмі виконувати неможливо, їх доводиться виконувати усно. Тому римська система числення в математичній практиці не застосовується.

З'ясуємо суть позиційного принципу запису чисел. Нехай g — деяке фіксоване число, більше від 1. Назвемо це число **основою системи числення**.

Кожне натуральне число m можна записати і притому єдиним способом у вигляді

$$m = a_n g^n + a_{n-1} g^{n-1} + \ldots + a_1 g + a_0, \qquad (1)$$

де a_i, $i = 0, 1 \ldots$, n — цілі невід'ємні числа, менші від g, причому $a_n \neq 0$.

Вираз (1) називають **записом числа** m **у системі числення з основою** g. Символи, якими позначають числа a_n, a_{n-1}, ..., a_1, a_0, називають **цифрами** числа m у системі числення з основою g (або «g-кова» система числення).

Вираз (1) скорочено записують так:

$$m = (a_n a_{n-1} \ldots a_2 a_1 a_0)_g. \qquad (2)$$

У системі числення з основою g використовуються g цифр: 0, 1, 2, ..., $g - 1$. При цьому основа числення g записується як 10.

Запис додатного дробового числа у будь-якій системі числення є зображення цього числа у вигляді суми степенів основи з цілими невід'ємними коефіцієнтами, меншими від основи, але не лише додатних і нульового, а й від'ємних цілих степенів. Для запису дробового числа, крім цифр, використовують ще один знак — кому. Дробове число $1 \cdot 8^3 + 2 \cdot 8^2 + 5 \cdot 8^1 + 4 \cdot 8^0 + 7 \cdot 8^{-1} + 6 \cdot 8^{-2} + 3 \cdot 8^{-3} + 2 \cdot 8^{-4}$, наприклад, записують так: $1254,\ 7632_8$.

Для кожного додатного дробового числа так само, як і для кожного натурального числа, в g-ковій системі числення існує тільки один запис.

Застосовуючи знак мінус, можна записувати в g-ковій системі числення й від'ємні числа.

Загальновживаною тепер є позиційна система числення з основою $g = 10$. Її називають **десятковою позиційною системою**.

Виконуючи арифметичні операції над числами, записаними в g-ковій системі числення, користуються правилами додавання, віднімання і множення «стовпцем» і ділення — «кутом». При цьому використовуються g-кові таблиці додавання і множення однозначних чисел.

Нехай натуральне число m задано в g-ковій системі числення. Щоб записати це число в s-ковій системі числення, треба спочатку записати число s в g-ковій системі, а потім виконати (в g-ковій системі числення!) кілька ділень числа m_g на число s_g і послідовно утворюваних часток доти, поки дістанемо частку, яка дорівнює нулю. Здобуті остачі треба спочатку виразити цифрами s-кової системи числення, записати їх у зворотному порядку. Записані таким чином остачі (це вже цифри в s-ковій системі числення) і є s-ковим записом числа m_g.

Перехід від g-кової системи числення до 10-кової виконують ще й так. Число a_g записують у вигляді

$$a_g = a_n g^n + a_{n-1} g^{n-1} + \ldots + a_1 g^1 + a_0 g^0.$$

Потім замість чисел $a_n, a_{n-1}, \ldots, a_1, a_0$ і g підставляють їхні десяткові записи і роблять відповідні обчислення. Десятковий запис результату є шуканим числом.

Оскільки десяткова система числення найзручніша для виконання тих або інших дій, то, щоб перейти від g-кової системи числення до s-кової, спочатку переходять від g-кової системи числення до 10-кової, а потім від 10-кової до s-кової.

Якщо $g = s^k$, $k \in \mathbb{N}$, то перехід від однієї системи числення до іншої значно спрощується.

ПРИКЛАДИ РОЗВ'ЯЗУВАННЯ ЗАДАЧ

1. Обчислити:

а) $202332_4 + 22222_4$; б) $220111_4 - 32323_4$; в) $23230301_4 : 113_4$.

Розв'язання. У четвірковій системі числення цифрами є: 0, 1, 2, 3. Складемо для них таблиці додавання і множення (табл. 4 і 5).

Таблиця 4

+	0	1	2	3
0	0	1	2	3
1	1	2	3	10
2	2	3	10	11
3	3	10	11	12

Таблиця 5

×	0	1	2	3
0	0	0	0	0
1	0	1	2	3
2	0	2	10	12
3	0	3	12	21

Тепер виконуємо дії:

а) $202\,332_4 + 22\,222_4 = 231\,220_4$

Перевірка: $231\,220_4 - 22\,222_4 = 202\,332_4$

б) $220\,111_4 - 32\,323_4 = 121\,122_4$

Перевірка: $121\,122_4 + 32\,323_4 = 220\,111_4$

в) $23230301_4 : 113_4$

232	200 203$_4$
303	
232	
1101	
1011	
30$_4$	

(остача)

Перевірка: $200203_4 \times 113_4 = 1201221 + 200203 + 200203 = 23\,230\,211_4$

$23\,230\,211_4 + 30_4 = 2\,323\,301_4$.

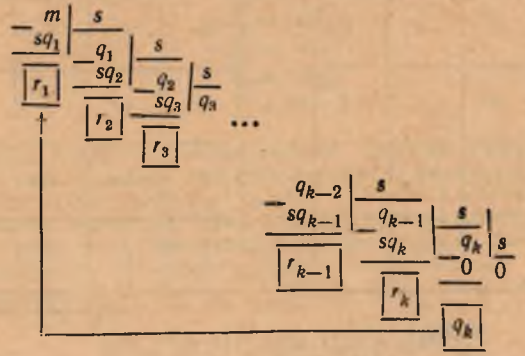
2. Перевести з однієї системи в іншу:

а) $138_{10} \to x_4$; б) $1340_{10} \to x_{15}$;

в) $10032_4 \to x_3$; г) $2032_4 \to x_{10}$.

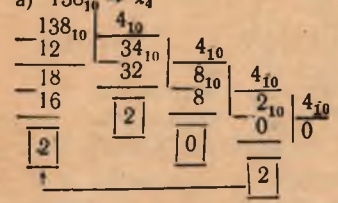
Розв'язання. Перехід від десяткової системи числення до s-кової системи відбувається за допомогою послідовного ділення числа m, заданого в десятковій системі, на число s, записане теж у десятковій системі. Маємо $m = sq_1 + r_1$. Тепер неповну частку q_1 ділимо на s. Дістаємо $q_1 = sq_2 + r_2$. Процес ділення продовжуємо доти, поки знайдемо неповну частку $q_k < s$. При цьому запишемо число m у s-ковій системі: $(q_k r_k r_{k-1} \ldots r_2 r_1)_s$.

Цей процес можна записати у вигляді такої схеми:



Стрілкою показано напрям від вищих до нижчих розрядів числа, записаного в системі з основою s, цифри числа m у цій системі взято в рамки.

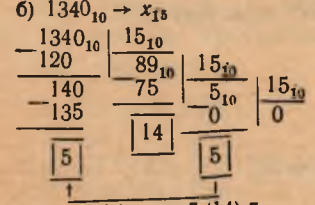
а) $138_{10} \to x_4$



Оскільки $4 < 10$, то всі остачі є цифрами в новій системі числення.

Отже, $138_{10} = 2022_4$.

б) $1340_{10} \to x_{15}$



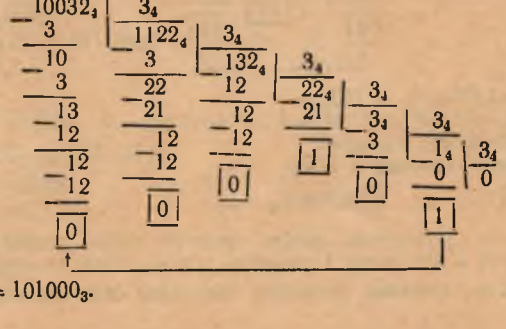
У 15-ковій системі числення число 14 є цифрою і позначається (14) або $\bar{4}$.

Отже, $1340_{10} = 5\,(14)\,5_{15}$.

Щоб перевести число с g-кової системи числення в s-кову, діють аналогічно, причому всі обчислення виконуються в g-ковій системі числення.

в) $10032_4 \to x_3$.

Число 3 в четвірковій системі числення записують так само. Тоді



Отже, $10032_4 = 101000_3$.

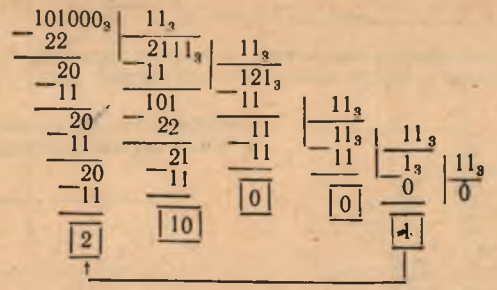
Перевірка. Число 4 у трійковій системі числення записують як 11_3. Використовуючи таблиці додавання і множення одноцифрових чисел у трійковій системі числення (табл. 6, 7), матимемо

Таблиця 6

+	0	1	2
0	0	1	2
1	1	2	10
2	2	10	11

Таблиця 7

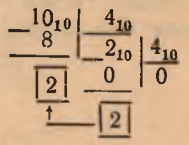
×	0	1	2
0	0	0	0
1	0	1	2
2	0	2	11



Отже, $101000_3 = 100\,(10_3)\,2_4 = 10032_4$, оскільки $10_3 = 3_4$.

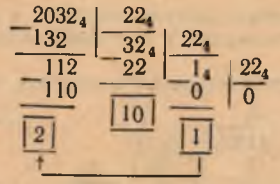
г) $2032_4 \to x_{10}$.

І спосіб. Число 10 в четвірковій системі числення записують так:



$$10_{10} = 22_4.$$

Тоді



Отже, $2032_4 = 1\,(10_4)\,2_{10} = 142_{10}$.

ІІ спосіб. $2032_4 = 2 \cdot 4^3 + 0 \cdot 4^2 + 3 \cdot 4^1 + 2 \cdot 4^0 = 2 \cdot 64 + 0 + 12 + 2 = 142_{10}$.

Як бачимо, результати однакові.

3. Перевести з однієї системи в іншу:

а) $1110111000111_2 \to x_8$; б) $3673401_8 \to x_2$.

Розв'язання. Застосуємо досить простий спосіб переведення з двійкової системи числення в вісімкову і навпаки (аналогічний спосіб використовують, коли g-кова і s-кова системи числення пов'язані співвідношенням $s = g^k$).

Складемо таблицю виразів цифр вісімкової системи числення в двійковій системі

$$\begin{aligned} 0_8 &= 000_2, \\ 1_8 &= 001_2, \\ 2_8 &= 010_2, \\ 3_8 &= 011_2, \\ 4_8 &= 100_2, \\ 5_8 &= 101_2, \\ 6_8 &= 110_2, \\ 7_8 &= 111_2. \end{aligned} \qquad (1)$$

Щоб перевести число з вісімкової системи числення в двійкову, треба кожну цифру цього числа замінити двійковою тріадою за формулами (1). В свою чергу, щоб перевести число з двійкової системи числення в вісімкову, треба розбити це число справа наліво на грані, кожна з яких містить по три цифри (якщо треба, то останню грань доповнюють до тріади нулями). Потім кожну з двійкових тріад замінюють вісімковою цифрою за формулами (1).

а) $1110111000111_2 \to x_8$.

$$(001)\,(110)\,(111)\,(000)\,(111)_2 = 16707_8.$$

б) $3673401_8 = 011110111011100000001_2 = 11110111011100000001_2$.

Задачі

6.1. Записати в десятковій системі числення такі числа римської нумерації: а) LXIV; б) CLIX; в) DXCVI; г) MCCV; д) MCDXXIX; е) MDCCCLXXIV.

6.2. Записати в римській нумерації числа: а) 26; б) 112; в) 1980.

6.3. Записати в десятковій системі числення: а) мільярд, б) більйон, в) трильйон.

6.4. Обчислити:

а) $1101_2 + 1011_2$;
б) $1011_2 \cdot 1101_2$;
в) $1000110_2 - 11011_2$;
г) $100011_2 : 101_2$;
д) $3604_7 \cdot 423_7$;
е) $7(10)1_{12} \cdot 5(11)73_{12}$;
є) $23054_7 + 4326_7$;
ж) $(10)\,(11)\,792_{12} + 9534(10)_{12} + 70(10)0_{12}$;
з) $26153_7 : 326_7$;
к) $8(10)05(11)_{12} : 9(10)_{12}$;
л) $101_8 : 32_8$.

6.5. Обчислити:

а) $11011{,}101_2 + 101{,}011_2$;
б) $11{,}001_2 \cdot 1{,}01_2$;
в) $111{,}01_2 \cdot 101{,}101_2$;
г) $0{,}25_8 \cdot 0{,}43_8$;
д) $2{,}5_8 \cdot 3{,}4_8$.

6.6. Обчислити:

а) $7306_8 + 25645_8 - 6774_8 - 26156_8$;
б) $(425_6 \cdot 54_6 - 531_6 \cdot 43_6) : 245_6$;
в) $20671_8 : 131_8 - 140_8$;
г) $23213_5 : 32_5 + 113_5 \cdot 3_5 - 1242_5$;
д) $232011_5 : 104_5 + 1234 \cdot 322_5 - 1022131_5$;
е) $(563_8 + 217_8) \cdot 15_8 + (2365_8 - 636_8) : 17_8 - 15122_8$;
є) $120111_3 : 102_3 + 201_3 \cdot 12_3 - 11220_3$;
ж) $6325_7 - 456_7 - 150335_7 : 23_7 - 551_7$;
з) $3215_7 \cdot 24_7 - 11461_7 : 25_7 + 1532_7 - 115044_7$;
к) $(4123_8 - 4221_8) \cdot 11_8 + (1222_8 + 773_8) : 3_8$;
л) $(3333_4 + 2222_4) \cdot 12_4 - (231020_4 + 3333333_4) : 23_4$;
м) $[(215_8 + 532_8) \cdot 16_8 - (11031_8 - 527_8) : 32_8] : 14775_8$;
н) $[(351_6 \cdot 14_6 - 1153_6 : 31_6 - 150_6) : 205_6] : 25_6$.

6.7. Записати в десятковій системі числення такі числа:

а) 100111_2;
б) 11001101_2;
в) 345_8;
г) 5071_8;
д) 1300_8;
е) 33311_7;
є) 4602_7;
ж) $(10)6(11)_{12}$;
з) 26014_7;
к) 42125_6;
л) 530415_6.

6.8. Записати в десятковій системі числення такі числа:

а) $0{,}111_2$;
б) $0{,}110_2$;
в) $11001,\ 1111_2$;
г) $437{,}321_8$;
д) $0{,}027_8$.

6.9. Перевести з однієї системи в іншу:

а) $33311_7 \to x_{12}$;
б) $21000122122_3 \to x_9$;
в) $4672510_9 \to x_3$;
г) $1111011011100001_2 \to x_8$;
д) $21066754_8 \to x_2$;
е) $206315_7 \to x_5$;
є) $32014_5 \to x_8$.

6.10. Перевести з десяткової системи числення в інші системи:

а) $2042 \to x_2,\ y_3,\ z_5$;
б) $2786 \to x_2,\ y_3,\ z_5$;
в) $729 \to x_7$;
г) $231632 \to x_7$;
д) $23163 \to x_8$;
е) $17527 \to x_8$.

6.11. Знайти x, якщо:

а) $201_x = 41_8$;
б) $203_x = 53_{10}$;
в) $106_x = 153_7$;
г) $236_x = 1240_5$;
д) $324_x = 10022_3$;
е) $541_x = 2014_6$;
є) $364_x = 3001_4$;
ж) $401_x = 265_7$;
з) $100_x = 34_7$.

6.12. Визначити основу системи числення, в якій виконуються такі рівності:

а) $12 + 13 = 30$;
б) $15 + 16 = 33$;
в) $35 + 40 = 115$;
г) $236 - 145 = 61$;
д) $263 - 214 = 46$;
е) $216 \cdot 3 = 654$;
є) $656 : 5 = 124$;
ж) $736 : 6 = 121$;
з) $1520 : 12 = 123$;
к) $10 \cdot 10 = 100$.

6.13. Довести, що:

а) число 144 є квадратом натурального числа в будь-якій g-ковій системі числення, $g > 4$;

б) число 1331 є кубом натурального числа в будь-якій g-ковій системі числення, $g > 3$;

в) в g-ковій системі числення числа $2(g-1)$ і $(g-1)^2$ записуються тими самими цифрами, але в зворотному порядку;

г) число $A = (a_n a_{n-1} \ldots a_1 a_0)_{12}$ ділиться на 8 (на 9), якщо на 8 (на 9) ділиться число, утворене його останніми двома цифрами $(a_1 a_0)_{12}$;

д) число $A = (a_n a_{n-1} \ldots a_1 a_0)_g$ ділиться на $g-1$, якщо $a_n + a_{n-1} + \ldots + a_1 + a_0$ ділиться на $g-1$;

е) натуральне число, десятковий запис якого є 3^n одиниць, ділиться на 3^n.

6.14. Записати в двійковій системі числення:

а) числа Ферма $F_k = 2^{2^k} + 1$, $k \in \mathbf{N}$;

б) парні досконалі числа $D = 2^{p-1}(2^p - 1)$, де p — просте число.

6.15. Знайти частку від ділення числа $(62xy427)_{10}$ на 99_{10}, а також невідомі цифри x і y, якщо ділення виконується без остачі.

6.16. Знайти невідомі цифри, якщо множення виконується в десятковій системі числення:

а)
```
   *2*3
 ×  **
 -------
  ***87
 *****
 -------
 2*004*
```

б)
```
     шість
   × шість
 ----------
    ******
   ******
  ******
 ******
 ----------
 *****шість
```

6.17. Знайти таке найменше натуральне число m, яке в десятковій системі числення закінчується цифрою 6, причому, якщо цю цифру записати на початку числа, то воно збільшиться в 4 рази.

6.18. Число $(42x4y)_{10}$ ділиться на 72_{10}. Знайти цифри x і y.

6.19. У десятковій системі числення знайти тризначне число x таке, що добуток його цифр дорівнює a і $x = a^2$.

6.20. Довести, що сума цифр квадрата будь-якого натурального числа не може дорівнювати числу 1985_{10}.

6.21. Нехай $2 \times (xyz)_{10} = (xyz)_g$. Знайти $(xyz)_{10}$ і g.

6.22. Знайти в десятковій системі числення таке двозначне число, яке у двійковій, четвірковій і вісімковій системах числення зображується однаковими цифрами, але різними для різних систем.

§ 7. Кільце, підкільце. Найпростіші властивості подільності в комутативному кільці. Дільники нуля та одиниці. Асоційовані елементи. Область цілісності, поле

Література

[1] — § 12, с. 132—136;
[2] — § 12, с. 133—141;
[3] — гл. 3, § 4, с. 104—107;
[4] — гл. VII, § 3, с. 350—358;
[8] — гл. 4, § 4, с. 172—176;
[24] — § 9, с. 30—32.

ТЕОРЕТИЧНІ ВІДОМОСТІ

Кільцем *називається непорожня множина K, в якій визначено дві бінарні алгебраїчні операції — додавання і множення, причому ва додаванням K є абелева група — адитивна група кільця K, а операція множення — асоціативна і пов'язана дистрибутивними законами (лівим і правим) в операцією додавання.*

Якщо операція множення в кільці K комутативна, то кільце називається **комутативним.**

Кільце, яке містить тільки один нульовий елемент, називається **нульовим.**

Ненульове кільце, в якому є нейтральний елемент відносно множення, називається **кільцем з одиницею.**

Комутативне кільце з одиницею, в якому для кожного його ненульового елемента існує обернений елемент, називається **полем.**

Елементи a і b кільця K називаються **дільниками нуля**, якщо $a \neq 0$, $b \neq 0$ і $ab = 0$. При цьому a називають **лівим**, а b — **правим дільником нуля.**

Ненульове комутативне кільце з одиницею без дільників нуля називається **областю цілісності.**

Підмножина K_1 кільця K називається **підкільцем кільця** K, якщо K_1 є кільце відносно операцій додавання і множення, визначених у кільці K. Якщо K_1 є підкільцем кільця K, то записують $K_1 \leqslant K$.

Для того щоб непорожня підмножина K_1 кільця K була його підкільцем, необхідно і достатньо, щоб сума $a+b$, різниця $a-b$ і добуток ab будь-яких елементів a і b підмножини K_1 належали до K_1 (**критерій підкільця**).

Елемент b кільця K називається **лівим (правим) дільником елемента** $a \in K$, якщо існує елемент $c \in K$ такий, що $a = bc$ (відповідно $a = cb$); при цьому a називається **правим (лівим) кратним елемента** b. Якщо K — комутативне кільце, то елементи b і a називають просто **«дільник»** і **«кратне»** і записують $a \vdots b$ (a ділиться на b) або $b \mid a$ (b є дільником a). У противному разі записують відповідно a не $\vdots\, b$ і b не $\mid a$.

Кільце називається **числовим**, якщо воно є підмножиною множини всіх комплексних чисел **C**.

Нехай K — деяке підкільце кільця раціональних чисел **Q**. Множину всіх чисел виду $a + b\sqrt{p}$, де $a, b \in K$ і p — деяке натуральне число, що не є точним квадратом, позначатимемо символом $K[\sqrt{p}]$, а множину всіх чисел виду $a+b\sqrt{p}i$ — символом $K[\sqrt{p}i]$. Зокрема, $Z[i]$ є множина всіх чисел виду $a+bi$, де $a, b \in \mathbf{Z}$ і $Q[i]$ — множина всіх чисел виду $a+bi$, де $a, b \in \mathbf{Q}$. Зауважимо, що кільце $Z[i]$ називають **кільцем цілих гауссових чисел.**

Елемент a, для якого в кільці K з одиницею існує обернений елемент a^{-1}, називають **оборотним** або **дільником одиниці**. Множина K^* всіх дільників одиниці кільця K з одиницею є мультиплікативною групою. K^* називають ще **групою дільників одиничного елемента** або **групою одиниць кільця** K. Елементи a і b області цілісності K називаються **асоційованими**, якщо $a = be$, де e — дільник одиниці. При цьому для асоційованих елементів a і b вживають таке позначення: $a \sim b$.

ПРИКЛАДИ РОЗВ'ЯЗУВАННЯ ЗАДАЧ

1. Довести, що множина $Z[\sqrt{3}]$ усіх чисел виду $a + b\sqrt{3}$, де a і b — цілі числа, є кільцем відносно звичайних операцій додавання і множення.

Розв'язання. Застосуємо прийом, який дає змогу скоротити процес доведення. Якщо треба довести, що деяка непорожня множина K_1 є кільцем, то її поміщають (якщо це можливо) в якесь відоме кільце K. Тоді треба лише довести, що K_1 є підкільце кільця K, звідки випливатиме, що K_1 — кільце.

Оскільки $Z[\sqrt{3}]$ є підмножиною, наприклад, кільця всіх дійсних чисел **R**, то доведемо, що $Z[\sqrt{3}]$ — підкільце кільця **R**. Застосуємо критерій підкільця. Насамперед, покажемо, що $Z[\sqrt{3}] \neq \varnothing$. Це справді так, бо, наприклад, $0 = 0 + 0 \cdot \sqrt{3} \in Z[\sqrt{3}]$. Нехай тепер $t = a + b\sqrt{3}$, $s = c + d\sqrt{3}$, де $a,b,c,d \in Z$, $t,s \in Z[\sqrt{3}]$. Покажемо, що $t+s \in Z[\sqrt{3}]$, $t-s \in Z[\sqrt{3}]$ і $t \cdot s \in Z[\sqrt{3}]$. Справді, $t \pm s = (a + b\sqrt{3}) \pm (c + d\sqrt{3}) = (a \pm c) + (b \pm d)\sqrt{3} \in Z[\sqrt{3}]$, оскільки $a \pm c \in Z$, $b \pm d \in Z$. Аналогічно для добутку дістаємо $t \cdot s = (a+b\sqrt{3})(c + d\sqrt{3}) = (ac + 3bd) + (ad + bc)\sqrt{3} \in Z[\sqrt{3}]$, оскільки для цілих чисел $a, b, c, d, 3$ маємо $ac, 3bd, ad, bc \in Z$.

Отже, $Z[\sqrt{3}]$ — підкільце кільця дійсних чисел **R**, а тому $Z[\sqrt{3}]$ — кільце.

Зауваження. У цій задачі замість кільця дійсних чисел **R** можна було б взяти, наприклад, кільце комплексних чисел **C** і, взагалі, таке довільне кільце K, що $K \geqslant Z[\sqrt{3}]$, тобто кільце K не обов'язково повинно бути мінімальним з усіх тих кілець, які містять підмножину $Z[\sqrt{3}]$.

2. Довести, що в кільці $Z[i]$ цілих гауссових чисел

$$(23 + 2i) \vdots (2 + 3i).$$

Розв'язання. За правилом ділення двох комплексних чисел, записаних в алгебраїчній формі, маємо

$$\frac{23 + 2i}{2 + 3i} = \frac{(23 + 2i)(2 - 3i)}{(2 + 3i)(2 - 3i)} = \frac{52 - 65i}{13} = 4 - 5i.$$

Отже, $23 + 2i = (2 + 3i)(4 - 5i)$, де $4 - 5i \in Z[i]$, а тому $(23 + 2i) \vdots (2 + 3i)$.

3. Довести, що в кільці $S = \{a + b\sqrt[3]{2} + c\sqrt[3]{4},\ a,b,c \in Z\}$ число $-19 + 10\sqrt[3]{2} + 20\sqrt[3]{4}$ ділиться на число $\left(1 - 3\sqrt[3]{2} + 5\sqrt[3]{4}\right)$.

Розв'язання. Покажемо, що в кільці S існує таке число $x + y\sqrt[3]{2} + z\sqrt[3]{4}$, що

$$-19 + 10\sqrt[3]{2} + 20\sqrt[3]{4} = \left(1 - 3\sqrt[3]{2} + 5\sqrt[3]{4}\right)\left(x + y\sqrt[3]{2} + z\sqrt[3]{4}\right).$$

Розкриваючи дужки в правій частині останньої рівності, дістаємо

$$(x + 10y - 6z) + (-3x + y + 10z)\sqrt[3]{2} + (5x - 3y + z)\sqrt[3]{4} = -19 + 10\sqrt[3]{2} + 20\sqrt[3]{4}.$$

Ця рівність можлива тільки тоді, коли x, y, z задовольняють систему рівнянь

$$\begin{cases} x + 10y - 6z = -19, \\ -3x + y + 10z = 10, \\ 5x - 3y + z = 20. \end{cases}$$

Розв'язавши цю систему, знаходимо $x=3$, $y=-1$, $z=2$. Оскільки $3-\sqrt[3]{2}+2\sqrt[3]{4}\in S$, то

$$\left(-19+10\sqrt[3]{2}+20\sqrt[3]{4}\right):\left(1-3\sqrt[3]{2}+5\sqrt[3]{4}\right).$$

4. У кільці $Z[i]$ цілих гауссових чисел знайти всі дільники одиниці.

Розв'язання. Оскільки одиничним елементом у кільці $Z[i]$ цілих гауссових чисел є число $1+0\cdot i=1$, то треба знайти всі такі числа $x+yi$ та $z+ti$, де $x, y, z, t\in Z$, що виконується рівність

$$(x+yi)(z+ti)=1.$$

Така рівність можлива, коли $|(x+yi)(z+ti)|=|1|$, тобто коли $|x+yi|\,|z+ti|=1$. Звідси $(x^2+y^2)(z^2+t^2)=1$. Оскільки x, y, z, t — цілі числа, то остання рівність можлива при умові $x^2+y^2=z^2+t^2=1$. Рівність $x^2+y^2=1$ можлива, в свою чергу, в таких випадках: 1) $x=1$, $y=0$; 2) $x=-1$, $y=0$; 3) $x=0$, $y=1$; 4) $x=0$, $y=-1$. Це означає, що $x+yi$ (відповідно $z+ti$) може мати лише чотири значення: $1, -1, i, -i$. При цьому $z+ti$ набуває відповідно значень: $1, -1, -i, i$. Отже, в кільці $Z[i]$ цілих гауссових чисел є чотири дільники одиниці: $1, -1, i, -i$. Ці елементи і утворюють групу одиниць кільця $Z[i]$, тобто

$$Z[i]^*=\{1, -1, i, -i\}.$$

Задачі

7.1. Які з заданих числових множин утворюють кільце відносно операцій додавання і множина? У кільцях з одиницею знайти всі дільники одиниці. Визначити пари таких кілець, в яких перше є підкільцем другого.

а) $\mathbf{Z}$;

б) $m\mathbf{Z}$ (множина цілих чисел, кратних m, $m\in\mathbf{Z}$); окремо розглянути випадки $m=0$ і $m=1$;

в) $Z[-\sqrt{2}]$ (множина чисел виду $a+b(-\sqrt{2})$, де $a, b\in\mathbf{Z}$);

г) $mZ[\sqrt{2}]$ (множина чисел виду $a+b\sqrt{2}$, де $a, b\in m\mathbf{Z}$);

д) $Z[i]$ (множина всіх чисел виду $a+bi$, де $a, b\in\mathbf{Z}$);

е) $mZ[i]$ (множина всіх чисел виду $a+bi$, де $a, b\in m\mathbf{Z}$);

є) $Z[\sqrt{2}i]$ (множина всіх чисел виду $a+b(i\sqrt{2})$, $a, b\in\mathbf{Z}$);

ж) $mZ[\sqrt{2}i]$ (множина всіх чисел виду $a+b(i\sqrt{2})$, $a, b\in m\mathbf{Z}$);

з) $Z[\sqrt[3]{2}]$ (множина всіх чисел виду $a+b\sqrt[3]{2}$, $a, b\in\mathbf{Z}$);

к) $Z[\sqrt{p}]$ (множина всіх чисел виду $a+b\sqrt{p}$, де $a, b\in\mathbf{Z}$, $p\in\mathbf{N}$ і p не є точним квадратом);

л) $Q[\sqrt[3]{2}]$ (множина всіх чисел виду $a+b\sqrt[3]{2}$, де $a, b\in\mathbf{Q}$);

м) $Q[\sqrt{2}]$ (множина всіх чисел виду $a+b\sqrt{2}$, де $a, b\in\mathbf{Q}$);

н) $\left\{\frac{a+bi\sqrt{3}}{2},\ a, b$ — цілі числа однакової парності$\right\}$.

7.2. Довести, що в довільному кільці K:

а) нуль — є елемент єдиний;

б) для будь-якого $a\in K$ протилежний елемент — a єдиний;

в) рівняння $b+x=a$ для будь-яких $a, b\in K$ має єдиний розв'язок $x=a+(-b)$;

г) якщо $a+b=a+c$, то $b=c$;

д) $a\cdot 0=0\cdot a=0$ для всіх $a\in K$;

е) $a(-b)=(-a)b=-ab$;

є) $a(b-c)=ab-ac$;

ж) $(b-c)a=ba-ca$;

з) якщо $ax=ay$, $a\neq 0$ і a не є дільником нуля, то $x=y$;

к) $a(-b)=(-b)a$, якщо $ab=ba$;

л) $a\cdot nb=nb\cdot a$, $n\in\mathbf{Z}$, якщо $ab=ba$.

7.3. Довести, що:

а) перетин довільного числа підкілець деякого кільця є його підкільцем;

б) множина K^* всіх дільників одиниці кільця K з одиницею утворює мультиплікативну групу (так звану групу одиниць кільця K);

в) у кільці, яке містить n елементів, для кожного елемента a з кільця виконується рівність $na=0$;

г) кільце з чотирьох елементів $0, 1, a, b$ і з правилами дій $a^2=b$, $b^2=a$, $ab=ba=1$, $1+1=0$, $1+a=b$ утворює поле;

д) підмножина $K_1=\{me\mid m\in\mathbf{Z}\}$ кільця K з одиницею e утворює підкільце;

е) непорожня скінченна підмножина K_1 кільця K є підкільцем тоді і тільки тоді, коли $(a+b)\in K_1$ і $ab\in K_1$ для будь-яких елементів $a, b\in K_1$;

є) поле не містить дільників нуля;

ж) дільник одиниці кільця з одиницею не може бути дільником нуля;

з) підкільцем у кільці раціональних чисел $\mathbf{Q}$ є множина m-цілих чисел, тобто всіх таких раціональних чисел, в яких знаменник взаємно простий з m, $m\in\mathbf{N}$;

к) $Q[\sqrt{p}]$ — поле, де $p\in\mathbf{N}$ не є квадратом натурального числа;

л) $Z[\sqrt{s}]=Z[\sqrt{s_1}]$, $Z[\sqrt{s}i]=Z[\sqrt{s_1}i]$, $Q[\sqrt{s}]=Q[\sqrt{s_1}]$, $Q[\sqrt{s}i]=Q[\sqrt{s_1}i]$, якщо $\sqrt{s}=t\sqrt{s_1}$ і s_1 не є квадратом натурального числа, $s, t, s_1\in N$.

7.4. Які із заданих множин матриць утворюють кільце відносно операцій додавання і множення? Які з кілець комутативні? Які містять одиницю? Знайти дільники нуля і одиниці. Знайти пари таких кілець, в яких перше є підкільцем другого.

а) $M(n, \mathbf{N})$ — множина квадратних матриць n-го порядку, елементи яких є натуральні числа;

б) $M(n, \mathbf{Z})$;

в) $M(n, \mathbf{Q})$;

г) $M(n, \mathbf{R})$;

д) $M(n, \mathbf{C})$;

ж) $\left\{\begin{pmatrix} a & 2b \\ b & a\end{pmatrix}\middle|\ a, b\in 3\mathbf{Z}\right\}$;

з) $\left\{\begin{pmatrix} a & 2b \\ b & a\end{pmatrix}\middle|\ a, b\in\mathbf{Q}\right\}$;

к) $\left\{\begin{pmatrix} a & -b \\ b & a\end{pmatrix}\middle|\ a, b\in\mathbf{Z}\right\}$;

л) $\left\{\begin{pmatrix} a & -b \\ b & a\end{pmatrix}\middle|\ a, b\in 2\mathbf{Z}\right\}$;

е) $M(n, 2\mathbf{Z})$;

м) $\left\{\begin{pmatrix} a & -b \\ b & a \end{pmatrix} \middle| a, b \in \mathbf{Q}\right\}$;

є) $\left\{\begin{pmatrix} a & 2b \\ b & a \end{pmatrix} \middle| a, b \in \mathbf{Z}\right\}$;

н) $\left\{\begin{pmatrix} a & -b \\ b & a \end{pmatrix} \middle| a, b \in \mathbf{R}\right\}$.

7.5. Які із заданих множин матриць утворюють кільце відносно операцій додавання і множення? Які з кілець комутативні? Які містять одиницю? У кільцях з одиницею знайти дільники нуля і одиниці. Знайти пари таких кілець, в яких перше є підкільцем другого.

а) $\left\{\begin{pmatrix} {}^1/_2 a & -{}^3/_2 b \\ {}^1/_2 b & {}^1/_2 a \end{pmatrix} \middle| a, b$ — цілі числа однакової парності$\right\}$;

б) $\left\{\begin{pmatrix} a & 0 \\ b & 0 \end{pmatrix} \middle| a, b \in \mathbf{Z}\right\}$;

є) $\left\{\begin{pmatrix} a & b \\ b & a \end{pmatrix} \middle| a, b \in \mathbf{Z}\right\}$;

в) $\left\{\begin{pmatrix} 0 & a \\ 0 & b \end{pmatrix} \middle| a, b \in \mathbf{Q}\right\}$;

ж) $\left\{\begin{pmatrix} a & 0 \\ 0 & b \end{pmatrix} \middle| a, b \in \mathbf{Z}\right\}$;

г) $\left\{\begin{pmatrix} 0 & 0 \\ a & b \end{pmatrix} \middle| a, b \in \mathbf{Z}\right\}$;

з) $\left\{\begin{pmatrix} a & b \\ 0 & a \end{pmatrix} \middle| a, b \in \mathbf{Z}\right\}$;

д) $\left\{\begin{pmatrix} a & b \\ 0 & 0 \end{pmatrix} \middle| a, b \in \mathbf{Q}\right\}$;

к) $\left\{\begin{pmatrix} a & b & c \\ 0 & a & b \\ 0 & 0 & a \end{pmatrix} \middle| a, b, c \in \mathbf{Z}\right\}$.

е) $\left\{\begin{pmatrix} a & -3b \\ b & a \end{pmatrix} \middle| a, b \in \mathbf{Q}\right\}$;

7.6. Нехай K — комутативна група відносно додавання. Чи буде K кільцем, якщо операцію множення введено так:

а) $a \cdot b = 0$, $a, b \in K$;
б) $a \cdot b = a + b$, $a, b \in K$;
в) $a \cdot b = a - b$, $a, b \in K$;
г) $a \cdot b = a$, $a, b \in K$;
д) $a \cdot b = b$, $a, b \in K$?

7.7. Які із заданих множин пар цілих чисел (a, b), $a, b \in \mathbf{Z}$ утворюють кільце, якщо операції додавання і множення пар введено так (дві пари рівні, якщо рівні їхні однойменні компоненти):

а) $(a, b) + (c, d) = (ac, bd)$,
$(a, b) \cdot (c, d) = (a + c, b + d)$;
б) $(a, b) + (c, d) = (a + c, b + d)$,
$(a, b) \cdot (c, d) = (a + b + c + d, 0)$;
в) $(a, b) + (c, d) = (a + c, b + d)$,
$(a, b) \cdot (c, d) = (0, 0)$;
г) $(a, b) + (c, d) = (a + c, b + d)$,
$(a, b) \cdot (c, d) = (ac, bd)$;
д) $(a, b) + (c, d) = (a + b, c + d)$,
$(a, b) \cdot (c, d) = (ab, cd)$;
е) $(a, b) + (c, d) = (a + c, b + d)$,
$(a, b) \cdot (c, d) = (ac + bd, ad + bc)$;

є) $(a, b) + (c, d) = (a + c, b + d)$,
$(a, b) \cdot (c, d) = (ac + 3bd, ad + bc)$;
ж) $(a, b) + (c, d) = (a + c, b + d)$,
$(a, b) \cdot (c, d) = (ac - 3bd, ad + bc)$?

Визначити комутативні кільця. Знайти дільники нуля та одиниці.

7.8. Довести, що:

а) скінченна область цілісності є полем;

б) усі елементи виду ab є дільниками нуля в кільці K, якщо a — дільник нуля, а b — довільний елемент з K;

в) $4 \vdots (1 + i\sqrt{3})$, 4 не $\vdots (2 + 2i\sqrt{3})$ в кільці $Z[\sqrt{3}i]$;

г) $(-8 + 3\sqrt{5}) \vdots (1 + 2\sqrt{5})$ в кільці $Z[\sqrt{5}]$;

д) $(-3 + 39i) \vdots (3 - 5i)$, $34i \vdots (5 + 3i)$, $25 \vdots (4 + 3i)$, $5 \vdots (1 + 2i)$, $(8 + 6i)$ не $\vdots (7 + 5i)$ в кільці $Z[i]$;

е) $(-7 + 18\sqrt{3}) \vdots (4 - \sqrt{3})$, $(5 + 2\sqrt{3}) \vdots (4 - \sqrt{3})$, $13 \vdots (4 - \sqrt{3})$, $13 \vdots (5 - 2\sqrt{3})$ в кільці $Z[\sqrt{3}]$;

є) множина всіх дільників одиниці в кільці $Z[\sqrt{3}]$ складається з елементів виду $\pm (2 + \sqrt{3})^n$, де $n \in \mathbf{Z}$;

ж) кільце K комутативне, якщо $a^2 = a$ для кожного $a \in K$. Чи справджується це твердження при умові $a^3 = a$?

з) $a^m = a$ для будь-якого елемента a поля P, яке містить m елементів.

7.9. Довести, що в області цілісності K:

а) $a \vdots a$, $a \in K$;
б) $a \vdots c$, якщо $a \vdots b$ і $b \vdots c$, $a, b, c \in K$;
в) $ab \vdots c$, якщо $a \vdots c$, $a, b, c \in K$;
г) $(a \pm b) \vdots c$, якщо $a \vdots c$ і $b \vdots c$, $a, b, c \in K$;
д) $(a \pm b)$ не$\vdots c$, якщо $a \vdots c$ і b не$\vdots c$, $a, b, c \in K$;
е) $0 \vdots a$, $a \in K$;
є) $a \vdots 1$, $a \in K$;
ж) $a \vdots be$, якщо $a \vdots b$ і e — дільник одиниці, $a, b, e \in K$;
з) $a \vdots b$ і $b \vdots a$ тоді і тільки тоді, коли $a = be$, де e — дільник одиниці, $a, b, e \in K$, $a \neq 0$.

7.10. Які з кілець задач 7.1, 7.4, 7.5, 7.6, 7.7 є областями цілісності? полями?

7.11. У множині D виразів $a + be$, де $a, b \in \mathbf{R}$, введемо операції додавання і множення:

$$(a + be) + (c + de) = (a + c) + (b + d)e,$$
$$(a + be)(c + de) = (ac + bd) + (ad + bc)e.$$

Довести, що D — комутативне кільце з одиницею і знайти всі дільники нуля (множина D називається **множиною подвійних чисел**).

7.12. Нехай у множині $\mathfrak{Q}$ виразів $a + b\varepsilon$, де $a, b \in \mathbf{R}$, введено операції додавання і множення:

$$(a + b\varepsilon) + (c + d\varepsilon) = (a + c) + (b + d)\varepsilon,$$
$$(a + b\varepsilon)(c + d\varepsilon) = ac + (ad + bc)\varepsilon.$$

Довести, що $\mathfrak{Q}$ — комутативне кільце з одиницею і знайти всі дільники нуля (множина $\mathfrak{Q}$ називається **множиною дуальних чисел**).

7.13. У множині K виразів $a+bi+cj+dk$, де $i^2=j^2=k^2=-1$, $ij=k$, $ji=-k$, $ik=-j$, $ki=j$, $jk=i$, $kj=-i$, $a, b, c, d \in \mathbf{R}$, введено операції додавання і множення:

$$(a_1+b_1i+c_1j+d_1k)+(a_2+b_2i+c_2j+d_2k)=$$
$$=(a_1+a_2)+(b_1+b_2)i+(c_1+c_2)j+(d_1+d_2)k;$$
$$(a_1+b_1i+c_1j+d_1k)(a_2+b_2i+c_2j+d_2k)=a_1a_2-b_1b_2-c_1c_2-$$
$$-d_1d_2+(a_1b_2+b_1a_2+d_1c_2-c_1d_2)i+(a_1c_2+c_1a_2-$$
$$-b_1d_2+d_1b_2)j+(a_1d_2+d_1a_2+b_1c_2-c_1b_2)k.$$

Довести, що K — некомутативне кільце з одиницею без дільників нуля (таку множину називають **множиною кватерніонів**).

7.14. Довести, що задані множини утворюють область цілісності (відносно операцій додавання і множення):

а) множина всіх раціональних чисел виду $\frac{m}{2^k}$, де $m, k \in \mathbf{Z}, k \geqslant 0$;

б) множина всіх дійсних чисел виду $a_1 2^{x_1}+a_2 2^{x_2}+\ldots+a_n 2^{x_n}$, де $n \in \mathbf{N}$, $a_1, a_2, \ldots, a_n \in \mathbf{Z}$, $x_1, x_2, \ldots, x_n$ — раціональні числа виду $\frac{m}{2^k}$, де m, k — цілі невід'ємні числа.

7.15. Нехай M — деяка множина, а $\mathfrak{M}$ — множина всіх підмножин множини M. Довести, що $\mathfrak{M}$ є кільцем з одиницею, всі елементи адитивної групи якого мають порядок 2, якщо операції додавання і множення введено так:

$$A+B=(A \cup B) \setminus (A \cap B),\ A \cdot B=A \cap B,\ A, B \in \mathfrak{M}.$$

7.16. Довести, що в області цілісності K:

а) відношення асоційованості на множині K є бінарним відношенням еквівалентності;

б) елементи a і b тоді і тільки тоді асоційовані, коли $a \vdots b$ і $b \vdots a$;

в) $a_1 : b_1$, якщо a асоційовано з a_1, а b з b_1 і $a : b$;

г) елементи $5+2\sqrt{3}$ і $4-\sqrt{3}$ асоційовані, якщо $K=Z[\sqrt{3}]$;

д) елементи $25-17\sqrt{2}$ і $7-\sqrt{2}$ асоційовані, якщо $K=Z[\sqrt{2}]$;

е) елементи $3-7\sqrt{5}$ і $113+51\sqrt{5}$ асоційовані, якщо $K=Z[\sqrt{5}]$;

є) елементи $7-2i$ і $2-7i$ асоційовані, якщо $K=Z[i]$.

§ 8. Ідеали кільця та операції над ними. Конгруенції і класи лишків за ідеалом. Фактор-кільце

Література

[1] — § 13, с. 141—147;
[2] — § 13, с. 143—150;
[3] — гл. 13, § 1, с. 430—434;
[8] — гл. 4, § 4, с. 176—183.

ТЕОРЕТИЧНІ ВІДОМОСТІ

Непорожня підмножина I кільця K називається **лівим (правим)** *ідеалом цього кільця, якщо виконуються такі умови:*

1) $a \pm b \in I$, де $a, b \in I$;

2) $ka \in I$ ($ak \in I$), де $a \in I$, $k \in K$.

Підмножина I кільця K, яка одночасно є лівим і правим ідеалом, називається **двостороннім ідеалом** або **ідеалом кільця** K.

У комутативному кільці кожен лівий і правий ідеали є двостороннім.

Кожен лівий і правий, а отже, двосторонній ідеал, є підкільцем кільця K.

Одиничним ідеалом кільця K називається кільце K.

Нульовим ідеалом кільця K називається нульове підкільце.

Нехай K — деяке комутативне кільце і a — будь-який його елемент. Множина елементів виду $xa+na$, де x — будь-який елемент кільця K, а n — будь-яке ціле число, є ідеал кільця K. Цей ідеал називають **головним ідеалом, породженим елементом** a, і позначають $<a>$. Якщо в кільці K є одиниця, то $<a>=Ka=\{ka$, де $k \in K\}$.

Аналогічно визначають поняття ідеалу, породженого кількома елементами $a_1, a_2, \ldots, a_s$, комутативного кільця K: $<a_1, a_2, \ldots, a_s>=\sum\limits_{i=1}^{s} x_i a_i+\sum\limits_{j=1}^{s} n_j a_j$, де $x_i \in K$, $n_j \in \mathbf{Z}$.

Множину всіх елементів виду $a+b$, де $a \in A$, $b \in B$, A, B — ідеали кільця K, називають **сумою ідеалів** A, B і позначають $A+B$.

Множину всіх елементів виду $a_1b_1+a_2b_2+\ldots+a_nb_n$, де $a_1, a_2, \ldots, a_n \in A$, $b_1, b_2, \ldots, b_n \in B$, A, B — ідеали кільця K, називають **добутком ідеалів** A, B і позначають AB. Перетин, сума і добуток ідеалів кільця K є також ідеал кільця K.

Елементи a і b кільця K називають **конгруентними за ідеалом** I (за модулем I), якщо $a-b \in I$. Це рівносильно тому, що елементи a і b належать тому самому суміжному класу адитивної групи K за її підгрупою I.

Висловлення «a конгруентно b за ідеалом I» записують так: $a \equiv b \pmod I$. Якщо $I=<k>$, то пишуть $a \equiv b \pmod k$.

Відношення конгруентності елементів на множині деякого кільця K за його ідеалом I є бінарним відношенням еквівалентності. Класи еквівалентності називають ще класами лишків кільця K за ідеалом I або суміжними класами групи K за підгрупою I.

Властивості конгруенцій за ідеалом I в кільці K:

1°. Обидві частини конгруенції можна помножити на будь-яке ціле число;

2°. До обох частин конгруенції можна додати будь-який елемент з кільця K;

3°. Обидві частини конгруенції можна помножити на будь-який елемент з кільця K;

4°. Конгруенції можна почленно додавати, віднімати і множити;

5° Клас $a+I$ лишків кільця K за ідеалом I з представником a позначають так: $\overline{a}=a+I$, як позначали раніше суміжний клас $a+I$ групи K за її підгрупою I з представником a.

Множину всіх класів лишків кільця K за його ідеалом I позначають $K/I=\overline{K}$. У цій множині алгебраїчними є операції додавання і множення класів лишків:

$$\overline{a}+\overline{b}=\overline{a+b},\quad \overline{a} \cdot \overline{b}=\overline{ab}.$$

Відносно цих операцій множина $\overline{K}$ утворює кільце, яке називають **фактор-кільцем** кільця K за ідеалом I. Фактор-кільце K/I називають ще **кільцем класів лишків**. Якщо $K=\mathbf{Z}$, а I — ідеал кільця $\mathbf{Z}$, то I — головний ідеал, породжений деяким числом m, $m \in Z$. Фактор-кільце $\mathbf{Z}/I=Z/<m>$ позначають $\mathbf{Z}_m$.

ПРИКЛАДИ РОЗВ'ЯЗУВАННЯ ЗАДАЧ

1. Нехай K_1 — підкільце кільця K, I — ідеал кільця K. Довести, що $K_1 \cap I$ — ідеал кільця K_1.

Розв'язання. Введемо позначення $D=K_1 \cap I$. Покажемо спочатку, що ідеал I, як і будь-який ідеал, містить нуль-елемент кільця K. Справді,

оскільки $I \neq \varnothing$, то в I існує хоч один елемент a. Тоді, згідно з першим пунктом означення ідеалу, елемент $a - a$, тобто 0, теж належить ідеалу I. Оскільки $0 \in K_1$, $0 \in I$, то $0 \in D$ і тому $D \neq \varnothing$.

Якщо $a, b \in D$, то $a, b \in K_1$ і $a, b \in I$. Згідно з означенням ідеалу і критерієм підкільця, $a \pm b \in I$, $a \pm b \in K_1$, а тому $a \pm b \in D$.

Нехай $a \in D$, $b \in K_1$. Покажемо, що ab і ba належать D. Справді, оскільки $D \subseteq K_1$, то $a, b \in K_1$ і за критерієм підкільця K_1 маємо, що

$$ab,\ ba \in K_1. \tag{1}$$

Оскільки $D \subseteq I$, а I — ідеал кільця K, то для будь-якого елемента $a \in D \subseteq I$ і будь-якого елемента $b \in K_1 \subseteq K$ маємо, що

$$ab,\ ba \in I. \tag{2}$$

З включень (1) і (2) випливає, що $ab,\ ba \in K_1 \cap I = D$.

Отже, $D = K_1 \cap I$ — ідеал кільця K_1.

2. Довести, що в кільці $M(2, \mathbf{Z})$ матриць другого порядку $\begin{pmatrix} a & b \\ c & d \end{pmatrix}$ з цілими елементами лівий ідеал утворює підмножина T матриць виду $\begin{pmatrix} 0 & m \\ 0 & n \end{pmatrix}$, де m, $n \in \mathbf{Z}$.

Розв'язання. Оскільки $\begin{pmatrix} 0 & 0 \\ 0 & 0 \end{pmatrix} \in T$, то $T \neq \varnothing$. Якщо $A, B \in T$, то $A = \begin{pmatrix} 0 & m \\ 0 & n \end{pmatrix}$, $B = \begin{pmatrix} 0 & k \\ 0 & l \end{pmatrix}$, де $m, n, k, l \in \mathbf{Z}$. Тоді $A \pm B = \begin{pmatrix} 0 & m \pm k \\ 0 & n \pm l \end{pmatrix} \in T$, оскільки $m \pm k,\ n \pm l \in \mathbf{Z}$. Нехай тепер

$$X \in M(2, \mathbf{Z}) \quad \text{і} \quad X = \begin{pmatrix} a & b \\ c & d \end{pmatrix},$$

де $a, b, c, d \in \mathbf{Z}$ і $A \in T$. Знайдемо добуток

$$X \cdot A = \begin{pmatrix} a & b \\ c & d \end{pmatrix} \begin{pmatrix} 0 & m \\ 0 & n \end{pmatrix} = \begin{pmatrix} 0 & am + bn \\ 0 & cm + dn \end{pmatrix}.$$

Оскільки $am + bn,\ cm + dn \in \mathbf{Z}$ і в матриці $X \cdot A$ на місцях з номерами 11 і 21 стоять нулі, то $X \cdot A \in T$. Отже, T — лівий ідеал кільця $M(2, \mathbf{Z})$.

Зауваження. Зрозуміло, що T не є правим ідеалом цього кільця, оскільки $A \cdot X = \begin{pmatrix} mc & md \\ nc & nd \end{pmatrix}$ і тому не завжди $A \cdot X \in T$. Отже, T не є двостороннім ідеалом.

3. Побудувати фактор-кільце $\mathbf{Z}/<6> = Z_6$ кільця цілих чисел $\mathbf{Z}$ за головним ідеалом $I = <6>$, породженим числом 6. Скласти таблиці додавання і множення для елементів фактор-кільця. Знайти всі дільники нуля цього фактор-кільця і обернені елементи.

Розв'язання. Як відомо, фактор-кільце K/I довільного кільця K за його ідеалом I є сукупність суміжних класів $\bar{0} = I$, $\bar{x} = x + I$, $\bar{y} = y + I$,..., для яких введено операції додавання і множення:

$$\bar{x} + \bar{y} = \overline{x + y},\quad \bar{x} \cdot \bar{y} = \overline{xy}. \tag{1}$$

У цьому разі

$$K = \mathbf{Z} = \{0, \pm 1, \pm 2, \ldots\},$$
$$I = <6> = \{0, \pm 6, \pm 12, \ldots\}.$$

Тоді

$$\bar{0} = 0 + <6> = \{0, \pm 6, \pm 12, \pm 18, \ldots\},$$
$$\bar{1} = 1 + <6> = \begin{Bmatrix} 1, & 7, & 13, & 19, \ldots \\ & -5, & -11, & -17, \ldots \end{Bmatrix},$$

$$\bar{2} = 2 + <6> = \begin{Bmatrix} 2, & 8, & 14, & 20, \ldots \\ & -4, & -10, & -16, \ldots \end{Bmatrix},$$
$$\bar{3} = 3 + <6> = \begin{Bmatrix} 3, & 9, & 15, & 21, \ldots \\ & -3, & -9, & -15, \ldots \end{Bmatrix},$$
$$\bar{4} = 4 + <6> = \begin{Bmatrix} 4, & 10, & 16, & 22, \ldots \\ & -2, & -8, & -14, \ldots \end{Bmatrix},$$
$$\bar{5} = 5 + <6> = \begin{Bmatrix} 5, & 11, & 17, & 23, \ldots \\ & -1, & -7, & -13, \ldots \end{Bmatrix}.$$

Побудовані класи лишків $\bar{0}, \bar{1}, \bar{2}, \bar{3}, \bar{4}, \bar{5}$ вичерпують всі класи лишків за модулем 6. Розглянемо, наприклад, клас лишків $\overline{341}$. Оскільки $341 = 336 + 5$, а $336 \in <6>$, то $\overline{341} = 341 + <6> = (5 + 336) + <6> = 5 + (336 + <6>) = 5 + <6> = \bar{5}$ (використано властивість класів лишків за ідеалом: якщо $a \in I$, то $a + I = I$). Користуючись формулами (1), складемо таблиці додавання і множення класів лишків — таблиці Келі (табл. 8, 9).

Таблиця 8

+	$\bar{0}$	$\bar{1}$	$\bar{2}$	$\bar{3}$	$\bar{4}$	$\bar{5}$
$\bar{0}$	$\bar{0}$	$\bar{1}$	$\bar{2}$	$\bar{3}$	$\bar{4}$	$\bar{5}$
$\bar{1}$	$\bar{1}$	$\bar{2}$	$\bar{3}$	$\bar{4}$	$\bar{5}$	$\bar{0}$
$\bar{2}$	$\bar{2}$	$\bar{3}$	$\bar{4}$	$\bar{5}$	$\bar{0}$	$\bar{1}$
$\bar{3}$	$\bar{3}$	$\bar{4}$	$\bar{5}$	$\bar{0}$	$\bar{1}$	$\bar{2}$
$\bar{4}$	$\bar{4}$	$\bar{5}$	$\bar{0}$	$\bar{1}$	$\bar{2}$	$\bar{3}$
$\bar{5}$	$\bar{5}$	$\bar{0}$	$\bar{1}$	$\bar{2}$	$\bar{3}$	$\bar{4}$

Таблиця 9

×	$\bar{0}$	$\bar{1}$	$\bar{2}$	$\bar{3}$	$\bar{4}$	$\bar{5}$
$\bar{0}$	$\bar{0}$	$\bar{0}$	$\bar{0}$	$\bar{0}$	$\bar{0}$	$\bar{0}$
$\bar{1}$	$\bar{0}$	$\bar{1}$	$\bar{2}$	$\bar{3}$	$\bar{4}$	$\bar{5}$
$\bar{2}$	$\bar{0}$	$\bar{2}$	$\bar{4}$	$\bar{0}$	$\bar{2}$	$\bar{4}$
$\bar{3}$	$\bar{0}$	$\bar{3}$	$\bar{0}$	$\bar{3}$	$\bar{0}$	$\bar{3}$
$\bar{4}$	$\bar{0}$	$\bar{4}$	$\bar{2}$	$\bar{0}$	$\bar{4}$	$\bar{2}$
$\bar{5}$	$\bar{0}$	$\bar{5}$	$\bar{4}$	$\bar{3}$	$\bar{2}$	$\bar{1}$

Для прикладу знайдемо:

$$\bar{4} + \bar{5} = \overline{4 + 5} = \bar{9} = \overline{9 - 6} = \bar{3},$$
$$\bar{4} \cdot \bar{5} = \overline{4 \cdot 5} = \overline{20} = \overline{20 - 6 \cdot 3} = \overline{20 - 18} = \bar{2},$$
$$\bar{5} \cdot \bar{5} = \overline{25} = \overline{25 - 6 \cdot 4} = \overline{25 - 24} = \bar{1}.$$

За таблицею множення, дільниками нуля є $\bar{2}, \bar{3}, \bar{4}$, оскільки $\bar{2} \neq \bar{0}$, $\bar{3} \neq \bar{0}$, $\bar{4} \neq \bar{0}$, але $\bar{2} \cdot \bar{3} = \bar{3} \cdot \bar{2} = \bar{4} \cdot \bar{3} = \bar{0}$. З цієї самої таблиці маємо $\bar{1}^{-1} = \bar{1}$, $\bar{5}^{-1} = \bar{5}$, оскільки $\bar{1} \cdot \bar{1} = \bar{1}$, $\bar{5} \cdot \bar{5} = \bar{1}$.

Задачі

8.1. Чи є ідеалами (лівим, правим, двостороннім):

а) перетин, сума і добуток двох ідеалів I_1, I_2 в довільному кільці K;

б) множина I всіх елементів виду $r_1a_1 + r_2a_2 + \ldots + r_na_n$, де $a_1, a_2, \ldots, a_n$ — деякі елементи підмножини A комутативного кільця K, а $r_1, r_2, \ldots, r_n$ — деякі елементи з K;

в) множина Ka всіх елементів виду xa, де x — будь-який елемент кільця K, a — довільний фіксований елемент цього кільця;

г) множина aK всіх елементів виду ax, де x — будь-який елемент кільця K, а a — довільний фіксований елемент цього кільця;

д) множина KaK всіх елементів виду

$$x_1ay_1 + x_2ay_2 + \ldots + x_nay_n,$$

де n — будь-яке натуральне число, x_i і y_i — будь-які елементи кільця K, a — довільний фіксований елемент цього кільця;

е) множина $2\mathbf{Z}$ в кільці $\mathbf{Z}$;

є) множина $m\mathbf{Z}$ в кільці $\mathbf{Z}$;

ж) множина $2Z[\sqrt{3}]$ в кільці $Z[\sqrt{3}]$;

з) множина $3Z[i]$ в кільці $Z[i]$;

к) множина $nK = \{nx \mid x \in K\}$ в K, де x — довільний елемент кільця K, n — фіксоване ціле число;

л) множина таких функцій $g(x)$, що $g(1/3) = 0$ в кільці неперервних функцій на відрізку $[-1; 1]$?

8.2. Чи є ідеалами такі підмножини:

а) множина $\left\{\begin{pmatrix} m & n \\ 0 & 0 \end{pmatrix}\right\}$ в кільці $M(2, \mathbf{Z})$, якщо $m, n \in \mathbf{Z}$;

б) множина $\left\{\begin{pmatrix} 0 & 0 \\ m & n \end{pmatrix}\right\}$ в кільці $M(2, \mathbf{Z})$, якщо $m, n \in \mathbf{Z}$;

в) множина $\left\{\begin{pmatrix} m & 0 \\ n & 0 \end{pmatrix}\right\}$ в кільці $M(2, \mathbf{Z})$, якщо $m, n \in \mathbf{Z}$;

г) множина $\left\{\begin{pmatrix} a & a \\ a & a \end{pmatrix} \middle| a \in \mathbf{Z}\right\}$ в кільці $\left\{\begin{pmatrix} a & b \\ b & a \end{pmatrix} \middle| a, b \in \mathbf{Z}\right\}$;

д) множина $\left\{\begin{pmatrix} a & 0 \\ 0 & 0 \end{pmatrix} \middle| a \in \mathbf{Z}\right\}$ в кільці $M(2, \mathbf{Z})$;

е) множина $\left\{\begin{pmatrix} a & 0 \\ 0 & b \end{pmatrix} \middle| a, b \in \mathbf{Z}\right\}$ в кільці $M(2, \mathbf{Z})$;

є) множина $\left\{\begin{pmatrix} 0 & d & e \\ 0 & 0 & d \\ 0 & 0 & 0 \end{pmatrix} \middle| d, e \in \mathbf{Z}\right\}$ в кільці $\left\{\begin{pmatrix} a & b & c \\ 0 & a & b \\ 0 & 0 & a \end{pmatrix} \middle| a, b, c \in \mathbf{Z}\right\}$;

ж) множина $\left\{\begin{pmatrix} a & b & c \\ 0 & a & b \\ 0 & 0 & a \end{pmatrix} \middle| a, b, c \in \mathbf{Z}\right\}$ в кільці $M(3, \mathbf{Z})$;

з) множина $\left\{\begin{pmatrix} 0 & 0 & 0 \\ 0 & a & 0 \\ 0 & 0 & 0 \end{pmatrix} \middle| a \in \mathbf{Z}\right\}$ в кільці $M(3, \mathbf{Z})$?

8.3. Довести, що:

а) непорожня підмножина I кільця K є його правим ідеалом тоді і тільки тоді, коли I — підкільце кільця K, причому $I \cdot K \leqslant I$;

б) непорожня підмножина I кільця K є його правим ідеалом тоді і тільки тоді, коли I — така підгрупа адитивної групи кільця K, що $I \cdot K \subseteq I$;

в) в кільці цілих чисел $\mathbf{Z}$ кожен його ідеал головний;

г) відношення конгруентності за ідеалом для елементів кільця K є бінарним відношенням еквівалентності;

д) $a \in (a + I)$ для будь-якого елемента a кільця K і його ідеалу I;

е) $I + x = I$ тоді і тільки тоді, коли $x \in I$, де I — ідеал кільця K, а x — елемент з K;

є) $I + x = I + d$, $I + y = I + d$, якщо $d \in (I + x) \cap (I + y)$, де I — ідеал, а x, y, d — представники класів лишків;

ж) $I + x \cap I + y = \varnothing$, якщо $I + x \neq I + y$, де I — ідеал кільця K, а x, y — представники класів лишків;

з) підмножина $\{x \mid xm = 0, x \in K, m \in \mathbf{Z}\}$ є ідеал кільця K;

к) $aK = K$, якщо a — дільник одиниці комутативного кільця K з одиницею, і навпаки, якщо a такий елемент комутативного кільця K, що $aK = K$, то K — кільце з одиницею і a — дільник одиниці.

8.4. Довести, що в комутативному кільці K з одиницею:

а) $a \in \langle a \rangle$, $a \in K$;

б) $\langle 0 \rangle = \{0\}$, $\langle 1 \rangle = K$;

в) $b - c \in \langle a \rangle$, якщо $b, c \in \langle a \rangle$;

г) $rb \in \langle a \rangle$, якщо $b \in \langle a \rangle$, де $r \in K$;

д) $a \mid b$ тоді і тільки тоді, коли $\langle a \rangle \subseteq \langle b \rangle$, де $a, b \in K$;

е) асоційовані елементи кільця K породжують той самий головний ідеал;

є) головний ідеал, породжений дільником e одиниці 1 кільця K, збігається з K, тобто $\langle e \rangle = \langle 1 \rangle = K$;

ж) головні ідеали, породжені елементами a і b, збігаються тоді і тільки тоді, коли a і b — асоційовані елементи і K — область цілісності;

з) у K всі ідеали головні, якщо K — поле, причому в K лише два ідеали: нульовий і одиничний;

к) мінімальний ідеал $I(A)$ кільця K, який містить підмножину A цього кільця, збігається з ідеалом $\langle A \rangle$, породженим підмножиною A.

8.5. У кільці цілих чисел $\mathbf{Z}$ виконати такі дії над його ідеалами:

а) $\langle 2 \rangle + \langle 3 \rangle$;
б) $\langle 2 \rangle \cap \langle 3 \rangle$;
в) $\langle 2 \rangle \cdot \langle 3 \rangle$;
г) $\langle 3 \rangle + \langle 6 \rangle$;
д) $\langle 3 \rangle \cap \langle 6 \rangle$;
е) $\langle 3 \rangle \cdot \langle 6 \rangle$;
є) $\langle 4 \rangle + \langle 10 \rangle$;
ж) $\langle 4 \rangle \cap \langle 10 \rangle$;
з) $\langle 4 \rangle \cdot \langle 10 \rangle$;
к) $\langle 5 \rangle + \langle 7 \rangle$;
л) $\langle 5 \rangle \cap \langle 7 \rangle$;
м) $\langle 5 \rangle \cdot \langle 7 \rangle$.

8.6. Довести, що в довільному кільці K для будь-якого ідеалу I:

а) $\langle 0 \rangle + I = I$;
б) $\langle 0 \rangle \cap I = \langle 0 \rangle$;
в) $\langle 0 \rangle \cdot I = \langle 0 \rangle$;
г) $K + I = K$;
д) $K \cap I = I$;
е) $K \cdot I \subseteq I$,

причому $K \cdot I = I$, якщо K — кільце з одиницею.

8.7. Довести, що:

а) $<2-\sqrt{3}> = Z[\sqrt{3}]$;

б) $<2+\sqrt{5}> = Z[\sqrt{5}]$;

в) $<3+\sqrt{7}> \supset <13+5\sqrt{7}>$ в $Z[\sqrt{7}]$;

г) $<8-3\sqrt{7}> = Z[\sqrt{7}]$;

д) $<i> = Z[i]$;

е) $<2i> = 2Z[i]$;

є) $<-3> = 3Z[i]$;

ж) $<3+4i> = <4-3i>$ в $Z[i]$.

8.8. У кільці цілих чисел Z знайти ідеали:

а) $<2, 5>$;
б) $<4, 6>$;
в) $<6, 15>$;
г) $<-1, 3>$;
д) $<2, 4, 6>$;
е) $<2, 3, 5>$;
є) $<4, 6, 8>$.

8.9. Нехай I — ідеал кільця K і $a \equiv b \pmod I$, $a, b \in K$. Довести, що:

а) $a+c \equiv b+c \pmod I$, $c \in K$;

б) $a+c \equiv b+d \pmod I$, якщо $c \equiv d \pmod I$, $c, d \in K$;

в) $-a \equiv -b \pmod I$;

г) $ma \equiv mb \pmod I$, $m \in \mathbf{Z}$;

д) $ac \equiv bc \pmod I$, $c \in K$;

е) $ac \equiv bd \pmod I$, якщо $c \equiv d \pmod I$, $c, d \in K$;

є) $a^n \equiv b^n \pmod I$, $n \in \mathbf{N}$.

8.10. Довести, що в кільці цілих чисел $\mathbf{Z}$ при $m \geqslant 1$ $a \equiv b \pmod m$ тоді і тільки тоді, коли $(a-b) \vdots m$. Що означає $a \equiv b \pmod 0$?

8.11. Побудувати фактор-кільця Z_2, Z_3, Z_4, Z_5. Скласти для їхніх елементів таблиці додавання і множення. Знайти всі дільники нуля і обернені елементи.

8.12. Які з фактор-кілець Z_2, Z_3, Z_4, Z_5 є полями?

8.13. Довести, що:

а) Z_m — поле, якщо m — просте число;

б) Z_m — кільце з дільниками нуля, якщо m — складене число;

в) кільце K, яке містить принаймні два елементи, є полем тоді і тільки тоді, коли в K немає ідеалів, крім $<0>$ і K.

8.14. Знайти всі дільники нуля у фактор-кільці Z_m, якщо:

а) $m=8$; б) $m=9$; в) $m=10$; г) $m=12$;
д) $m=14$; е) $m=15$; є) $m=16$.

8.15. Знайти обернені елементи для елементів фактор-кільця Zm, якщо:

а) $m=7$; б) $m=8$; в) $m=9$;
г) $m=10$; д) $m=11$; е) $m=12$;
є) $m=13$; ж) $m=14$; з) $m=15$; к) $m=16$.

8.16. У кільці цілих гауссових чисел $Z[i]$ побудувати фактор-кільце $Z[i]/<m>$. Скласти для елементів фактор-кільця таблиці додавання і множення, знайти всі дільники нуля і обернені елементи, якщо:

а) $m=2$; б) $m=3$; в) $m=2i$;
г) $m=-3i$; д) $m=i$.

8.17. У фактор-кільці $Z[i]/<m>$ кільця цілих гауссових чисел $Z[i]$ за ідеалом $<m>$, породженим елементом m, знайти кількість елементів, усі дільники нуля і елементи $\bar{a}^{-1}$, якщо:

а) $m=4$, $\bar{a}=\bar{i}$; $\overline{3i}$; $\overline{1+2i}$;

б) $m=5$, $\bar{a}=\bar{2}$; $\overline{4i}$; $\overline{3+2i}$;

в) $m=6i$, $\bar{a}=\overline{2+5i}$; $\overline{4+i}$.

8.18. Побудувати фактор-кільце $Z[\sqrt{3}]/2Z[\sqrt{3}]$ кільця $Z[\sqrt{3}]$ за його ідеалом $2Z[\sqrt{3}]$. Скласти для елементів фактор-кільця таблиці додавання і множення, знайти всі дільники нуля і обернені елементи.

8.19. Довести, що фактор-кільце K/I кільця K з одиницею за будь-яким його ідеалом I містить також одиничний елемент.

§ 9. Гомоморфізми та ізоморфізми кілець. Теорема про гомоморфізми кілець

Література

[1] — § 13, с. 147—150;
[2] — § 13, с. 150—153;
[3] — гл. 13, § 1, с. 434—437;
[4] — гл. VII, § 4, с. 360—362;
[8] — гл. 4, § 4, с. 178—183.

ТЕОРЕТИЧНІ ВІДОМОСТІ

Однозначним (взаємно однозначним) *відображенням множини A на множину B називається таке відображення φ, при якому:*

1) кожен елемент a з множини A відображується на єдиний елемент b з множини B; при цьому кажуть, що b — образ елемента a, а a — прообраз елемента b, і пишуть $\varphi(a)=b$;

2) кожен елемент b з множини B є образом хоч одного (єдиного) елемента a з A.

Існують ще однозначні і взаємно однозначні відображення з множини в множину, з множини на множину, множини в множину.

Ми користуватимемося в основному відображенням всієї першої множини на всю другу множину.

Однозначне (взаємно однозначне) відображення φ кільця K на кільце K_1 називається **гомоморфним (ізоморфним)** відображенням, якщо виконуються такі дві умови:

1) образ суми довільних двох елементів a і b з кільця дорівнює сумі їхніх образів: $\varphi(a+b)=\varphi(a)+\varphi(b)$;

2) образ добутку довільних двох елементів a і b з кільця K дорівнює добутку їхніх образів: $\varphi(a \cdot b)=\varphi(a) \cdot \varphi(b)$.

Якщо φ — гомоморфізм кільця K на кільце K_1, то φ є **епіморфізм** кільця K. У цьому разі кажуть, що K_1 є гомоморфним образом кільця K, і пишуть

$$K \simeq K_1 \text{ або } \varphi: K \simeq K_1.$$

Якщо K ізоморфно відображується на K_1, то пишуть

$$K \cong K_1 \text{ або } \varphi: K \cong K_1.$$

Будь-яке ізоморфне відображення є одночасно і гомоморфним відображенням, але не завжди навпаки.

Властивості гомоморфних (ізоморфних) відображень кільця K на кільце K_1 такі:

1°. Образом нульового елемента першого кільця є нульовий елемент другого кільця: $\varphi(0)=O_1$;

2°. Образом $\varphi(-a)$ елемента $-a$, протилежного даному елементу a, є елемент $-\varphi(a)$, протилежний образу $\varphi(a)$, тобто $\varphi(-a) = -\varphi(a)$;

3°. Якщо в кільці K є одиничний елемент e, то його образ $\varphi(e)$ є одиничний елемент кільця K_1; якщо в кільці K для елемента a існує обернений елемент a^{-1}, то $\varphi(a^{-1})$ є оберненим елементом до елемента $\varphi(a)$ в кільці K_1.

Нехай φ є гомоморфне відображення кільця K на кільце K_1. Множину D всіх елементів кільця K, які гомоморфізмом φ відображуються в O_1 кільця K_1, називають **ядром гомоморфізму** φ і позначають так: $D = \operatorname{Ker}\varphi$. Отже, $\operatorname{Ker}\varphi = \{d \mid d \in K, \varphi(d) = O_1\}$.

Ядро $D = \operatorname{Ker}\varphi$ будь-якого гомоморфізму φ кільця K на кільце K_1 є ідеалом кільця K.

Теорема про гомоморфізми кілець. *Фактор-кільце* $K / \operatorname{Ker}\varphi$ *кільця* K *ва ядром* $\operatorname{Ker}\varphi$ *гомоморфізму* $K \simeq K_1$ *ізоморфне кільцю* K_1, *тобто* $K / \operatorname{Ker}\varphi \cong K_1$.

ПРИКЛАДИ РОЗВ'ЯЗУВАННЯ ЗАДАЧ

1. Встановити гомоморфне відображення довільного кільця K на фактор-кільце $\overline{K} = K/I$ кільця K за будь-яким його ідеалом I.

Розв'язання. Задамо відображення φ множини K на множину $\overline{K}$ так: $\varphi(a) = \bar{a}$, тобто $\varphi(a) = a + I$, де $a \in K$. Інакше кажучи, кожному елементу a з кільця K поставимо у відповідність клас лишків $\bar{a}$ з кільця $\overline{K}$ з представником a. Тоді φ є однозначним відображенням всього кільця K на все кільце $\overline{K}$. Справді, якщо $\bar{b} \in \overline{K}$, то $\bar{b} = b + I$, де $b \in K$ і тому $\varphi(b) = \bar{b}$. Покажемо, що $\varphi(a+b) = \varphi(a) + \varphi(b)$ і $\varphi(a \cdot b) = \varphi(a) \cdot \varphi(b)$ для довільних елементів a, $b \in K$. Знаходимо:

$$\varphi(a+b) = \overline{a+b}, \text{ і } \varphi(a) + \varphi(b) = \bar{a} + \bar{b}.$$

Оскільки $\overline{a+b} = \bar{a} + \bar{b}$, то $\varphi(a+b) = \varphi(a) + \varphi(b)$. Далі маємо: $\varphi(ab) = \overline{ab}$ і $\varphi(a) \cdot \varphi(b) = \bar{a} \cdot \bar{b}$. Оскільки $\overline{a \cdot b} = \bar{a} \cdot \bar{b}$, то $\varphi(a \cdot b) = \varphi(a) \cdot \varphi(b)$. Отже, φ є гомоморфним відображенням кільця K на кільце $\overline{K}$. Його називають **природним гомоморфізмом** кільця K на фактор-кільце K/I.

Зауваження. Якщо $I \neq \{0\}$, то φ не є ізоморфізмом.

2. Встановити гомоморфне відображення φ кільця цілих чисел $\mathbf{Z}$ на кільце T і побудувати фактор-кільце $\mathbf{Z} / \operatorname{Ker}\varphi$ кільця $\mathbf{Z}$ за ядром $\operatorname{Ker}\varphi$ гомоморфізму φ, якщо $T = \{\theta, e\}$, а операції додавання і множення в T задано табл. 10, 11.

Таблиця 10

+	θ	e
θ	θ	e
e	e	θ

Таблиця 11

×	θ	e
θ	θ	θ
e	θ	e

Розв'язання. Згідно з таблицями, елемент θ — нульовий, а e — одиничний елемент кільця T. Задамо відображення φ кільця $\mathbf{Z}$ на кільце T так:

$$\varphi(z) = \begin{cases} \theta, & \text{якщо } z \text{ парне;} \\ e, & \text{якщо } z \text{ непарне, де } z \in \mathbf{Z}. \end{cases}$$

Зрозуміло, що φ — однозначне відображення всієї множини $\mathbf{Z}$ на всю множину T. Покажемо, що $\varphi(z+t) = \varphi(z) + \varphi(t)$ і $\varphi(z \cdot t) = \varphi(z) \cdot \varphi(t)$ для довільних z, $t \in \mathbf{Z}$.

З точністю до позначень можливі три випадки: 1) z і t — парні; 2) z і t — непарні; 3) z — парне, t — непарне. Розглянемо кожен з них.

1) Якщо z і t парні, то $\varphi(z) = \varphi(t) = \theta$. Тоді $\varphi(z) + \varphi(t) = \varphi(z) \cdot \varphi(t) = \theta$. Оскільки $z+t$, $z \cdot t$ — парні, то $\varphi(z+t) = \varphi(z \cdot t) = \theta$. Отже, $\varphi(z+t) = \varphi(z) + \varphi(t)$ і $\varphi(z \cdot t) = \varphi(z) \cdot \varphi(t)$;

2) якщо z і t непарні, то $\varphi(z) = \varphi(t) = e$, $\varphi(z) + \varphi(t) = e + e = \theta$ і $\varphi(z) \cdot \varphi(t) = e \cdot e = e$. Оскільки $z+t$ — парне, а $z \cdot t$ непарне, то $\varphi(z+t) = \theta$, $a\varphi(z \cdot t) = e$. Тоді знову $\varphi(z+t) = \varphi(z) + \varphi(t)$ і $\varphi(z \cdot t) = \varphi(z) \cdot \varphi(t)$;

3) якщо z парне, а t непарне, то $\varphi(z) = \theta$, $\varphi(t) = e$. Тоді $\varphi(z) + \varphi(t) = \theta + e = e$, $\varphi(z) \cdot \varphi(t) = \theta \cdot e = \theta$. Оскільки $z+t$ непарне, а $z \cdot t$ парне, то $\varphi(z+t) = e$, $\varphi(z \cdot t) = \theta$ і тому $\varphi(z+t) = \varphi(z) + \varphi(t)$ і $\varphi(z \cdot t) = \varphi(z) \cdot \varphi(t)$. Отже, φ є гомоморфне відображення кільця K на кільце T. Із задання відображення φ випливає, що $\operatorname{Ker}\varphi = 2\mathbf{Z}$. Тоді $\mathbf{Z} / \operatorname{Ker}\varphi = \mathbf{Z} / 2\mathbf{Z} = \{\bar{0}, \bar{1}\}$, де

$$\bar{0} = 2\mathbf{Z} = \{0, \pm 2, \pm 4, \ldots\},$$

$$\bar{1} = 1 + 2\mathbf{Z} = \{1, 3, 5, \ldots\} = \{-1, -3, \ldots\}.$$

Очевидно, що $\mathbf{Z} / 2\mathbf{Z} \cong T$. Це досягається за допомогою нового відображення ψ: $\psi(\bar{0}) = \theta$, $\psi(\bar{1}) = e$.

Зауваження. На практиці не завжди вдається відразу вдало підібрати відображення φ. Його треба задавати таким чином, щоб задовольнялися вже перші загальновідомі ознаки. Так, у розглянутому прикладі не можна покласти $\varphi(z) = e$ при парному z, бо тоді б нульовий елемент першого кільця перейшов би в одиничний елемент другого кільця, що суперечить теорії і т. д.

Задачі

9.1. Довести, що:

а) відображення $\varphi(a+bi) = a+bi$ і $\psi(a+bi) = a-bi$ вичерпують усі ізоморфні відображення поля комплексних чисел $\mathbf{C}$ на себе;

б) відображеннями $\varphi(a + b\sqrt{2}) = a + b\sqrt{2}$ і $\psi(a + b\sqrt{2}) = a - b\sqrt{2}$ вичерпуються всі ізоморфізми поля $Q[\sqrt{2}]$ на себе, при яких $\varphi(x) = x$ і $\psi(x) = x$ для довільного $x \in \mathbf{Q}$;

в) гомоморфізм двох кілець є їхнім ізоморфізмом тоді і тільки тоді, коли ядро цього гомоморфізму збігається з нульовим елементом першого кільця;

г) гомоморфний образ області цілісності є кільцем, але не завжди є областю цілісності;

д) кільця $Z[\sqrt{7}]$ і $Z[\sqrt{11}]$ не ізоморфні між собою.

9.2. Довести, що при гомоморфізмі φ двох кілець K і K_1:

а) $\varphi(0) = 0_1$;

б) $\varphi(-a) = -\varphi(a)$;

в) $\varphi(a-b) = \varphi(a) - \varphi(b)$;

г) $\varphi(e) = e_1$ (якщо в K існує одиниця e);

д) $\varphi(a^{-1}) = [\varphi(a)]^{-1}$ (якщо в K для a існує обернений елемент a^{-1});

е) ядро гомоморфізму $\operatorname{Ker}\varphi$ є ідеалом кільця K.

9.3. Які можливі гомоморфізми поля P на поле P_1?

9.4. Довести, що ненульове комутативне кільце K з одиницею є полем тоді і тільки тоді, коли довільний гомоморфізм кільця K на ненульове кільце є ізоморфізмом.

9.5. Довести, що ізоморфними між собою є такі кільця:

а) $Z[\sqrt{2}]$ і $\left\{\begin{pmatrix} a & b \\ 2b & a \end{pmatrix} \middle| a, b \in \mathbf{Z}\right\}$;

б) $2Z[\sqrt{3}]$ і $\left\{\begin{pmatrix} a & 3b \\ b & a \end{pmatrix} \middle| a, b \in 2\mathbf{Z}\right\}$;

в) $Q[\sqrt{3}]$ і $\left\{\begin{pmatrix} a & 3b \\ b & a \end{pmatrix} \middle| a,\ b \in \mathbf{Q}\right\}$;

г) $Z[i]$ і $\left\{\begin{pmatrix} a & b \\ -b & a \end{pmatrix} \middle| a,\ b \in \mathbf{Z}\right\}$;

д) $3Z[i]$ і $\left\{\begin{pmatrix} a & -b \\ b & a \end{pmatrix} \middle| a,\ b \in 3\mathbf{Z}\right\}$;

е) $Q[i]$ і $\left\{\begin{pmatrix} a & -b \\ b & a \end{pmatrix} \middle| a,\ b \in \mathbf{Q}\right\}$;

є) $Z[\sqrt{3}i]$ і $\left\{\begin{pmatrix} a & -3b \\ b & a \end{pmatrix} \middle| a,\ b \in \mathbf{Z}\right\}$;

ж) $\left\{\frac{a+bi\sqrt{3}}{2} \middle|\ a,\ b$ — цілі числа однакової парності$\right\}$ і

$$\left\{\begin{pmatrix} \frac{1}{2}a & -\frac{3}{2}b \\ \frac{1}{2}b & \frac{1}{2}a \end{pmatrix} \middle|\ a,\ b \text{ — цілі числа однакової парності}\right\};$$

з) $Q[\sqrt{3}i]$ і $\left\{\begin{pmatrix} a & -3b \\ b & a \end{pmatrix} \middle| a,\ b \in \mathbf{Q}\right\}$.

9.6. Нехай φ — відображення кільця $K = \left\{\begin{pmatrix} a & b \\ b & a \end{pmatrix} \middle| a,\ b \in \mathbf{Z}\right\}$ на кільце $\mathbf{Z}$ цілих чисел, причому $\varphi\left(\begin{pmatrix} a & b \\ b & a \end{pmatrix}\right) = a - b$. Довести, що φ — гомоморфізм, і знайти його ядро.

9.7. Нехай φ — відображення кільця цілих чисел $\mathbf{Z}$ на кільце класів лишків $Z_3 = \{\bar{0}, \bar{1}, \bar{2}\}$, причому

$$\varphi(z) = \begin{cases} \bar{0}, & \text{якщо } z \text{ ділиться на 3;} \\ \bar{1}, & \text{якщо } z \text{ при діленні на 3 дає остачу 1;} \\ \bar{2}, & \text{якщо } z \text{ при діленні на 3 дає остачу 2.} \end{cases}$$

Довести, що φ є гомоморфізм, і знайти його ядро.

9.8. Нехай φ — відображення кільця діагональних матриць $K = \left\{\begin{pmatrix} a & 0 \\ 0 & b \end{pmatrix} \middle| a,\ b \in \mathbf{Q}\right\}$ на кільце раціональних чисел $\mathbf{Q}$, причому $\varphi\left(\begin{pmatrix} a & 0 \\ 0 & b \end{pmatrix}\right) = a$ для будь-яких $a,\ b \in \mathbf{Q}$. Довести, що φ — гомоморфізм, і знайти його ядро.

9.9. Нехай φ — відображення кільця K всіх неперервних функцій на відрізку $[-1; 2]$ на кільце дійсних чисел $\mathbf{R}$, причому $\varphi(f) = f(1)$ для будь-якої функції $f \in K$. Довести, що φ — гомоморфізм, і знайти його ядро.

9.10. Нехай M і M_1 — множини з бінарними операціями додавання і множення. Довести, що M_1 є кільце, якщо M є кільце, і існує гомоморфне відображення множини M на M_1.

9.11. Довести, що:

а) будь-який ідеал I кільця K є ядром гомоморфізму при відображенні кільця K на фактор-кільце K/I;

б) підмножина I кільця K є ядром гомоморфізму цього кільця на деяке кільце K_1 тоді і тільки тоді, коли I є ідеалом кільця K;

в) будь-яке кільце, гомоморфне кільцю K, ізоморфне деякому фактор-кільцю цього кільця.

9.12. Знайти (з точністю до ізоморфізму) всі скінченні кільця з чотирьох елементів, які містять 0 і 1.

9.13. Знайти (з точністю до ізоморфізму) всі скінченні кільця, які містять pq елементів, де p і q — різні прості числа.

9.14. Довести, що довільне кільце, яке містить просте число p елементів, або ізоморфне полю класів лишків Z_p, або ізоморфне адитивній групі лишків з нульовим множенням.

9.15. Довести, що кільце матриць

$$\left\{\begin{pmatrix} a+bi & c+di \\ -c+di & a-bi \end{pmatrix} \middle|\ a,\ b,\ c,\ d \in \mathbf{R}\right\}$$

ізоморфне кільцю кватерніонів $a+bi+cj+dk$ над полем дійсних чисел (див. задачу 7.13).

9.16. Довести, що:

а) $Z_4/2Z_4 \cong Z_2$;

б) $Z_6/2Z_6 \cong Z_2$;

в) $Z_6/3Z_6 \cong Z_3$;

г) $Z_8/4Z_8 \cong Z_4$;

д) $Z_m/nZ_m \cong Z_n$, якщо $n,\ m \in \mathbf{N}$ і $m \vdots n$;

е) $[Q\sqrt{7}] \not\cong Q[\sqrt{11}]$.

§ 10. Характеристика кільця з одиницею. Поле часток області цілісності. Прості та складені елементи області цілісності. Арифметика кільця головних ідеалів та евклідового кільця

Література

[1] — § 12, с. 136—141, § 13, с. 150—153, § 14, с. 153—155;
[2] — § 12, с. 137—143, § 13, с. 153—156, § 14, с. 156—158;
[3] — гл. 13, § 2, с. 439—445, § 3, с. 445—448.

ТЕОРЕТИЧНІ ВІДОМОСТІ

Характеристикою *кільця K з одиницею e називають число 0, якщо $ne = 0$ тільки при $n = 0$; характеристикою кільця K називають натуральне число p, якщо $pe = 0$ і немає такого натурального числа $m < p$, що $me = 0$.*

Характеристика будь-якого числового кільця дорівнює нулю. Кожне натуральне число n є характеристикою деякого кільця з одиницею, наприклад, n є характеристикою кільця класів лишків Z_n.

Якщо K — кільце характеристики n, то для будь-якого елемента $a \in K$ маємо $na = 0$.

Характеристикою області цілісності (характеристикою будь-якого поля) є або нуль, або просте число.

Якщо K — область цілісності характеристики 0, то $na \neq 0$ для будь-якого ненульового елемента $a \in K$ і будь-якого цілого числа $n \in \mathbf{Z}$, $n \neq 0$.

Для кожної області цілісності K існує поле T, що містить як підкільце область цілісності K. При цьому кожен елемент поля T дорівнює частці деяких двох елементів області цілісності K. Поле T називають **полем часток** або **полем відношень області цілісності** K. Будь-які два поля часток T і T_1 тієї самої області цілісності K ізоморфні між собою: $T \cong T_1$.

Поле часток кільця цілих чисел $\mathbf{Z}$ є полем раціональних чисел $\mathbf{Q}$.

Запис $a \sim b$ означає, що елементи a і b кільця K з одиницею асоційовані.

Елемент a області цілісності K називають **простим** або **нерозкладним, незвідним**, якщо:

1) $a \neq 0$;

2) a не є дільником одиниці;

3) a, крім дільників одиниці і асоційованих ним, ніяких інших дільників не має.

Елемент a області цілісності K називається **складеним** або **розкладним, звідним**, якщо a, крім дільників одиниці та асоційованих з ним, має ще хоча б один дільник.

Будь-який елемент b області цілісності K, асоційований з простим елементом a, також простий.

Елемент c області цілісності K називають **спільним дільником елементів** $a_1, a_2, \ldots, a_n$, якщо кожен з цих елементів ділиться на c. **Найбільшим спільним дільником** елементів $a_1, a_2, \ldots, a_n$ називають такий спільний дільник цих елементів, який ділиться на будь-який інший їхній спільний дільник.

Найбільший спільний дільник елементів $a_1, a_2, \ldots, a_n$ позначається символом $(a_1, a_2, \ldots, a_n)$ і визначається з точністю до множника, що є дільником одиниці.

Елементи a і b області цілісності K **називають взаємно простими**, якщо вони не мають спільних дільників, відмінних від дільників одиниці, тобто якщо $(a, b) = 1$.

Якщо a — будь-який, а p — простий елемент області цілісності K, то $(a, p) = 1$ або p.

Ідеал I_1 комутативного з одиницею кільця K ділиться на ідеал I_2 цього ж кільця, якщо $I_1 \subseteq I_2$.

Відношення подільності ідеалів транзитивне і рефлексивне.

Ідеал I комутативного з одиницею кільця K називається **найбільшим спільним дільником ідеалів** I_1 і I_2 цього кільця, якщо:

а) I є дільником I_1 і I_2;

б) I ділиться на будь-який спільний дільник I_1 і I_2.

Будь-які два ідеали I_1 і I_2 комутативного кільця з одиницею K мають найбільший спільний дільник, яким є ідеал, породжений множиною $I_1 \cup I_2$, тобто найменший ідеал, який містить ідеали I_1 і I_2.

Найбільший спільний дільник головних ідеалів $\langle a \rangle$ і $\langle b \rangle$ комутативного кільця з одиницею K складається з елементів виду $ra + sl$, де $r, s \in K$.

Найменшим спільним кратним ідеалів I_1 і I_2 комутативного кільця з одиницею K називають такий ідеал I цього кільця, що $I \vdots I_1$ і $I \vdots I_2$ і будь-який ідеал, кратний I_1 і I_2, ділиться на I.

Найменшим спільним кратним ідеалів I_1 і I_2 **є** їх перетин $I_1 \cap I_2$.

Об'єднання зростаючого ряду $I_1 \subset I_2 \subset \ldots \subset I_n \subset \ldots$ ідеалів кільця K є ідеалом цього кільця.

Область цілісності, в якій кожен ідеал головний, називається **кільцем головних ідеалів**.

У кільці головних ідеалів K виконуються такі властивості:

1°. Будь-який набір елементів $a_1, a_2, \ldots, a_n$ кільця K має найбільший спільний дільник d, причому $d = k_1a_1 + k_2a_2 + \ldots + k_na_n$, де $k_1, k_2, \ldots, k_n \in K$;

2°. Будь-які два найбільші спільні дільники елементів $a_1, a_2, \ldots, a_n$ кільця K асоційовані в K;

3°. $d = (a_1, a_2, \ldots, a_n)$ тоді і тільки тоді, коли $\langle a_1, a_2, \ldots, a_n \rangle = \langle d \rangle$, $a_1, a_2, \ldots, a_n, d \in K$;

4°. Якщо $d = (a, b)$ і $d \neq 0$, то $\left(\frac{a}{d}, \frac{b}{d}\right) = 1$, де $a, b, d \in K$;

5°. Елементи a і b кільця K взаємно прості тоді і тільки тоді, коли в кільці K є такі елементи r і s, що $ra + sb = 1$;

6°. Якщо $a, b, c \in K$ і $(a, b) = (a, c) = 1$, то $(a, bc) = 1$;

7°. Якщо $a, b, c \in K$, $ab \vdots c$ і $(a, c) = 1$, то $b \vdots c$;

8°. Якщо $a, b, c \in K$, $a \vdots b$, $a \vdots c$ і $(b, c) = 1$, то $a \vdots bc$;

9°. Якщо p — простий елемент кільця K, то фактор-кільце $K/\langle p \rangle$ є поле;

10°. Якщо добуток кількох елементів кільця K ділиться на простий елемент $p \in K$, то, принаймні, один із множників ділиться на p;

11°. У кільці K не існує нескінченної строго зростаючої послідовності ідеалів;

12°. У кільці K кожен відмінний від нуля елемент, що не є дільником одиниці, розкладається в добуток простих множників;

13°. Якщо $a = p_1p_2 \ldots p_r$ і $a = q_1q_2 \ldots q_s$ є два розклади елемента a кільця K в добутки простих множників, то $r = s$, і при відповідній нумерації множників справджуються рівності $q_i = p_ie_i$, $i = 1, 2, \ldots, r$, де e_i — деякий дільник одиниці кільця K.

Елемент c називають **спільним кратним елементів** $a_1, a_2, \ldots, a_n$ кільця головних ідеалів K, якщо c ділиться в K на кожен з цих елементів.

Найменшим спільним кратним елементів $a_1, a_2, \ldots, a_n$ кільця головних ідеалів K називають таке їхнє спільне кратне, на яке ділиться будь-яке спільне кратне цих елементів. Найменше спільне кратне елементів $a_1a_2, \ldots, a_n$ позначають $[a_1, a_2, \ldots, a_n]$.

Будь-які два найменших спільних кратних елементів $a_1, a_2, \ldots, a_n$ кільця головних ідеалів K асоційовані в K.

Якщо K — кільце головних ідеалів, то $m = [a_1, a_2, \ldots, a_n]$ тоді і тільки тоді, коли $\langle a_1 \rangle \cap \langle a_2 \rangle \cap \ldots \cap \langle a_n \rangle = \langle m \rangle$, $a_1, a_2, \ldots, a_n \in K$, $m \in K$.

Для будь-якого набору $a_1, a_2, \ldots, a_n$ елементів кільця головних ідеалів K існує найменше спільне кратне.

Якщо K — кільце головних ідеалів, то $[ac, bc] \sim c[a, b]$ для будь-яких елементів $a, b, c \in K$.

Якщо a, b — ненульові елементи кільця головних ідеалів K, то

$$[a, b] \sim \frac{ab}{(a, b)}.$$

Область цілісності K називають **евклідовим кільцем**, якщо існує відображення φ множини відмінних від 0 елементів цієї області цілісності в множину цілих невід'ємних чисел $\mathbf{N}^\circ$, тобто $K \setminus \{0\} \to \mathbf{N}^\circ$, яке задовольняє таку умову: для будь-яких елементів $a, b \in K$, $b \neq 0$ в K існують такі елементи q і r, що $a = bq + r$, причому $r = 0$ або $\varphi(r) < \varphi(b)$.

Число $\varphi(a)$ називають ще **нормою елемента** a.

Кожне евклідове кільце є кільцем головних ідеалів.

Кільце K називають **факторіальним**, якщо воно є областю цілісності і будь-який елемент кільця, відмінний від нуля і дільників одиниці, однозначно (з точністю до дільників одиниці і порядку множників) розкладається на добуток простих множників.

Кільця головних ідеалів і евклідові кільця факторіальні.

Нехай $a = up_1^{\alpha_1}p_2^{\alpha_2} \ldots p_m^{\alpha_m}$, $b = vp_1^{\beta_1}p_2^{\beta_2} \ldots p_m^{\beta_m}$, де $p_1, p_2, \ldots, p_m$ — попарно різні прості елементи факторіального кільця K, u, v — дільники одиниці цього кільця. Тоді $[a, b] = p_1^{\gamma_1}p_2^{\gamma_2} \ldots p_m^{\gamma_m}$, де

$$\gamma_i = \max\{\alpha_i, \beta_i\}, \quad (a, b) = p_1^{\delta_1}p_2^{\delta_2} \ldots p_m^{\delta_m},$$

де $\delta_i = \min\{\alpha_i, \beta_i\}$, $i = 1, 2, \ldots, m$.

ПРИКЛАДИ РОЗВ'ЯЗУВАННЯ ЗАДАЧ

1. Довести, що характеристикою області цілісності є або нуль, або просте число.

Розв'язання. Нехай K — область цілісності, а e — одиниця кільця K. Якщо $me \neq 0$ для жодного натурального числа m, то характеристика кільця K дорівнює нулю.

Нехай тепер $me = 0$ і m найменше натуральне число, що має цю властивість, тобто m — характеристика кільця K. Тоді $m \neq 1$, оскільки $e \neq 0$. Якщо m просте число, то твердження задачі доведено.

Нехай m складене число. Тоді існують натуральні числа s і t такі, що $1 < s$, $t < m$ і $m = st$. Внаслідок комутативності кільця K маємо

$$0 = me = (st)e = (se)(te).$$

Крім того, оскільки m — характеристика кільця K і $s < m$, $t < m$, то $se \neq 0$, $te \neq 0$ і тому $(se) \cdot (te) = me \neq 0$, бо K, як область цілісності, є кільцем без дільників нуля. Отже, прийшли до суперечності.

2. У кільці цілих гауссових чисел $Z[i]$ знайти найбільший спільний дільник чисел $6 - 17i$ та $18 + i$.

Розв'язання. Алгоритм Евкліда для знаходження найбільшого спільного дільника двох цілих гауссових чисел такий самий, як і відповідний алгоритм для цілих чисел, тільки замість порівняння абсолютних величин виконується порівняння норм. Нагадаємо, що нормою цілого гауссового числа z, $z = a + bi$, $a, b \in \mathbf{Z}$ називається число $a^2 + b^2$, яке позначають $\mathrm{Nr}z$. Очевидно, що $\mathrm{Nr}z = |z|^2 = z \cdot \bar{z}$, де $|z|$ — модуль, а $\bar{z}$ — спряжене до z. Остання, відмінна від нуля, остача в алгоритмі Евкліда і є найбільшим спільним дільником заданих чисел.

Застосуємо алгоритм Евкліда до чисел $6 - 17i$ та $18 + i$.

Оскільки $\mathrm{Nr}(6 - 17i) = \mathrm{Nr}(18 + i) = 325$, то $6 - 17i$ ділимо з остачею на $18 + i$. Використовуємо правило ділення комплексних чисел в алгебраїчній формі:

$$\frac{6 - 17i}{18 + i} = \frac{(6 - 17i)(18 - i)}{(18 + i)(18 - i)} = \frac{91 - 312i}{325}.$$

Зрозуміло, що $\mathrm{Nr}(91 - 312i) > \mathrm{Nr}(325)$, оскільки $91^2 + 312^2 > 325^2$. Виділимо тоді цілу частину так, щоб у дробу, який залишається, норма чисельника була строго менша норми знаменника. Дістанемо

$$\frac{91 - 312i}{325} = \frac{91 + 13i - 325i}{325} = \frac{-325i}{325} + \frac{91 + 13i}{325} = -i + \frac{91 + 13i}{325}.$$

Тут $\mathrm{Nr}(91 + 13i) < \mathrm{Nr}(325)$, бо $91^2 + 13^2 < 325^2$. Тоді

$$\frac{6 - 17i}{18 + i} = -i + \frac{91 + 13i}{325}.$$

Звідси

$$6 - 17i = (18 + i)(-i) + (5 + i), \qquad (1)$$

причому

$$\mathrm{Nr}(5 + i) < \mathrm{Nr}(18 + i) \text{ і } 5 + i \text{ — перша остача.}$$

Оскільки $\mathrm{Nr}(18 + i) > \mathrm{Nr}(5 + i)$, то

$$\frac{18 + i}{5 + i} = \frac{91 - 13i}{26} = \frac{7 - i}{2}.$$

Внаслідок того що $\mathrm{Nr}(7 - i) > \mathrm{Nr}(2)$, можна виділити цілу частину:

$$\frac{7 - i}{2} = \frac{6 + 1 - i}{2} = 3 + \frac{1 - i}{2}.$$

Тут $\mathrm{Nr}(1 - i) < \mathrm{Nr}(2)$, бо $1^2 + 1^2 < 2^2$. Тоді

$$\frac{18 + i}{5 + i} = 3 + \frac{1 - i}{2}.$$

Звідси

$$18 + i = (5 + i) \cdot 3 + (3 - 2i), \qquad (2)$$

причому $\mathrm{Nr}(3 - 2i) < \mathrm{Nr}(5 + i)$ і $3 - 2i$ є друга остача. Оскільки $\mathrm{Nr}(5 + i) > \mathrm{Nr}(3 - 2i)$, то число $5 + i$ ділимо на $3 - 2i$ з остачею:

$$\frac{5 + i}{3 - 2i} = \frac{13 + 13i}{13} = 1 + i.$$

Отже, $5 + i = (3 - 2i)(1 + i) + 0$, і тому третя остача дорівнює нулю. Згідно з алгоритмом Евкліда, найбільший спільний дільник чисел $6 - 17i$ та $18 + i$ дорівнює останній відмінній від нуля остачі в алгоритмі послідовного ділення з остачею, тобто

$$(6 - 17i,\ 18 + i) \sim 3 - 2i$$

(тут поставлено знак асоційованості, бо найбільшим спільним дільником чисел $6 - 17i$ та $18 + i$ є також числа $(3 - 2i)(-1) = -3 + 2i$, $(3 - 2i)i = 2 + 3i$, $(3 - 2i)(-i) = -2 - 3i$, тобто всі числа, асоційовані з числом $3 - 2i$ в $Z[i]$).

Зауваження

1. Якщо задано два цілих гауссових числа z_1 і z_2 і $\mathrm{Nr}(z_1) > \mathrm{Nr}(z_2)$, то ділення з остачею можна виконувати не за правилом ділення комплексних чисел в алгебраїчній формі, а за тим самим прийомом, який застосовували до виділення цілої частини з дробу виду $\frac{a + bi}{c}$, де $a, b, c \in \mathbf{Z}$. Наприклад, для чисел $18 + i$ і $5 + i$ маємо

$$\frac{18 + i}{5 + i} = \frac{15 + 3i + 3 - 2i}{5 + i} = 3 + \frac{3 - 2i}{5 + i}$$

і тому $18 + i = (5 + i) \cdot 3 + (3 - 2i)$. Тут процес ділення з остачею коротший. Проте, оскільки це не завжди можливо, то краще для всіх $z_2 \in \mathbf{Z}$ і $\mathrm{Nr}(z_1) > \mathrm{Nr}(z_2)$ ділення виконувати так, як у прикладі 2.

2. На закінчення розв'язання треба зробити перевірку. Слід, наприклад, перевірити, чи діляться задані числа на знайдений найбільший спільний дільник. Маємо

$$6 - 17i = (3 - 2i)(4 - 3i),\quad 18 + i = (3 - 2i)(4 + 3i).$$

Ще можна було б перевірити, чи будуть числа $4 - 3i$ та $4 + 3i$ взаємно простими.

3. Як своєрідну перевірку можна використати також лінійне зображення найбільшого спільного дільника через задані числа. Так, з рівності (2) дістаємо

$$3 - 2i = (18 + i) - (5 + i) \cdot 3. \qquad (3)$$

З рівності (1) знаходимо

$$5 + i = (6 - 17i) - (18 + i)(-i).$$

Підставляємо це значення в рівність (3):

$$3 - 2i = (18 + i) - [(6 - 17i) - (18 + i)(-i)] \cdot 3 = (6 - 17i)(-3) + (18 + i)(1 - 3i).$$

Виконавши в правій частині останньої рівності необхідні перетворення, впевнюємося, що лінійне зображення знайдено правильно.

4. Аналогічно знаходиться найбільший спільний дільник чисел у кільці $Z[\sqrt{p}]$ або $Z[\sqrt{p}i]$, де p не є точним квадратом. При цьому

$$\mathrm{Nr}(a + b\sqrt{p}i) = a^2 + b^2p,\ \mathrm{Nr}(a + b\sqrt{p}) = |a^2 - b^2p|,\ a, b \in \mathbf{Z}.$$

3. Простим чи складеним є ціле гауссове число $3+2i$?

Розв'язання. Зрозуміло, що $3+2i \neq 0$ і $3+2i$ не є дільником одиниці в кільці $Z[i]$ (в $Z[i]$ дільниками одиниці є числа $1, -1, i, -i$). Використаємо норму цілого гауссового числа і покажемо, що $3+2i$ є простим числом. Оскільки $\mathrm{Nr}(3+2i)=13$, то, припустивши, що $3+2i$ є складене число, дістаємо

$$3+2i=(a+bi)(c+di), \tag{1}$$

де $a+bi$, $c+di$ не є дільниками одиниці і не є асоційованими з числом $3+2i$, $a, b, c, d \in Z$. З рівності (1) маємо

$$13=(a^2+b^2)(c^2+d^2). \tag{2}$$

Для цілих чисел a, b, c, d ця рівність можлива тільки тоді, коли $a^2+b^2=13$, $c^2+d^2=1$ або $a^2+b^2=1$, $c^2+d^2=13$. При цьому дістаємо, що $c+di$ або відповідно $a+bi$ є дільниками одиниці, що суперечить припущенню. Отже, $3+2i$ не може бути складеним числом. Оскільки $3+2i \neq 0$ і $3+2i$ не є дільником одиниці, то $3+2i$ є просте число в кільці $Z[i]$.

4. Довести, що число 4 в кільці $Z[\sqrt{3}i]$ неоднозначно розкладається в добуток простих множників.

Розв'язання. Знайдемо спочатку дільники одиниці в $Z[\sqrt{3}i]$. Нехай $a+b\sqrt{3}i$, $c+d\sqrt{3}i$ — дільники одиниці, $a, b, c, d \in Z$. Тоді

$$(a+b\sqrt{3}i)(c+d\sqrt{3}i)=1.$$

Знайдемо норму обох частин цієї рівності:

$$(a^2+3b^2)(c^2+3d^2)=1. \tag{1}$$

(Нагадаємо, що норму числа $a+b\sqrt{3}i$ знаходять за формулою

$$\mathrm{Nr}(a+b\sqrt{3}i)=(a^2+3b^2).$$

Рівність (1) виконується, якщо

$$a^2+3b^2=c^2+3d^2=1. \tag{2}$$

Рівність (2), в свою чергу, виконується при $a=\pm 1$, $b=0$, $c=\pm 1$, $d=0$. Отже, в кільці $Z[\sqrt{3}i]$ лише два дільники одиниці: 1, -1.

Доведемо, що для числа 4 в кільці $Z[\sqrt{3}i]$ є два різних розклади в добуток простих множників: $4=2\cdot 2=(1+\sqrt{3}i)(1-\sqrt{3}i)$. Для цього покажемо, що 2, $1+\sqrt{3}i$, $1-\sqrt{3}i$ є прості числа в $Z[\sqrt{3}i]$, а пари чисел 2, $1+\sqrt{3}i$ та 2, $1-\sqrt{3}i$ не є асоційованими. Оскільки в кільці $Z[\sqrt{3}i]$ асоційовані числа відрізняються тільки знаком, то покажемо, що 2, $1+\sqrt{3}i$, $1-\sqrt{3}i$ є прості числа в $Z[\sqrt{3}i]$. Якщо $2=(a+b\sqrt{3}i)(c+d\sqrt{3}i)$, то знайшовши норми від обох частин, дістанемо $4=(a^2+3b^2)(c^2+3d^2)$. Число 4 розкладається в добуток натуральних чисел двома способами: $4=2\cdot 2=1\cdot 4$. Якщо $a^2+3b^2=2$, то $b^2<1$, тобто $b=0$. Тоді $a^2=2$, що неможливо для цілого числа a. Отже, $a^2+3b^2=1$ або $a^2+3b^2=4$. Якщо $a^2+3b^2=1$, то $a+b\sqrt{3}i$ — дільник одиниці. Якщо $a^2+3b^2=4$, то $c^2+3d^2=1$ і $c+d\sqrt{3}i$ — дільник одиниці. Отже, 2 є просте число в кільці $Z[\sqrt{3}i]$. Оскільки $\mathrm{Nr}(1\pm\sqrt{3}i)=4$, то аналогічно доводять, що числа $1\pm\sqrt{3}i$ є простими. Отже, число 4 в кільці $Z[\sqrt{3}i]$ розкладається на прості множники двома різними способами.

Зауваження

1. Зрозуміло, що цей метод доведення можна перенести на будь-яке кільце $Z[\sqrt{p}i]$, де p не є точним квадратом, а $p+1$ — складене натуральне число. Тоді в $Z[\sqrt{p}i]$ число $p+1$ разкладатиметься на прості множники двома різними способами.

2. Аналогічно можна довести неоднозначність розкладу на добуток простих множників чисел виду $p-1$ в кільцях $Z[\sqrt{p}]$, де p не є квадратом натурального числа, а $p-1$ є складене натуральне число.

Задачі

10.1. Довести, що:

а) характеристикою будь-якого поля є нуль або просте число;

б) найменше підполе будь-якого поля характеристики нуль ізоморфне полю раціональних чисел;

в) характеристика фактор-кільця Z/mZ кільця цілих чисел за ідеалом mZ дорівнює числу m;

г) $na=0$ для будь-якого елемента a кільця K характеристики n;

д) характеристика будь-якого числового кільця дорівнює нулю.

10.2. Довести, що в будь-якому полі P для його елементів a, b, c, d, де $b\neq 0$, $d\neq 0$:

а) $\frac{a}{b}=\frac{c}{d}$ тоді і тільки тоді, коли $ad=bc$;

б) $\frac{a}{b}+\frac{c}{d}=\frac{ad+bc}{bd}$;

в) $\frac{a}{b}-\frac{c}{d}=\frac{ad-bc}{bd}$;

г) $\frac{a}{b}\cdot\frac{c}{d}=\frac{ac}{bd}$;

д) $\frac{a}{b}:\frac{c}{d}=\frac{ad}{bc}$ при $c\neq 0$;

е) $\left(\frac{a}{b}\right)^{-1}=\frac{b}{a}$ при $a\neq 0$.

10.3. Нехай K — область цілісності, P — множина всіх дробів $\frac{a}{b}$ елементів $a, b\in K$, $b\neq 0$. На множині P існує бінарне відношення $\frac{a}{b}\,R\,\frac{c}{d}$ тоді і тільки тоді, коли $ad=bc$, $d\neq 0$. Довести, що:

а) R — бінарне відношення еквівалентності;

б) $((a, b))=((c, d))$, $((0, b))=((0, d))$,
$((ad, bd))=((a, b))$, $((b, b))=((d, d))$, де $((x, y))$ — клас еквівалентності R, який визначається парою (x, y), $y\neq 0$;

в) якщо $((a, b))+((c, d))=((ad+bc, bd))$, $((a, b))\cdot((c, d))=((ac, bd))$, то з рівностей $((a, b))=((a', b'))$ і $((c, d))=((c', d'))$ випливають рівності $((a, b))+((c, d))=((a', b'))+((c', d'))$ і $((a, b))\cdot((c, d))=((a', b'))\cdot((c', d'))$;

г) множина S класів еквівалентності R з введеними в п. в) операціями додавання і множення є полем (його називають **полем часток області цілісності** K);

д) множина $K'=\{((a, e))\mid a\in K\}$ є підкільцем кільця S, де e — одиниця кільця K, причому K' ізоморфне K.

10.4. Довести, що:

а) будь-яке підполе S_1 поля S, яке містить ненульове підкільце K, містить також всі дроби $\frac{a}{b}$, де $a \in K$, $b \in K$, $b \neq 0$. Точніше кажучи, всі елементи x з S такі, що $x = \frac{a}{b}$;

б) підмножина P поля S, яка складається з елементів виду $x = \frac{a}{b}$, де a, $b \in K$, $b \neq 0$, є мінімальним підполем, що містить K, якщо K — ненульове підкільце поля S;

в) якщо K — підкільце поля S, то найменше підполе в S, яке містить K, складається з дробів $\frac{a}{b}$, $a \in K$, $b \in K$, $b \neq 0$. Дроби $\frac{a}{b}$ і $\frac{c}{d}$ рівні тоді і тільки тоді, коли $ad = bc$;

г) будь-яка область цілісності K є підкільцем деякого поля S;

д) поле часток кільця цілих чисел Z є полем раціональних чисел Q;

е) поле часток кільця цілих гауссових чисел $Z[i]$ є полем раціональних комплексних чисел $Q[i]$;

є) множина $P = \left\{ \frac{ke}{ne} \,\middle|\, k,\ n \in \mathbf{Z} \right\}$ є мінімальним підполем поля R, якщо e — одиниця поля R;

ж) існує єдиний ізоморфізм поля P на поле P', який продовжує ізоморфізм φ, якщо P і P' — поля часток відповідно областей цілісності K і K' і φ — ізоморфізм K на K'.

з) поле часток S довільного поля P з точністю до ізоморфізму є цим самим полем P;

10.5. Нехай K — область цілісності. Довести, що:

а) $a \in \langle d \rangle$, $b \in \langle d \rangle$, якщо $\langle a, b \rangle = \langle d \rangle$;

б) $d \mid (a, b)$, якщо $\langle a, b \rangle = \langle d \rangle$;

в) існують такі $x, y \in K$, що $ax + by = d$, якщо $\langle a, b \rangle = \langle d \rangle$;

г) $d : c$, якщо $a : c$, $b : c$ і $\langle a, b \rangle = \langle d \rangle$;

д) $d \sim (a, b)$, якщо $\langle a, b \rangle = \langle d \rangle$ (знак «$\sim$» означає асоційованість);

е) ненульовий елемент a кільця K, який не є дільником одиниці і не розкладається на прості множники, має хоч один власний дільник, який теж не розкладається на прості множники;

є) якщо виконується п. е), то існує така нескінченна послідовність елементів кільця K : $a, a_1, a_2, \ldots, a_n, \ldots$, в якій кожен наступний елемент є власним дільником попереднього; при цьому $\langle a \rangle \subset \langle a_1 \rangle \subset \langle a_2 \rangle \subset \ldots \subset \langle a_n \rangle \subset \ldots$, тобто в K існує нескінченна послідовність ідеалів, в якій кожен наступний ідеал строго містить попередній;

ж) $(a, b) \sim nd$, якщо $(a, b) \sim d$ і n — дільник одиниці;

з) $c \sim d$, якщо $(a, b) \sim d$, $(a, b) \sim c$;

к) K — факторіальне кільце, якщо в K кожен ненульовий елемент, який не є дільником одиниці, розкладається в добуток простих множників і для будь-якого простого елемента $p \in K$ виконується умова: якщо $ab : p$, то $a : p$ або $b : p$.

10.6. Нехай K — кільце головних ідеалів. Довести, що:

а) кожні два елементи a, b, $b \neq 0$, мають (a, b);

б) $(a, p) \sim 1$ або p, якщо p — простий елемент;

в) якщо $a_1 a_2 \ldots a_n : p$, то хоча б один з елементів a_i ділиться на p, коли p — простий елемент;

г) якщо $\langle a_1 \rangle \subset \langle a_2 \rangle \subset \langle a_3 \rangle \subset \ldots \subset \langle a_n \rangle \subset \ldots$, то при деякому a_n $\bigcup_{i=1}^{\infty} \langle a_i \rangle = \langle a_n \rangle$;

д) в K не існує жодної послідовності ідеалів, в якій кожен наступний ідеал строго містить попередній;

е) в K кожен ненульовий елемент, який не є дільником одиниці, розкладається в добуток простих множників;

є) $d \sim (a, b)$ тоді і тільки тоді, коли $\langle d \rangle = \langle a \rangle + \langle b \rangle$, $a \neq 0$, $b \neq 0$;

ж) $k \sim [a, b]$ тоді і тільки тоді, коли $\langle k \rangle = \langle a \rangle \cap \langle b \rangle$, $a \neq 0$, $b \neq 0$;

з) K — факторіальне кільце.

10.7. Нехай K — евклідове кільце. Довести, що:

а) якщо $a \sim b$, то $\mathrm{Nr}(a) = \mathrm{Nr}(b)$;

б) якщо $a : b$ і $\mathrm{Nr}(a) = \mathrm{Nr}(b)$, то $a \sim b$;

в) $\mathrm{Nr}(a) = \mathrm{Nr}(1)$ тоді і тільки тоді, коли $1 \sim a$;

г) якщо $a \neq 0$ і a не ~ 1, то $\mathrm{Nr}(a) > \mathrm{Nr}(1)$;

д) $\mathrm{Nr}(b) < \mathrm{Nr}(a)$, якщо b — власний дільник a;

е) у будь-якому ненульовому ідеалі I кільця K існує такий ненульовий елемент r, що $\mathrm{Nr}(r) \leqslant \mathrm{Nr}(c)$ для будь-якого ненульового елемента $c \in I$; при цьому $I = \langle m \rangle$;

є) K — кільце головних ідеалів;

ж) K — факторіальне кільце.

10.8. Нехай K — факторіальне кільце. Довести, що:

а) $a : d$ тоді і тільки тоді, коли $d \sim p_1^{k_1} p_2^{k_2} \ldots p_s^{k_s}$, якщо $a \sim p_1^{n_1} p_2^{n_2} \ldots p_s^{n_s}$, $0 \leqslant k_i \leqslant n_i$, $i = 1, 2, \ldots, s$;

б) $[a, b] \sim p_1^{\gamma_1} p_2^{\gamma_2} \ldots p_s^{\gamma_s}$, де $\gamma_i = \max\{\alpha_i, \beta_i\}$; $(a, b) \sim p_1^{\delta_1} p_2^{\delta_2} \ldots p_s^{\delta_s}$, де $\delta_i = \min\{\alpha_i, \beta_i\}$, $i = 1, 2, \ldots, s$, якщо $a \sim p_1^{\alpha_1} p_2^{\alpha_2} \ldots p_s^{\alpha_s}$, $b \sim p_1^{\beta_1} p_2^{\beta_2} \ldots p_s^{\beta_s}$, p_i, p_j — попарно різні прості елементи, $i, j = 1, 2, \ldots, s$, $i \neq j$;

в) $(a, b_1 b_2 \ldots b_s) \sim 1$, якщо $(a, b_1) \sim \ldots \sim (a, b_s) \sim 1$;

г) $c : a_1 a_2 \ldots a_s$, якщо $c : a_i$ і $(a_i, a_j) \sim 1$, $i, j = 1, 2, \ldots, s$, $i \neq j$;

д) $c : a$, якщо $(a, b) \sim 1$ і $bc : a$;

е) $(a, p) \sim 1$ або p, якщо p — простий елемент;

є) якщо $a_1 a_2 \ldots a_s : p$, то хоча б один з елементів a_i ділиться на p, коли p — простий елемент;

ж) $(ka, kb) \sim kd$, якщо $k \neq 0$ і $(a, b) \sim d$;

з) $\left(\frac{a}{d}, \frac{b}{d}\right) \sim 1$, якщо $(a, b) \sim d$;

к) якщо $(a, b) \sim d$, $a : c$ і $b : c$, то $\frac{d}{e} \sim \left(\frac{a}{c}, \frac{b}{c}\right)$;

л) $[a, b] \sim ab$, якщо $(a, b) \sim 1$ і a, b — ненульові елементи;

м) $k[a, b] \sim [ka, kb]$, $\frac{ab}{d} \sim [a, b]$, якщо a, b, k — ненульові елементи;

н) існують такі елементи x, $y \in K$, що $a \sim x^n$, $b \sim y^n$, якщо $(a, b) \sim 1$; $ab = c^n$;

о) $[a, (b, c)] \sim ([a, b], [a, c])$.

10.9. Нехай $Z[i]$ — кільце цілих гауссових чисел. Довести, що:

а) для кожного $a \in Q[i]$ існує таке $z \in Z[i]$, що $|a - z|^2 \leqslant \frac{1}{2}$;

б) для будь-яких z, $t \in Z[i]$ існує таке $u \in Z[i]$, що $|z - tu|^2 < |t|^2$;

в) $Z[i]$ — евклідове кільце з нормою $\mathrm{Nr}(z) = |z|^2$, $z \in Z[i]$.

10.10. Нехай $K = \left\{ \frac{a + bi\sqrt{3}}{2} \mid a, b \in \mathbf{Z}, a, b \text{ однакової парності} \right\}$. Довести, що:

а) для кожного $a \in Q[i]$ існує таке $z \in K$, що $|a - z|^2 \leqslant \frac{3}{4}$;

б) для будь-яких z, $t \in K$ існує таке $u \in K$, що $|z - tu|^2 < |t|^2$;

в) K — евклідове кільце з нормою $\mathrm{Nr}(z) = |z|^2$, $z \in K$.

10.11. Довести, що наступні кільця є кільцями головних ідеалів:

а) кільце всіх раціональних чисел $\frac{m}{n}$ з непарним натуральним знаменником n і цілим чисельником m;

б) довільне поле P;

в) кільце $Z[\sqrt{19}i]$.

10.12. Довести, що дані кільця є евклідовими:

а) кільце $Z[\sqrt{2}]$ з нормою $\mathrm{Nr}(a + b\sqrt{2}) = |a^2 - 2b^2|$, $a, b \in \mathbf{Z}$.

б) кільце $Z[\sqrt{3}]$ з нормою $\mathrm{Nr}[a + b\sqrt{3}] = |a^2 - 3b^2|$, $a, b \in Z$.

10.13. Довести, що в довільному кільці K:

а) $I = \bigcup_{k=1}^{\infty} I_k$ є ідеал кільця K, якщо $I_1 \subseteq I_2 \subseteq \ldots \subseteq I_k \subseteq \ldots$ є послідовність зростаючих ідеалів кільця K;

б) $a = bc$ тоді і тільки тоді, коли в кільці K $<a> \subseteq <b>$;

в) $a \sim b$ тоді і тільки тоді, коли $<a> = <b>$, K — кільце з одиницею;

г) a не $\sim b$ тоді і тільки тоді, коли $<a> \neq <b>$, а K — кільце з одиницею.

10.14. Знайти породжуючі елементи даних ідеалів кільця цілих чисел $\mathbf{Z}$:

а) $<4, 6, 8> + <10, 15, 20>$;

б) $<4, 6, 8> \cap <10, 15, 20>$;

в) $<3, 6, 9> + <15, 30, 45>$;

г) $<3, 6, 9> \cap <15, 30, 45>$;

д) $<m, n, s> + <k, t, f>$, $k, m, n, s, t, f \in \mathbf{Z}$;

е) $<m, n, s> \cap <k, t, f>$, $k, m, n, s, t, f \in \mathbf{Z}$.

10.15. Знайти найбільший спільний дільник і найменше спільне кратне таких цілих гауссових чисел:

а) $4 + 3i$ та $3 + i$;

б) $6 + i$ та $5 + 7i$;

в) $8 + 12i$ та $10 + 4i$;

г) $5 - 5i$ та $7 - i$;

д) $11 - 3i$ та $3 + 7i$;

е) $5 + 6i$ та $6 + 5i$;

є) $7 + 3i$ та $5 + 2i$.

10.16. Знайти найбільший спільний дільник даних елементів кільця $Z[\sqrt{2}]$:

а) $7 + \sqrt{2}$ і $-5 - 5\sqrt{2}$;

б) $5 + 2\sqrt{2}$ і $6 - \sqrt{2}$.

10.17. Знайти лінійне зображення найбільшого спільного дільника $d = ax + by$, де числа a, b задано в задачах 10.15 і 10.16.

10.18. Довести, що:

а) ціле гауссове число є простим, якщо його норма є простим натуральним числом;

б) будь-яке просте ціле гауссове число є дільником одного і тільки одного простого натурального числа;

в) норма простого цілого гауссового числа є або простим натуральним числом, або квадратом простого натурального числа;

г) просте натуральне число тоді і тільки тоді є нормою цілого гауссового числа, коли воно дорівнює сумі квадратів двох натуральних чисел;

д) усі прості натуральні числа виду $p = 4n + 3$, $n = 0, 1, 2, \ldots$ є простими цілими гауссовими числами.

10.19. Нехай K — множина дійсних чисел виду $a_1 \cdot 2^{x_1} + a_2 \cdot 2^{x_2} + \ldots + a_n \cdot 2^{x_n}$, де n — довільне натуральне число, $a_1, a_2, \ldots, a_n$ — будь-які цілі числа, $x_1, x_2, \ldots, x_n$ — будь-які числа виду $2^{\frac{m}{k}}$, де m, k — цілі невід'ємні числа, $k \neq 0$. Довести, що K є область цілісності, в якій порушується існування розкладу на прості множники (як приклад взяти число 2).

10.20. Довести, що наступні кільця є прикладом кілець з порушенням однозначності розкладу на прості множники: а) $Z[\sqrt{3}i]$; б) $Z[\sqrt{5}i]$; в) $Z[\sqrt{17}i]$; г) $Z[\sqrt{19}i]$.

10.21. Довести, що в кільці $Z[\sqrt{3}i]$ простими є такі елементи: а) 2; б) -2; в) $1 + \sqrt{3}i$; г) $1 - \sqrt{3}i$.

10.22. Довести, що в кільці $Z[i]$ простими є такі елементи: а) 3; б) -3; в) 7; г) -7; д) $2 + i$; е) $2 - i$; є) $3 + 2i$; ж) $3 - 2i$; з) $4 + 5i$; к) $4 - 5i$.

10.23. Довести, що прості натуральні числа 2, 5, 11, 13 не є простими цілими гауссовими числами.

10.24. Знайти канонічний розклад цілих гауссових чисел:

а) 5; б) $5 - 5i$; в) $3 + i$; г) $-90 + 180i$;

д) $-182 - 126i$; е) $7 + 8i$; є) 41.

Розділ III. ТЕОРІЯ КОНГРУЕНЦІЙ З АРИФМЕТИЧНИМИ ЗАСТОСУВАННЯМИ

§ 11. Конгруенції в кільці цілих чисел та їхні найпростіші властивості

Література

[1] — § 15, с. 162—167;
[2] — § 15, с. 166—169;
[3] — гл. 12, § 1, с. 397—399;
[10] — гл. III, § 1—3, с. 41—44;
[11] — гл. 7, с. 72—77;
[12] — гл. II, § 1, с. 36—43;
[14] — § 15, с. 66—71.

ТЕОРЕТИЧНІ ВІДОМОСТІ

Серед багатьох означень конгруентності двох цілих чисел a і b за модулем m розглянемо три.

Означення 1. *Цілі числа a і b називають конгруентними за модулем m, де m — ціле число, якщо їхня різниця $a - b$ ділиться на m.* Позначення:

$$a \equiv b \pmod m.$$

Якщо a і b не конгруентні за модулем m, то пишуть

$$a \not\equiv b \pmod m.$$

Означення 2. *Цілі числа a і b називають конгруентними за модулем m, де $m \in Z$, якщо вони при діленні на m дають однакові остачі.*

Означення 3. *Цілі числа a і b називають конгруентними за модулем m, де $m \in Z$, якщо існує таке ціле число q, що $a = b + mq$.*

Означення 1, 2, 3 рівносильні.

Основні властивості конгруенцій

1°. Відношення конгруентності за даним модулем є бінарне відношення еквівалентності на множині цілих чисел. Класи еквівалентності називають **класами лишків за даним модулем;**

2°. Конгруенції за одним модулем можна почленно додавати, віднімати і множити;

3°. До обох частин конгруенції можна додати будь-яке ціле число (це дає змогу переносити будь-який доданок з однієї сторони в другу з протилежним знаком);

4°. До будь-якої частини конгруенції можна додати довільне ціле число, кратне модулю;

5°. Обидві частини конгруенції можна помножити на те саме ціле число;

6°. Обидві частини конгруенції можно поділити на їхній спільний дільник, якщо він взаємно простий з модулем;

7°. Якщо у виразі

$$f(a_1, a_2, \ldots, a_k) = \sum A a_1^{n_1} a_2^{n_2} \ldots a_k^{n_k}$$

усі коефіцієнти A і числа $a_1, a_2, \ldots, a_k$ замінити на конгруентні їм за модулем m коефіцієнти B і числа $b_1, b_2, \ldots, b_k$ відповідно, то вираз

$$g(b_1, b_2, \ldots, b_k) = \sum B b_1^{n_1} b_2^{n_2} \ldots b_k^{n_k}$$

буде конгруентний заданому за модулем m:

$$f(a_1, a_2, \ldots, a_k) \equiv g(b_1, b_2, \ldots, b_k) \pmod m$$

8°. Обидві частини конгруенції і модуль можна множити на те саме ціле число.

9°. Обидві частини конгруенції і модуль можна скорочувати на їхній спільний дільник.

10°. Якщо конгруенція має місце за кількома модулями, то вона має місце і за модулем, який дорівнює спільному найменшому кратному цих модулів.

11°. Якщо конгруенція має місце за модулем m, то вона має місце за модулем d, де d — довільний дільник числа m.

12°. Якщо одна частина конгруенції і модуль діляться на деяке число, то й друга частина конгруенції ділиться на те саме число.

13°. Якщо $a \equiv b \pmod m$, то $(a, m) = (b, m)$.

ПРИКЛАДИ РОЗВ'ЯЗУВАННЯ ЗАДАЧ

1. Чи конгруентні числа 78, 210 і 346 з числом 27 за модулем 11?
Розв'язання. Віднімемо від даних чисел число 27. Дістанемо 51, 183 і 319. З них тільки 319 ділиться на 11, а тому тільки 346 конгруентне 27 за модулем 11, тобто $346 \equiv 27 \pmod{11}$.

2. Довести, що коли $100a + 10b + c \equiv 0 \pmod{21}$, то $a - 2b + 4c \equiv 0 \pmod{21}$, $a, b, c \in Z$.
Розв'язання. Нехай $100a + 10b + c \equiv 0 \pmod{21}$. Помноживши обидві частини цієї конгруенції на 4, матимемо

$$400a + 40b + 4c \equiv 0 \pmod{21}. \tag{1}$$

При цьому мають місце конгруенції:

$$400a \equiv a \pmod{21}, \quad \text{бо} \quad 400a - a = 399a \vdots 21, \tag{2}$$

$$40b \equiv -2b \pmod{21}, \quad \text{бо} \quad 40b - (-2b) = 42b \vdots 21, \tag{3}$$

$$4c \equiv 4c \pmod{21}, \quad \text{бо} \quad 4c - 4c = 0 \vdots 21. \tag{4}$$

Додавши почленно ці конгруенції, дістанемо

$$400a + 40b + 4c \equiv a - 2b + 4c \pmod{21}. \tag{5}$$

Беручи до уваги конгруенцію (1), матимемо

$$a - 2b + 4c \equiv 0 \pmod{21}.$$

3. Знайти остачу від ділення $1532^5 - 1$ на 9.
Розв'язання. Зрозуміло, що нераціонально знаходити число $1532^5 - 1$, а потім остачу від ділення цього числа на 9. Слід скористатися властивостями конгруенцій за модулем 9. Нам треба знайти таке ціле невід'ємне число x, що $x \equiv 1532^5 - 1 \pmod 9$ і $x < 9$. Оскільки $1530 \vdots 9$, то $1532^5 \equiv (1532 - 1530)^5 \pmod 9$, тобто $1532^5 \equiv 2^5 \pmod 9$. Проте $2^5 = 32 \equiv 5 \pmod 9$. Отже, $1532^5 \equiv 5 \pmod 9$. Віднімемо почленно від цієї конгруенції конгруенцію $1 \equiv 1 \pmod 9$. Матимемо $1532^5 - 1 \equiv 4 \pmod 9$. Оскільки $0 < 4 < 9$, то $x = 4$. Отже, число $1532^5 - 1$ при діленні на 9 дає остачу 4.

4. Довести, що числа виду $3^{2^{4n+1}} + 2$, $n \in N$ є складеними.
Розв'язання. Оскільки $4 \equiv -1 \pmod 5$, то $2^{4n+1} = 2 \cdot 4^{2n} \equiv 2 \pmod 5$. Тоді число 2^{4n+1} має вид $5k + 2$, де $k \in N$, а тому $3^{2^{4n+1}} + 2 = 3^{5k+2} + 2$. Оскільки $243 \equiv 1 \pmod{11}$, а $3^5 \equiv 323$, то $3^{5k+2} + 2 = 9 \cdot 243^k + 2 \equiv 0 \pmod{11}$. Отже, $3^{2^{4n+1}} + 2 \vdots 11$. Беручи до уваги нерівність $3^{2^{4n+1}} + 2 > 11$, маємо, що $3^{2^{4n+1}} + 2$ є складене число.

Задачі

11.1. Серед чисел $a_1, a_2, \ldots, a_n$ знайти всі пари різних чисел, конгруентних за модулем m, якщо:

а) $a_1 = 216$, $a_2 = 134$, $a_3 = 214$, $a_4 = 303$, $a_5 = 21$, $m = 5$;

б) $a_1 = 135$, $a_2 = 106$, $a_3 = 181$, $a_4 = 225$, $a_5 = 167$, $a_6 = 452$, $m = 15$;

в) $a_1 = 217$, $a_2 = 42$, $a_3 = 182$, $a_4 = 241$, $m = 12$.

11.2. Які з чисел a, b, c конгруентні числу d за модулем m, якщо:

а) $a = 137$, $b = 343$, $c = 633$, $d = 13$, $m = 31$;

б) $a = 217$, $b = 201$, $c = 186$, $d = 11$, $m = 19$;

в) $a = 234$, $b = 634$, $c = 104$, $d = 9$, $m = 25$.

11.3. Довести, що:

а) означення 1—3 еквівалентні між собою;

б) властивості 1—13 справедливі;

в) якщо у многочлені з цілими коефіцієнтами $f(x) = a_n x^n + a_{n-1}x^{n-1} + \ldots + a_1 x + a_0$, який задано на множині цілих чисел $\mathbf{Z}$, усі коефіцієнти a_i замінити на коефіцієнти b_i, конгруентні a_i за модулем m, то дістанемо многочлен $g(x) = b_n x^n + b_{n-1}x^{n-1} + \ldots + b_1 x + b_0$, конгруентний многочлену $f(x)$, тобто $f(x) = g(x) \pmod m$;

г) якщо $f(x) = a_n x^n + a_{n-1}x^{n-1} + \ldots + a_1 x + a_0$ — многочлен від одного аргументу x з цілими коефіцієнтами і $x \equiv x' \pmod m$, то $f(x) \equiv f(x') \pmod m$;

д) $n^2 - 1 \equiv 0 \pmod 8$, якщо n — непарне число;

е) $a \equiv r \pmod m$, де r — остача від ділення a на m.

є) $a \equiv b \left(\mathrm{mod}\ \frac{m}{(x, m)}\right)$, якщо $ax \equiv bx \pmod m$;

ж) якщо $ac \equiv bd \pmod m$, $a \equiv b \pmod m$ і $(a, m) = 1$, то $c \equiv d \pmod m$.

11.4. Записати у вигляді конгруенцій такі умови:

а) -38 і -3 дають при діленні на 7 однакові остачі;

б) при діленні на 8 число 53 дає остачу 5;

в) $a+2$ ділиться на 5;

г) $a^2 - b^2$ ділиться на $a - b$ $(a \neq b)$;

д) знайти остачу r від ділення -73 на 8;

е) 20 є остача від ділення числа 389 на 41;

є) числа 219 і 129 дають неоднакові остачі при діленні на 7.

11.5. Охарактеризувати конгруенціями числа n, якщо:

а) n — парне число;

б) n — непарне число;

в) n має вид $4k + 1$, $k \in \mathbf{Z}$;

г) n має вид $5k + 3$, $k \in \mathbf{Z}$;

д) n має вид $7k - 2$, $k \in \mathbf{Z}$;

е) n має вид $-3 + 8k$, $k \in \mathbf{Z}$.

11.6. Довести, що:

а) $121 \equiv 13\,145 \pmod 2$;

б) $121347 \equiv 92\,817 \pmod{10}$;

в) $31 \equiv -9 \pmod{10}$;

г) $(m-1)^2 \equiv 1 \pmod m$;

д) $2m + 1 \equiv (m+1)^2 \pmod m$;

е) $26^{30} - 1 \equiv 0 \pmod{5 \cdot 7 \cdot 11 \cdot 31}$;

є) $26^{15} + 1 \equiv 0 \pmod{3 \cdot 7 \cdot 31}$;

ж) $26^{26} \equiv 14^{14} \pmod{10}$;

з) $17^{72} \equiv 1 \pmod{10}$;

к) $2^{11 \cdot 31} \equiv 2 \pmod{11 \cdot 31}$;

л) $3^{14} \equiv -1 \pmod{29}$;

м) $11 \cdot 13 \cdot 18 \cdot 19 \cdot 2322 \equiv 6 \pmod 7$.

11.7. Довести, що:

а) $5^{1812} \not\equiv 1964 \pmod{25}$;

б) $7^{103} \not\equiv 3 \pmod{27}$;

в) $4^{1965} \not\equiv 25 \pmod{10}$;

г) $30 \cdot 17 \not\equiv 81 \cdot 19 \pmod 6$;

д) $11^{207} \not\equiv 6 \pmod{27}$;

е) $6^{89} \not\equiv 7 \pmod{16}$;

є) $13^{25} \not\equiv 5 \pmod{30}$;

ж) $7^{101} \not\equiv 3 \pmod{35}$;

з) $8^{107} \not\equiv 7 \pmod{14}$;

к) $26^{15} - 1 \not\equiv 0 \pmod{5 \cdot 7}$;

л) $7^{100} \not\equiv 3 \pmod{125}$;

м) $(2n+1)(2m+1) \not\equiv 2k \pmod 6$, $n, m, k \in \mathbf{Z}$.

11.8. Нехай p — просте число. Довести, що:

а) $(a+b)^p \equiv a^p + b^p \pmod p$, $a, b \in \mathbf{Z}$;

б) $C_{p-1}^k \equiv (-1)^k \pmod p$;

в) $C_{p-2}^k \equiv (-1)^k (k+1) \pmod p$;

г) $a^p \equiv b^p \pmod{p^{n+1}}$, якщо $a \equiv b \pmod{p^n}$;

д) $1^{2k+1} + 2^{2k+1} + 3^{2k+1} + \ldots + (p-1)^{2k+1} \equiv 0 \pmod p$, де $p > 2$;

е) $p^{p+2} + (p+2)^p \equiv 0 \pmod{2p+2}$, якщо $p > 2$;

є) числа $-\frac{p-1}{2}, -\frac{p-3}{2}, \ldots, -1, 0, 1, \ldots, \frac{p-3}{2}, \frac{p-1}{2}$ попарно неконгруентні між собою за модулем p, $p > 2$.

11.9. Знайти остачу від ділення:

а) 15^{231} на 14;

б) $15^{231} + 2$ на 16;

в) $1532^5 - 1$ на 9;

г) $12^{1231} + 14^{4324}$ на 13;

д) 208^{208} на 23;

е) $2^{15783} - 7$ на 25;

є) $3^{79821} + 5$ на 17;

ж) $10^{2732} + 10$ на 22;

з) $18^{2815} - 3$ на 14;

к) $2^{100} + 5^{200}$ на 29;

л) $13^{1054} - 23 \cdot 16^{285} + 22^{17}$ на 15;

м) $29^{2929} - 34^{3434} + 29 \cdot 41 \cdot 6^{231} - 24 \cdot 17^{120}$ на 31;

н) a на 73, якщо $a^{100} \equiv 2 \pmod{73}$ і $a^{101} \equiv 69 \pmod{73}$. Як зміниться відповідь, якщо a ділити на 79 і $a^{25} \equiv 3 \pmod{79}$, $a^{26} \equiv 29 \pmod{79}$, $(a, 79) = 1$?

11.10. Довести, що:

а) $a-b-c \vdots 2$, якщо $a+b-c \vdots 2$;
б) $18a+5b \vdots 19$, якщо $11a+2b \vdots 19$;
в) $2a+7b \vdots 17$, якщо $a-5b \vdots 17$;
г) $4a+23b \vdots 16$, якщо $12a-7b \vdots 16$;
д) $10a+7b \vdots 19$, якщо $a-5b \vdots 19$;
е) $11a-b+2c \vdots 21$, якщо $16a-11b+c \vdots 21$;
є) $a-7b \vdots 31$, якщо $6a-11b \vdots 31$;
ж) $a+b+8c \vdots 21$, якщо $50a+8b+c \vdots 21$;
з) $5a+b \vdots 17$, якщо $15a+3b \vdots 17$;
к) $a-4b+41c \vdots 199$, якщо $50a-b+60c \vdots 388$.

11.11. Довести, що при будь-якому натуральному n:

а) $2^{3^n} \equiv -1 \pmod{3^{n+1}}$;
б) $10^n+17 \equiv 0 \pmod 3$;
в) $3^{4n+3} \equiv 17 \pmod{10}$;
г) $24^{2n+1} \cdot 21^{n+2} \equiv 3^{n+2} \cdot 17^{2n+1} \pmod{19}$;
д) $48^{3n+1}+16^{3n+1}+1 \equiv 0 \pmod{13}$;
е) $2^{3^{4n+1}}+3$ — складене число;
є) $(m-1)^{m^n} \equiv -1 \pmod{m^{n+1}}$, де $m>1$ — непарне число;
ж) $3^{n+4} \equiv -1 \pmod{10}$, якщо $3^n \equiv -1 \pmod{10}$;
з) $2^{5^n} \equiv 1 \pmod{31}$;
к) $3 \cdot 10^n+24 \equiv 0 \pmod{54}$.

11.12. Довести, що задані рівняння не мають розв'язків у натуральних числах:

а) $2^x+7^y=19^z$;
б) $2^x+5^y=19^z$;
в) $24^x+36^y=61^z$;
г) $20^x+50^y=71^z$.

11.13. Довести, що при будь-яких цілих a, b і невід'ємному n:

а) $(11a+5)^{2n+1}+(11b+6)^{2n+1} \equiv 0 \pmod{11}$;
б) $(13a+3)^{3n+2}+(13b-4)^{3n+2}+1 \equiv 0 \pmod{13}$;
в) $9^{3n+1}+3^{3n+1}+1 \equiv 0 \pmod{13}$.

11.14. Знайти такі натуральні k, l, m, щоб при будь-якому цілому a справджувалися такі конгруенції:

а) $a^{3k}+a^{3l+1}+a^{3m+2} \equiv 0 \pmod{a^2+a+1}$;
б) $a^{3k}-a^{3l+1}+a^{3m+2} \equiv 0 \pmod{a^2-a+1}$;
в) $a^{3k}+a^{3l+1}+a^{3m+2} \equiv 0 \pmod{a^4+a^2+1}$.

11.15. Знайти останню цифру чисел:

а) 2^{3^4};

б) 9^{9^9};

в) $\left(\ldots\left(\left((7^7)^7\right)^7\right)^{\cdots}\right)^7$ — піднесення до степеня повторюється 1000 раз;

г) $7^{7^{\ldots^{(7^{(7^7)})^{\cdots}}}}$ — піднесення до степеня повторюється 1000 раз.

11.16. Знайти останні дві цифри чисел:

а) 2^{999};
б) 3^{999};
в) 2^{341};
г) 289^{289};
д) 203^{203203};
е) $14^{14^{14}}$;
є) 9^{9^9};
ж) $7^{9^{9^9}}$.

11.17. Нехай $F_n=2^{2^n}+1$ — число Ферма, де $n=0, 1, 2, \ldots$. Довести, що:

а) $F_5 \vdots 641$[1];

б) число F_n закінчується цифрою 7 при всіх n, крім $n=0$ і $n=1$.

§ 12. Класи лишків, повна і зведена системи лишків за даним модулем

Література

[1] — § 15, с. 166—168, § 16, с. 168—170;
[2] — § 15, с. 169—171, § 16, с. 171—173;
[3] — гл. 12, § 2, 3, с. 399—404;
[10] — гл. III, § 4, 5, с. 45—46;
[11] — гл. 8, 9, с. 77—92;
[12] — гл. II, § 2, 3, с. 43—51;
[13] — § 16—18, с. 66—78.

ТЕОРЕТИЧНІ ВІДОМОСТІ

Відношення конгруентності за даним модулем m є бінарним відношенням еквівалентності на множині цілих чисел Z. Класи еквівалентностей називають **класами лишків за даним модулем. Лишком (або представником) класу за модулем** m називають будь-яке число цього класу. Кільце цілих чисел Z розкладається на m класів лишків. До класу лишків, який містить число a, належать усі цілі числа x виду $x=a+mt$, де $t \in Z$. Цей клас позначатимемо символом $K_a^{(m)}$, причому, якщо йдеться тільки про класи лишків за тим самим модулем m, то можна писати K_a. Число a називають **представником класу лишків** $K_a^{(m)}$.

Представником класу лишків $K_a^{(m)}$ може бути будь-який елемент цього класу, тобто $K_a^{(m)}=K_b^{(m)}$, якщо $b \in K_a^{(m)}$. Якщо $K_a^{(m)} \cap K_b^{(m)} \neq \varnothing$, то $K_a^{(m)}=K_b^{(m)}$. Якщо $d>1$, то $K_a^m=K_a^{(dm)} \cup K_{(a+m)}^{(dm)} \cup K_{a+2m}^{(dm)} \cup \ldots \cup K_{a+(d-1)m}^{(dm)}$;

$$K_a^{(m)}+K_b^{(m)}=K_{a+b}^{(m)}, \quad K_a^{(m)}K_b^{(m)}=K_{ab}^{(m)}.$$

Множина всіх класів лишків за модулем m відносно додавання класів утворює комутативну групу, її називають **групою класів лишків.**

Множина класів лишків кільця цілих чисел за даним модулем m утворює комутативне кільце з одиницею, його позначають Z_m.

Якщо m — складене число, то в Z_m є дільники нуля, причому, якщо $m=m_1m_2$, то зокрема,

$$K_{m_1}^{(m)}K_{m_2}^{(m)}=K_0^{(m)}, \text{ де } K_{m_1}^{(m)} \neq K_0^{(m)} \text{ і } K_{m_2}^{(m)} \neq K_0^{(m)}.$$

Якщо m — просте число, то Z_m — скінченне поле.

Повною системою лишків за модулем m називають будь-яку систему лишків, утворену з m чисел, взятих по одному з кожного класу лишків.

Існують такі основні повні системи лишків:

[1] Це було доведено ще Л. Ейлером (1707—1783).

а) повна система найменших невід'ємних лишків;
б) повна система найменших за абсолютною величиною лишків;
в) повна система найменших натуральних лишків.

Якщо $(a, m) = 1$, то клас $K_a^{(m)}$ називають **взаємно простим** з модулем m.

Зведеною системою лишків за модулем m називають будь-яку систему лишків, утворену з $\varphi(m)$ чисел, взятих по одному з кожного класу, взаємно простого з модулем m.

Якщо $(a, m) = 1$, b — довільне ціле число, а x пробігає повну систему лишків за модулем m, то й вираз $ax + b$ також пробігає деяку повну систему лишків за модулем m (не обов'язково ту саму).

Якщо $(a, m) = 1$, а x пробігає зведену систему лишків за модулем m, то лінійна форма ax також пробігає деяку зведену систему лишків за модулем m (не обов'язково ту саму).

Множина класів лишків за модулем m, взаємно простих з m, утворює відносно множення класів комутативну групу, її називають **мультиплікативною групою класів лишків, взаємно простих з модулем.**

ПРИКЛАДИ РОЗВ'ЯЗУВАННЯ ЗАДАЧ

1. Чи утворює повну систему лишків за модулем 8 система чисел

$$S = \{-7, 2, 16, 20, 27, 39, 46, -3\}?$$

Розв'язання. Щоб визначити, чи є деяка система чисел повною системою лишків за деяким модулем m, треба: 1) впевнитися, що цих чисел є m, 2) показати, що всі вони між собою попарно неконгруентні за модулем m. При цьому доцільно замінити кожне з даних чисел конгруентним йому найменшим невід'ємним числом (це неважко зробити, знайшовши остачу від ділення заданого числа на модуль).

У розглядуваному прикладі маємо: 1) чисел у системі є 8; 2) $-7 \equiv 1 \pmod 8$, $2 \equiv 2 \pmod 8$, $16 \equiv 0 \pmod 8$, $20 \equiv 4 \pmod 8$, $27 \equiv 3 \pmod 8$, $39 \equiv 7 \pmod 8$, $46 \equiv 6 \pmod 8$, $-3 \equiv 5 \pmod 8$. Дістали нову систему 1, 2, 0, 4, 3, 7, 6, 5, яка є повною системою лишків за модулем 8.

Зауваження. 1. Якщо модуль m є невелике число, можна знайти всі попарні різниці заданих чисел і довести їхню подільність на m. Якщо жодна з різниць не ділиться на m, то задана сукупність чисел є повною системою лишків за модулем m, у противному разі — не є нею.

2. Замінивши кожне число системи S його остачею від ділення на 8, визначимо, до якого класу $K_a^{(8)}$ належить кожне число із системи S, а саме — $-7 \in K_1^{(8)}$, $2 \in K_2^{(8)}$, $16 \in K_0^{(8)}$, $20 \in K_4^{(8)}$, $27 \in K_3^{(8)}$, $39 \in K_7^{(8)}$, $46 \in K_6^{(8)}$, $-3 \in K_5^{(8)}$.

Оскільки всі числа з S належать до різних класів за модулем 8 і всі класи мають представників у цій системі, то S — повна система лишків за модулем 8.

2. Показати, що коли x пробігає зведену систему лишків за модулем 10, то й x^3 пробігає зведену систему лишків за модулем 10.

Розв'язання. Відомо, що числа зведеної системи лишків взаємно прості з модулем. Взаємно простими з 10 є лише такі цілі числа, які закінчуються цифрами 1, 3, 7, 9. Четвірки S таких чисел попарно неконгруентні між собою за модулем 10, а оскільки $\varphi(10) = \varphi(2 \cdot 5) = 2 \cdot 5\left(1 - \frac{1}{2}\right)\left(1 - \frac{1}{5}\right) = 4$, то S — зведена система лишків за модулем 10. Нехай x пробігає довільну зведену систему лишків S за модулем 10. Якщо числа системи S, що закінчуються цифрами 1, 3, 7, 9, піднести до куба, то дістанемо систему S' чисел, які закінчуються цифрами 1, 7, 3, 9. Цю систему й пробігає x^3. Система S' утворює також зведену систему лишків за модулем 10, оскільки: а) чисел у системі є $4 = \varphi(10)$, б) усі числа системи S' попарно неконгруентні між собою за модулем 10; в) усі числа системи S' взаємно прості з числом 10.

3. У множині класів лишків за модулем 15 знайти:
а) усі дільники нуля;
б) усі дільники одиниці;

в) клас, протилежний класу $K_7^{(15)}$;
г) клас, обернений до класу $K_{11}^{(15)}$.

Розв'язання. а) Оскільки дільником нуля є кожен клас $K_a^{(15)}$, для якого знайдеться такий клас $K_x^{(15)}$, що $K_a^{(15)} K_x^{(15)} = K_0^{(15)}$, де $K_a^{(15)} \neq K_0^{(15)} \neq K_x^{(15)}$, тобто такий клас $K_x^{(15)}$, що $ax \vdots 15$, де $1 \leqslant a, x \leqslant 14$, то фактично дільниками нуля є всі ті класи $K_a^{(15)}$, в яких представник a не взаємно простий з 15. Отже, дільниками нуля є такі класи: $K_3^{(15)}$, $K_5^{(15)}$, $K_6^{(15)}$, $K_9^{(15)}$, $K_{10}^{(15)}$, $K_{12}^{(15)}$.

б) Аналогічні міркування для дільників одиниці показують, що дільниками одиниці є всі ті класи $K_a^{(15)}$, в яких представник a взаємно простий з 15. Справді, якщо $(a, 15) = 1$, то знайдуться такі цілі числа u і v, що $au + 15v = 1$. Тоді $K_{au+15v} = K_1$, проте $K_{au+15v} = K_{au} + K_{15v}$, а $K_{15v} = K_0$, $K_{au} = K_a \cdot K_u$. Отже, $K_a \cdot K_u = K_1$. Звідси, зокрема, $(K_a)^{-1} = K_u$, тобто ми вивели формулу для знаходження класу, оберненого до класу K_a, якщо $(a, 15) = 1$.

Випишемо дільники одиниці: $K_1^{(15)}$, $K_2^{(15)}$, $K_4^{(15)}$, $K_7^{(15)}$, $K_8^{(15)}$, $K_{11}^{(15)}$, $K_{13}^{(15)}$, $K_{14}^{(15)}$.

в) Знайдемо такий клас $K_x^{(15)}$, що $K_7^{(15)} + K_x^{(15)} = K_0^{(15)}$. Оскільки $K_7^{(15)} + K_x^{(15)} = K_{7+x}^{(15)}$, то шукатимемо таке ціле число x, що $7 + x \vdots 15$. Найменшим таким числом є 8. Отже, $x = 8$ і тому $-K_7^{(15)} = K_8^{(15)}$.

г) Знайдемо такий клас $K_u^{(15)}$, що $K_{11}^{(15)} \cdot K_u^{(15)} = K_1^{(15)}$. Оскільки $(11, 15) = 1$, то, згідно з пунктом б), цей клас можна знайти, знайшовши спочатку за допомогою алгоритму Евкліда число u. До чисел 11 і 15 застосуємо алгоритм Евкліда. Маємо:

$$\begin{aligned} 15 &= 11 \cdot 1 + 4, \\ 11 &= 4 \cdot 2 + 3, \\ 4 &= 3 \cdot 1 + 1. \end{aligned}$$

Звідси

$$\begin{aligned} 4 &= 15 - 11 \cdot 1, \\ 3 &= 11 - 4 \cdot 2, \\ 1 &= 4 - 3 \cdot 1. \end{aligned}$$

Тоді

$$\begin{aligned} 1 &= 4 - 3 \cdot 1 = 4 - (11 - 4 \cdot 2) \cdot 1 = 11 \cdot (-1) + 4 \cdot 3 = \\ &= 11 \cdot (-1) + (15 - 11 \cdot 1) \cdot 3 = 11 \cdot (-4) + 15 \cdot 3. \end{aligned}$$

Отже, $u = -4$, а $K_u^{(15)} = K_{-4}^{(15)}$.

Оскільки $K_{-4}^{(15)} = K_{11}^{(15)}$, то $\left(K_{11}^{(15)}\right)^{-1} = K_{11}^{(15)}$, тобто клас $K_{11}^{(15)}$ є оберненим до себе.

Зауваження

1. У подальшому, знайшовши дільники нуля (дільники одиниці), говоритимемо, що відмінні від дільників нуля і самого нуля елементи є дільниками одиниці (відмінні від дільників одиниці і від нуля елементи є дільниками нуля).

2. У пунктах а) і б), не обмежуючись тільки переліком дільників нуля та одиниці, можна виписати відповідні конкретні пари. У розглянутому прикладі такими парами відповідно є:

$$K_3^{(15)} \text{ і } K_5^{(15)}, \quad K_6^{(15)} \text{ і } K_5^{(15)} \text{ і т. д.},$$

$$K_2^{(15)} \text{ і } K_8^{(15)}, \quad K_4^{(15)} \text{ і } K_4^{(15)} \text{ і т. д.}$$

3. Клас $K_u^{(m)}$, обернений до класу $K_a^{(m)}$, можна іноді швидко знаходити усно, підбираючи таке число u, щоб добуток $a \cdot u$ при діленні на m давав остачу 1.

Так для класу $K_{11}^{(15)}$ класи $K_1^{(15)}$, $K_2^{(15)}$, $K_4^{(15)}$, $K_7^{(15)}$, $K_8^{(15)}$ не підійшли б, оскільки числа $1 \cdot 11 = 11$, $2 \cdot 11 = 22$, $4 \cdot 11 = 44$, $7 \cdot 11 = 77$, $8 \cdot 11 = 88$ при діленні на 15 дають остачу, відмінну від 1. При цьому, звичайно, дільники нуля $K_3^{(15)}$, $K_5^{(15)}$, $K_6^{(15)}$ $K_9^{(15)}$, $K_{10}^{(15)}$ не випробовуються, бо вони вже дільниками одиниці не можуть бути. Оскільки $11 \cdot 11 = 121$ і $121 = 15 \cdot 8 + 1$, то $\left(K_{11}^{(15)}\right)^{-1} = K_{11}^{(15)}$.

4. Для знаходження класу $\left(K_a^{(m)}\right)^{-1}$, оберненого до класу $K_a^{(m)}$, існує ще один спосіб. Нехай $(a, m) = 1$, у противному разі клас $K_a^{(m)}$ взагалі не має оберненого класу. Нехай P_{n-1} — чисельник передостаннього підхідного дробу $\frac{P_{n-1}}{Q_{n-1}}$ для числа $\frac{m}{a}$, $\frac{m}{a} = \frac{P_n}{Q_n}$. Оскільки $\frac{m}{a}$ — нескоротний дріб, то $m = P_n$, $a = Q_n$. За однією з властивостей підхідних дробів маємо

$$\frac{P_n}{Q_n} - \frac{P_{n-1}}{Q_{n-1}} = \frac{(-1)^{n-1}}{Q_{n-1} Q_n}.$$

Отже,

$$\frac{m}{a} - \frac{P_{n-1}}{Q_{n-1}} = \frac{(-1)^n}{Q_{n-1} \cdot Q_n}.$$

Звідси

$$Q_{n-1} \cdot m - aP_{n-1} = (-1)^{n-1}.$$

Тоді

$$a(-1)^n P_{n-1} \equiv 1 \pmod{m}.$$

Згідно з цією конгруенцією, клас $K_{(-1)^{n-1} P_{n-1}}^{(m)}$ є оберненим до класу $K_a^{(m)}$. Отже,

$$\left(K_a^{(m)}\right)^{-1} = K_{(-1)^n P_{n-1}}^{(m)}.$$

Для розглянутого прикладу маємо (табл. 12), де $m = 15$, $a = 11$, $n = 3$, $P_{n-1} = P_2 = 4$. Тоді

$$\left(K_{11}^{(15)}\right)^{-1} = K_{(-1)^3 \cdot 4}^{(15)} = K_{-4}^{(15)} = K_{11}^{(15)}.$$

Таблиця 12

i	-1	0	1	2	3
q_i	—	1	2	1	3
P_i	1	1	3	4	15
Q_i	0	1	2	3	11

Задачі

12.1. Замінити найменшим невід'ємним і найменшим за абсолютною величиною лишками такі числа:

а) 70 за модулем 32;
б) 327 за модулем 30;
в) 184 за модулем 16;
г) 333 за модулем 67;
д) 586 за модулем 13;
е) 799 за модулем 99;
є) 14 за модулем 15;
ж) 5353 за модулем 781;
з) —337 за модулем 56;
к) 337 за модулем — 56;
л) 1000 за модулем — 17;
м) 501 за модулем 503;
н) —700 за модулем — 51.

12.2 Знайти повну систему найменших невід'ємних лишків за модулем: а) 1; б) 2; в) 3; г) 4; д) 5; е) 6; є) 7; ж) 8; з) 9; к) 10; л) 12; м) 15; н) 20.

12.3. Знайти повну систему найменших за абсолютною величиною лишків за модулем: а) 1; б) 2; в) 3; г) 4; д) 5; е) 6; є) 7; ж) 8; з) 9; к) 10; л) 12; м) 15; н) 20.

12.4. Знайти повну систему найменших натуральних лишків за модулем: а) 1; б) 2; в) 3; г) 4; д) 5; е) 6; є) 7; ж) 8; з) 9; к) 10; л) 12; м) 15; н) 20.

12.5. Знайти повну систему найбільших недодатних лишків за модулем: а) 1; б) 2; в) 3; г) 4; д) 5; е) 6; є) 7; ж) 8; з) 9; к) 10; л) 12; м) 15; н) 20.

12.6. Знайти повну систему найбільших від'ємних лишків за модулем: а) 1; б) 2; в) 3; г) 4; д) 5; е) 6; є) 7; ж) 8; з) 9; к) 10; л) 12; м) 15; н) 20.

12.7. Знайти хоч одну довільну повну систему лишків, відмінну від знайдених у задачах 12.2—12.6, за модулем: а) 1; б) 2; в) 3; г) 4; д) 5; е) 6; є) 7; ж) 8; з) 9; к) 10; л) 12; м) 15; н) 20.

12.8. Знайти відповідні зведені системи лишків для задач 12.2—12.7.

12.9. Чи утворюють повну систему лишків за модулем m такі числа:

а) 25, —20, 16, 54, —21, 26, 37, —17, якщо $m = 8$;
б) 25, —9, —6, 420, —18, 30, 6, якщо $m = 7$;
в) —46, —45, 37, 32, —48, —40, якщо $m = 6$;
г) 43, 25, —23, 28, —50, —40, 31, якщо $m = 7$;
д) —261, —130, 170, 313, 973, 1000, 55, 1668, якщо $m = 8$;
е) 605, —189, 242, —311, 143, 40, —51, 194, якщо $m = 8$;
є) 809, 402, 1616, 220, 227, 439, 446, якщо $m = 8$;
ж) 921, 92, —18, 28, —109, 40, —22, —2, 15, якщо $m = 9$;
з) 134, 128, —19, 37, 28, —23, —32, 5, 41, —35, —33, якщо $m = 11$;
к) 39, 66, 30, 19, —11, 55, 31, 46, 25, 47, 50, 35, 101, якщо $m = 13$?

12.10. Чи утворюють зведену систему лишків за модулем m такі числа:

а) 19, —1, 25, —19, якщо $m = 8$;
б) 19, 95, 29, 49, —20, —64, 27, якщо $m = 9$;
в) 13, —13, 29, —29, якщо $m = 10$;
г) 19, 35, 25, —19, якщо $m = 12$;
д) —11, —55, —29, 35, якщо $m = 12$;
е) —181, 231, 413, —349, якщо $m = 12$?

12.11. Довести, що:

а) коли x пробігає повну систему лишків за модулем 11, то й $3x+2$ теж пробігає повну систему лишків за модулем 11;

б) коли x пробігає повну систему лишків за модулем 10, то й x^5 пробігає повну систему лишків за модулем 10;

в) система чисел 2, 4, ..., $2m$ становить повну систему лишків за модулем m, якщо m непарне;

г) члени арифметичної прогресії a, $a+d$, ..., $a+d(n-1)$ утворюють повну систему лишків за модулем n, якщо $(d, n)=1$;

д) коли $(a, b)=1$, x пробігає повну систему лишків за модулем b, y пробігає повну систему лишків за модулем a, а c — будь-яке число, то $ax+by+c$ пробігає повну систему лишків за модулем ab;

е) коли $m=a_1a_2\ldots a_s$, де всі a_i попарно взаємно прості, $m_i=\frac{m}{a_i}$, $i=1, 2, \ldots, s$, c — довільне ціле число, x_i пробігають відповідно повні системи лишків за модулем m_i, то $m_1x_1+m_2x_2+\ldots+m_sx_s+c$ пробігає повну систему лишків за модулем m;

є) система чисел $0, 2^1, 2^2, \ldots, 2^{10}$ утворює повну систему лишків за модулем 11;

ж) вираз $3x+7y$ пробігає повну систему лишків за модулем 21, якщо $x=0, 1, 2, 3, 4, 5, 6$, а $y=0, 1, 2$;

з) повну систему лишків за модулем $m_1m_2\ldots m_s$ пробігає вираз $x_1+m_1x_2+m_1m_2x_3+\ldots+m_1m_2\ldots m_{s-1}x_s$, якщо $m_1, m_2, \ldots, m_s$ — натуральні, попарно взаємно прості числа, а $x_1, x_2, \ldots, x_s$ пробігають повні системи лишків за модулем $m_1, m_2, \ldots, m$ відповідно.

12.12. Довести, що:

а) коли x пробігає зведену систему лишків за модулем 7, то й $10x$ пробігає зведену систему лишків за модулем 7;

б) коли x пробігає зведену систему лишків за модулем 9, то $7x^5$ теж пробігає зведену систему лишків за модулем 9;

в) числа $6m-1$ і $6m+1$ при кожному цілому m утворюють зведену систему лишків за модулем 6;

г) система чисел $\pm1, \pm2, \ldots, \pm\frac{p-3}{2}, \frac{p-1}{2}$ є зведеною системою лишків за непарним простим модулем p;

д) система чисел $3^1, 3^2, 3^3, 3^4, 3^5, 3^6$ утворює зведену систему лишків за модулем 7;

е) система чисел $5^1, 5^2, 5^3, 5^4, 5^5, 5^6$ утворює зведену систему лишків за модулем 7;

є) коли числа $ax_1, ax_2, \ldots, ax_{\varphi(m)}$ утворюють зведену систему лишків за модулем m, то відповідні числа $x_1, x_2, \ldots, x_{\varphi(m)}$ також утворюють зведену систему лишків за модулем m;

ж) якщо $(a, m)=1$, $b\equiv0 \pmod m$ і x пробігає зведену систему лишків за модулем m, то $ax+b$ також пробігає зведену систему лишків за модулем m;

з) якщо $(a, m)=d$ і x пробігає зведену систему лишків за модулем $\frac{m}{d}$, то й $\frac{a}{d}x$ також пробігає зведену систему лишків за модулем $\frac{m}{d}$;

к) $K_{a^{p-1}}^{(p)}=K_1^{(p)}$, де p — просте число, a не ділиться на p.

12.13. Об'єднанням яких класів лишків є класи лишків:

а) $K_1^{(6)}$, $K_3^{(6)}$, $K_5^{(6)}$ за модулем 48;

б) $K_1^{(13)}$, $K_3^{(13)}$, $K_5^{(13)}$, $K_7^{(13)}$ за модулем 52;

в) $K_2^{(10)}$, $K_3^{(10)}$, $K_5^{(10)}$, $K_9^{(10)}$ за модулем 30.

12.14. Знайти класи лишків, обернені до таких класів:

а) $K_2^{(3)}$; б) $K_3^{(4)}$; в) $K_3^{(5)}$; г) $K_5^{(7)}$;

д) $K_7^{(8)}$; е) $K_5^{(9)}$; є) $K_7^{(10)}$; ж) $K_5^{(11)}$;

з) $K_{57}^{(61)}$; к) $K_{196}^{(501)}$; л) $K_{190}^{(501)}$; м) $K_{233}^{(1498)}$; и) $K_{501}^{(1993)}$.

§ 13. Теореми Ейлера і Ферма

Література

[1] — § 16, с. 174—175;
[2] — § 16, с. 178—179;
[3] — гл. 12, § 3, с. 408—409;
[10] — гл. 3, § 6;
[11] — гл. 2, с. 96—106;
[12] — гл. II, § 5, с. 57—60;
[14] — § 19, с. 79—80.

ТЕОРЕТИЧНІ ВІДОМОСТІ

Теорема Ейлера. *Якщо* $m>1$ і $(a, m)=1$, то

$$a^{\varphi(m)}\equiv1 \pmod m.$$

Теорема Ферма (мала теорема Ферма). *Якщо число* p *просте і* $(a, p)=1$, *то* $a^{p-1}\equiv1 \pmod p$.

Наслідок. *Якщо* p *— просте число,* a *— будь-яке ціле число, то* $a^p\equiv a \pmod p$.

ПРИКЛАДИ РОЗВ'ЯЗУВАННЯ ЗАДАЧ

1. Знайти остачу від ділення: а) 223^{2123} на 52; б) 264^{1020} на 138.

Розв'язання. а) Якщо треба знайти остачу від ділення a^s на m, де $(s, m)=1$ і $s\geqslant\varphi(m)$, то s можна подати у вигляді (за теоремою про ділення остачею): $s=\varphi(m)q+r$, де $0\leqslant r<\varphi(m)$. Оскільки $a^{\varphi(m)}\equiv1 \pmod m$, то

$$a^s=a^{\varphi(m)q+r}=(a^{\varphi(m)})^q\cdot a^r\equiv a^r \pmod m,$$

де a^r може бути значно меншим, ніж a^s.
У цьому разі маємо

$$52=2^2\cdot13,\quad \varphi(52)=2^2\cdot13\left(1-\frac{1}{2}\right)\left(1-\frac{1}{13}\right)=24,$$

$$223=52\cdot4+15,\quad 2123=24\cdot88+11.$$

Тоді

$$223^{2123}=(52\cdot4+15)^{24\cdot88+11}\equiv15^{11}=15^9\cdot15^2=(15^3)^3\cdot225\equiv$$
$$\equiv(3375)^3\cdot17\equiv(-5)^3\cdot17\equiv(-125)\cdot17\equiv(-21)\cdot17=-357\equiv7 \pmod{52}.$$

Отже, 223^{2123} при діленні на 52 дає остачу 7.

б) Якщо $(a, m)\neq1$ і $(a^s, m)=d>1$, то знаходимо спочатку таке найменше k, що $a^k\,\vdots\,d$. Тоді $a^k=a_1d$, $m=m_1d$, де вже $(a, m_1)=1$. Позначимо через x остачу від ділення a^s на m. Тоді

$$x\equiv a^s=a^{s-k}\cdot a^k=a^{s-k}\cdot a_1d \pmod{m_1, d}.$$

Звідси $x = x_1 d$, де

$$x_1 \equiv a^{s-k} a_1 \pmod{m_1}.$$

Тепер x_1 знайдемо як добуток остач від ділення a^{s-k} і a_1 на m_1. Оскільки $(a,\ m_1) = 1$, то остачу від ділення a^{s-k} на m_1 можна знайти за теоремою Ейлера.

Маємо (264, 138) = 6. Якщо $x \equiv 264^{1020} \pmod{138}$, то $x = 6x_1$. Оскільки $264 \equiv 126 \pmod{138}$, то $264^{1020} \equiv 126^{1020} \pmod{138}$. Найменшим k таким, що $126^k \vdots 6$, є 1. Тоді $a_1 = 126 : 6 = 21$, $m_1 = 138 : 6 = 23$ і $x_1 \equiv 21 \cdot 126 \pmod{23}$. Оскільки $\varphi(23) = 22$ і $1019 = 22 \cdot 46 + 7$, то

$$x_1 \equiv 21 \cdot 11^{1019} \equiv 21 \cdot 11^{22 \cdot 46 + 7} = 21 \cdot (11^{22})^{46} \cdot 11^7 \equiv$$
$$\equiv 21 \cdot 11^7 \equiv (-2) \cdot 11 \cdot 11^6 = -22 \cdot 11^6 \equiv 11^6 = (121)^3 \equiv$$
$$\equiv 6^3 = 36 \cdot 6 \equiv (-10) \cdot 6 = -60 \equiv 9 \pmod{23}.$$

Тоді $x = 9 \cdot 6 = 54$. Отже, 264^{1020} при діленні на 138 дає остачу 54.

2. Знайти останні дві цифри числа 243^{402}.

Розв'язання. Досить знайти остачу від ділення 243^{402} на 100. Маємо

$$243^{402} \equiv 43^{402} \pmod{100}.$$

Оскільки (43, 100) = 1, а

$$\varphi(100) = 2^2 \cdot 5^2 \left(1 - \frac{1}{2}\right)\left(1 - \frac{1}{5}\right) = 40,$$

то $43^{40} \equiv 1 \pmod{100}$. Оскільки $402 = 40 \cdot 10 + 2$, то

$$43^{402} = 43^{40 \cdot 10 + 2} \equiv 43^2 = 1849 \equiv 49 \pmod{100}.$$

Отже, останніми двома цифрами числа 243^{402} є 4 і 9.

Зауваження. Щоб знайти k останніх цифр числа a, досить знайти остачу від ділення цього числа на 10^k.

3. Довести, що $13^{176} - 1 \vdots 89$.

Розв'язання. Оскільки $13^{176} - 1 = (13^{88})^2 - 1 = (13^{88} - 1)(13^{88} + 1)$, а 89 — просте число, то досить показати, що на 89 ділиться хоч один з множників $13^{88} - 1$ чи $13^{88} + 1$. Згідно з малою теоремою Ферма,

$$13^{88} \equiv 1 \pmod{89},$$

звідки $13^{88} - 1 \vdots 89$. Отже, $13^{176} - 1 \vdots 89$.

Задачі

13.1. Чи справджується теорема Ейлера для таких чисел:

а) $a = 2,\ m = 9$;
б) $a = 2,\ m = 15$;
в) $a = 3,\ m = 4$;
г) $a = 3,\ m = 9$;
д) $a = 3,\ m = 16$;
е) $a = 4,\ m = 9$;
є) $a = 5,\ m = 24$;
ж) $a = 2,\ m = 33$;
з) $a = 3,\ m = 24$?

13.2. Чи справджується мала теорема Ферма для таких чисел:

а) $a = 2,\ p = 3$;
б) $a = 2,\ p = 5$;
в) $a = 3,\ p = 2$;
г) $a = 10,\ p = 5$;
д) $a = 5,\ p = 2$;
е) $a = 5,\ p = 3$;
є) $a = 5,\ p = 7$;
ж) $a = 4,\ p = 3$;
з) $a = 4,\ p = 5$;
к) $a = 14,\ p = 7$?

13.3. Користуючись теоремою Ейлера, знайти остачу від ділення:

а) 7^{67} на 12;
б) 109^{345} на 14;
в) 197^{157} на 35;
г) 356^{273} на 39;
д) 383^{175} на 45;
е) 293^{275} на 48;
є) 439^{291} на 60;
ж) 527^{144} на 65;
з) 353^{160} на 75;
к) 485^{84} на 129.

13.4. Користуючись малою теоремою Ферма, знайти остачу від ділення:

а) 93^{253} на 7;
б) 5008^{10000} на 5, 7, 11, 13;
в) 42^{50} на 17;
г) 20^{59} на 17;
д) 2598^{33} на 17;
е) 230^{347} на 37;
є) 71^{50} на 67;
ж) 512^{402} на 101.

13.5. Знайти остачу від ділення:

а) 45^{83} на 24;
б) 6^{76} на 26;
в) 96^{113} на 92;
г) 204^{41} на 111;
д) 460^{150} на 425.

13.6. Знайти остачу від ділення:

а) $7^{100} + 8^{100}$ на 5;
б) $10^{100} + 40^{100}$ на 7;
в) $3^{100} + 4^{100}$ на 7;
г) $5^{50} + 25^{70}$ на 9;
д) $25^{80} + 40^{80}$ на 11;
е) $15^{60} + 20^{30}$ на 13;
є) $5^{70} + 7^{50}$ на 12;
ж) $3^{500} + 7^{500}$ на 101;
з) $(12\,371^{56} + 145)^{28}$ на 111;
к) $3 \cdot 5^{75} + 4 \cdot 7^{100}$ на 132.

13.7. Знайти дві останні цифри числа:

а) 3^{100};
б) 3^{219};
в) 11^{243};
г) 13^{219};
д) 17^{900};
е) 19^{882};
є) 903^{1294};
ж) 573^{1931};
з) 2^{100};
к) 2^{153};
л) 102^{54}.

13.8. Розв'язати ті з задач 11.9 і 11.16, до яких можна застосувати теореми Ейлера і Ферма.

13.9. Довести, що:

а) $2^{11 \cdot 31} \equiv 2 \pmod{11 \cdot 31}$;
б) $2^{19(73-1)} \equiv 1 \pmod{19 \cdot 73}$;
в) $5^{17 \cdot 19} \equiv 23 \pmod{17 \cdot 19}$;
г) $2^{1093 \cdot 1092} \equiv 1 \pmod{1093^2}$;
д) $2^{73 \cdot 37 - 1} \equiv 1 \pmod{73 \cdot 37}$.

13.10. Довести, що:

а) $a^7 - a \vdots 42$;
б) $a^{11} - a \vdots 66$;
в) $a^{21} - a^3 \vdots 27$;
г) $a^{42} - a^2 \vdots 100$;
д) $a^{103} - a^3 \vdots 125$;
е) $a^{12} - b^{12} \vdots 65$, якщо $(a,\ 65) = (b,\ 65) = 1$;
є) $a^{13} - a \vdots 2730$;
ж) $a^{560} - 1 \vdots 561$, $(a,\ 561) = 1$;
з) $a^{561} - a \vdots 11$;

к) $a^{10} - a^6 - a^4 + 1 \vdots 35$, $(a, 35) = 1$.

13.11. Нехай p — просте число. Довести, що:

а) $a^p \equiv b^p \pmod{p^2}$, якщо $a^p = b^p \pmod{p}$;

б) $a^{1+2+\ldots+(p-1)} + 1 \vdots p$ або $a^{1+2+\ldots+(p-1)} - 1 \vdots p$, якщо $p > 2$, $(a, p) = 1$;

в) $a^{1+2+\ldots+(p-1)} + 1 \vdots p$ і $a^{1+2+\ldots+(p-1)} - 1 \vdots p$, якщо $p = 2$; $(a, 2) = 1$;

г) $1^{k(p-1)} + 2^{k(p-1)} + \ldots + (p-1)^{k(p-1)} \equiv -1 \pmod{p}$;

д) $a^p \equiv \pm 1 \pmod{p^2}$, якщо $a^p \equiv \pm 1 \pmod{p}$;

е) $p^{q-1} + q^{p-1} \equiv 1 \pmod{pq}$, якщо q — просте число і $p \neq q$;

є) $8p^2 + 1$ є простим числом, якщо $p = 3$;

ж) $p = 3$, якщо $5^{p^2} + 1 \equiv 0 \pmod{p^2}$;

з) $4p + 1$ є складеним числом, якщо $p > 3$, а $2p + 1$ — простим числом;

к) $qa^p + pa^q \equiv a(p + q) \pmod{pq}$, якщо q — просте число, $(a, p) = (a, q) = 1$.

13.12. Знайти остачу від ділення:

а) a^{100} на 125, $a \in \mathbf{Z}$;

б) $2^{\varphi(m)-1}$ на число m, якщо воно непарне і $m > 1$;

в) $4^{\varphi(m)-1}$ на число m, якщо воно непарне і $m > 1$.

13.13. Довести, що:

а) $a_1^5 + a_2^5 + \ldots + a_n^5 \equiv 0 \pmod{30}$, якщо $a_1 + a_2 + \ldots + a_n \equiv 0 \pmod{30}$, $a_1, a_2, \ldots, a_n \in \mathbf{Z}$;

б) $a^{100n+1} \equiv a \pmod{1000}$, якщо $n \in \mathbf{N}$, $(a, 10) = 1$;

в) $n^2 \equiv 1 \pmod{24}$, якщо $(n, 6) = 1$;

г) $a^{6m} + a^{6n} \equiv 0 \pmod{7}$ тоді і тільки тоді, коли $a \vdots 7$, $m, n \in \mathbf{N}$;

д) $(a-1)a(a+2) \equiv 0 \pmod{504}$, якщо a є кубом деякого цілого числа.

§ 14. Конгруенції першого степеня з одним невідомим та застосування їх

Література

[1] — § 17, с. 175—180;
[2] — § 17, с. 179—183;
[3] — гл. 12, § 4, с. 409—411;
[10] — гл. IV, § 2, 3, с. 54—58;
[12] — гл. III, § 2, 4, 5, с. 64—68, 79—87;
[14] — § 21, 22, с. 85—94.

ТЕОРЕТИЧНІ ВІДОМОСТІ

Конгруенцією з одним невідомим за модулем m називають конгруенцію виду

$$f(x) = a_n x^n + a_{n-1} x^{n-1} + \ldots + a_1 x + a_0 \equiv 0 \pmod{m}, \qquad (1)$$

ліва частина якої містить многочлен з цілими коефіцієнтами. Якщо a_n не $\vdots m$, то n називається **степенем конгруенції**.

Розв'язком конгруенції (1) називають клас лишків за модулем m, кожне число якого задовольняє цю конгруенцію.

Якщо a — число, яке задовольняє конгруенцію (1), то записують $x \equiv a \pmod{m}$, або $x = K_a^{(m)}$, де $0 \leqslant a < m$.

Конгруенції з одним невідомим називають рівносильними, якщо множини їхніх розв'язків збігаються.

Операції, які не порушують множину розв'язків конгруенцій (у подальшому називатимемо їхніми **елементарними перетвореннями**):

а) додавання до обох частин конгруенції будь-якого многочлена з цілими коефіцієнтами;

б) додавання до однієї частини конгруенції многочлена з коефіцієнтами, кратними модулю;

в) множення (ділення) обох частин конгруенції на число, яке взаємно просте з модулем (яке є їхнім спільним дільником);

г) множення обох частин конгруенції та їхнього модуля на натуральне число.

Конгруенція

$$ax \equiv b \pmod{m}, \qquad (2)$$

де a не $\vdots m$, називається **конгруенцією 1-го степеня з одним невідомим**.

Якщо $(a, m) = 1$, то конгруенція (2) має єдиний розв'язок.

Якщо $(a, m) = d$, $d > 1$ і $b \vdots d$, то конгруенція (2) має d розв'язків.

Якщо $(a, m) = d$, $d > 1$ і b не $\vdots d$, то конгруенція (2) не має розв'язків.

Найбільш поширеними способами розв'язування конгруенції 1-го степеня є такі:

I. **Спосіб спроб.** Підстановка в конгруенцію (2) чисел повної системи лишків за модулем m (доцільно брати повну систему найменших за абсолютною величиною лишків). Цей спосіб використовується при невеликих модулях.

II. **Штучний спосіб.** Зведення даної конгруенції за допомогою елементарних перетворень до рівносильної їй конгруенції з коефіцієнтом при x, який дорівнює 1.

III. **Спосіб Ейлера:** Розв'язок знаходять за формулою

$$x \equiv ba^{\varphi(m)-1} \pmod{m}, \qquad (3)$$

де $\varphi(m)$ — функція Ейлера.

IV. **Застосування ланцюгових дробів.** Розв'язок знаходять за формулою

$$x \equiv (-1)^n P_{n-1} b \pmod{m}, \qquad (4)$$

де P_{n-1} — чисельник передостаннього підхідного дробу у розкладі $\frac{m}{a}$ в ланцюговий дріб.

V. **Застосування класів лишків.** Розв'язок знаходять за формулою

$$x = K_b^{(m)} \left(K_a^{(m)}\right)^{-1}, \qquad (5)$$

де $\left(K_a^{(m)}\right)^{-1}$ — клас лишків, обернений до класу лишків $K_a^{(m)}$.

Зауваження

1. Формули (3) — (5) справедливі тільки при $(a, m) = 1$. Тому розв'язування конгруенції (2) будь-яким способом треба починати з відшукання (a, m).

2. Число x_0 (клас лишків $K_{x_0}^{(m)}$) вважається розв'язком конгруенції (2), якщо x_0 задовольняє (2) і $0 \leqslant x_0 < m$.

За допомогою конгруенцій першого степеня з одним невідомим можна розв'язувати невизначені рівняння першого степеня з двома невідомими (див. § 5).

Якщо x_0 — розв'язок конгруенції (2), то $\left\{x_0, \frac{b - ax_0}{m}\right\}$ є розв'язком невизначеного рівняння першого степеня з двома невідомими

$$ax + my = b. \qquad (6)$$

Якщо $\{x_0, y_0\}$ — деякий розв'язок рівняння (6), то множину розв'язків цього рівняння знаходять за формулами

$$x' = x_0 + \frac{m}{d} t, \quad y' = y_0 - \frac{a}{d} t, \qquad (7)$$

де t — довільне ціле число, а $d = (a, m)$.

Якщо числа $m_1, m_2, \ldots, m_k$ попарно взаємно прості, то система з одним невідомим

$$\begin{aligned} x &\equiv c_1 \pmod{m_1}, \\ x &\equiv c_2 \pmod{m_2}, \\ &\cdots\cdots\cdots \\ x &\equiv c_k \pmod{m_k} \end{aligned} \tag{8}$$

має єдиний розв'язок

$$x \equiv x_0 \pmod{M}, \tag{9}$$

де

$$M = m_1 m_2 \ldots m_k, \quad x_0 = M_1 y_1 c_1 + M_2 y_2 c_2 + \ldots + M_k y_k c_k,$$

причому числа M_i і y_i визначають з таких умов:

$$M_i = \frac{M}{m_i}, \quad M_i y_i \equiv 1 \pmod{m_i}, \quad i = 1, 2, \ldots, k.$$

У загальному випадку, коли числа $m_1, m_2, \ldots, m_k$ можуть не бути попарно взаємно простими, систему (8) розв'язують ще так: з першої конгруенції системи (8) знаходять

$$x = c_1 + m_1 t_1, \quad \text{де} \quad t_1 \in Z. \tag{10}$$

Це значення x підставляють у другу конгруенцію системи (8) і розв'язують її відносно t_1. Значення t_1 підставляють у рівність (10) і здобуте значення x підставляють у третю конгруенцію системи (8) і т. д. Зрозуміло, що на якомусь кроці можна дістати конгруенцію, яка не має розв'язків. Тоді вся система несумісна.

ПРИКЛАДИ РОЗВ'ЯЗУВАННЯ ЗАДАЧ

1. Користуючись способом спроб, розв'язати конгруенцію

$$2x \equiv 5 \pmod 9.$$

Розв'язання. Спочатку знаходимо $(2, 9) = 1$. Отже, задана конгруенція має єдиний розв'язок. Випробуємо лишки з повної системи абсолютно найменших лишків за модулем 9, тобто числа $0, \pm 1, \pm 2, \pm 3, \pm 4$. Маємо:

$$\begin{aligned} 2 \cdot 0 &= 0 \not\equiv 5 \pmod 9, \\ 2 \cdot 1 &= 2 \not\equiv 5 \pmod 9, \\ 2(-1) &= -2 \not\equiv 5 \pmod 9, \\ 2 \cdot 2 &= 4 \not\equiv 5 \pmod 9, \\ 2 \cdot (-2) &= -4 \equiv 5 \pmod 9. \end{aligned}$$

Отже, число — 4 задовольняє конгруенцію. Запишемо загальний розв'язок, який відповідає цьому окремому розв'язку. Оскільки $-4 \in K_5^{(9)}$, то

$$x \equiv 5 \pmod 9, \quad \text{або} \quad x = K_5^{(9)}.$$

Процес випробування можна вже припинити, оскільки довели, що конгруенція має єдиний розв'язок.

2 Користуючись штучним способом, розв'язати конгруенцію

$$27x \equiv 47 \pmod{38}.$$

Розв'язання. Знаходимо $(27, 38) = 1$. Отже, задана конгруенція має єдиний розв'язок. Додамо до правої частини конгруенції число — 38, яке кратне модулю. Дістаємо

$$27x \equiv 9 \pmod{38}.$$

Поділимо обидві частини цієї конгруенції на 9:

$$3x \equiv 1 \pmod{38}.$$

Додамо до правої частини модуль:

$$3\lambda = 39 \pmod{38}.$$

Поділимо обидві частини останньої конгруенції на 3:

$$x \equiv 13 \pmod{38}.$$

Це і є розв'язок заданої конгруенції.

Зауваження. Відомо, що коли $(a, m) = 1$, то для будь-якого цілого числа b існують такі цілі числа s і t, що $0 \leqslant s < a$ і $b + sm = at$. Отже, розв'язком конгруенції $ax \equiv b \pmod m$, де $(a, m) = 1$ є $x \equiv t \pmod m$, і тому будь-яку конгруенцію першого степеня з одним невідомим можна розв'язати штучним способом. Справді, якщо конгруенція має розв'язки, то досить розглянути випадок, коли $(a, m) = 1$. Тоді конгруенцію $ax \equiv b \pmod m$ послідовно замінюють еквівалентними їй конгруенціями:

$$ax \equiv b \pm m \pmod m, \quad ax \equiv b \pm 2m \pmod m, \ldots,$$

поки не дістануть конгруенцію, в якій ліву і праву частини можна скоротити на a.

3. Користуючись способом Ейлера, розв'язати конгруенцію

$$27x \equiv 24 \pmod{102}.$$

Розв'язання. Знаходимо $(27, 102) = 3$. Задана конгруенція має три розв'язки, оскільки $24 \vdots 3$. Поділимо обидві частини і модуль заданої конгруенції на 3:

$$9x \equiv 8 \pmod{34}.$$

Оскільки тут $a = 9$, $m = 34$, $b = 8$, то за формулою (3) маємо

$$x \equiv ba^{\varphi(m)-1} \pmod m,$$

або

$$x \equiv 8 \cdot 9^{\varphi(34)-1} \pmod{34}.$$

Тепер знайдемо $\varphi(34)$. Оскільки $34 = 2 \cdot 17$, то

$$\varphi(34) = 2 \cdot 17 \cdot \left(1 - \frac{1}{2}\right)\left(1 - \frac{1}{17}\right) = 16.$$

Тоді $x \equiv 8 \cdot 9^{15} \pmod{34}$. Число $8 \cdot 9^{15}$ замінимо найменшим невід'ємним лишком за модулем 34. Дістаємо

$$x \equiv 8 \cdot 9^{15} \equiv 8 \cdot 3^{30} \equiv 8 \cdot 3^{16} \equiv 8 \cdot (2187)^2 \equiv 8 \cdot 11^2 \equiv 16 \pmod{34}.$$

Отже, $x \equiv 16 \pmod{34}$ є розв'язок конгруенції $9x \equiv 8 \pmod{34}$. Тоді конгруенція $27x \equiv 24 \pmod{102}$ має розв'язки:

$$\begin{aligned} x &\equiv 16 \pmod{102}, \\ x &\equiv 50 \pmod{102}, \\ x &\equiv 84 \pmod{102}, \end{aligned}$$

або коротше

$$x \equiv 16;\ 50;\ 84 \pmod{102}.$$

Зауваження. Недоліком способу Ейлера є те, що при великому $\varphi(m)$ знаходження найменшого невід'ємного лишку того класу чисел за модулем m, до якого належить число $ba^{\varphi(m)-1}$, стає громіздким.

4. Використовуючи ланцюгові дроби, розв'язати конгруенцію

$$220x \equiv 28 \pmod{348}.$$

Розв'язання. Знаходимо $(220, 348) = 4$. Оскільки $28 \vdots 4$, то задана конгруенція має чотири розв'язки. Поділимо обидві частини і модуль заданої конгруенції на 4:

$$55x \equiv 7 \pmod{87}.$$

Розв'яжемо цю конгруенцію за допомогою ланцюгових дробів. Розкладемо $\frac{87}{55}$ у ланцюговий дріб і обчислимо його підхідні дроби. Дістанемо таблицю елементів q_i і чисельників P_i (табл. 13).

Таблиця 13

t	-1	0	1	2	3	4	5	6
q_t		1	1	1	2	1	1	4
P_t	1	1	2	3	8	11	19	87

Отже, $n = 6$, $P_{n-1} = 19$. Оскільки $b = 7$, $m = 87$, то за формулою (4)

$$x \equiv (-1)^n P_{n-1} b \pmod m.$$

Отже,

$$x \equiv (-1)^6 19 \cdot 7 \equiv 133 \equiv 46 \pmod{87}$$

є розв'язком конгруенції $55x \equiv 7 \pmod{87}$. Тоді задана конгруенція має розв'язки

$$x \equiv 46;\ 133;\ 220;\ 307 \pmod{348}.$$

Зауваження. Перш ніж застосувати цей спосіб, слід спочатку (якщо це необхідно), використовуючи властивості конгруенцій, зробити коефіцієнт при невідомому невід'ємним і меншим за модуль.

5. Застосовуючи класи лишків, розв'язати конгруенцію

$$37x \equiv 25 \pmod{107}.$$

Розв'язання. Знаходимо $(37,\ 107) = 1$. Отже, задана конгруенція має єдиний розв'язок. Запишемо конгруенцію у вигляді

$$K_{37}^{(107)} K_x^{(107)} = K_{25}^{(107)}.$$

Знайдемо $\left(K_{37}^{(107)}\right)^{-1}$ — клас лишків за модулем 107, обернений до класу $K_{37}^{(107)}$. Для цього застосуємо до чисел 107 і 37 алгоритм ділення з остачею. Матимемо

$$107 = 37 \cdot 2 + 33,$$
$$37 = 33 \cdot 1 + 4,$$
$$33 = 4 \cdot 8 + 1.$$

Розглядаючи цей процес знизу вверх, виразимо 1 через числа 107 і 33:

$$1 = 33 - 4 \cdot 8 = 33 - (37 - 33 \cdot 1) \cdot 8 = 33 \cdot 9 + 37\,(-8) =$$
$$= (107 - 37 \cdot 2) \cdot 9 + 37\,(-8) = 107 \cdot 9 + 37\,(-26).$$

Отже, $1 = 107 \cdot 9 + 37\,(-26)$. Це означає, що $\left(K_{37}^{(107)}\right)^{-1} = K_{-26}^{(107)}$, тобто

$$\left(K_{37}^{(107)}\right)^{-1} = K_{-26+107}^{(107)} = K_{81}^{(107)}.$$

Тоді за формулою (5) маємо

$$x = K_b^{(m)} \left(K_a^{(m)}\right)^{-1}, \quad \text{або} \quad x = K_{28}^{(107)} \cdot K_{81}^{(107)} = K_{2025}^{(107)} = K_{99}^{(107)}.$$

Отже, $x = K_{99}^{(107)}$ є розв'язком заданої конгруенції, тобто $x \equiv 99 \pmod{107}$.

Зауваження. Процес розв'язування конгруенції першого степеня з одним невідомим будь-яким способом слід закінчувати перевіркою.

6. Розв'язати в цілих числах невизначене рівняння $27x + 38y = 47$.

Розв'язання. Оскільки число y повинно бути цілим, то різниця $27x - 47$ має ділитися на 38. Дістаємо

$$27x \equiv 47 \pmod{38}.$$

Розв'яжемо цю конгруенцію. Знаходимо $(27,\ 38) = 1$. Отже, конгруенція має єдиний розв'язок. Застосуємо штучний спосіб. Додамо до правої частини число -38, яке кратне модулю:

$$27x \equiv 9 \pmod{38}.$$

Поділимо обидві частини цієї конгруенції на 9:

$$3x \equiv 1 \pmod{38}.$$

Додамо до правої частини модуль:

$$3x \equiv 39 \pmod{38}.$$

Поділимо обидві частини на 3:

$$x \equiv 13 \pmod{38}.$$

Отже, $x \equiv 13 \pmod{38}$ є розв'язком конгруенції $27x \equiv 47 \pmod{38}$. Тоді

$$\left\{13,\ \frac{47 - 27 \cdot 13}{38}\right\} = \{13,\ -8\}$$

є окремим розв'язком заданого рівняння. Загальний розв'язок заданого рівняння дістаємо за формулами (7):

$$x' = x_0 + \frac{m}{d} t, \quad y' = y_0 - \frac{a}{d} t,$$

де $x_0 = 13$, $y_0 = -8$, $m = 38$, $a = 27$, $d = 1$. Отже,

$$\{x' = 13 + 38t,\ y' = -8 - 27t\} —$$

загальний розв'язок заданого невизначеного рівняння, де t — довільне ціле число.

7. Розв'язати систему конгруенцій

$$\begin{cases} 3x \equiv 11 \pmod{17}, \\ 15x \equiv 35 \pmod{13}, \\ 21x \equiv 33 \pmod{30}. \end{cases}$$

Розв'язання. Розв'язуючи кожну конгруенцію, замінимо задану систему еквівалентною їй системою конгруенцій:

$$\begin{cases} x \equiv 15 \pmod{17}, \\ x \equiv 11 \pmod{13}, \\ x \equiv 3 \pmod{10}. \end{cases}$$

Оскільки модулі конгруенцій попарно взаємно прості, то можна використати формулу (9). Знаходимо:

$$M = 17 \cdot 13 \cdot 10 = 2210,$$
$$M_1 = \frac{2210}{17} = 130,$$
$$M_2 = \frac{2210}{13} = 170,$$
$$M_3 = \frac{2210}{10} = 221.$$

Розв'яжемо такі конгруенції:

$$130y_1 \equiv 1 \pmod{17}, \quad 170y_2 \equiv 1 \pmod{13}, \quad 221y_3 \equiv 1 \pmod{10}.$$
$$y_1 = 14, \qquad y_2 = 1, \qquad y_3 = 1.$$

Згідно з формулою (9), дістанемо

$$x = x_0 = 130 \cdot 14 \cdot 15 + 170 \cdot 1 \cdot 11 + 211 \cdot 1 \cdot 3 = 29\,833 \equiv 1103 \pmod{2210}.$$

Зауваження. 1. Якщо деяка з конгруенцій системи має кілька розв'язків, то їх слід об'єднати і записати як один розв'язок за меншим модулем, бо в противному разі треба буде розв'язувати стільки систем, скільки розв'язків має конгруенція.

2. Розв'язки системи конгруенцій можуть мати різні форми запису. Так, якщо розв'язки третьої конгруенції з прикладу 7 ми записали б у вигляді $x \equiv 3,\ 13,\ 23 \pmod{30}$, то довелося б розв'язувати такі три системи конгруенцій:

$$\begin{cases} x \equiv 15 \pmod{17}, \\ x \equiv 11 \pmod{13}, \\ x \equiv 3 \pmod{30}; \end{cases} \quad \begin{cases} x \equiv 15 \pmod{17}, \\ x \equiv 11 \pmod{13}, \\ x \equiv 13 \pmod{30}; \end{cases} \quad \begin{cases} x \equiv 15 \pmod{17}, \\ x \equiv 11 \pmod{13}, \\ x \equiv 23 \pmod{30}. \end{cases}$$

Дістали б три розв'язки:

$$x \equiv 5523 \pmod{6630}, \quad x \equiv 3313 \pmod{6630}, \quad x \equiv 1103 \pmod{6630}.$$

Зазначимо, що множина чисел, які визначаються цими розв'язками, збігається з множиною чисел, що визначаються одним розв'язком, здобутим раніше,

$$x \equiv 1103 \pmod{2210}.$$

8. Розв'язати систему конгруенцій

$$\begin{cases} 2x \equiv 19 \pmod{15}, \\ 3x \equiv 41 \pmod{20}, \\ 6x \equiv 37 \pmod{35}. \end{cases}$$

Розв'язання. Розв'язуючи кожну конгруенцію, замінимо задану систему еквівалентною їй системою конгруенцій:

$$\begin{cases} x \equiv 2 \pmod{15}, \\ x \equiv 7 \pmod{20}, \\ x \equiv 12 \pmod{35}. \end{cases}$$

З першої конгруенції маємо $x = 2 + 15t$, де $t \in \mathbf{Z}$. Щоб визначити t, підставимо значення x у другу конгруенцію:

$$2 + 15t \equiv 7 \pmod{20}.$$

Звідси $t \equiv 3 \pmod 4$, або $t = 3 + 4s$, де $s \in \mathbf{Z}$. Тоді

$$x = 2 + 15t = 2 + 15(3 + 4s) = 47 + 60s,$$

причому x задовольняє вже перші дві конгруенції системи. Серед чисел x вибе• ремо такі, які б задовольняли й третю конгруенцію. Для цього знайдемо s з умови

$$47 + 60s \equiv 12 \pmod{35}.$$

Звідси $s \equiv 0 \pmod 7$, тобто $s = 7k$, де $k \in \mathbf{Z}$. Маємо $x = 47 + 60s = 47 + 60 \cdot 7k = 47 + 420k$. Отже, $x \equiv 47 \pmod{420}$ — розв'язок заданої системи.

Задачі

14.1. За способом спроб розв'язати такі конгруенції:

а) $2x \equiv 1 \pmod 3$;
б) $8x \equiv 3 \pmod 4$;
в) $6x \equiv 7 \pmod 5$;
г) $3x \equiv 22 \pmod 7$;
д) $4x \equiv 6 \pmod{10}$;
е) $12x \equiv 1 \pmod 7$;
є) $5x \equiv 7 \pmod{11}$;
ж) $8x \equiv 16 \pmod{12}$.

14.2. За штучним способом розв'язати такі конгруенції:

а) $7x \equiv 8 \pmod{13}$;
б) $6x \equiv 11 \pmod{14}$;
в) $8x \equiv 10 \pmod{14}$;
г) $11x \equiv -32 \pmod{27}$;
д) $16x \equiv 50 \pmod{23}$;
е) $25x \equiv 1 \pmod{37}$;
є) $17x \equiv 23 \pmod{41}$;
ж) $32x \equiv 43 \pmod{51}$.

14.3. За способом Ейлера розв'язати такі конгруенції:

а) $5x \equiv 7 \pmod{13}$;
б) $29x \equiv 3 \pmod{12}$;
в) $5x \equiv 26 \pmod{12}$;
г) $8x \equiv 17 \pmod{19}$;
д) $27x \equiv 11 \pmod{34}$;
е) $24x \equiv 1 \pmod{15}$;
є) $15x \equiv 23 \pmod{22}$;
ж) $12x \equiv 51 \pmod{39}$.

14.4. Застосовуючи ланцюгові дроби, розв'язати такі конгруенції:

а) $15x \equiv 37 \pmod{98}$;
б) $32x \equiv 182 \pmod{119}$;
в) $105x \equiv 72 \pmod{147}$;
г) $97x \equiv 53 \pmod{169}$;
д) $-50x \equiv 67 \pmod{177}$;
е) $69x \equiv 393 \pmod{201}$;
є) $192x \equiv 9 \pmod{327}$;
ж) $365x \equiv 50 \pmod{395}$;
з) $-639x \equiv 177 \pmod{924}$;
к) $1296x \equiv 1105 \pmod{2413}$;
л) $1215x \equiv 560 \pmod{2755}$;
м) $1919x \equiv 1717 \pmod{4009}$.

14.5. Застосовуючи класи лишків, розв'язати такі конгруенції:

а) $21x \equiv 17 \pmod{23}$;
б) $5x \equiv 7 \pmod{24}$;
в) $17x \equiv 19 \pmod{24}$;
г) $13x \equiv -1 \pmod{30}$;
д) $28x \equiv 33 \pmod{35}$;
е) $12x \equiv 24 \pmod{30}$;
є) $9x \equiv 18 \pmod{41}$;
ж) $11x \equiv 31 \pmod{50}$.

14.6. Розв'язати штучним способом конгруенції задач 14.3 і 14.5.

14.7. Розв'язати такі конгруенції:

а) $(a + b)x \equiv a^2 + b^2 \pmod{ab}$, $(a, b) = 1$;
б) $(a^2 + b^2)x \equiv a - b \pmod{ab}$, $(a, b) = 1$;
в) $(a + b)^2 x \equiv a^2 - b^2 \pmod{ab}$, $(a, b) = 1$;
г) $(a - b)x \equiv a^2 + b^2 \pmod{ab}$, $(a, b) = 1$;
д) $2x \equiv 1 + p \pmod p$, де p — просте непарне число;
е) $(m - 1)x \equiv 1 \pmod m$;
є) $(m + 1)^2 x \equiv a \pmod m$;
ж) $ax \equiv 1 \pmod p$, де p — просте число і $(a, p) = 1$.

14.8. Скласти конгруенцію першого степеня з одним невідомим за модулем 15 так, щоб вона мала:

а) єдиний розв'язок;
б) 3 або 5 розв'язків;
в) 2, 4, 6, 14 розв'язків.

14.9. Розв'язати в цілих числах невизначені рівняння:

а) $2x + 3y = 4$;
б) $4x - 3y = 2$;
в) $3x + 4y = 13$;
г) $5x + 4y = 3$;
д) $3x + 8y = 5$;
е) $17x + 13y = 1$;
є) $23x + 15y = 19$;
ж) $17x - 16y = 31$;
з) $91x - 28y = 35$;
к) $17x - 39y = 26$;
л) $50x - 42y = 34$;
м) $47x - 105y = 4$;
н) $47x - 111y = 89$.

14.10. Розв'язати системи конгруенцій:

а) $\begin{cases} 3x \equiv 5 \pmod 7, \\ 2x \equiv 1 \pmod 5; \end{cases}$
б) $\begin{cases} 3x \equiv 1 \pmod{20}, \\ 2x \equiv 3 \pmod{15}; \end{cases}$
в) $\begin{cases} 3x \equiv 1 \pmod 5, \\ 5x \equiv 4 \pmod 7; \end{cases}$
г) $\begin{cases} 14x \equiv 12 \pmod{18}, \\ x \equiv 5 \pmod{25}; \end{cases}$
д) $\begin{cases} x \equiv b_1 \pmod{13}, \\ x \equiv b_2 \pmod{17}; \end{cases}$
е) $\begin{cases} 3x + 4y \equiv 29 \pmod{143}, \\ 2x - 9y \equiv 59 \pmod{143}; \end{cases}$
є) $\begin{cases} x + 2y \equiv 0 \pmod 5, \\ 3x + 2y \equiv 2 \pmod 5; \end{cases}$
ж) $\begin{cases} 5x - y \equiv 3 \pmod 6, \\ 2x + 2y \equiv 5 \pmod 6. \end{cases}$

14.11. Розв'язати системи конгруенцій:

а) $\begin{cases} x \equiv 3 \pmod 8, \\ x \equiv 11 \pmod{20}, \\ x \equiv 1 \pmod{15}; \end{cases}$

б) $\begin{cases} x \equiv 2 \pmod 3, \\ x \equiv 3 \pmod 4, \\ x = 4 \pmod 5; \end{cases}$

в) $\begin{cases} x \equiv 1 \pmod 2, \\ x \equiv 3 \pmod 5, \\ x \equiv 6 \pmod 9; \end{cases}$

г) $\begin{cases} x \equiv 2 \pmod 7, \\ x \equiv 5 \pmod 9, \\ x \equiv 11 \pmod{15}; \end{cases}$

д) $\begin{cases} x \equiv 4 \pmod 7, \\ x \equiv 9 \pmod{13}, \\ x \equiv 1 \pmod{17}; \end{cases}$

е) $\begin{cases} x \equiv 5 \pmod{12}, \\ x \equiv 2 \pmod 8, \\ x \equiv 2 \pmod{11}; \end{cases}$

є) $\begin{cases} x \equiv 2 \pmod{15}, \\ x \equiv 7 \pmod{20}, \\ x \equiv 12 \pmod{35}; \end{cases}$

ж) $\begin{cases} x \equiv 4 \pmod 5, \\ x \equiv 1 \pmod{12}; \\ x \equiv 7 \pmod{14}; \end{cases}$

з) $\begin{cases} x \equiv 5 \pmod 8, \\ x \equiv 4 \pmod{11}, \\ x \equiv 6 \pmod{17}; \end{cases}$

к) $\begin{cases} x \equiv b_1 \pmod{25}, \\ x \equiv b_2 \pmod{27}, \\ x \equiv b_3 \pmod{59}; \end{cases}$

л) $\begin{cases} x \equiv 1 \pmod 3, \\ x \equiv 4 \pmod 5, \\ x \equiv 2 \pmod 7, \\ x \equiv 9 \pmod{11}, \\ x \equiv 3 \pmod{13}. \end{cases}$

14.12. Розв'язати системи конгруенцій:

а) $\begin{cases} 3x \equiv 1 \pmod{10}, \\ 4x \equiv 3 \pmod 5, \\ 2x \equiv 7 \pmod 9); \end{cases}$

б) $\begin{cases} 2x \equiv 3 \pmod 5, \\ 3x \equiv 5 \pmod 7, \\ 3x \equiv 3 \pmod 9); \end{cases}$

в) $\begin{cases} 4x \equiv 1 \pmod 9, \\ 5x \equiv 3 \pmod 7, \\ 4x \equiv 5 \pmod{12}; \end{cases}$

г) $\begin{cases} 7x \equiv 3 \pmod{11}, \\ 3x \equiv 2 \pmod 5, \\ 15x \equiv 5 \pmod{35}; \end{cases}$

д) $\begin{cases} 3x \equiv 7 \pmod{10}, \\ 2x \equiv 5 \pmod{15}, \\ 7x \equiv 5 \pmod{12}; \end{cases}$

е) $\begin{cases} 5x \equiv 3 \pmod 9, \\ 4x \equiv 7 \pmod{13}, \\ 8x \equiv 4 \pmod{14}, \\ x \equiv 2 \pmod{17}; \end{cases}$

є) $\begin{cases} 2x \equiv 7 \pmod{13}, \\ 5x \equiv 8 \pmod{17}, \\ 14x \equiv 35 \pmod{19}, \\ 3x \equiv 7 \pmod{31}. \end{cases}$

14.13. Знайти точки з цілими координатами, які лежать на прямих $4x - 7y = 9$, $2x + 9y = 15$ і $5x - 13y = 12$ на одному перпендикулярі до осі абсцис.

14.14. При яких значеннях a мають розв'язки такі системи:

а) $\begin{cases} x \equiv a \pmod 6, \\ x \equiv 1 \pmod{10}, \\ x \equiv 2 \pmod{21}, \\ x \equiv 3 \pmod{11}; \end{cases}$

б) $\begin{cases} 2x \equiv a \pmod 4, \\ 3x \equiv 4 \pmod{10}; \end{cases}$

в) $\begin{cases} x \equiv 5 \pmod{18}, \\ x \equiv 8 \pmod{21}, \\ x \equiv a \pmod{35}; \end{cases}$

г) $\begin{cases} x \equiv 3 \pmod{11}, \\ x \equiv 11 \pmod{20}, \\ x \equiv 1 \pmod{15}, \\ x \equiv a \pmod 8)? \end{cases}$

14.15. Знайти хоча б одне значення m, при якому несумісною є система

$$\begin{cases} x \equiv 3 \pmod 6, \\ x \equiv 7 \pmod m). \end{cases}$$

14.16. Скільки точок з цілими координатами лежать на прямій $8x - 13y + 6 = 0$ між прямими $x = -100$ і $x = 150$?

14.17. Довести, що всередині прямокутника, обмеженого прямими $x = -2$, $x = 5$ і $y = -1$, $y = 2$, на прямій $3x - 7y = 1$ не має жодної точки з цілими координатами.

14.18. Скільки точок з цілими координатами лежать на заданих прямих між точками з абсцисами a_1 і a_2:

а) $10x - 11y = 15$, $a_1 = -30$, $a_2 = 50$;
б) $31x - 47y = 23$, $a_1 = 23$, $a_2 = -50$;
в) $101x - 39y = 89$, $a_1 = 0$, $a_2 = 100$;
г) $8x - 13y + 6 = 0$, $a_1 = -100$, $a_2 = 150$;
д) $7x + 29y = 584$, $a_1 = -20$, $a_2 = 160$;
е) $90x - 74y = 50$, $a_1 = -100$, $a_2 = 200$?

14.19. Нехай точки A і B мають цілі координати $A(x_1, y_1)$, $B(x_2, y_2)$. Довести, що на відрізку AB число внутрішніх точок з цілими координатами дорівнює $d - 1$, де

$$d = (y_1 - y_2,\ x_1 - x_2).$$

14.20. Через скільки точок з цілими координатами проходять сторони трикутника з вершинами:

а) $A(2, 3)$, $B(7, 8)$, $C(13, 5)$;
б) $A(2, 1)$, $B(20, 7)$, $C(8, 15)$?

14.21. Знайти відстань r між сусідніми точками з цілими координатами, які лежать на прямій $ax + by = c$, $(a, b) = 1$.

14.22. При якій умові дріб $\frac{c}{ab}$ можна подати у вигляді суми двох дробів із знаменниками a і b $(a, b, c \in \mathbf{Z})$?

14.23. Відгадати день народження, якщо сума добутків числа місяця на 12 і номера місяця на 31 дорівнює 339. У чому суть відгадування?

14.24. Для перевезення зерна є мішки по 60 і 80 кг. Скільки таких мішків потрібно для перевезення 440 кг зерна?

14.25. На будівництво газопроводу на трасу завдовжки 283 м було доставлено труби, довжина яких 5 і 7 м. Скільки труб доставили?

14.26. Скільки квитків по 30 і 50 коп. можна купити на 14 крб. 90 коп.?

§ 15. Конгруенції вищих степенів з одним невідомим

Література

[1] — § 18, с. 180—184;
[2] — § 18, с. 183—187;
[3] — гл. 12, § 4, с. 411—413;
[5] — гл. VIII, § 4, с. 297—316;
[10] — гл. IV, § 4, 5, с. 58—63;
[11] — гл. 15, § 1, гл. 16, с. 126—131, с. 135—139;
[12] — гл. III, § 6, 7, с. 87—101;
[14] — § 24, 25, с. 94—105.

ТЕОРЕТИЧНІ ВІДОМОСТІ

Якщо $m_1, m_2, \ldots, m_s$ — попарно взаємно прості числа, то конгруенція

$$f(x) = a_0x^n + a_1x^{n-1} + \ldots + a_{n-1}x + a_n \equiv 0 \pmod{m_1m_2 \ldots m_s} \tag{1}$$

еквівалентна системі конгруенцій

$$\left.\begin{aligned} f(x) &\equiv 0 \pmod{m_1},\\ f(x) &\equiv 0 \pmod{m_2},\\ &\cdots\cdots\cdots\\ f(x) &\equiv 0 \pmod{m_s}. \end{aligned}\right\} \tag{2}$$

Число розв'язків конгруенції (1) дорівнює $k_1k_2 \ldots k_s$, де $k_1, k_2, \ldots, k_s$ дорівнює відповідно числу розв'язків кожної з конгруенцій (2). Отже, треба розв'язати конгруенцію виду

$$f(x) \equiv 0 \pmod{p^\alpha}, \tag{3}$$

де p — просте число, $\alpha \in \mathbb{N}$.

Будь-який розв'язок

$$x \equiv a \pmod{p} \tag{4}$$

конгруенції

$$f(x) \equiv 0 \pmod{p} \tag{5}$$

при умові, що $f'(a)$ не $\vdots\, p$, є одним з розв'язків конгруенції (3).

Якщо $f'(a) \vdots\, p$, то розв'язок (4) або не дає жодного розв'язку для (3), або дає кілька розв'язків.

Нехай $x \equiv a \pmod{p^{k-1}}$ — розв'язок конгруенції $f(x) \equiv 0 \pmod{p^{k-1}}$. Тоді число $x = a + p^{k-1}t$, $t \in \mathbb{Z}$, є розв'язком конгруенції $f(x) \equiv 0 \pmod{p^k}$ тоді і тільки тоді, коли відповідне значення t задовольняє конгруенцію

$$f'(a)\,t \equiv -\frac{f(a)}{p^{k-1}} \pmod{p}. \tag{6}$$

Якщо конгруенція (6) не має розв'язків, то в класі розв'язків $x \equiv a \pmod{p^{k-1}}$ конгруенції $f(x) \equiv 0 \pmod{p^{k-1}}$ немає жодного розв'язку конгруенції $f(x) \equiv 0 \pmod{p^k}$.

Якщо конгруенція (6) має розв'язки і $f'(a) \vdots\, p$, то будь-яке ціле число t задовольняє конгруенцію (6), а тому $t \equiv 0, 1, \ldots, p-1 \pmod{p}$ є розв'язками (6). Тоді клас розв'язків $x \equiv a \pmod{p^{k-1}}$ конгруенції $f(x) \equiv 0 \pmod{p^{k-1}}$ дає p розв'язків конгруенції $f(x) \equiv 0 \pmod{p^k}$, а саме: $x \equiv a,\ a + p^{k-1},\ a + 2p^{k-1}, \ldots, a + (p-1)p^{k-1} \pmod{p^k}$.

Якщо конгруенція (6) має розв'язки і $f'(a)$ не ділиться на p, то це є єдиний розв'язок $t \equiv t_0 \pmod{p}$. Тоді з класу розв'язків $x \equiv a \pmod{p^{k-1}}$ конгруенції $f(x) \equiv 0 \pmod{p^{k-1}}$ дістаємо єдиний розв'язок $x \equiv a + p^{k-1}t_0 \pmod{p^k}$ конгруенції $f(x) \equiv 0 \pmod{p^k}$.

Конгруенцію (5) завжди можна замінити еквівалентною конгруенцією того самого степеня із старшим коефіцієнтом, що дорівнює одиниці. Для цього слід обидві частини конгруенції (5) домножити на число b, яке задовольняє конгруенцію $a_0y \equiv 1 \pmod{p}$. Це число визначається однозначно, оскільки $(a_0, p) = 1$.

Конгруенцію (5) можна замінити еквівалентною їй конгруенцією степеня не вище $p-1$ за тим самим модулем (згідно з теоремою про пониження степеня конгруенції). Для цього треба в конгруенції (5) замінити вираз $f(x)$ на $r(x)$, де $r(x)$ — остача від ділення $f(x)$ на $x^p - x$. Ділення $f(x)$ на $x^p - x$ можна фактично й не виконувати, а просто замінювати кожне x^s у лівій частині (5) на x^r, де r — остача від ділення s на $p-1$ при умові, що остачу 0 замінюємо числом $p-1$.

Якщо a_0 не ділиться на p, то конгруенція (5) степеня $n < p$ має не більш ніж n різних розв'язків.

Конгруенція (5) має більш як n розв'язків тоді і тільки тоді, коли всі коефіцієнти в лівій частині (n) діляться на p, тобто коли конгруенція тотожна.

Конгруенція (5) степеня $n < p$, в якій $a_0 = 1$, $(a_n, p) = 1$, має n розв'язків тоді і тільки тоді, коли всі коефіцієнти остачі від ділення $x^p - x$ на $f(x)$ діляться на p.

Теорема Вільсона. *Натуральне число $n > 1$ тоді і тільки тоді є простим, коли $(n-1)! + 1 \equiv 0 \pmod{n}$.*

Якщо p — просте число, то конгруенція

$$x^{p-1} - 1 \equiv 0 \pmod{p}$$

має точно $p-1$ розв'язок.

Якщо p — просте число і d — натуральний дільник числа $p-1$, то конгруенція

$$x^d \equiv 1 \pmod{p}$$

має точно d розв'язків.

ПРИКЛАДИ РОЗВ'ЯЗУВАННЯ ЗАДАЧ

1. Розв'язати конгруенцію $f(x) \equiv x^{17} + 2x^{11} + 3x^8 - 4x^7 + 2x - 3 \equiv 0 \pmod{5}$.

Розв'язання. Замінимо цю конгруенцію еквівалентною їй конгруенцією степеня не вище 4 за тим самим модулем 5. Поділимо $f(x)$ на $x^5 - x$. Дістанемо

$$f(x) = (x^5 - x)(x^{12} + x^8 + 2x^6 + x^4 + 3x^3 - 2x^2 + 1) + 3x^4 - 2x^3 + 3x - 3.$$

Замінивши всі коефіцієнти остачі найменшими лишками за модулем 5, дістанемо, що задана конгруенція еквівалентна конгруенції

$$r(x) = 3x^4 + 3x^3 + 3x + 2 \equiv 0 \pmod{5}. \tag{1}$$

Замінимо цю конгруенцію еквівалентною їй конгруенцією із старшим коефіцієнтом, що дорівнює 1. Спочатку розв'яжемо конгруенцію

$$3y \equiv 1 \pmod{5}.$$

Додамо до правої частини модуль:

$$3y \equiv 6 \pmod{5}.$$

Поділимо обидві частини на 3:

$$y \equiv 2 \pmod 5.$$

Домножимо конгруенцію (1) на 2:

$$6x^4 + 6x^3 + 6x + 4 \equiv 0 \pmod 5.$$

Замінимо останню конгруенцію еквівалентною їй:

$$x^4 + x^3 + x - 1 \equiv 0 \pmod 5. \tag{2}$$

Оскільки $x \not\equiv 0 \pmod 5$, то $(x, 5) = 1$, а тому $x^{5-1} \equiv 1 \pmod 5$. Тоді конгруенція (2) матиме вигляд

$$x^3 + x \equiv 0 \pmod 5. \tag{3}$$

Оскільки $(x, 5) = 1$, то обидві частини конгруенції (3) можна скоротити на x:

$$x^2 + 1 \equiv 0 \pmod 5. \tag{4}$$

Конгруенція (4) має такі очевидні розв'язки: $x \equiv 2 \pmod 5$ і $x \equiv 3 \pmod 5$. Отже, конгруенція (1) має два розв'язки: $x \equiv 2;\ 3 \pmod 5$.

Зауваження. Замість того щоб ділити $f(x)$ на $x^5 - x$, можна було б замінити x^s на x^r, де r — остача від ділення s на $5 - 1 = 4$, причому, якщо s ділиться на 4, то покладемо $r = 4$. Тоді

$$x^{17} \equiv x \pmod 5,$$

$$2x^{11} \equiv 2x^3 \pmod 5,$$

$$3x^8 \equiv 3x^4 \pmod 5,$$

$$-4x^7 \equiv x^3 \pmod 5.$$

Отже,

$$f(x) \equiv 3x^4 + 3x^3 + 3x + 2 \equiv 0 \pmod 5.$$

2. Розв'язати конгруенцію

$$f(x) \equiv x^5 + 10x^3 + x + 6 \equiv 0 \pmod{108}. \tag{1}$$

Розв'язання. Оскільки $108 = 2^2 \cdot 3^3$, то задана конгруенція еквівалентна системі

$$\begin{cases} f(x) \equiv 0 \pmod 4, \\ f(x) \equiv 0 \pmod{27}. \end{cases} \tag{2}$$

Перша з цих конгруенцій після спрощення матиме вигляд

$$x^5 + 2x^3 + x + 2 \equiv 0 \pmod 4. \tag{3}$$

Випробовуючи лишки 0, $\pm 1, 2$ за модулем 4, впевнюємося, що конгруенція (3) має єдиний розв'язок

$$x \equiv 2 \pmod 4. \tag{4}$$

Щоб розв'язати другу конгруенцію системи (2), треба спочатку розв'язати конгруенцію

$$f(x) \equiv 0 \pmod 3, \tag{5}$$

або після спрощення

$$x^5 + x^3 + x \equiv 0 \pmod 3. \tag{6}$$

Оскільки

$$x^5 \equiv x^1 \pmod 3,$$

$$x^3 \equiv x^1 \pmod 3,$$

то конгруенція (6) еквівалентна конгруенції

$$3x \equiv 0 \pmod 3,$$

тобто $0 \equiv 0 \pmod 3$.

Отже, конгруенція (5) виконується при будь-якому значенні x. Це означає, що вона має такі розв'язки:

$$x \equiv 0;\ 1;\ 2 \pmod 3.$$

Використовуючи ці класи чисел за модулем 3, розв'яжемо конгруенцію

$$x^5 + 10x^3 + x + 6 \equiv 0 \pmod 9,$$

або еквівалентну їй конгруенцію

$$x^5 + x^3 + x + 6 \equiv 0 \pmod 9. \tag{7}$$

Нехай

$$g(x) = x^5 + x^3 + x + 6.$$

Випробуємо тепер кожен клас за модулем 3.

У класі $x \equiv 0 \pmod 3$ беремо числа $x = 3t$, де t задовольняє співвідношення

$$g'(0) \cdot t \equiv -\frac{g(0)}{3} \pmod 3.$$

Оскільки $g'(x) = 5x^4 + 3x^2 + 1$, $g'(0) = 1$ і $g(0) = 6$, то $t \equiv -2 \pmod 3$, тобто $t \equiv 1 \pmod 3$, або $t = 3s + 1$, $s \in Z$.

Дістаємо $x = 3t = 3(3s + 1) = 9s + 3$. Ці числа утворюють один клас розв'язків конгруенції (7):

$$x \equiv 3 \pmod 9. \tag{8}$$

У класі $x \equiv 1 \pmod 3$ беремо числа $x = 1 + 3t$, де t задовольняє співвідношення

$$g'(1) \cdot t \equiv -\frac{g(1)}{3} \pmod 3.$$

Оскільки $g'(1) = 9$, $g(1) = 9$, то

$$9t \equiv -3 \pmod 3.$$

Цю конгруенцію задовольняє будь-яке значення t, тобто $t = 3s$, $t = 3s + 1$, $t = 3s + 2$, де $s \in Z$. Тоді $x = 1 + 9s$, $x = 4 + 9s$, $x = 7 + 9s$. Отже, маємо ще три розв'язки конгруенції (7):

$$x \equiv 1;\ 4;\ 7 \pmod 9. \tag{9}$$

У класі $x \equiv 2 \pmod 3$ беремо числа $x = 2 + 3t$, де t задовольняє співвідношення

$$g'(2) \cdot t \equiv -\frac{g(2)}{3} \pmod 3.$$

Оскільки $g'(2) = 93$, $g(2) = 48$, то

$$93t \equiv -16 \pmod 3$$

або $0 \equiv 2 \pmod 3$.

Ця суперечність свідчить про те, що в класі чисел $x \equiv 2 \pmod 3$ немає розв'язків конгруенції (7).

За допомогою знайдених класів розв'язків $f(x) \equiv 0 \pmod 9$ дістанемо розв'язки конгруенції

$$f(x) \equiv x^5 + 10x^3 + x + 6 \equiv 0 \pmod{27}. \tag{10}$$

Випробовуємо кожен з класів (8) і (9).

У класі $x \equiv 3 \pmod 9$ беремо числа $x = 9t + 3$, де t задовольняє конгруенцію

$$f'(3) \cdot t \equiv -\frac{f(3)}{9} \pmod 3.$$

Оскільки $f'(x) = 5x^4 + 30x^2 + 1$, $f'(3) = 676$, $f(3) = 522$, то $676t \equiv -58 \pmod 3$, або $t \equiv 2 \pmod 3$, звідки $t = 3s + 2$, $s \in Z$.

Тоді $x = 9(3s + 2) + 3 = 27s + 21$, $s \in \mathbf{Z}$.
Ці числа утворюють один клас розв'язків конгруенції (10)

$$x \equiv 21 \pmod{27}. \qquad (11)$$

У класі $x \equiv 1 \pmod 9$ беремо числа $x = 9t + 1$, де t задовольняє конгруенцію

$$f'(1) \cdot t \equiv -\frac{f(1)}{9} \pmod 3.$$

Оскільки $f'(1) = 36$, $f(1) = 18$, то $36t \equiv -2 \pmod 3$. Тут $(36,3) = 3$, а -2 не ділиться на 3, тому остання конгруенція розв'язків не має. Це означає, що в класі чисел $x \equiv 1 \pmod 9$ немає розв'язків конгруенції (10).
У класі $x \equiv 4 \pmod 9$ візьмемо числа $x = 9t + 4$, де t задовольняє конгруенцію

$$f'(4) \cdot t \equiv -\frac{f(4)}{9} \pmod 3.$$

Оскільки $f'(4) = 1761$, $f(4) = 1674$, то

$$1761t \equiv -186 \pmod 3.$$

Тут $(1761,3) = 3$, $-186 \vdots 3$ і тому остання конгруенція має три розв'язки $t \equiv 0; 1; 2 \pmod 3$. Отже, дістаємо ще три розв'язки конгруенції (10):

$$x \equiv 4; 13; 22 \pmod{27}. \qquad (12)$$

У класі $x \equiv 7 \pmod 9$ знаходимо числа $x = 9t + 7$, де t задовольняє конгруенцію

$$f'(7) \cdot t \equiv -\frac{f(7)}{9} \pmod 3.$$

Оскільки $f'(7) = 13\,476$, $f(7) = 20\,250$, то

$$13\,476t \equiv -2250 \pmod 3.$$

Тут $(13\,476,3) = 3$ і $-2250 \vdots 3$ і тому остання конгруенція має три розв'язки $t \equiv 0, 1, 2 \pmod 3$.
Відповідно до цього, маємо останні три розв'язки конгруенції (10):

$$x \equiv 7; 16; 25 \pmod{27}. \qquad (13)$$

Таким чином, щоб знайти розв'язки конгруенції (1), треба розв'язати сім систем:

$$1)\begin{cases} x \equiv 2 \pmod 4, \\ x \equiv 4 \pmod{27}; \end{cases} \qquad 4)\begin{cases} x \equiv 2 \pmod 4, \\ x \equiv 16 \pmod{27}; \end{cases}$$

$$2)\begin{cases} x \equiv 2 \pmod 4, \\ x \equiv 7 \pmod{27}; \end{cases} \qquad 5)\begin{cases} x \equiv 2 \pmod 4, \\ x \equiv 21 \pmod{27}; \end{cases}$$

$$3)\begin{cases} x \equiv 2 \pmod 4, \\ x \equiv 13 \pmod{27}; \end{cases} \qquad 6)\begin{cases} x \equiv 2 \pmod 4, \\ x \equiv 22 \pmod{27}; \end{cases}$$

$$7)\begin{cases} x \equiv 2 \pmod 4, \\ x \equiv 25 \pmod{27}. \end{cases}$$

Розв'язуючи ці системи, знаходимо:
1) $x \equiv 58 \pmod{108}$; 2) $x \equiv 34 \pmod{108}$; 3) $x \equiv 94 \pmod{108}$; 4) $x \equiv 70 \pmod{108}$; 5) $x \equiv 102 \pmod{108}$; 6) $x \equiv 22 \pmod{108}$; 7) $x \equiv 106 \pmod{108}$.
Отже, конгруенція (1) має сім розв'язків: $x \equiv 22; 34; 58; 70; 94; 102; 106 \pmod{108}$.

Задачі

15.1. Знайти конгруенції того самого степеня із старшим коефіцієнтом 1, еквівалентні таким конгруенціям:
а) $3x^3 - 5x^2 - 2 \equiv 0 \pmod{11}$;
б) $27x^3 + 14x^2 - 10x + 13 \equiv 0 \pmod{59}$;

в) $70x^6 + 78x^5 + 25x^4 + 68x^3 + 52x^2 + 4x + 3 \equiv 0 \pmod{101}$;
г) $a_0x^n + a_1x^{n-1} + \ldots + a_{n-1}x + a_n \equiv 0 \pmod m$, $(a_0, m) = 1$.

15.2. Звести задані конгруенції до еквівалентних їм конгруенцій, степінь яких менше за модуль:
а) $x^8 + 2x^7 + x^5 - x^4 - x + 3 \equiv 0 \pmod 5$;
б) $3x^{14} + 4x^{13} + 3x^{12} + 2x^{11} + x^9 + 2x^8 + 4x^7 + x^6 + 3x^4 + x^3 + 4x^2 + 2x \equiv 0 \pmod 5$;
в) $x^{16} + 3x^8 - 5x^7 - x^4 + 6x - 2 \equiv 0 \pmod 7$;
г) $2x^{17} + 6x^{16} + x^{14} + 5x^{12} + 3x^{11} + 2x^{10} + x^9 + 5x^8 + 2x^7 + 3x^5 + 4x^4 + 6x^3 + 4x^2 + x + 4 \equiv 0 \pmod 7$;
д) $6x^{18} + 18x^{15} + 3x^4 - 8x^3 + x^2 + 3 \equiv 0 \pmod{11}$.

15.3. Спростити задані конгруенції (понизити степені, зменшити коефіцієнти за абсолютною величиною, зробити так, щоб старший коефіцієнт дорівнював 1) і розв'язати способом підбору:
а) $x^5 + x^3 + x^2 + 4 \equiv 0 \pmod 3$;
б) $6x^4 + 17x^2 - 16 \equiv 0 \pmod 3$;
в) $28x^9 + 29x^8 - 26x^7 + 20x^4 - 17x + 23 \equiv 0 \pmod 3$;
г) $x^5 + 2x^4 - 2x^3 - 2x^2 + 2x - 1 \equiv 0 \pmod 3$;
д) $x^5 + x^4 - x^2 - 5x + 1 \equiv 0 \pmod 3$;
е) $x^7 + 2x^6 + x^5 + 4x^3 - 2x^2 - 4x + 2 \equiv 0 \pmod 5$;
є) $x^7 + 3x^6 + x^5 - x^3 - 3x^2 - 4x + 4 \equiv 0 \pmod 5$;
ж) $x^7 + 5x^5 - x^3 - 9x + 3 \equiv 0 \pmod 5$;
з) $34x^{10} - 29x^7 + 43x^4 - 19x + 37 \equiv 0 \pmod 5$;
к) $6x^{10} - 12x + 1 \equiv 0 \pmod 5$;
л) $x^7 - 3x^6 + x^5 - 15x^4 - x^3 + 4x^2 - 4x + 2 \equiv 0 \pmod 5$.

15.4. Спростити задані конгруенції і розв'язати їх способом підбору:
а) $5x^{24} + 4x^{23} + 4x^{22} + 2x^{21} + x^{20} + 6x^{19} + 4x^{18} + 3x^{17} + 4x^{16} + 6x^{15} + 5x^{14} + 2x^{13} + x^{12} + 2x^{11} + x^{10} + 3x^9 + 4x^8 + 2x^7 + 5x^6 + 6x^5 + 5x^4 + 3x^3 + 4x^2 + 4x + 2 \equiv 0 \pmod 7$;
б) $x^{13} - x^{11} + x^9 - x^7 + x^5 + x^3 + x + 1 \equiv 0 \pmod 7$;
в) $10x^{42} - 5x^{30} + 10x^{18} + 9x^{12} + 4 \equiv 0 \pmod 7$;
г) $75x^{13} - 62x^{12} - 53x^{11} - 24x^6 + 13x - 27 \equiv 0 \pmod 7$;
д) $6x^{13} - 3x^{12} - 2x^{11} - 6x^3 + 3x^2 + 7x + 2 \equiv 0 \pmod{11}$;
е) $13x^{23} - 30x^{22} - 2x^{13} + 1 \equiv 0 \pmod{11}$;
є) $120x^{91} + 14x^{15} + x^{11} - 3x^5 + 9x^2 - x + 6 \equiv 0 \pmod{11}$;
ж) $x^{14} - x^{13} + 12x^2 + 2x + 1 \equiv 0 \pmod{13}$;
з) $300x^{90} + 259x^{67} - 95x^{23} - 1 \equiv 0 \pmod{23}$.

15.5. Розкласти конгруенції на лінійні множники за заданим модулем:
а) $x^3 + 4x^2 - 3 \equiv 0 \pmod 5$;
б) $x^3 - 2x + 1 \equiv 0 \pmod 5$;
в) $x^4 - 20x^3 + 90x^2 - 135x + 54 \equiv 0 \pmod 5$;
г) $3x^3 + 2x^2 - 2x - 3 \equiv 0 \pmod 5$;
д) $x^4 - 12x^3 + 46x^2 - 53x - 12 \equiv 0 \pmod 7$;
е) $5x^3 + 4x^2 - 8x - 1 \equiv 0 \pmod 7$;
є) $6x^3 + 5x^2 - 2x - 9 \equiv 0 \pmod{11}$;
ж) $x^3 + 3x^2 - 3 \equiv 0 \pmod{17}$;
з) $x^3 + 11x^2 + 8x + 3 \equiv 0 \pmod{23}$;
к) $x^4 + 15x^3 + 4x^2 + 4x - 15 \equiv 0 \pmod{29}$;

л) $x^3 - 13x^2 - 3x + 11 \equiv 0 \pmod{31}$.

15.6. Довести, що:

а) конгруенція $x^3 + ax + b \equiv 0 \pmod 7$ при $(a, 7) = (b, 7) = 1$ не має трьох розв'язків;

б) $(p-2)! \equiv 1 \pmod p$, якщо p — просте число;

в) $2(p-3)! + 1 \equiv 0 \pmod p$, якщо p — просте число;

г) числа p і $p+2$ є простими (тобто простими числами-близнюками) тоді і тільки тоді, коли $4[(p-1)! + 1] + p \equiv 0 \pmod{p(p+2)}$ (**теорема Клемента**);

д) $[(2n)!]^2 \equiv -1 \pmod p$, якщо p — просте число і $p = 4n + 1$, $n \in \mathbf{N}$;

е) $[(2n+1)!]^2 \equiv 1 \pmod p$, якщо p — просте число і $p = 4n + 3$, $n \in \mathbf{N}$;

є) $a^p + (p-1)!\,a \equiv 0 \pmod p$, якщо a — довільне ціле число і p — просте число;

ж) натуральне число $p > 2$ є простим тоді і тільки тоді, коли $(p-2)! - 1 \equiv 0 \pmod p$ (**критерій Лейбніца**).

15.7. Розв'язати такі конгруенції:

а) $x^2 - 3x + 2 \equiv 0 \pmod 6$;

б) $x^4 + 2x^3 - x^2 - x - 1 \equiv 0 \pmod 6$;

в) $3x^3 - x^2 + 4x + 2 \equiv 0 \pmod{10}$;

г) $2x^5 + x^3 + 2x \equiv 0 \pmod{10}$;

д) $x^6 - x^5 - x^2 + 4x - 1 \equiv 0 \pmod{10}$;

е) $x^8 + 5x^6 - x^5 - x^4 - 5x^2 + 8x - 3 \equiv 0 \pmod{15}$;

є) $x^6 + 3x^5 - x^2 - x - 7 \equiv 0 \pmod{15}$;

ж) $3x^3 + 6x^2 + x + 10 \equiv 0 \pmod{15}$;

з) $x^9 + x^7 - x^3 + 4x + 1 \equiv 0 \pmod{21}$;

к) $3x^2 + 7x + 5 \equiv 0 \pmod{34}$;

л) $x^7 + x^2 \equiv 0 \pmod{35}$;

м) $2x^2 - 7x + 6 \equiv 0 \pmod{55}$.

15.8. Розв'язати такі конгруенції:

а) $6x^3 + 27x^2 + 17x + 20 \equiv 0 \pmod{30}$;

б) $4x^3 - 5x^2 + 7x + 21 \equiv 0 \pmod{105}$.

15.9. Розв'язати такі конгруенції:

а) $x^6 + x^5 - x^2 + 2x + 2 \equiv 0 \pmod{25}$;

б) $x^6 - x^5 - x^2 + 4x + 2 \equiv 0 \pmod{25}$;

в) $x^4 - 4x^3 + 2x^2 + x + 6 \equiv 0 \pmod{25}$;

г) $5x^3 + 3x + 1 \equiv 0 \pmod{25}$;

д) $3x^3 - 5x^2 - 15 \equiv 0 \pmod{49}$;

е) $3x^4 - 2x^2 + 3x + 1 \equiv 0 \pmod{49}$;

є) $5x^3 + 4x^2 - 6x + 5 \equiv 0 \pmod{49}$;

ж) $x^9 - 2x^7 - x^3 + 7x + 2 \equiv 0 \pmod{49}$;

з) $x^2 + 3x + 5 \equiv 0 \pmod{121}$.

15.10. Розв'язати такі конгруенції:

а) $4x^3 - 8x - 13 \equiv 0 \pmod{27}$;

б) $x^5 + 2x^4 + 3x^3 + x^2 + x + 1 \equiv 0 \pmod{27}$;

в) $x^4 + 7x + 4 \equiv 0 \pmod{27}$;

г) $7x^4 + 19x + 25 \equiv 0 \pmod{27}$;

д) $9x^2 + 29x + 62 \equiv 0 \pmod{64}$;

е) $x^3 - 2x^2 - 30x + 41 \equiv 0 \pmod{125}$;

є) $x^3 + 2x + 2 \equiv 0 \pmod{125}$;

ж) $6x^3 - 7x - 11 \equiv 0 \pmod{125}$;

з) $3x^3 - 7x - 69 \equiv 0 \pmod{125}$;

к) $x^4 + 4x^3 + 2x^2 + 2x + 12 \equiv 0 \pmod{625}$.

15.11. Розв'язати такі конгруенції:

а) $x^5 - 7x^4 + 11x^3 - 5x + 1 \equiv 0 \pmod{12}$;

б) $x^5 - x^4 + 2x^3 - x^2 + 5x - 2 \equiv 0 \pmod{12}$;

в) $x^5 - 2x^3 + 5x - 2 \equiv 0 \pmod{18}$;

г) $x^5 + 2x^5 - x^2 + x + 4 \equiv 0 \pmod{40}$;

д) $x^8 - x^6 + x^3 + x + 3 \equiv 0 \pmod{45}$;

е) $x^4 + 3x^3 + 2x + 6 \equiv 0 \pmod{45}$;

є) $x^4 + 4x^3 + 2x^2 + x + 12 \equiv 0 \pmod{45}$;

ж) $x^4 - 3x^3 - 4x^2 - 2x - 2 \equiv 0 \pmod{50}$;

з) $x^8 + 2x^7 - x^2 + 3x - 2 \equiv 0 \pmod{63}$;

к) $x^2 - 3x + 23 \equiv 0 \pmod{63}$;

л) $x^7 + x^5 - x^3 + 3x - 3 \equiv 0 \pmod{175}$;

м) $2x^3 - 5x - 32 \equiv 0 \pmod{175}$;

н) $31x^4 + 57x^3 + 96x + 191 \equiv 0 \pmod{225}$.

15.12. Знайти необхідну і достатню умову того, що конгруенція $x^n \equiv a \pmod p$, де p — просте число, $(a, p) = 1$, $n < p$, має тільки n розв'язків.

15.13. Які з наступних конгруенцій мають n розв'язків, де n — степінь конгруенції:

а) $x^3 \equiv 1 \pmod 7$;

б) $x^4 \equiv 1 \pmod{11}$;

в) $x^5 \equiv 10 \pmod{11}$?

Знайти ці розв'язки.

15.14. Скільки розв'язків мають конгруенції:

а) $x^6 \equiv 1 \pmod 7$;

б) $x^{p-1} \equiv 1 \pmod p$, де p — просте число;

в) $x^{\varphi(20)} \equiv 1 \pmod{20}$;

г) $x^{\varphi(m)} \equiv 1 \pmod m$;

д) $x^{\frac{p-1}{2}} \equiv 1 \pmod p$, де p — непарне просте число;

е) $x^{\frac{p-1}{2}} \equiv -1 \pmod p$, де p — непарне просте число?

15.15. Довести, що конгруенція $x^n \equiv 1 \pmod p$ має n розв'язків, якщо p — просте число і $p \equiv 1 \pmod n$.

15.16. Конгруенцію $11x^2 \equiv 65 \pmod{103}$ задовольняє число $x_0 = 31$. Знайти всі розв'язки цієї конгруенції.

15.17. Перевірити теорему Вільсона при: а) $p = 5$; б) $p = 7$; в) $p = 11$; г) $p = 13$.

15.18. Довести, що $x^{5p+1} \equiv x^6 \pmod p$, де p — просте число.

15.19. Розв'язати систему конгруенцій:

$$\begin{cases} x^4 + 2x + 1 \equiv 0 \pmod 4; \\ x^3 + 3 \equiv 0 \pmod{10}. \end{cases}$$

§ 16. Конгруенції другого степеня, квадратичні лишки і квадратичні нелишки, символ Лежандра

Література

[1] — § 18, с. 184—192;
[2] — § 18, с. 187—196;
[10] — гл. V, § 1—4, с. 68—80;
[11] — гл. 21, 22, с. 172—200;
[12] — гл. III, § 10, с. 110—124;
[14] — § 25—28, с. 105—136.

ТЕОРЕТИЧНІ ВІДОМОСТІ

Конгруенцію другого степеня виду

$$a_1y^2 + a_2y + a_3 \equiv 0 \pmod{n},\ a_1 \not\equiv 0 \pmod{n} \qquad (1)$$

завжди можна звести до двочленної конгруенції виду

$$x^2 \equiv a \pmod{m}, \qquad (2)$$

де $a = a_2^2 - 4a_1a_3$, $x = 2a_1y + a_2$, $m = 4an$.

Для цього слід обидві частини і модуль конгруенції (1) домножити на $4a$ і зробити відповідні перетворення.

Якщо конгруенція (2) має хоча б один розв'язок, то a називається **квадратичним лишком за модулем** m, у противному разі a називається **квадратичним нелишком за модулем** m. При цьому $(a, m) = 1$.

Розв'язування конгруенції виду (2) за складеним модулем зводиться до розв'язування таких конгруенцій:

1) $x^2 \equiv a \pmod{p}$, де p — непарне просте число; (3)

2) $x^2 \equiv a \pmod{p^\alpha}$, де p — непарне просте число, $\alpha > 1$; (4)

3) $x^2 \equiv a \pmod{2^\alpha}$, де $\alpha \geqslant 1$. (5)

Найбільш важливим є той випадок, коли модуль є непарним простим числом. При цьому досить обмежитися випадком, коли $(a, p) = 1$, оскільки в противному разі конгруенція (3) має єдиний розв'язок $x \equiv 0 \pmod{p}$.

Отже, надалі розглядатимемо таку конгруенцію:

$$x^2 \equiv a \pmod{p},\ (a, p) = 1, \text{ де } p \text{ — просте непарне число.} \qquad (6)$$

Якщо a — квадратичний лишок за модулем p, то конгруенція (6) має два розв'язки.

Для будь-якого простого непарного числа p половина лишків зведеної системи лишків є квадратичними лишками, а половина — квадратичними нелишками.

При простому непарному p число a є квадратичним лишком за модулем p тоді і тільки тоді, коли $a^{\frac{p-1}{2}} \equiv 1 \pmod{p}$, і квадратичним нелишком тоді і тільки тоді, коли $a^{\frac{p-1}{2}} \equiv -1 \pmod{p}$ (**критерій Ейлера**).

Теорема Ейлера. *Добуток двох квадратичних лишків або нелишків є квадратичним лишком за модулем p; добуток квадратичного лишку на нелишок є квадратичним нелишком.*

Добуток ряду чисел $a, b, \ldots, c$ дає квадратичний лишок або нелишок залежно від того, парне чи непарне число нелишків буде серед множників.

Для ефективного використання критерію Ейлера вводиться так званий **символ Лежандра** $\left(\frac{a}{p}\right)$ (читається: «символ Лежандра a відносно p», або коротше «a відносно p», або «a до p»), a називається чисельником, а p — знаменником символу Лежандра.

Символ Лежандра $\left(\frac{a}{p}\right)$ визначається для всіх цілих чисел a, які не діляться на просте непарне число p, рівністю

$$\left(\frac{a}{p}\right) = \begin{cases} 1, & \text{якщо } a \text{ є квадратичним лишком за модулем } p, \\ -1, & \text{якщо } a \text{ є квадратичним нелишком за модулем } p. \end{cases}$$

Критерій Ейлера тоді коротко записується так:

$$a^{\frac{p-1}{2}} \equiv \left(\frac{a}{p}\right) \pmod{p}.$$

Основні властивості символу Лежандра:

1°. Якщо $a \equiv b \pmod{p}$, то $\left(\frac{a}{p}\right) = \left(\frac{b}{p}\right)$;

2°. $\left(\frac{a^2}{p}\right) = 1$;

3°. $\left(\frac{1}{p}\right) = 1$;

4°. $\left(\frac{-1}{p}\right) = (-1)^{\frac{p-1}{2}}$;

5°. $\left(\frac{ab\ldots c}{p}\right) = \left(\frac{a}{p}\right)\left(\frac{b}{p}\right)\ldots\left(\frac{c}{p}\right)$;

6°. $\left(\frac{ab^2}{p}\right) = \left(\frac{a}{p}\right)$;

7°. $\left(\frac{a^n}{p}\right) = \left(\frac{a}{p}\right)^n$;

8°. $\left(\frac{2}{p}\right) = (-1)^{\frac{p^2-1}{8}}$;

9°. Якщо p і q — різні непарні прості числа, то

$$\left(\frac{q}{p}\right) = \left(\frac{p}{q}\right) \cdot (-1)^{\frac{p-1}{2} \cdot \frac{q-1}{2}}$$

(закон взаємності квадратичних лишків).

Узагальненням символу Лежандра є **символ Якобі** $\left(\frac{a}{m}\right)$ (читається: «символ Якобі a відносно m»). Він визначається для будь-яких непарних натуральних чисел $m > 1$ і чисел a, взаємно простих з m, рівністю

$$\left(\frac{a}{m}\right) = \left(\frac{a}{p}\right)\left(\frac{a}{q}\right)\ldots\left(\frac{a}{r}\right),$$

де $m = p \cdot q \ldots r$ є розкладом m на прості множники (серед них можуть бути і рівні), тобто як добуток символів Лежандра. Для символу Якобі зберігаються властивості 1) — 9) символу Лежандра, проте для символу Якобі йдеться не про непарні прості числа p, а про непарні натуральні числа $m > 1$, для властивості 9) — про взаємно прості непарні числа, відмінні від 1. Тому при визначенні символу Лежандра зручно розглядати його як символ Якобі. При цьому часто немає потреби виділяти з чисельника символу його непарні прості множники.

Конгруенція $x^2 \equiv a \pmod{p^n}$, де p — непарне просте число, $n > 1$, $(a, p) = 1$, має два розв'язки, якщо $\left(\frac{a}{p}\right) = 1$, і не має їх зовсім, якщо $\left(\frac{a}{p}\right) = -1$.

Для конгруенції $x^2 \equiv a \pmod{2^\alpha}$, $(a, 2) = 1$, необхідними умовами існування розв'язків є $a \equiv 1 \pmod{4}$ при $\alpha = 2$; $a \equiv 1 \pmod{8}$ при $\alpha \geqslant 3$.

Якщо ці умови виконуються, то існує один розв'язок при $\alpha = 1$; два розв'язки при $\alpha = 2$ і чотири розв'язки при $\alpha \geqslant 3$.

Для конгруенції загального виду $x^2 \equiv a \pmod m$, $m = 2^\alpha p_1^{\alpha_1} p_2^{\alpha_2} \dots p_k^{\alpha_k}$, $(a, m) = 1$, необхідними і достатніми умовами існування розв'язків є: $a \equiv 1 \pmod 4$ при $\alpha = 2$; $a \equiv 1 \pmod 8$ при $\alpha \geqslant 3$

$$\left(\frac{a}{p_1}\right) = \left(\frac{a}{p_2}\right) = \dots = \left(\frac{a}{p_k}\right) = 1.$$

Якщо жодну з цих умов не порушено, то число розв'язків дорівнюватиме:

2^k — при $\alpha = 0$ і $\alpha = 1$; 2^{k+1} — при $\alpha = 2$; 2^{k+2} — при $\alpha \geqslant 3$.

ПРИКЛАДИ РОЗВ'ЯЗУВАННЯ ЗАДАЧ

1. Звести конгруенцію другого степеня $4x^2 - 11x - 3 \equiv 0 \pmod{13}$ до двочленної.

Розв'язання. Для простого модуля старший коефіцієнт взаємно простий з ним. Тоді процес зведення заданої конгруенції до двочленної можна скоротити і навіть залишити модуль незмінним. Визначимо множник k так, щоб $4k \equiv 1 \pmod{13}$. Матимемо $k \equiv 10 \pmod{13}$. Домножаючи обидві частини заданої конгруенції на 10 за модулем 13, дістаємо

$$40x^2 - 110x - 30 \equiv 0 \pmod{13},$$

або

$$x^2 - 6x - 4 \equiv 0 \pmod{13}. \qquad (1)$$

Виділимо в лівій частині цієї конгруенції повний квадрат

$$x^2 - 2 \cdot 3x + 9 - 9 - 4 \equiv 0 \pmod{13},$$

або

$$(x-3)^2 - 13 \equiv 0 \pmod{13}.$$

Остаточно

$$(x-3)^2 \equiv 0 \pmod{13}.$$

Зауваження

1. При розв'язуванні задач такого типу треба намагатися спростити процес виділення повного квадрату, для цього є різні способи. Зокрема, у розглянутому прикладі від заданої конгруенції можна було б перейти до такої конгруенції:

$$4x^2 - 24x - 16 \equiv 0 \pmod{13}. \qquad (2)$$

Оскільки $(4, 13) = 1$, то на 4 можна скоротити обидві частини конгруенції (2):

$$x^2 - 6x - 4 \equiv 0 \pmod{13}.$$

Дістали конгруенцію (1).

2. Часто процес зведення конгруенції до двочленної завершується простим розв'язанням її. Так,

$$x - 3 \equiv 0 \pmod{13}, \text{ або } x \equiv 3 \pmod{13}.$$

2. Скільки розв'язків має конгруенція $x^2 \equiv 219 \pmod{383}$?

Розв'язання. Знайдемо символ Лежандра $\left(\frac{219}{383}\right)$. Оскільки $219 = 3 \cdot 73$, а 383 — просте число, то, згідно з властивістю 5,

$$\left(\frac{219}{383}\right) = \left(\frac{3}{383}\right) \cdot \left(\frac{73}{383}\right).$$

Обчислимо окремо символи Лежандра $\left(\frac{3}{383}\right)$ і $\left(\frac{73}{383}\right)$. Оскільки 3 і 383 — різні прості непарні числа, то внаслідок закону взаємності 9) дістаємо

$$\left(\frac{3}{383}\right) = \left(\frac{383}{3}\right) \cdot (-1)^{\frac{383-1}{2} \cdot \frac{3-1}{2}} = -\left(\frac{383}{3}\right).$$

За властивістю 1) маємо

$$\left(\frac{383}{3}\right) = \left(\frac{2}{3}\right),$$

бо $383 \equiv 2 \pmod 3$.

За властивістю 8)

$$\left(\frac{2}{3}\right) = (-1)^{\frac{3^2-1}{8}} = -1.$$

Отже, $\left(\frac{3}{383}\right) = -(-1) = 1$. Щоб спростити запис, а також полегшити процес перевірки, доцільно при кожному переході під знаком рівності ставити номер властивості, на основі якої відбувається цей перехід. Наприклад,

$$\left(\frac{73}{383}\right) \underset{9}{=} \left(\frac{383}{73}\right) \cdot (-1)^{\frac{383-1}{2} \cdot \frac{73-1}{2}} = \left(\frac{383}{73}\right) \underset{1}{=} \left(\frac{18}{73}\right) =$$

$$= \left(\frac{2 \cdot 3^2}{73}\right) \underset{6}{=} \left(\frac{2}{73}\right) \underset{8}{=} (-1)^{\frac{73^2-1}{8}} = 1.$$

Остаточно

$$\left(\frac{219}{383}\right) = \left(\frac{3}{383}\right) \cdot \left(\frac{73}{383}\right) = 1 \cdot 1 = 1.$$

Таким чином, задана конгруенція має два розв'язки.

Зауваження

1. Слід уважно застосовувати властивість 9), оскільки якщо хоч одне з чисел p чи q є складеним, застосування цієї властивості може призвести до помилок в обчисленні символу Лежандра.

2. Розглядаючи символ Лежандра як окремий випадок символу Якобі і користуючись властивостями останнього, можна символ Лежандра обчислити швидше. Наприклад,

$$\left(\frac{219}{383}\right) \underset{9}{=} \left(\frac{383}{219}\right) \cdot (-1)^{\frac{383-1}{2} \cdot \frac{219-1}{2}} = -\left(\frac{383}{219}\right) \underset{1}{=} \left(\frac{164}{219}\right) =$$

$$= \left(\frac{41 \cdot 2^2}{219}\right) \underset{6}{=} -\left(\frac{41}{219}\right) \underset{9}{=} -\left(\frac{219}{41}\right) \cdot (-1)^{\frac{219-1}{2} \cdot \frac{41-1}{2}} =$$

$$= -\left(\frac{219}{41}\right) \underset{1}{=} -\left(\frac{14}{41}\right) \underset{6}{=} -\left(\frac{2}{41}\right)\left(\frac{7}{41}\right) \underset{8}{=} (-1)^{\frac{41^2-1}{8}} \left(\frac{7}{41}\right) =$$

$$= -\left(\frac{7}{41}\right) \underset{9}{=} -\left(\frac{41}{7}\right)(-1)^{\frac{41-1}{2} \cdot \frac{7-1}{2}} = -\left(\frac{41}{7}\right) \underset{1}{=} -\left(\frac{-1}{7}\right) \underset{4}{=} -(-1)^{\frac{7-1}{2}} = 1.$$

3. Зауважимо, що коли p — просте непарне число, то символ Лежандра $\left(\frac{a}{p}\right)$ є для конгруенції $x^2 \equiv a \pmod p$ символом Якобі $\left(\frac{a}{p}\right)$ і навпаки. Тому для

конгруенцій за простим модулем можна не розрізняти символів Лежандра і Якобі, що дає змогу при обчисленні символів Лежандра не розкладати чисельник на прості множники. Треба тільки виділяти множники, що дорівнюють 2. Якщо $\left(\frac{a}{p}\right)=1$, то ця конгруенція має два розв'язки; якщо $\left(\frac{a}{p}\right)=-1$, конгруенція розв'язків не має. Для конгруенції $x^2\equiv a \pmod m$, де m — непарне складене число, символ Лежандра не існує, а символ Якобі існує. Проте, якщо символ Якобі $\left(\frac{a}{m}\right)=1$ і m — непарне складене число, то це ще не означає, що конгруенція $x^2\equiv a \pmod m$ має розв'язки. Так, конгруенція $x^2\equiv 2 \pmod{15}$ розв'язків не має, а символ Якобі для неї $\left(\frac{2}{15}\right)=\left(\frac{2}{3}\right)\left(\frac{2}{5}\right)=(-1)^{\frac{15^2-1}{8}}=1$.

Задачі

16.1. Розв'язати конгруенції, звівши їх до двочленних
а) $3x^2-5x-7\equiv 0 \pmod 5$;
б) $3x^2-x\equiv 0 \pmod 5$;
в) $2x^2+4x-1\equiv 0 \pmod 5$;
г) $2x^2-4x-5\equiv 0 \pmod 7$;
д) $2x^2+5x-1\equiv 0 \pmod 7$;
е) $3x^2+2x\equiv 1 \pmod 7$;
є) $4x^2\equiv 7x+3 \pmod{11}$;
ж) $5x^2+7x+1\equiv 0 \pmod{13}$;
з) $4x^2-11x-3\equiv 0 \pmod{13}$.

16.2. Розв'язати задані конгруенції, звівши їх до двочленних:
а) $3x^2+6x+1\equiv 0 \pmod{10}$;
б) $4x^2+3x+3\equiv 0 \pmod{15}$;
в) $3x^2+7x+8\equiv 0 \pmod{17}$;
г) $6x^2+3x+1\equiv 0 \pmod{17}$;
д) $3x^2+13x-10\equiv 0 \pmod{19}$;
е) $12x^2-6x-7\equiv 0 \pmod{19}$;
є) $7x^2+15x-11\equiv 0 \pmod{23}$;
ж) $x^2-5x+6\equiv 0 \pmod{24}$;
з) $12x^2-8x-15\equiv 0 \pmod{44}$.

16.3. Користуючись критерієм Ейлера, знайти всі квадратичні лишки за модулями: а) 5; б) 7; в) 11; г) 13; д) 17; е) 23; є) 37; ж) 53.

16.4. Розв'язати способом проб такі конгруенції:
а) $x^2\equiv 2 \pmod 7$;
б) $x^2\equiv 4 \pmod 7$;
в) $x^2\equiv 3 \pmod 7$.

16.5. Обчислити символи Лежандра:
а) $\left(\frac{13}{7}\right)$; б) $\left(\frac{22}{13}\right)$; в) $\left(\frac{19}{67}\right)$; г) $\left(\frac{37}{67}\right)$; д) $\left(\frac{56}{73}\right)$; е) $\left(\frac{47}{73}\right)$;
є) $\left(\frac{54}{83}\right)$; ж) $\left(\frac{68}{113}\right)$; з) $\left(\frac{63}{131}\right)$.

16.6. Користуючись символом Якобі, обчислити символи Лежандра:
а) $\left(\frac{283}{563}\right)$; б) $\left(\frac{251}{577}\right)$; в) $\left(\frac{241}{593}\right)$; г) $\left(\frac{323}{607}\right)$; д) $\left(\frac{346}{643}\right)$; е) $\left(\frac{3153}{1201}\right)$;
є) $\left(\frac{20\,470}{1847}\right)$; ж) $\left(\frac{2108}{2003}\right)$; з) $\left(\frac{3149}{5987}\right)$.

16.7. Знайти кількість розв'язків таких конгруенцій:
а) $x^2\equiv 3 \pmod{31}$;
б) $x^2\equiv 2 \pmod{31}$;
в) $x^2\equiv 5 \pmod{73}$;
г) $x^2\equiv 3 \pmod{101}$;
д) $x^2\equiv 226 \pmod{563}$;
е) $x^2\equiv 429 \pmod{563}$;
є) $x^2\equiv 579 \pmod{821}$;
ж) $x^2\equiv 728 \pmod{919}$;
з) $x^2\equiv 847 \pmod{1087}$;
к) $x^2\equiv 3766 \pmod{5987}$.

16.8. Знайти x, якщо:
а) $\left(\frac{x}{3}\right)=1$; б) $\left(\frac{x}{5}\right)=1$; в) $\left(\frac{x}{7}\right)=1$; г) $\left(\frac{x}{11}\right)=1$; д) $\left(\frac{x}{15}\right)=1$;
е) $\left(\frac{x}{15}\right)=-1$.

16.9. Довести, що:
а) конгруенція $x^2\equiv a \pmod p$ має розв'язки

$$x\equiv a^{k+1},\quad p=a^{k+1} \pmod p,$$

якщо p — просте число виду $4k+3$, а число a — квадратичний лишок за модулем p;
б) конгруенція $x^2\equiv a \pmod p$ має розв'язки

$$x\equiv a^{k+1}\cdot 2^{(2k+1)t} \pmod p,$$

де $t=0$ при $a^{2k+1}\equiv 1 \pmod p$ і $t=1$ при $a^{2k+1}\equiv -1 \pmod p$, якщо p — просте число виду $8k+5$ і a — квадратичний лишок за модулем p;
в) рівняння $11y=5x^2-7$ не виконується при жодних цілих числах x і y;
г) при діленні добутку двох послідовних цілих чисел на число 13 остача ніколи не дорівнює 1;
д) $2^{\frac{p-1}{2}}\equiv\begin{cases}1 \pmod p, & \text{якщо } p \text{ — просте число виду } 8k+7,\\ -1 \pmod p, & \text{якщо } p \text{ — просте число виду } 8k+3,\end{cases}$
е) $\left(\frac{a}{p}\right)\left(\frac{-a}{p}\right)=\begin{cases}1, & \text{якщо } p \text{ — просте число виду } 4k+1,\\ -1, & \text{якщо } p \text{ — просте число виду } 4k+3;\end{cases}$
є) $\left(\frac{3}{p}\right)=\begin{cases}1, & \text{якщо } p \text{ — просте число виду } 12k+1 \text{ або } 12k+11,\\ -1, & \text{якщо } p \text{ — просте число виду } 12k+5 \text{ або } 12k+7;\end{cases}$
ж) конгруенція $x^2\equiv a \pmod{16}$, $a\equiv 1 \pmod 8$ має розв'язки: $x\equiv x_0,\ 16-x_0,\ x_0+8,\ 8-x_0 \pmod{16}$, де x_0 — один з розв'язків заданої конгруенції; аналогічно за модулем 2^α, $\alpha>4$,

$$x\equiv x_0,\ 2^\alpha-x_0,\ x_0+2^{\alpha-1},\ 2^{\alpha-1}-x_0 \pmod{2^\alpha}.$$

16.10. Використовуючи результати задач 16,9, а), б), розв'язати конгруенції:
а) $x^2\equiv 2 \pmod{311}$;
б) $x^2\equiv 3 \pmod{47}$;
в) $x^2\equiv 7 \pmod{29}$;
г) $x^2\equiv 3 \pmod{37}$.

16.11. Чи проходять через точки з цілими координатами такі параболи:
а) $43y=x^2-42$;
б) $73y=x^2-37$;
в) $83y=x^2-34$;
г) $443y=x^2-152$?

16.12. Розв'язати в цілих числах рівняння:
а) $4x^2-5y-6=0$;
б) $15x^2-7y^2-9=0$;
в) $5x^2-11y-7=0$;
г) $x^2-10x-11y+5=0$;
д) $x^2-21x-13y+110=0$.

16.13. Довести, що:
а) розв'язки конгруенції $x^2+1\equiv 0 \pmod p$, де p — просте число виду $4m+1$, мають вид $x=1\cdot 2\ldots 2m$; $p-1\cdot 2\ldots 2m \pmod p$;
б) конгруенція $x^2+1\equiv 0 \pmod p$ має розв'язки тоді і тільки тоді, коли p — просте число виду $4m+1$;

в) конгруенція $x^2 + 2 \equiv 0 \pmod p$ має розв'язки тоді і тільки тоді, коли p — просте число виду $8m + 1$ або $8m + 3$;

г) конгруенція $x^2 + 3 \equiv 0 \pmod p$ має розв'язки тоді і тільки тоді, коли p — просте число виду $6m + 1$;

д) множина простих чисел виду $4m + 1$ нескінченна;

е) множина простих чисел виду $6m + 1$ нескінченна;

є) канонічний розклад числа виду $a^2 + b^2$, де $(a, b) = 1$, містить тільки прості числа виду $4m + 1$;

ж) незалежно від простого непарного модуля p конгруенції

$$(x^2 - 13)(x^2 - 17)(x^2 - 221) \equiv 0 \pmod p,$$

$$(x^2 - 3)(x^2 - 5)(x^2 - 7)(x^2 - 11)(x^2 - 1155) \equiv 0 \pmod p$$

мають завжди хоч один розв'язок;

з) конгруенція $x^2 \equiv -7 \pmod{p^\alpha}$, де p — непарне просте число виду $7n + 1$, має розв'язки при будь-якому натуральному α;

к) конгруенція $x^2 \equiv -11 \pmod{4p}$, де p — непарне просте число виду $11n + 2$, не має розв'язків;

л) для будь-якого натурального n число $1 + 2 + \ldots + n$ не може закінчуватися цифрою 7.

16.14. Використовуючи результат задачі 16.9, ж), розв'язати такі конгруенції:

а) $x^2 \equiv 9 \pmod{16}$;
б) $x^2 \equiv 17 \pmod{32}$;
в) $x^2 \equiv 25 \pmod{32}$;
г) $x^2 \equiv 41 \pmod{64}$;
д) $x^2 \equiv 57 \pmod{64}$;
е) $x^2 \equiv 65 \pmod{128}$;
є) $x^2 \equiv 73 \pmod{128}$;
ж) $x^2 \equiv 145 \pmod{256}$.

16.15. Розв'язати конгруенції:

а) $x^2 \equiv 7 \pmod{27}$;
б) $x^2 \equiv 59 \pmod{125}$;
в) $x^2 \equiv 91 \pmod{243}$;
г) $x^2 - 3x + 2 \equiv 0 \pmod{400}$.

16.16. Довести, що:

а) $\left(\frac{-6}{p}\right) = \begin{cases} 1, & \text{якщо } p \text{ — просте число і } p \equiv 1, 5, 7, 11 \pmod{24}, \\ -1, & \text{якщо } p \text{ — просте число і } p \equiv 13, 17, 19, 23 \pmod{24}; \end{cases}$

б) $\left(\frac{ab}{p}\right) = (-1)^{\frac{p-1}{2}}$, якщо p — непарний простий дільник числа $ax^2 + by^2$, де a, b, x, y — цілі числа і $(ax, by) = 1$;

в) $10\,541 = 83 \cdot 127$, якщо $10\,541 = 3 \cdot 59^2 + 2 \cdot 7^2$;

г) непарні прості дільники p чисел виду $x^2 + 2y^2$ при $(x, y) = 1$ мають вид $p = 8n + 1$, $p = 8n + 3$;

д) непарні прості дільники p чисел виду $2x^2 - y$ і $x^2 - 2y^2$ при $(x, y) = 1$ мають вид $p = 8n + 1$, $p = 8n + 7$.

§ 17. Порядок числа і класу лишків за модулем. Первісні корені, існування їх та кількість за простим модулем

Література

[1] — § 19, с. 193—201;
[2] — § 19, с. 196—204;
[3] — гл. 12, § 5, с. 413—416;
[10] — гл. VI, § 1—3, с. 86—90;
[11] — гл. 17, 18, с. 139—152;
[12] — гл. IV, § 1, 2, с. 125—136;
[14] — § 29, 30, с. 137—144.

ТЕОРЕТИЧНІ ВІДОМОСТІ

Нехай $a \in \mathbf{Z}$, $m \in \mathbf{N}$ і $(a, m) = 1$. **Порядком числа a за модулем m** називається таке найменше натуральне число δ, що $a^\delta \equiv 1 \pmod m$. Число δ позначають ще як $\delta = P_m(a)$ і називають **показником**, до якого належить число a за модулем m. Оскільки за теоремою Ейлера $a^{\varphi(m)} \equiv 1 \pmod m$, то число δ завжди існує і $\delta \leqslant \varphi(m)$. Якщо $\delta = \varphi(m)$, то число a називають **первісним коренем за модулем m**.

Якщо $a \equiv b \pmod m$, то $P_m(a) = P_m(b)$. Ця властивість дає змогу казати про порядок класу лишків, а саме: **клас лишків $K_a^{(m)}$ має порядок δ за модулем m**, якщо порядок його представника за цим самим модулем дорівнює δ.

Якщо $\delta = \varphi(m)$, то клас лишків називається **класом первісних коренів за модулем m**.

Якщо $\delta = P_m(a)$, то числа $1 = a^0, a^1, a^2, \ldots, a^{\delta-1}$ попарно неконгруентні між собою за модулем m.

Якщо a — первісний корінь за модулем m, тобто $P_m(a) = \varphi(m)$, то числа $1 = a^0, a^1, a^2, \ldots, a^{\varphi(m)-1}$ утворюють зведену систему лишків за модулем m.

Якщо $P_m(a) = \delta$, то $a^k \equiv a^l \pmod m$ тоді і тільки тоді, коли $k \equiv l \pmod \delta$. Зокрема, $a^k \equiv 1 \pmod m$ тоді і тільки тоді, коли $k \vdots \delta$.

Якщо $P_m(a) = \delta$ і $a^k \equiv 1 \pmod m$, то $k \vdots \delta$.

Якщо $P_m(a) = \delta$, то $\varphi(m) \vdots \delta$.

Якщо $(P_m(a), P_m(b)) = 1$, то $P_m(a \cdot b) = P_m(a) \cdot P_m(b)$.

Якщо $P_m(x) = ab$, то $P_m(x^a) = b$.

Якщо $P_m(a), P_m(b), \ldots, P_m(c)$ — попарно взаємно прості числа, то $P_m(ab \ldots c) = P_m(a) P_m(b) \ldots P_m(c)$. $P_m(a^s) = P_m(a)$ тоді і тільки тоді, коли $(s, P_m(a)) = 1$.

$$P_m(a^k) = \frac{P_m(a)}{(P_m(a), k)}.$$

Якщо $P_m(a) = k$, то класи лишків $K_a^{(m)}, K_{a^2}^{(m)}, \ldots, K_{a^k}^{(m)}$ є різними розв'язками конгруенції $x^k \equiv 1 \pmod m$.

Якщо m — просте число, то зазначені класи лишків вичерпують усі розв'язки даної конгруенції.

За простим модулем p кожен дільник d числа $p-1$ є порядком для $\varphi(d)$ класів лишків. Зокрема, *існує* $\varphi(p-1)$ *класів первісних коренів* (**теорема Гаусса**).

Якщо g — первісний корінь за простим модулем p, то інші первісні корені містяться серед степенів $g^2, g^3, \ldots, g^{p-1}$ і мають вигляд g^k, де $(k, p-1) = 1$ і $k < p - 1$.

Якщо $p - 1 = q_1^{k_1} q_2^{k_2} \ldots q_s^{k_s}$ — канонічний розклад числа $p - 1$, то число g тоді і тільки тоді є первісним коренем за простим модулем p, коли

$$g^{\frac{p-1}{q_i}} \not\equiv 1 \pmod p$$

для всіх $i = 1, 2, \ldots, s$.

Первісні корені існують тільки за модулями $m = 2, 4, p^\alpha$ і $2p^\alpha$, де p — просте непарне число, а $\alpha \geqslant 1$.

Нехай g — первісний корінь за простим модулем p. Тоді можна знайти таке число t, що число u, яке визначається з умови

$$(g + pt)^{p-1} = 1 + p^u,$$

не ділиться на p. Відповідне число $g + pt$ є первісним коренем за модулем p^α при будь-якому $\alpha > 1$.

Нехай $\alpha \geqslant 1$ і g — первісний корінь за модулем p^α. Непарне з чисел g і $g + p$ є також первісним коренем за модулем $2p^\alpha$.

Якщо $c = \varphi(m)$ і $q_1, q_2, \ldots, q_k$ — різні прості дільники числа c, то число g, взаємно просте з m, тоді і тільки тоді є первісним коренем за модулем m; коли

$$g^{\frac{c}{q_i}} \not\equiv 1 \pmod{m}$$

для всіх $i = 1, 2, \ldots, k$.

ПРИКЛАДИ РОЗВ'ЯЗУВАННЯ ЗАДАЧ

1. Знайти порядок $P_m(a)$ числа a за модулем m, якщо:

а) $a = 2$, $m = 15$; б) $a = 3$, $m = 15$; в) $a = 8$, $m = 15$.

Розв'язання. Щоб знайти порядок $P_m(a)$ числа a за модулем m, слід забезпечити виконання таких вимог:

1) $(a, m) = 1$;

2) $P_m(a)$ — дільник числа $\varphi(m)$;

3) $P_m(a)$ — найменше з тих натуральних чисел k, для яких виконується конгруенція

$$a^k \equiv 1 \pmod{m}.$$

а) Маємо $(2, 15) = 1$. Знаходимо $\varphi(15)$. Оскільки $15 = 3 \cdot 5$, то $\varphi(15) = 3 \cdot 5\left(1 - \frac{1}{3}\right)\left(1 - \frac{1}{5}\right) = 8$.

Отже, $P_{15}(2)$ міститься серед чисел 1, 2, 4, 8. Записуємо послідовно:

$$2^1 \equiv 2 \not\equiv 1 \pmod{15},$$
$$2^2 \equiv 4 \not\equiv 1 \pmod{15},$$
$$2^4 \equiv 16 \equiv 1 \pmod{15}.$$

Отже, $P_{15}(2) = 4$.

б) Оскільки $(3, 15) = 3 \neq 1$, то для числа $a = 3$ за модулем 15 порядку не існує.

в) Оскільки $(8, 15) = 1$ і $8 = 2^3$, то $P_{15}(8)$ існує, його визначають за формулою

$$P_{15}(2^3) = \frac{P_{15}(2)}{(P_{15}(2), 3)} = \frac{4}{(4, 3)} = 4.$$

Зауваження

1. Щоб знайти порядок $P_m(a)$ числа a за модулем m, слід використовувати обчислення, зроблені на попередньому етапі. Так, якщо вже знайдено $a^k \equiv a_0 \pmod{m}$, де $k \mid \varphi(m)$, то щоб знайти a^l, де $l > k$ і $l \mid \varphi(m)$, треба використати те, що $a^k \equiv a_0 \pmod{m}$.

2. Процес знаходження порядку числа може водночас бути процесом знаходження первісних коренів за даним модулем m. Для цього слід визначити, які з чисел мають порядок $\varphi(m)$.

2. Знайти всі первісні корені за модулем 7.

Розв'язання. Первісних коренів за простим модулем $p = 7$ є $\varphi(p - 1) = \varphi(6) = 2$. Вони містяться серед чисел $ЗСЛ_7$:

$$ЗСЛ_7 = \{1, 2, 3, 4, 5, 6\}.$$

Оскільки $p - 1 = 6$ у канонічному розкладі має вигляд $p - 1 = 2 \cdot 3$, то досліджувати слід числа виду $a^{\frac{p-1}{3}}$ і $a^{\frac{p-1}{2}}$, тобто числа a^2 і a^3, де $a \in ЗСЛ_7$.

Знайдемо перший первісний корінь. Перевіряємо число 2 (зрозуміло, що число 1 тільки за модулем 2 є первісним і тому в інших випадках перевірка не має смислу).

$$2^2 \equiv -3 \pmod{7}, \quad 2^3 \equiv 1 \pmod{7}.$$

Оскільки $3 < 6$, то 2 не є первісним коренем за модулем 7.

Перевіряємо число 3:

$$3^2 \equiv 2 \pmod{7}, \quad 3^3 \equiv -1 \pmod{7}.$$

Тоді $3^6 \equiv 1 \pmod{7}$. Отже, порядком числа 3 є 6, тобто 3 є первісним коренем за модулем 7.

Другий первісний корінь міститься серед чисел виду 3^k, де $(k, p - 1) = (k, 6) = 1$ і $1 < k < 6$. Ці умови задовольняє тільки число $k = 5$. Отже, другим первісним коренем є число 3^5. Оскільки $3^5 \equiv 5 \pmod{7}$, то первісними коренями за модулем 7 є числа 3 і 5.

Задачі

17.1. Знайти порядок числа a за модулем m, якщо:

а) $a = 2$, $m = 5$;
б) $a = 4$, $m = 5$;
в) $a = 5$, $m = 8$;
г) $a = 10$, $m = 13$;
д) $a = 4$, $m = 15$;
е) $a = 2$, $m = 15$;
є) $a = 2$, $m = 17$;
ж) $a = 7$, $m = 20$;
з) $a = 7$, $m = 22$;
к) $a = 6$, $m = 39$;
л) $a = 7$, $m = 43$;
м) $a = 5$, $m = 108$;
н) $a = 2$, $m = 133$.

17.2. Знайти порядки всіх класів лишків за модулем m, якщо: а) $m = 11$; б) $m = 19$; в) $m = 21$.

17.3. Знайти порядки чисел a, b, c, d за модулем m, якщо:

а) $a = 7$, $b = 9$, $c = 12$; $m = 13$;
б) $a = 5$, $b = 8$, $c = 13$; $m = 17$;
в) $a = 5$, $b = 8$, $c = 10$; $d = 16$; $m = 33$;
г) $a = 10$, $b = 25$, $c = 50$; $m = 39$;
д) $a = 5$, $b = 15$, $c = 21$, $d = 35$; $m = 44$.

17.4. Знайти порядок числа: а) 10 за модулем $13 \cdot 31$; б) $m - 1$ за модулем m.

17.5. Знайти всі первісні корені за такими модулями: а) 11; б) 13; в) 15; г) 19; д) 49; е) 81.

17.6. Знайти число первісних коренів і найменший з них за такими модулями: а) 10; б) 18; в) 19; г) 31; д) 37.

17.7. Знайти найменший первісний корінь за такими модулями: а) 7; б) 17; в) 23; г) 41; д) 53; е) 50; є) 54; ж) 71; з) 242; к) 289; л) 578; м) 625.

17.8. Знаючи, що 3 є первісним коренем за модулем 29, знайти решту первісних коренів за цим модулем.

17.9. Знаючи, що 2 задовольняє конгруенцію $x^8 \equiv 1 \pmod{17}$, знайти всі розв'язки цієї конгруенції.

17.10. Знаючи, що $P_{29}(4) = 14$, знайти решту чисел, які мають порядок 14 за модулем 29.

17.11. Знаючи, що 2 — первісний корінь за модулем 37, довести, що $2^{18} \equiv 6^2 \pmod{37}$.

17.12. Знаючи, що $P_{29}(12) = 4$, $P_{29}(23) = 7$, знайти $P_{29}(15)$.

17.13. Знайти всі натуральні значення x, які задовольняють конгруенції:

а) $4^x \equiv 1 \pmod{3}$; г) $2^x \equiv 1 \pmod{25}$;

б) $5^x \equiv 1 \pmod 8$; д) $6^x \equiv 1 \pmod{49}$;
в) $5^x \equiv 1 \pmod 9$; е) $2^x \equiv 1 \pmod{49}$.

17.14. Знаючи, що 2 є первісний корінь за модулем 131, знайти всі розв'язки конгруенції $x^3 \equiv 16 \pmod{131}$.

17.15. Знайти ті значення b, при яких мають розв'язки конгруенції: а) $4^x \equiv b \pmod 9$; б) $5^x \equiv b \pmod 9$.

17.16. Нехай p — просте непарне число. Довести, що:

а) серед первісних коренів за модулем p не може бути квадратів;

б) $\left(\frac{a}{p}\right) = 1$, якщо a — первісний корінь за модулем p;

в) $\left(\frac{a^{2n+1}}{p}\right) = 1$, якщо a — первісний корінь за модулем p і $n \in \mathbf{N}$;

г) $P_p(ab) = P_p(a) \cdot P_p(b)$, якщо $(P_p(a), P_p(b)) = 1$;

д) за модулем p існують первісні корені;

е) $a^k + 1 \vdots p$, якщо $P_p(a) = 2k$;

є) добуток двох первісних коренів за модулем p не є первісним коренем за цим модулем;

ж) якщо $n \geqslant 1$, то існує $(p-1) \cdot \varphi(p-1)$ різних первісних коренів за модулем p^n, не конгруентних за модулем p^2;

з) якщо $n > 1$, то існує тільки $\varphi(\varphi(p^n))$ різних первісних коренів за модулем p^n;

к) якщо $n > 1$, то існує $\varphi(\varphi(p^n))$ різних первісних коренів за модулем $2p^n$;

л) $a \cdot b$ не є первісним коренем за модулем p, якщо a і b не є ними за цим самим модулем;

м) якщо p — число виду $4k+1$ і g — первісний корінь за модулем p; то $p-g$ — первісний корінь за модулем p;

н) $a^k \equiv -1 \pmod p$, якщо $P_p(a) = 2k$ і a не $\vdots\ p$.

17.17. Довести, що не існує первісних коренів за модулем m, якщо:

а) $m = 8$;

б) $m = 2^\alpha$, $\alpha \geqslant 3$;

в) $m = 36$;

г) $m = 2^\alpha p$, де $\alpha > 1$ і p — непарне просте число;

д) m — непарне складене число, яке ділиться, принаймні, на два різних простих множники.

17.18. Нехай p — просте непарне число. Довести, що

а) p має вигляд $1 + k \cdot 2^{n+1}$, якщо $p/2^{2^n} + 1$ і $n > 1$;

б) p має вигляд $1 + k \cdot 2^n$, якщо $p/2^{2^n} - 1$ і $n > 1$;

в) прості непарні дільники числа $a^p - 1$, де $a \in \mathbf{N}$ і $a > 1$ є дільниками числа $a - 1$ або мають вигляд $2px + 1$;

г) прості непарні дільники числа $a^p + 1$ є дільниками числа $a + 1$ або мають вигляд $2px + 1$;

д) множина простих чисел виду $2px + 1$, $x \in \mathbf{N}$, є нескінченною;

е) a є первісним коренем за модулем p^α, $\alpha \geqslant 2$, якщо a є первісним коренем за модулем p^2;

є) $P_{p^k}(a) = P_{2p^k}(a)$, якщо a — непарне число, $a \vdots p$, $k \in \mathbf{N}$; зокрема, довільний непарний первісний корінь g за модулем p^k є ним і за модулем $2p^k$.

17.19. Довести, що:

а) первісний корінь за модулем $m > 2$ завжди є квадратичним нелишком за модулем m;

б) $P_{a^{m-1}}(a) = m$, якщо a, $m \in \mathbf{N}$ і $a > 1$;

в) $\varphi(a^m - 1) \equiv 0 \pmod m$, якщо a, $m \in \mathbf{N}$ і $a > 1$;

г) $P_m(a) = \left[P_{p_1^{\alpha_1}}(a), P_{p_2^{\alpha_2}}(a), \ldots, P_{p_s^{\alpha_s}}(a)\right]$, якщо $(a, m) = 1$ і $m = p_1^{\alpha_1} p_2^{\alpha_2} \ldots p_s^{\alpha_s}$ — канонічний розклад числа m;

д) $P_{p^k}(a) = d$, якщо $a^d \equiv 1 \pmod{p^k}$, де $d = P_{p^{k-1}}(a)$, p — просте число, $k \in \mathbf{N}$, $k > 1$, і $(a, p^k) = 1$;

е) $P_{p^k}(a) = p^d$, якщо $a^d \not\equiv 1 \pmod{p^k}$, де $d = P_{p^{k-1}}(a)$, p — просте число, $k \in \mathbf{N}$, $k > 1$, і $(a, p^k) = 1$;

є) $P_{5929}(16) = 1155$;

ж) число a є первісним коренем за модулем m тоді і тільки тоді, коли клас лишків $K_a^{(m)}$ є твірним елементом мультиплікативної групи кільця Z_m.

§ 18. Індекси за простим модулем. Двочленні конгруенції за простим модулем; таблиці індексів і застосування їх

Література

[1] — § 19, с. 201—204;
[2] — § 19, с. 204—207;
[3] — гл. 12, § 5, с. 416—420;
[10] — гл. VI, § 4, с. 90—92;
[11] — гл. 19, гл. 20, с. 163—172;
[12] — гл. IV, § 3, 4, с. 136—146;
[13] — § 31, 32, с. 144—152.

ТЕОРЕТИЧНІ ВІДОМОСТІ

Нехай g — первісний корінь за простим модулем p, $a \in \mathbf{Z}$ і $(a, p) = 1$. Ціле невід'ємне число γ називається **індексом числа a за модулем p при основі g**, якщо

$$g^\gamma \equiv a \pmod p. \tag{1}$$

Взагалі, довільне значення x, яке задовольняє конгруенцію

$$b^x \equiv d \pmod m, \tag{2}$$

називається **індексом числа d за модулем m при основі b** і позначається

$$x \equiv \operatorname{ind}_b d \pmod m. \tag{3}$$

При цьому m може бути й складеним числом, проте

$$(d, m) = (b, m) = 1.$$

Означення індексу можна записати ще так:

$$b^{\operatorname{ind}_b d} \equiv d \pmod m. \tag{4}$$

Користуючись цим означенням, складають таблицю індексів за даною основою і модулем. Таблиці індексів за кожним простим модулем p (не дуже великим) містять дві таблиці: одна — знаходження індексу за числом, а друга — знаходження числа за індексом (таблиця антиіндексів).

Основні властивості індексів

1°. Усі індекси числа a за простим модулем p утворюють клас чисел за модулем $p-1$. Точніше, якщо γ і γ^1 — індекси числа a за модулем p (при будь-якій тій самій основі), то

$$\gamma \equiv \gamma^1 \pmod{p-1};$$

2°. Для того щоб $a \equiv b \pmod{p}$, необхідно і достатньо, щоб $\operatorname{ind}_g a \equiv \operatorname{ind}_g b \pmod{p-1}$;

Якщо значення чисел або індексів виходять за межі таблиць, то ці дві властивості дають змогу переходити до найменших невід'ємних лишків: для чисел — за модулем p, для індексів — за модулем $p-1$.

3°. $\operatorname{ind}_g 1 \equiv 0 \pmod{p-1}$;

4°. $\operatorname{ind}_g g \equiv 1 \pmod{p-1}$;

5°. $\operatorname{ind}_g (a_1 a_1 \dots a_s) \equiv \operatorname{ind}_g a_1 + \operatorname{ind}_g a_2 + \dots + \operatorname{ind}_g a_s \pmod{p-1}$;

6°. $\operatorname{ind}_g a^n \equiv n \operatorname{ind}_g a \pmod{p-1}$;

7°. Якщо $a \vdots b$, то $\operatorname{ind}_g \frac{a}{b} \equiv \operatorname{ind}_g a - \operatorname{ind}_g b \pmod{p-1}$.

Зазначимо, що перехід від конгруенції між числами до конгруенції їхніх індексів називається **індексацією**, а зворотний перехід — **потенціюванням**.

Якщо задано двочленну конгруенцію n-го степеня за простим модулем

$$ax^n \equiv b \pmod{p}, \quad (a, p) = 1, \quad n \in \mathbb{N}, \tag{5}$$

то її розв'язок знаходять з конгруенції

$$n \operatorname{ind} x \equiv \operatorname{ind} b - \operatorname{ind} a \pmod{p-1}. \tag{6}$$

ПРИКЛАДИ РОЗВ'ЯЗУВАННЯ ЗАДАЧ

1. Скласти таблиці індексів та антиіндексів за модулем 23.

Розв'язання. Знайдемо один з первісних коренів за модулем 23 (найчастіше це найменший з первісних коренів). Перевіряючи безпосередньо, дістанемо, що число 5 є одним з первісних коренів за модулем 23, причому найменшим з них. Справді,

$$\varphi(23) = 22 \text{ і } 5^2 \not\equiv 1 \pmod{23},\ 5^{11} \not\equiv 1 \pmod{23}, \text{ а } 5^{22} \equiv 1 \pmod{23}.$$

Отже, $\delta_{23}(5) = 22$, тому 5 є первісний корінь за модулем 23. Візьмемо його за основу таблиці індексів і знайдемо найменші невід'ємні лишки степенів

$$5^0, 5^1, 5^2, \dots, 5^{22}$$

за модулем 23:

$5^0 \equiv 1 \pmod{23}$, $5^8 \equiv 16 \pmod{23}$, $5^{16} \equiv 3 \pmod{23}$,
$5^1 \equiv 5 \pmod{23}$, $5^9 \equiv 11 \pmod{23}$, $5^{17} \equiv 15 \pmod{23}$,
$5^2 \equiv 2 \pmod{23}$, $5^{10} \equiv 9 \pmod{23}$, $5^{18} \equiv 6 \pmod{23}$,
$5^3 \equiv 10 \pmod{23}$, $5^{11} \equiv 22 \pmod{23}$, $5^{19} \equiv 7 \pmod{23}$,
$5^4 \equiv 4 \pmod{23}$, $5^{12} \equiv 18 \pmod{23}$, $5^{20} \equiv 12 \pmod{23}$,
$5^5 \equiv 20 \pmod{23}$ $5^{13} \equiv 21 \pmod{23}$, $5^{21} \equiv 14 \pmod{23}$.
$5^6 \equiv 8 \pmod{23}$, $5^{14} \equiv 13 \pmod{23}$,
$5^7 \equiv 17 \pmod{23}$, $5^{15} \equiv 19 \pmod{23}$,

Отже, $\operatorname{ind}_5 1 = 0$, $\operatorname{ind}_5 5 = 1$, $\operatorname{ind}_5 2 = 2$, $\operatorname{ind}_5 10 = 3$, $\operatorname{ind}_5 4 = 0$, $\operatorname{ind}_5 20 = 5, \dots$

Складаємо таблицю індексів за модулем 23 з основою 5 (табл. 14).

Таблиця 14

N	0	1	2	3	4	5	6	7	8	9
0		0	2	16	4	1	18	19	6	10
1	3	9	20	14	21	17	8	7	12	15
2	5	13	11							

Тут номер рядка означає число десятків, а номер стовпця — число одиниць заданого числа. На перетині певного рядка і стовпця знаходиться відповідний індекс. Так, індекс числа 18 знайдемо на перетині рядка з номером 1 і стовпця з номером 8, тобто $\operatorname{ind}_5 18 = 12$.

Щоб побудувати таблиці антиіндексів, використаємо таблицю індексів. Маємо (табл. 15):

Таблиця 15

I	0	1	2	3	4	5	6	7	8	9
0	1	5	2	10	4	20	8	17	16	11
1	9	22	18	21	13	19	3	15	6	7
2	12	14								

Зауваження. Оскільки вибір основи для складання таблиць індексів за даним модулем є довільним, то в різних підручниках і посібниках такі таблиці не не завжди збігаються. Проте це не впливає на остаточний результат при розв'язуванні задач за допомогою індексів. У таблицях індексів, які наведено в кінці цього посібника, вказано основу g, а також канонічний розклад числа $p-1$ для даного простого модуля p.

2. Розв'язати конгруенцію

$$17x^{18} \equiv 22 \pmod{23}. \tag{1}$$

Розв'язання. Беремо індекси від обох частин конгруенції

$$\operatorname{ind} 17 + 18 \operatorname{ind} x \equiv \operatorname{ind} 22 \pmod{22}.$$

За табл. 14 маємо

$$\operatorname{ind} 17 = 7,\ \operatorname{ind} 22 = 11$$

і тому

$$7 + 18 \operatorname{ind} x \equiv 11 \pmod{22},$$

або

$$18 \operatorname{ind} x \equiv 4 \pmod{22}. \tag{2}$$

Дістали лінійну конгруенцію відносно $\operatorname{ind} x$. Розв'яжемо її. Оскільки $(18, 22) = 2$ і $4 \vdots 2$, то ця конгруенція має два розв'язки. Знайдемо їх штучним способом. Скоротимо спочатку обидві частини і модуль на 2:

$$9 \operatorname{ind} x \equiv 2 \pmod{11}.$$

Додамо до правої частини число -11:

$$9 \operatorname{ind} x \equiv -9 \pmod{11}.$$

Скоротимо обидві частини на 9:

$$\operatorname{ind} x \equiv -1 \pmod{11}.$$

Звідси дістаємо два розв'язки конгруенції (2):

$$\operatorname{ind} x \equiv 10{,}21 \pmod{22}.$$

За табл. 15 знаходимо відповідні два значення невідомого x:

$$x \equiv 9,\ 14 \pmod{23}.$$

Зауваження

1. Зрозуміло, що розв'язування конгруенцій за допомогою індексів можливе для довільного модуля, якщо тільки є відповідні таблиці індексів.

2. При індексуванні конгруенції за модулем m відбувається перехід до конгруенції за модулем $\varphi(m)$, а при потенціюванні конгруенції за модулем $\varphi(m)$ — перехід до конгруенції за модулем m.

Задачі

18.1. Скласти таблиці індексів за модулем p з основою g, якщо:

а) $p = 3,\ g = 2$;
б) $p = 5,\ g = 2$;
в) $p = 5,\ g = 3$;
г) $p = 7,\ g = 3$;
д) $p = 7,\ g = 5$;
е) $p = 11,\ g = 2$;
є) $p = 13;\ g = 2$;
ж) $p = 29,\ g = 2$.

18.2. Скласти таблицю індексів за складеним модулем $m = 27$ з основою $g = 5$.

18.3. Нехай g — первісний корінь за модулем m. Довести, що:

а) конгруенція $b \equiv c \pmod m$ виконується тоді і тільки тоді, коли $\operatorname{ind}_g b \equiv \operatorname{ind}_g c \pmod{\varphi(m)}$ (тут $(b,\ m) = 1$);

б) $\operatorname{ind}_m a = \operatorname{ind}_{2m} a$, якщо $m = p^\alpha$, p — просте непарне число, $(a,\ 2p) = 1$.

18.4. Нехай g і t — два первісних корені за простим модулем p. Довести, що:

а) $\operatorname{ind}_g a \equiv \operatorname{ind}_t a \cdot \operatorname{ind}_g t \pmod{(p-1)}$;
б) $\operatorname{ind}_t a \equiv \operatorname{ind}_g a \cdot \operatorname{ind}_t g \pmod{(p-1)}$;
в) $\operatorname{ind}_t g \cdot \operatorname{ind}_g t \equiv 1 \pmod{(p-1)}$;
г) $\operatorname{ind}_g a \equiv \operatorname{ind}_t a\,(\operatorname{ind}_t g)^{\varphi(p-1)-1} \pmod{(p-1)}$

(**формула переходу** від системи індексів з основою t до системи індексів з основою g).

18.5. Розв'язати лінійні конгруенції:

а) $7x \equiv 23 \pmod{17}$;
б) $5x \equiv 13 \pmod{27}$;
в) $8x \equiv -11 \pmod{37}$;
г) $47x \equiv 23 \pmod{73}$;
д) $53x \equiv 37 \pmod{79}$;
е) $125x \equiv 7 \pmod{79}$;
є) $65x \equiv 38 \pmod{83}$;
ж) $23x \equiv 9 \pmod{97}$;
з) $37x \equiv 5 \pmod{221}$.

18.6. Розв'язати конгруенції другого степеня:

а) $x^2 \equiv 15 \pmod{17}$;
б) $x^2 \equiv 10 \pmod{27}$;
в) $x^2 \equiv 47 \pmod{53}$;
г) $x^2 \equiv 58 \pmod{61}$;
д) $x^2 \equiv 59 \pmod{67}$;
е) $x^2 \equiv -28 \pmod{67}$;
є) $x^2 \equiv 54 \pmod{71}$;
ж) $x^2 \equiv 40 \pmod{83}$;
з) $3x^2 - 5x - 2 \equiv 0 \pmod{11}$;
к) $2x^2 - 7x + 28 \equiv 0 \pmod{43}$;
л) $3x^2 - 8x + 44 \equiv 0 \pmod{47}$;
м) $x^2 \equiv 29 \pmod{59^2}$;
н) $x^2 \equiv 61 \pmod{73^2}$.

18.7. Довести, що:

а) конгруенція $x^n \equiv a \pmod m$, $(a, m) = 1$ має тоді і тільки тоді розв'язки, коли $\operatorname{ind} a : d$, де $d = (n,\ \varphi(m))$. Якщо конгруенція має розв'язки, то їх всього d;

б) конгруенція $x^n \equiv a \pmod p$, де p — просте непарне число, має розв'язки тоді і тільки тоді, коли

$$a^{\frac{p-1}{d}} \equiv 1 \pmod p, \text{ де } d = (n,\ p-1);$$

в) число a тоді і тільки тоді є квадратичним лишком за модулем непарного простого числа p, коли за цим модулем $\operatorname{ind} a$ — число парне;

г) порядок $\delta = P_m(a)$ визначається рівністю $(\operatorname{ind} a,\ \varphi(m)) = \frac{\varphi(m)}{\delta}$. Зокрема, належність числа a до первісних коренів за модулем m визначається рівністю $(\operatorname{ind} a,\ \varphi(m)) = 1$;

д) користуючись властивостями індексів, можна встановити справедливість теореми Вільсона;

е) для простого числа p виду $2^n + 1$, де $n > 3$, число 3 є первісним коренем;

є) індекс числа -1 за простим непарним модулем p при будь-якій основі дорівнює $\frac{p-1}{2}$.

18.8. Скільки розв'язків мають такі конгруенції:

а) $x^{15} \equiv 6 \pmod{37}$;
б) $x^{16} \equiv 10 \pmod{37}$;
в) $3x^3 \equiv 2 \pmod{37}$;
г) $7x^7 \equiv 11 \pmod{41}$;
д) $3x^{12} \equiv 31 \pmod{41}$;
е) $5x^{30} \equiv 37 \pmod{41}$;
є) $x^5 \equiv 3 \pmod{71}$;
ж) $x^{21} \equiv 5 \pmod{71}$;
з) $x^{15} \equiv 46 \pmod{97}$;
к) $x^{55} \equiv 17 \pmod{97}$;
л) $x^{60} \equiv 79 \pmod{97}$?

18.9. Розв'язати такі двочленні конгруенції:

а) $x^{10} \equiv 33 \pmod{37}$;
б) $x^3 \equiv 34 \pmod{41}$;
в) $x^8 \equiv 31 \pmod{41}$;
г) $x^{12} \equiv 37 \pmod{41}$;
д) $x^5 \equiv 37 \pmod{43}$;
е) $x^{27} \equiv 39 \pmod{43}$;
є) $x^{35} \equiv 17 \pmod{67}$;
ж) $x^{30} \equiv 14 \pmod{67}$;
з) $x^{12} \equiv 27 \pmod{83}$;
к) $x^{48} \equiv 2 \pmod{97}$.

18.10. Розв'язати такі двочленні конгруенції:

а) $3x^3 \equiv 4 \pmod 7$;
б) $2x^8 \equiv 5 \pmod{13}$;
в) $15x^4 \equiv 17 \pmod{23}$;
г) $27x^5 \equiv 25 \pmod{31}$;
д) $13x^3 \equiv 24 \pmod{37}$;
е) $37x^8 \equiv 59 \pmod{61}$;
є) $23x^5 \equiv 15 \pmod{73}$;
ж) $37x^6 \equiv 69 \pmod{73}$;
з) $37x^{15} \equiv 62 \pmod{73}$;
к) $44x^{21} \equiv 53 \pmod{73}$;
л) $27x^{30} \equiv 41 \pmod{79}$.

18.11. Розв'язати конгруенції:

а) $5x^{11} + 19 \equiv 0 \pmod{29}$;
б) $25x^7 + 7 \equiv 0 \pmod{31}$;
в) $17x^5 + 3 \equiv 0 \pmod{37}$;
г) $8x^9 + 17 \equiv 0 \pmod{41}$;
д) $7x^{13} + 23 \equiv 0 \pmod{47}$;
е) $x^7 + 27 \equiv 0 \pmod{53}$;
є) $x^{11} + 36 \equiv 0 \pmod{71}$.

18.12. Знайти найменше натуральне число x, яке задовольняє такі конгруенції:

а) $8^x \equiv 1 \pmod{13}$;
б) $27^x \equiv 1 \pmod{17}$;
в) $5^x \equiv 17 \pmod{31}$;
г) $11^x \equiv 17 \pmod{31}$;
д) $24^x \equiv 1 \pmod{31}$;
е) $32^x \equiv 15 \pmod{37}$;
є) $23^x \equiv 37 \pmod{41}$;
ж) $13^x \equiv 25 \pmod{43}$;

з) $16^x \equiv 11 \pmod{53}$; л) $44^x \equiv 19 \pmod{71}$;
к) $2^x \equiv 7 \pmod{67}$; м) $18^x \equiv 53 \pmod{79}$.

18.13. Розв'язати двочленні показникові конгруенції:
а) $3 \cdot 8^x \equiv 7 \pmod{23}$; г) $15 \cdot 7^{2x} \equiv 8 \cdot 3^{3x} \pmod{31}$;
б) $12^{7x} \equiv 15 \pmod{31}$; д) $25^{5x} \equiv 47 \pmod{61}$;
в) $21^{3x} \equiv 21^5 \pmod{29}$; е) $6 \cdot 11^x \equiv 56 \pmod{61}$.

18.14. Розв'язати конгруенції:
а) $13 \cdot 7^{5x} + 1 \equiv 0 \pmod{67}$;
б) $7 \cdot 5^x + 1 \equiv 0 \pmod{73}$;
в) $11 \cdot 5^{3x} + 70 \equiv 0 \pmod{79}$;
г) $8 \cdot 7^x + 4 \equiv 0 \pmod{83}$.

18.15. Знайти порядок числа a за модулем m, якщо:
а) $a = 6$, $m = 7$; д) $a = 27$, $m = 47$;
б) $a = 6$, $m = 23$; е) $a = 13$, $m = 53$;
в) $a = 7$, $m = 29$; є) $a = 10$, $m = 1739$.
г) $a = 18$, $m = 41$; ж) $a = 32$, $m = 4331$.

18.16. Знаючи, що за простим модулем p $\operatorname{ind}_g(a) \equiv b \pmod{(p-1)}$, знайти за цим модулем $\operatorname{ind}_t a$, якщо:
а) $p = 47$, $g = 5$, $a = 34$, $b = 34$, $t = 10$;
б) $p = 73$, $g = 5$, $a = 54$, $b = 26$, $t = 11$;
в) $p = 71$, $g = 7$, $a = 66$, $b = 63$, $t = 13$;
г) $p = 71$, $g = 7$, $a = 56$, $b = 19$, $t = 11$.

18.17. Чи є первісними коренями за модулем 59 такі числа: а) 2; б) 3; в) 6; г) 8; д) 12; е) 13; є) 14; ж) 19?

18.18. Знаючи, що 2 є первісний корінь за модулями 101 і 163, розв'язати конгруенції:
а) $3 \cdot 5^x \equiv 4 \cdot 3^{2x+1} \pmod{101}$;
б) $2^x \equiv 3 \cdot 5^{3x} \pmod{163}$.

18.19. Користуючись критерієм Ейлера та застосовуючи властивості індексів, з'ясувати, які з чисел 15, 16, 17, 18, 19, 20 є квадратичними лишками за такими модулями: а) 23; б) 29; в) 41; г) 59; д) 79; е) 89.

18.20. Серед чисел зведеної системи лишків за модулем p знайти ті, порядок яких дорівнює числу r, якщо:
а) $p = 43$, $r = 6$; в) $p = 61$, $r = 10$;
б) $p = 43$, $r = 42$; г) $p = 61$, $r = 60$.

§ 19. Арифметичні застосування теорії конгруенцій

Література

[1] — § 20, с. 205—210;
[2] — § 20, с. 207—213;
[3] — гл. 12, § 6, с. 421—429;
[10] — гл. XXIII, с. 201—209;
[12] — гл. V, с. 147—160;
[14] — § 33—36, с. 154—169.

ТЕОРЕТИЧНІ ВІДОМОСТІ

Теорія конгруенцій має ряд арифметичних застосувань. Основними з них є:
1) виведення ознак подільності;
2) обчислення остач при діленні;
3) перевірка результатів арифметичних дій;
4) визначення довжини періоду при перетворенні звичайного дробу в десятковий.

Нехай в g-ковій системі числення число N має вигляд

$$N = a_0 + a_1 g^1 + \ldots + a_n g^n.$$

Позначимо через r_k абсолютно найменші лишки числа g^k за модулем m, тобто $g^k \equiv r_k \pmod{m}$, $k = 0, 1, \ldots, n$ і $r_0 = 1$. Тоді $N \equiv R_m \pmod{m}$, де $R_m \equiv a_0 r_0 + a_1 r_1 + \ldots + a_n r_n \pmod{m}$ **(ознака подільності Паскаля).**

З конгруенції $N \equiv R_m \pmod{m}$ випливає, що при діленні на m числа N і R_m дають однакові остачі. Зокрема, число N ділиться на m тоді і тільки тоді, коли на m ділиться R_m. Покладаючи $g = 10$, $m = 2, 3, 4, 5 \ldots$, дістаємо конкретні ознаки подільності. З метою обчислення остач від ділення, крім ознаки Паскаля, використовують також теореми Ейлера і Ферма, властивості індексів тощо.

Якщо

$$N \equiv f(N_1, N_2, \ldots, N_k), \tag{1}$$

де f — многочлен від цілих чисел $N_1, N_2 \ldots, N_k$ з цілими коефіцієнтами, то виконується конгруенція

$$N \equiv f(N_1', N_2', \ldots, N_k') \pmod{m}, \tag{2}$$

де m — будь-яке натуральне число, N_i' — остача від ділення N_i на m, $i = 1, 2, \ldots, k$. Конгруенція (2) є умова, необхідна для рівності (1), але не достатня. Інакше кажучи, якщо (2) не виконується, то не виконується й (1); якщо (2) виконується, наприклад, для $m = 9$ або $m = 11$, то напевно помилки в обчисленнях (1) не виявлено. Так, виконуючи перевірку для $m = 9$, помилку не виявили, оскільки: 1) не було взято до уваги нуль у доданку або множнику; 2) в результаті цифри записані не в тому порядку; 3) неповні добутки перебувають не на своїх місцях; 4) взагалі, помилка становить число, кратне 9. Під час складних обчислень доцільно робити дві перевірки: одну за модулем 9, а другу — за модулем 11.

Нескоротний дріб виду $\frac{a}{2^\alpha \cdot 5^\beta c}$, де $c > 1$, $c \neq 2$ і $c \neq 5$, у скінченний десятковий дріб не перетворюється.

Якщо $\frac{a}{b}$ — нескоротний дріб і $(b, 10) = 1$, то цей дріб перетворюється у чистий періодичний десятковий дріб. При цьому число цифр у періоді дорівнює порядку $p_b(10)$ числа 10 за модулем b.

Якщо $\frac{a}{b}$ — нескоротний дріб і $b = 2^\alpha 5^\beta b_1$, де $(b_1, 10) = 1$, то цей дріб перетворюється в мішаний періодичний десятковий дріб. При цьому число цифр у періоді дорівнює γ, де γ — більше з чисел α і β; число цифр у періоді дорівнює порядку $p_{b_1}(10)$ числа 10 за модулем b_1.

ПРИКЛАДИ РОЗВ'ЯЗУВАННЯ ЗАДАЧ

1. Вивести ознаку подільності на 11.

Розв'язання. Нехай $N = a_0 + a_1 \cdot 10^1 + a_2 \cdot 10^2 + \ldots + a_n \cdot 10^n$ — десятковий запис числа N. Оскільки $m = 11$, то $10^k \equiv (-1)^k \pmod{11}$ і тому $R_{11} \equiv a_0 - a_1 + a_2 - \ldots$, або $R_{11} = (a_0 + a_2 + a_4 + \ldots) - (a_1 + a_3 + a_5 + \ldots)$. Враховуючи, що цифри a_{2k} з парними індексами в числі N стоять на непарних місцях (починаючи справа наліво), то можна таким чином сформулювати ознаку подільності на 11:

Число N ділиться на 11 тоді і тільки тоді, коли різниця між сумою цифр, які стоять на непарних місцях, і сумою цифр, що стоять на парних місцях, ділиться на 11.

Зауваження. Беручи до уваги, що $10^2 \equiv 1 \pmod{11}$, можна дістати іншу ознаку подільності числа N на $m = 11$. Маємо: $N = b_0 + b_1 10^2 + \ldots + b_l (10)^{2l}$, де $b_0 = a_1 a_0$ — цифра одиниць першого розряду, $b_1 = a_3 a_2$ — цифра одиниць другого розряду і т. д. Враховуючи, що $(10^2)^k \equiv 1 \pmod{11}$, $k = 1, 2, \ldots, l$, дістаємо: $N \equiv R_{11} \equiv b_0 + b_1 + \ldots + b_l \pmod{11}$. Інакше кажучи, число N ділиться на 11 тоді і тільки тоді, коли на 11 ділиться сума двоцифрових чисел, утворених відповідними гранями числа N при його розбитті справа наліво.

2. Знайти остачу від ділення $N = 13^{37} \cdot 12^{41}$ на 35.

Розв'язання. Оскільки $35 = 5 \cdot 7$, то шукану остачу знаходять як найменший невід'ємний розв'язок системи конгруенцій

$$\begin{cases} x \equiv r_1 \pmod 5, \\ x \equiv r_2 \pmod 7, \end{cases}$$

де r_1 і r_2 — відповідні остачі від ділення числа N на числа 5 і 7. Спочатку знайдемо остачу від ділення N на 5:

$$r_1 \equiv 13^{37} \cdot 12^{41} \equiv 3^{37} \cdot 2^{41} \pmod 5.$$

Беручи індекси в обох частинах конгруенції, маємо

$$\operatorname{ind} r_1 \equiv 37 \operatorname{ind} 3 + 41 \operatorname{ind} 2 \equiv \operatorname{ind} 3 + \operatorname{ind} 2 \equiv 3 + 1 \equiv 0 \pmod 4.$$

Звідси $r \equiv 1 \pmod 5$.

Аналогічно знаходимо остачу від ділення N на 7:

$$r_2 \equiv 13^{37} \cdot 12^{41} \equiv (-1)^{37} \cdot (-2)^{41} \equiv 2^{41} \pmod 7;$$

$$\operatorname{ind} r_2 \equiv 41 \operatorname{ind} 2 \equiv 41 \cdot 2 \equiv 82 \equiv 4 \pmod 6,$$

звідки $r_2 \equiv 4 \pmod 7$.

Розв'язуємо систему конгруенцій

$$\begin{cases} x \equiv 1 \pmod 5, \\ x \equiv 4 \pmod 7. \end{cases}$$

З першої конгруенції знаходимо $x = 5k + 1$, $k \in N$.

Підставляємо це значення в другу конгруенцію $5k + 1 \equiv 4 \pmod 7$ і розв'язуємо її відносно k:

$$\begin{aligned} 5k &\equiv 3 \pmod 7, \\ 5k &\equiv 10 \pmod 7, \\ k &\equiv 2 \pmod 7, \\ k &= 7s + 2, s \in N. \end{aligned}$$

Тоді $x = 5k + 1 = 5(7s + 2) + 1 = 35s + 11$, тобто $x \equiv 11 \pmod{35}$. Отже, шукана остача дорівнює числу 11.

Зауваження. Зрозуміло, що цю остачу можна було знайти, скориставшись лише теоремами Ейлера і Ферма, що значно скорочує обчислення. Справді, $\varphi(35) = 24$, $(13, 35) = (12, 35) = 1$, тому $13^{24} \equiv 12^{24} \equiv 1 \pmod{35}$. Тоді

$$13^{37} \cdot 12^{41} \equiv (13 \cdot 12)^{37} \cdot 12^4 \equiv 16^{13} \cdot 2^3 \cdot 3^4 \equiv 2^{80}(-32^4) \equiv$$
$$\equiv 2^{80} \equiv 2^8 \equiv 2^5 \cdot 2^3 \equiv -3 \cdot 8 \equiv 11 \pmod{35}.$$

Отже, при діленні на 35 число $13^{37} \cdot 12^{41}$ дає остачу 11.

3. Перевірити правильність виконання арифметичних дій над цілими числами:

а) $1042 \cdot 10182 + 42932 - 18265 = 10634311$,

б) $4325 \cdot 897 = 451425$.

Розв'язання. Замінимо рівності а) і б) конгруенціями за модулем 9:

а) $7 \cdot 12 + 20 - 22 \equiv 19 \pmod 9$, або $1 \equiv 1 \pmod 9$;

б) $14 \cdot 24 \equiv 21 \pmod 9$. Застосуємо ще раз «правило дев'ятки»: $5 \cdot 6 \equiv 3 \pmod 9$, або $3 \equiv 3 \pmod 9$.

Отже, перевірка числом 9 не виявила помилок в обох обчисленнях. Щоб бути впевненим у правильності виконаних арифметичних дій, треба перевірити ці результати за модулем 11:

а) $(-3)(-4) + 10 + 6 \equiv -5 \pmod{11}$, або $6 \equiv 6 \pmod{11}$;

б) $2 \cdot 6 \not\equiv 7 \pmod{11}$.

Отже, у прикладі б) дії виконано неправильно, тоді як у виконанні арифметичних дій над цілими числами у прикладі а) помилки не виявлено.

Зауваження. На практиці розглянуті обчислення виконуються простіше: для кожного числа обчислюється остача від ділення його на 9 (на 11); потім здобуті остачі замінюються своїми остачами і т. д. Це стосується і всіх проміжних обчислень.

4. Знайти число цифр до періоду і довжину періоду періодичного дробу, в який перетворюється дріб $\frac{13}{420}$.

Розв'язання. Знаменник цього дробу має канонічний розклад: $420 = 2^2 \cdot 3 \cdot 5 \cdot 7$. Оскільки $\gamma = \max(\alpha, \beta) = 2$ — більший з показників степенів цифр 2 і 5, то періодичний десятковий дріб має дві цифри до періоду. Щоб знайти порядок $\delta = P_{21}(10)$ числа 10 за модулем 21, використаємо один загальний прийом. З конгруенції $10^\delta \equiv 1 \pmod b$ випливає, що $\underbrace{99\ldots9}_{\delta \text{ раз}} \equiv 0 \pmod b$. Отже, δ можна знайти так: ділимо 9 на b, потім 99 на b і т. д., поки не дістанемо в остачі нуль. Число дев'яток при цьому, а отже, й число цифр частки (якщо $b > 9$, то враховувати слід і нуль, який відповідає першій дев'ятці) дорівнюватимуть шуканому порядку $\delta = P_b(10)$ числа 10 за модулем b.

У розглядуваному прикладі $b = 3 \cdot 7 = 21$. Виконаємо ділення:

```
 99 | 21
-84 | 047619
 159
-147
  129
 -126
   39
  -21
  189
 -189
    0
```

У частці маємо 6 цифр, беручи до уваги також 0, який відповідає першій дев'ятці. Отже, $\delta = \delta_{21}(10) = 6$, тобто період дробу $\frac{13}{420}$ складається з шести цифр.

Задачі

19.1. Вивести ознаки подільності на: а) 2; б) 3; в) 4; г) 5; д) 7; е) 9; є) 10; ж) 11; з) 13; к) 25; л) 37; м) 50.

19.2. Довести, що:

а) число $a = 10a_1 + a_0$ ділиться на 7 тоді і тільки тоді, коли $(a_1 - 2a_0) \vdots 7$;

б) на 11 діляться ті і тільки ті цілі числа, в яких різниця між числом, записаним всіма цифрами, крім останньої, і числом, записаним цією останньою цифрою, ділиться на 11;

в) на 11 діляться ті і тільки ті цілі числа, в яких сума двох чисел, одне з яких записане двома останніми цифрами, а друге — рештою цифр, ділиться на 11.

19.3. Довести, що в g-ковій системі числення:

а) число a ділиться на m, де $m \mid g + 1$, тоді і тільки тоді, коли різниця між сумами цифр числа a на парних і непарних місцях ділиться на m;

б) число a ділиться на m, де $m \mid g - 1$, тоді і тільки тоді, коли сума цифр числа a ділиться на m;

в) число a ділиться на m, де $m \mid g^k$, тоді і тільки тоді, коли число, записане останніми k цифрами числа a, ділиться на m.

19.4. Користуючись ознаками подільності, встановити, чи ділиться число a на m, якщо:

а) $a = 56704$, $m = 7$; 11 або 13;
б) $a = 24829$, $m = 7$;
в) $a = 454111$, $m = 7$;
г) $a = 53746$, $m = 11$;
д) $a = 63364$, $m = 7$;
е) $a = 973126$, $m = 13$;
є) $a = 96736068$, $m = 11$;
ж) $a = 20794$, $m = 37$;
з) $a = 2575163$, $m = 37$.

19.5. Користуючись ознаками подільності:

а) знайти канонічний розклад числа 244943325;
б) знайти канонічний розклад числа 282321246671737;
в) знайти x, y, z, якщо $(13x\,45z)_{10} \vdots 792$;
г) знайти x, y, якщо $(7x36y5)_{10} \vdots 1375$;
д) знайти канонічний розклад числа 90799;
е) знайти канонічний розклад числа 3058487;
є) записати п'ятизначні числа, які діляться на 55 і середні цифри яких становлять число 809;
ж) довести, що коли до будь-якого тризначного числа дописати справа це саме число, то утворене число ділиться на 7, 11, 13.

19.6. Не виконуючи ділення, знайти остачу від ділення a на m, якщо:

а) $a = 3\,989\,713$, $m = 37$;
б) $a = 27\,877\,165$, $m = 37$;
в) $a = 31\,127\,567$, $m = 37$;
г) $a = 125 \cdot 465$, $m = 61$;
д) $a = 34\,521_7$, $m = 6_7$.

19.7. Знайти остачу від ділення:

а) 763^{17} на 29;
б) 342^{256} на 29;
в) 581^{3792} на 37;
г) 10^{10} на 67;
д) 244^{408} на 73;
е) 749^{193} на 79;
є) 341^{245} на 89;
ж) 175^{411} на 629;
з) 272^{1141} на 135;
к) 35^{100} на 1242;
л) 20^{6n+5} на 9, $n \in \mathbf{N}$.

19.8. Знайти остачу від ділення:

а) $53^{29} \cdot 43^{17}$ на 37;
б) $378^{561} \cdot 427^{921}$ на 41;
в) $37^{20} \cdot 23^{12}$ на 61;
г) $3^{19 \cdot 37 - 1}$ на $19 \cdot 37$;
д) $(5\,622 + 179 - 346) \cdot 923$ на 23;
е) $(631^{57} + 250^{28}) \cdot 926$ на 12;
є) $7^{161} - 3^{80}$ на 100;
ж) $(12\,371^{56} + 34)^{28}$ на 111.

19.9. Довести, що

а) $14^{120} - 1 \vdots 45$;
б) $13^{176} - 1 \vdots 89$;
в) $372\,654^{500} + 72 \cdot 10^7 \vdots 18$;
г) $2^{1093} - 2 \vdots 1093^2$;
д) $43^{23} + 23^{43} \vdots 66$;
е) $222^{555} + 555^{222} \vdots 7$;
є) $220^{119^9} + 69^{220^{119}} + 119^{69^{220}} \vdots 102$.

19.10. Нехай m, $n \in \mathbf{N}$. Довести, що:

а) $n^7 + 6n \vdots 7$;
б) $10^n(9n - 1) + 1 \vdots 9$;
в) $3 \cdot 5^{2n+1} + 2^{3n+1} \vdots 17$;
г) $6^{2n+1} + 5^{n+2} \vdots 31$;
д) $20^m + 16^m - 3^m - 1 \vdots 323$, якщо $m = 2n$;
е) $mn(m^{60} - n^{60}) \vdots 56\,786\,730$;
є) $m^{96} - b^{96} \vdots 144$, якщо $(m, 12) = (n, 12) = 1$.

19.11. За правилом «дев'ятки» перевірити правильність виконання арифметичних дій над цілими числами:

а) $375\,819 + 726\,345 + 807\,611 = 1\,909\,775$;
б) $732 \cdot 421 = 308172$;
в) $73416 \cdot 8539 = 626899224$;
г) $24667 + 18265 = 42932$;
д) $5433153 : 4371 = 1243$;
е) $375426 \cdot 3846 = 1443888276$;
є) $\sqrt{73818} = 271^2 + 377$.

19.12. Перевірити правильність виконання арифметичних дій числами 9 і 11:

а) $387912 - 203756 = 185146$;
б) $8740297 - 561245 = 8179052$;
в) $5839131309 : 67377 = 85847$.

19.13. Знайти довжину періоду при перетворенні у десятковий дріб нескоротного звичайного дробу із знаменником: а) 17; б) 19; в) 29; г) 37; д) 43; е) 59; є) 67; ж) 73; з) 89; к) 97.

19.14. Знайти довжину періоду при перетворенні у десятковий дріб нескоротного звичайного дробу із знаменником: а) 21; б) 33; в) 39; г) 49; д) 51; е) 77; є) 91; ж) $11 \cdot 17$; з) $13 \cdot 17$; к) $17 \cdot 23$; л) $53 \cdot 59$; м) $53 \cdot 73$.

19.15. Знайти кількість цифр до періоду і довжину періоду при перетворенні у десятковий дріб нескоротного звичайного дробу із знаменником: а) 140; б) 220; в) 450; г) 528; д) 540; е) 550; є) 665; ж) 816; з) 950; к) 1150; л) 2380; м) 26500.

19.16. Знайти знаменник дробу $\frac{1}{b}$, який перетворюється у десятковий чистий періодичний дріб:

а) з двома цифрами в періоді;
б) з трьома цифрами в періоді.

19.17. Знайти:

а) $\frac{14}{19}$, знаючи, що $\frac{1}{19} = 0,(052\,631\,578\,947\,368\,421)$;
б) $\frac{107}{143}$, якщо $\frac{1}{11} = 0,(09)$ і $\frac{1}{13} = 0,(076\,923)$;
в) a, якщо $\frac{a}{73} = 0,(86\,301\,369)$ і $\frac{1}{73} = 0,(01\,369\,863)$;
г) a, якщо $\frac{a}{73} = 0,(30\,136\,986)$ і $\frac{1}{73} = 0,(01\,369\,863)$.

19.18. Довести, що

а) сума $\frac{1}{n-1} + \frac{1}{n} + \frac{1}{n+1}$, $n > 1$, перетворюється у мішаний десятковий періодичний дріб;
б) коли p — просте число, $p \neq 2$, $p \neq 5$ і дріб $\frac{1}{p}$ перетворюєть-

ся в чистий періодичний дріб з парним числом δ цифр у періоді $\frac{1}{p}=0,\ (a_1a_2\ldots a_{\frac{\delta}{2}-1}a_{\frac{\delta}{2}}a_{\frac{\delta}{2}+1}\ldots a_{\delta-1}a_\delta)$, то $a_{\frac{\delta}{2}+i}=9-a_i,\quad i=1, 2, \ldots, \frac{\delta}{2}$. (Перевірити для числа $\frac{1}{7}$);

в) звичайний дріб $\frac{1}{pq}$, де p, q — прості числа, відмінні від 2 і 5, перетворюється в нескінченний періодичний дріб з довжиною періоду $\left[\frac{p-1}{d}, \frac{q-1}{\delta}\right]$, де

$$d=(\text{ind } 10,\ p-1),\ \delta=(\text{ind } 10,\ q-1)$$

(у першому випадку ind10 беруть за модулем p, у другому — за модулем q);

г) коли 10 є первісним коренем за модулем m, то періоди всіх нескоротних дробів із знаменником m утворюються в результаті кругових перестановок тієї самої системи $k=\varphi(m)$ цифр.

19.19. Перетворити у звичайні такі періодичні дроби: а) 3, (27); б) 0,35 (62); в) 11, 12 (31); г) 5, 1 (538).

Розділ IV. МНОГОЧЛЕНИ ВІД ОДНІЄЇ ЗМІННОЇ

§ 20. Кільце многочленів над областю цілісності. Алгебраїчна і функціональна рівність многочленів

Література

[1] — § 21, с. 211—227;
[2] — § 21, с. 214—230;
[3] — гл. 14, § 1, с. 459—468;
[7] — § 7, с. 42—50;
[6] — § 20, с. 130—133;
[8] — гл. 5, § 2, с. 207—211.

ТЕОРЕТИЧНІ ВІДОМОСТІ

Нехай K — довільна область цілісності з одиницею і $\mathbf{R}$ — її підкільце з одиницею.

Елемент $x\in K$ називається алгебраїчним над кільцем R, якщо в $\mathbf{R}$ існують такі елементи $a_0, a_1, a_2, \ldots, a_n$, які не всі дорівнюють 0, що

$$a_nx^n+a_{n-1}x^{n-1}+\ldots+a_1x+a_0=0.$$

Елемент, який не є алгебраїчним над $\mathbf{R}$, називається **трансцендентним над R**.

Мінімальне розширення кільця $\mathbf{R}$, яке містить трансцендентний над $\mathbf{R}$ елемент x, називається **простим трансцендентним розширенням кільця R**, або **кільцем многочленів від однієї змінної над R**, і позначається через $R[x]$. Елементи цього кільця називають **многочленами від x над R** і позначають символами $f(x)$, $g(x)$ і т. д. Нуль кільця $R[x]$ називають **нулевим многочленом** або **нуль-многочленом**.

Будь-який ненульовий многочлен $f(x)$ над кільцем $\mathbf{R}$ можна єдиним чином подати у вигляді

$$f(x)=a_nx^n+a_{n-1}x^{n-1}+\ldots+a_1x+a_0, \qquad (1)$$

де $a_0, a_1, \ldots, a_n\in\mathbf{R}$ і $a_n\neq 0$.

Вираз (1) називають **канонічною формою** ненульового многочлена $f(x)$. Канонічною формою нуль многочлена вважатимемо 0.

Доданок a_kx^k $(k=0, 1, 2\ldots, n)$ канонічної форми (1) ненульового многочлена $f(x)$ називається **k-м членом (членом k-го степеня)**, a_k — **k-м коефіцієнтом (коефіцієнтом k-го члена)**, a_0 називається також **вільним членом многочлена** $f(x)$. Член n-го (найбільшого) степеня називається **старшим членом**, його коефіцієнт a_n — **старшим коефіцієнтом**, а його степінь — **степенем многочлена** $f(x)$ і позначають $\deg f$.

Нуль-многочленові не приписують ніякого степеня.

Два многочлени з кільця $R[x]$ дорівнюють один одному тоді і тільки тоді, коли вони мають однакові степені і попарно рівні відповідні коефіцієнти (**алгебраїчна рівність многочленів**).

Кільце многочленів $R[x]$ є областю цілісності.

Степінь суми двох многочленів (з яких хоча б один є ненульовим) не перевищує більшого з степенів цих многочленів. Степінь добутку двох многочленів (відмінних від нуль-многочлена) дорівнює сумі степенів цих многочленів.

Якщо многочлен $f(x)$ з кільця $R[x]$ має канонічну форму (1) і $a\in\mathbf{R}$, то елемент

$$a_na^n+a_{n-1}a^{n-1}+\ldots+a_1a+a_0$$

кільця $\mathbf{R}$ називають **значенням многочлена** $f(x)$ при $x=a$ і позначають через $f(a)$.

Кожен многочлен $f(x)$ з кільця $R[x]$ визначає відображення $\varphi_f : \mathbf{R}\to\mathbf{R}$ таке, що $\varphi_f(a)=f(a)$.

Якщо область цілісності $\mathbf{R}$ має характеристику 0, то многочлени $f(x), g(x)\in R[x]$ дорівнюють один одному тоді і тільки тоді, коли рівні функції φ_f та φ_g, які вони визначають (**функціональна рівність многочленів**).

Алгебраїчне і функціональне тлумачення многочленів рівносильні над областю цілісності характеристики 0.

ПРИКЛАДИ РОЗВ'ЯЗУВАННЯ ЗАДАЧ

1. Знайти всі цілі числа a і b, при яких многочлен $f(x)=x^4+ax^3+bx^2-8x+4$ є квадратом деякого многочлена $g(x)$ з кільця $Z[x]$, та записати многочлен $g(x)$.

Розв'язання. Многочлен $f(x)$ має степінь 4. Тому степінь шуканого многочлена $g(x)$ (якщо він існує!) дорівнює 2. Нехай $g(x)=mx^2+nx+p$, $m\neq 0$, і многочлени $f(x)$ та $(g(x))^2$ дорівнюють один одному.

Запишемо многочлен $(g(x))^2$ у канонічній формі:

$$(g(x))^2=(mx^2+nx+p)^2=m^2x^4+2mnx^3+(2mp+n^2)x^2+2np+p^2.$$

З умови рівності многочленів маємо систему рівнянь:

$$\begin{cases} m^2=1,\\ 2mn=a,\\ 2mp+n^2=b,\\ 2np=-8,\\ p^2=4. \end{cases}$$

З першого рівняння системи знаходимо, що $m\in\{1, -1\}$, а з останнього $p\in\{2, -2\}$. Це означає що дана система рівнянь рівносильна сукупності чотирьох систем:

$$\begin{cases} m=1,\\ p=2,\\ n=-2,\\ a=-4,\\ b=8, \end{cases} \quad \begin{cases} m=1,\\ p=-2,\\ n=2,\\ a=4,\\ b=0. \end{cases} \quad \begin{cases} m=-1,\\ p=2,\\ n=-2,\\ a=4,\\ b=0, \end{cases} \quad \begin{cases} m=-1,\\ p=-2,\\ n=2,\\ a=-4,\\ b=8. \end{cases}$$

Таким чином, якщо $a=-4$ і $b=8$, то існують два многочлени $g_1(x)=-x^2+2x-2$ і $g_2(x)=x^2-2x+2$, які задовольняють умову задачі. Якщо $a=4$

і $b=0$, то $g_1(x)=x^2+2x-2$ і $g_2(x)=-x^2-2x+2$. Цим вичерпуються всі можливі випадки шуканого зображення многочлена $f(x)$.

2. Перевірити, чи є кільцем множина K всіх многочленів з кільця $Z[x]$, в яких вільний член ділиться на 5.

Розв'язання. Нехай

$$f(x)=a_nx^n+\ldots+a_1x+5a_0,$$

$$g(x)=b_mx^m+\ldots+b_1x+5b_0 \text{ і } m\geqslant n.$$

Тоді

$$f(x)+g(x)=b_mx^m+\ldots+(a_n+b_n)x^n+\ldots+(a_1+b_1)x+(5a_0+5b_0)=$$

$$=b_mx^m+\ldots+(a_n+b_n)x^n+\ldots+(a_1+b_1)x+5(a_0+b_0),$$

$$f(x)-g(x)=(-b_m)x^m+\ldots+(a_n-b_n)x^n+\ldots+(a_1-b_1)x+5(a_0-b_0),$$

$$f(x)\cdot g(x)=a_nb_mx^{n+m}+\ldots+(5a_1b_0+5a_0b_1)x+5\cdot 5a_0b_0.$$

Це означає, що $f(x)+g(x)$, $f(x)-g(x)$ і $f(x)\cdot g(x)$ також є елементами множини K. Отже, K є підкільцем кільця $Z[x]$.

3. Многочлен $f(x)$ з кільця $Z_5[x]$, степінь якого не вище за 4, має ту властивість, що $f(\bar{a})=\bar{0}$ для всіх $\bar{a}\in Z_5$. Довести, що $f(x)$ є нуль-многочленом.

Розв'язання. Нехай $f(x)=\bar{a}x^4+\bar{b}x^3+\bar{c}x^2+\bar{d}x+\bar{e}$. Тоді

$$f(\bar{0})=\bar{e}=\bar{0},$$
$$f(\bar{1})=\bar{a}+\bar{b}+\bar{c}+\bar{d}+\bar{e}=\bar{0},$$
$$f(\bar{2})=\bar{a}+\bar{3b}+\bar{4c}+\bar{2d}+\bar{e}=\bar{0},$$
$$f(\bar{3})=\bar{a}+\bar{2b}+\bar{4c}+\bar{3d}+\bar{e}=\bar{0},$$
$$f(\bar{4})=\bar{a}+\bar{4b}+\bar{c}+\bar{4d}+\bar{e}=\bar{0}.$$

Звідси дістаємо систему рівнянь у полі Z_5:

$$\begin{cases}\bar{a}+\bar{b}+\bar{c}+\bar{d}=\bar{0},\\ \bar{a}+\bar{3b}+\bar{4c}+\bar{2d}=\bar{0},\\ \bar{a}+\bar{2b}+\bar{4c}+\bar{3d}=\bar{0},\\ \bar{a}+\bar{4b}+\bar{c}+\bar{4d}=\bar{0}\end{cases} \text{ або } \begin{cases}\bar{a}+\bar{b}+\bar{c}+\bar{d}=\bar{0},\\ \bar{2b}+\bar{3c}+\bar{d}=\bar{0},\\ \bar{b}+\bar{3c}+\bar{2d}=\bar{0},\\ \bar{3b}+\bar{3d}=\bar{0}.\end{cases}$$

Далі

$$\begin{cases}\bar{a}+\bar{b}+\bar{c}+\bar{d}=\bar{0},\\ \bar{b}-\bar{d}=\bar{0},\\ \bar{b}+\bar{3c}+\bar{2d}=\bar{0},\\ \bar{b}+\bar{d}=\bar{0}\end{cases} \text{ і } \bar{a}=\bar{b}=\bar{c}=\bar{d}=\bar{0}.$$

Таким чином, усі коефіцієнти многочлена $f(x)$ дорівнюють нулю, тобто $f(x)$ є нуль-многочленом.

4. Довести, що в многочлена

$$f(x)=(-\sin^2\alpha\cdot x^3+\cos^2\alpha\cdot x+x)^{1983}$$

з дійсними коефіцієнтами суми коефіцієнтів членів парного і непарного степенів однакові, і знайти їх.

Розв'язання. Якщо $g(x)=a_nx^n+\ldots+a_1x+a_0$ — деякий многочлен над областю цілісності K з одиницею, то $g(1)=a_n+\ldots+a_1+a_0$ і $g(-1)=(-1)^na_n+\ldots-a_1+a_0$, тобто значення многочлена при $x=1$ дорівнює сумі всіх коефіцієнтів, а при $x=-1$ дорівнює різниці між сумами коефіцієнтів парного і непарного степенів.

Позначимо суми коефіцієнтів членів парного і непарного степенів многочлена $f(x)$ через s_0 і s_1 відповідно.

Тоді

$$s_0+s_1=f(1)=(-\sin^2\alpha+\cos^2\alpha+1)^{1983}=(1+\cos 2\alpha)^{1983}=2^{1983}\cdot\cos^{3966}\alpha,$$

$$s_0-s_1=f(-1)=(\sin^2\alpha+\cos^2\alpha-1)^{1983}=0.$$

З другої рівності маємо $s_0=s_1$, а з першої

$$s_0=s_1=2^{1982}\cdot\cos^{3966}\alpha.$$

Задачі

20.1. Знайти канонічну форму многочлена:

а) $f(x)=(x+\sqrt{2})^4+(x-\sqrt{2})^4-(x^3+3x-1)(x^2+7x+2)$ у кільці $R[x]$;

б) $f(x)=(x-\bar{1})^3$ у кільці $Z_3[x]$;

в) $f(x)=(\bar{4}x^3+\bar{2}x^2-\bar{3}x+\bar{1})(x^2-\bar{2}x+\bar{3})$ у кільці $Z_5[x]$.

20.2. Встановити рівність чи відмінність між многочленами:

а) $f_1(x)=5^{-\log_5 2}x^3-\sqrt{4-2\sqrt{3}}\,x^2+2x-\operatorname{tg}\frac{\pi}{4}$,

$f_2(x)=\left(1-\sin\frac{\pi}{6}\right)x^3+(i-1)^2x^2+2-i$,

$f_3(x)=\frac{1}{2}x^3+(\sqrt{3}-1)x^2-2i^2x-i^4$,

$f_4(x)=\cos\frac{\pi}{3}x^3+2i^3x^2+i^7+2$,

$f_5(x)=\left(\frac{1}{6}+\operatorname{tg}^2\frac{\pi}{6}\right)x^3+\left(\operatorname{tg}\frac{\pi}{3}-1\right)x^2-4\cos^2\frac{\pi}{3}x-2^0$ у кільці $C[x]$;

б) $f_1(x)=(\bar{4}x+\bar{3})^2$, $f_2(x)=-x^2+\bar{4}x+\bar{4}$ та $f_3(x)=\bar{4}x^2-x+\bar{3}$ у кільці $Z_5[x]$.

20.3. Довести, що в кільці $Z_5[x]$ многочлени $f(x)=(x+\bar{3})^5$ і $g(x)=x^5+\bar{3}$ дорівнюють один одному.

20.4. Довести, що для будь-якого простого числа p і цілого a, $1\leqslant a\leqslant p-1$, многочлени $f(x)=(x+\bar{a})^p$ і $g(x)=x^p+\bar{a}$ рівні в кільці $Z_p[x]$.

20.5. При яких значеннях a, b і c наступні многочлени з кільця $Z[x]$ рівні між собою:

а) $f(x)=ax^2(x+1)+b(x^2+1)(x-6)+cx(x^2+1)$ та $g(x)=x^2+5x+6$;

б) $f(x)=ax(x^2+3)+bx(x-1)+c(x+1)$ та $g(x)=2x^3+5x^2+8x+7$?

20.6. Знайти всі значення a, при яких наступні многочлени є квадратом деякого многочлена $g(x)$ з того самого кільця, і записати $g(x)$:

а) $f(x)=x^4+6x^3+11x^2+ax+1$ з кільця $Z[x]$;

б) $f(x) = \bar{4}x^4 + \bar{a}x^2 - \bar{1}$ з кільця $Z_5[x]$;
в) $f(x) = 9x^4 - 12x^3 + 16x^2 - 8x + a$ з кільця $Z[x]$.

20.7. Знайти всі цілі a і b, при яких многочлен

$$f(x) = x^3 + ax^2 + 12x + b$$

є кубом деякого многочлена з кільця $Z[x]$.

20.8. Знайти всі цілі числа a і b, при яких многочлен $f(x) = x^4 + ax^3 + bx - 8x + 1$ є квадратом деякого многочлена $g(x)$ з кільця $Z[x]$, та записати многочлен $g(x)$.

20.9. Чи може многочлен

$$f(x) = 8x^6 - 36ax^5 + 66a^2x^4 - 63a^3x^3 + 33a^4x^2 - 9a^5x + a^6$$

з дійсними коефіцієнтами бути кубом многочлена $g(x)$ з цілими коефіцієнтами?

20.10. Яким умовам мають задовольняти цілі числа a, b і c, щоб многочлен $f(x) = 4x^4 - 4ax^3 + 4bx^2 + 2a(c+1)x + (c+1)^2$ був квадратом деякого многочлена з цілими коефіцієнтами?

20.11. Знайти цілі числа a, b і c, для яких виконується рівність $\frac{x+5}{(x-1)(x-2)(x-3)} = \frac{a}{x-1} + \frac{b}{x-2} + \frac{c}{x-3}$.

20.12. Чи існує в кільці $R[x]$ квадратний тричлен, який є квадратом деякого многочлена і такий, що зберігає цю властивість при будь-якій перестановці своїх коефіцієнтів?

20.13. Кожен з двох многочленів $f(x)$ і $g(x)$ над областю цілісності K є сумою квадратів двох многочленів з кільця $K[x]$. Довести, що многочлен $s(x) = f(x) \cdot g(x)$ має цю властивість.

20.14. Записати у вигляді суми квадратів двох многочленів з кільця $Z[x]$ такі многочлени:
а) $f(x) = (x^2+1)(x^2+9)$;
б) $f(x) = (x^2 - 2x + 5)(x^2 + 16x + 73)$.

20.15. Чи є кільцем множина всіх многочленів з кільця $Z[x]$
а) в яких змінна x має тільки парний степінь;
б) в яких змінна x має тільки непарний степінь;
в) які не містять вільного члена;
г) коефіцієнти яких кратні даному натуральному числу k;
д) степінь яких не перевищує числа 10;
е) степінь яких не менший числа 2?

20.16. Довести, що з функціональної точки зору наступні многочлени дорівнюють один одному:
а) $f(x) = x^3 - \bar{2}x^2$ і $g(x) = x^2 - \bar{2}x$ з кільця $Z_3[x]$;
б) $f(x) = \bar{2}x^2 + x + \bar{1}$ і $g(x) = \bar{2}x^3 + \bar{2}x^2 + \bar{2}x + \bar{1}$ з кільця $Z_3[x]$;
в) $f(x) = x^{10} + \bar{4}x^2$ і $g(x) = \bar{4}x^5 + x$ з кільця $Z_5[x]$.

20.17. За допомогою многочлена з кільця $Z_2[x]$ задати кожне відображення поля Z_2 в себе.

20.18. Довести, що для будь-якої області цілісності K в кільці $K[x]$ не існує двох многочленів першого степеня, які різні в алгебраїчному і рівні у функціональному розумінні.

20.19. Довести, що для будь-якої скінченної області цілісності K існує ненульовий многочлен $f(x)$ в кільці $K[x]$ такий, що $f(a) = 0$ для всіх $a \in K$.

20.20. Довести, що кожне відображення скінченної області цілісності K в себе можна задати деяким многочленом з $K[x]$.

20.21. Довести, що відображення $f(x) = \sqrt[5]{x}$ множини дійсних чисел $\mathbf{R}$ в себе не можна задати деяким многочленом з кільця $R[x]$.

20.22. Знайти суму коефіцієнтів таких многочленів:
а) $f(x) = (1 - 5x + 4x^3)(3x+5)^3$ в кільці $Z[x]$;
б) $f(x) = (1 + 2x - 4x^2)^{1983} \cdot (1 - 7x + 5x^2)^{1982}$ в кільці $Z[x]$;
в) $f(x) = \bar{2} + (x^2 - \bar{6}x + \bar{5})(x^5 + \bar{3}x^4 - \bar{2}x^3 + x^2 - x) + (x^2 - \bar{3}x + \bar{1})(x^3 + \bar{5}x + \bar{2})$ у кільці $Z_7[x]$.

20.23. Многочлен $g(x)$ над областю цілісності K з одиницею має однакові суми коефіцієнтів членів парного і непарного степенів, які дорівнюють s. Знайти суму коефіцієнтів членів парного степеня многочлена $f(x) = [g(x)]^k$, де $k \in \mathbf{N}$.

20.24. Довести, що многочлен

$$f(x) = (1 - x + 2x^2 - 3x^3 + \ldots + 50x^{50})(1 + x + 2x^2 + \ldots + 50x^{50})$$

не містить членів з непарними степенями.

20.25. Довести, що кожен коефіцієнт при парному степені змінної x члена многочлена $f(x) = (1 + 5x^2 - x^3)^k$ не менший коефіцієнта при такому самому степені x члена многочлена $g(x) = (1 - 5x^2 - x^3)^k$.

20.26. Знайти цілі числа a, при яких наступні многочлени розкладаються в добуток двох многочленів $g_1(x) = x + b$ і $g_2(x) = x + c$ з цілими коефіцієнтами:
а) $f(x) = (x-a)(x-10) + 1$,
б) $f(x) = (x+a)(x+1) - 1$.

20.27. Довести, що в кільці $Z[x]$ немає многочлена $f(x)$ такого, щоб $f(7) = 11$ і $f(11) = 13$.

20.28. Довести, що многочлен $f(x) = \frac{1}{n!}x(x-1)\ldots(x-(n-1))$ з кільця $Q[x]$, заданий для деякого фіксованого натурального числа n, набуває цілих значень при будь-яких цілих значеннях змінної x.

20.29. Довести, що для кожного многочлена $f(x)$ з кільця $Z[x]$ і будь-яких цілих чисел a і b число $f(a + \sqrt{b}) + f(a - \sqrt{b})$ є цілим.

§ 21. Відношення подільності в кільці многочленів. Ділення з остачею. Ідеали кільця многочленів

Література

[1] — § 22, с. 227—238;
[2] — § 22, с. 231—241;
[3] — гл. 14, § 2, с. 469—470;
[5] — гл. VII, § 3, с. 262—265; гл. IX, § 1, 2, с. 316—322;
[6] — § 20, 21, с. 133—137;
[7] — § 8, с. 50—54,
[8] — гл. 5, § 2, с. 216—218.

ТЕОРЕТИЧНІ ВІДОМОСТІ

Нехай P — деяке поле. Многочлен $f(x) \in P[x]$ ділиться на $g(x) \in P[x]$ (записують $f(x) \vdots g(x)$), якщо існує многочлен $s(x) \in P[x]$ такий, що $f(x) = g(x) \cdot s(x)$.

Відношення подільності многочленів над полем P має такі властивості:

1°. $\underset{f(x),g(x),h(x)\in P[x]}{\forall} [f(x) \vdots g(x) \wedge g(x) \vdots h(x) \Rightarrow f(x) \vdots h(x)]$;

2°. $\underset{f(x),g(x),h(x)\in P[x]}{\forall} [f(x) \vdots h(x) \wedge g(x) \vdots h(x) \Rightarrow (f(x) \pm g(x)) \vdots h(x)]$;

3°. $\underset{f(x),h(x)\in P[x]}{\forall} [f(x) \vdots h(x) \Rightarrow \underset{g(x)\in P[x]}{\forall} [f(x)\, g(x) \vdots h(x)]]$;

4°. $\underset{f(x)\in P[x]}{\forall} \underset{c\in P\setminus\{0\}}{\forall} [f(x) \vdots c]$;

5°. $\underset{f(x),g(x)\in P[x]}{\forall} \underset{c\in P\setminus\{0\}}{\forall} [f(x) \vdots g(x) \Rightarrow f(x) \vdots cg(x)]$;

6°. $\underset{f(x),g(x)\in P[x]}{\forall} [f(x) \vdots g(x) \wedge g(x) \vdots f(x) \Rightarrow \underset{c\in P}{\exists} f(x) = cg(x)]$.

Говорять, що многочлен $f(x) \in P[x]$ ділиться з остачею на многочлен $g(x) \neq 0$ з кільця $P[x]$, якщо в $P[x]$ існують такі многочлени $s(x)$ і $r(x)$, що:

1) $f(x) = g(x) \cdot s(x) + r(x)$;

2) $r(x) = 0$ або $\deg r < \deg g$.

При цьому $f(x)$ називають **діленим**, $g(x)$ — **дільником**, $s(x)$ — **часткою**, $r(x)$ — **остачею**.

Довільний многочлен $f(x)$ з кільця $P[x]$ ділиться з остачею на будь-який ненульовий многочлен $g(x)$ з цього кільця, причому частка і остача визначаються однозначно.

Кільце $P[x]$ многочленів над довільним полем P є кільцем головних ідеалів. Кільце $P[x]$ многочленів над полем P є евклідовим.

Для знаходження частки і остачі від ділення многочлена

$$f(x) = a_n x^n + \ldots + a_1 x + a_0 \text{ на } g(x) = b_m x^m + \ldots + b_1 x + b_0$$

над полем P (а при певних умовах і над областю цілісності K) застосовують різні методи. Зокрема, **метод ділення кутом, метод невизначених коефіцієнтів** та **за допомогою табличних схем.**

Розглянемо одну з можливих табличних схем, яка має іноді переваги перед рештою методів. Нехай $n \geqslant m$. Якщо

$$f(x) = g(x)\, s(x) + r(x) \text{ і } s(x) = c_{n-m} x^{n-m} + \ldots + c_1 x + c_0$$

та $r(x) = d_{m-1} x^{m-1} + \ldots + d_1 x + d_0$, то схема має вигляд (табл. 16).

У таблиці є $n+2$ стовпці і $n-m+3$ рядки. Через σ_i, $1 \leqslant i \leqslant n-m$, позначено суму елементів $(i+2)$-го стовпця, які стоять між першим та $(i+2)$-м рядками. Через δ_j, $0 \leqslant j \leqslant m-1$, позначено суму елементів відповідного стовпця, які стоять між першим і останнім рядками. Таблиця заповнюється так:

1) знаходять $\dfrac{a_n}{b_m}$ і записують його в останній рядок другого стовпця;

2) число c_{n-m} множать на коефіцієнти дільника і послідовно записують у другий рядок зліва направо (при цьому кілька останніх клітин можуть бути порожніми);

3) обчислюють різницю $a_{n-1} - \sigma_1$ і записують її у клітинці на перетині третього рядка і третього стовпця;

4) знаходять число $c_{n-m-1} = \dfrac{a_{n-1} - \sigma_1}{b_m}$ і записують його в третій клітинці останнього рядка;

5) за аналогією з 2) заповнюють третій рядок (при цьому порожньою буде клітинка з другого стовпця).

Таблиця 16

	a_n	a_{n-1}	a_{n-2}	...	a_m	a_{m-1}	...	a_0
b_m	a_n	$b_{m-1}\dfrac{a_n}{b_m}$	$b_{m-2}\dfrac{a_n}{b_m}$	...				
b_{m-1}		$a_{n-1} - \sigma_1$	$b_{m-1}\dfrac{a_{n-1}-\sigma_1}{b_m}$	...				
b_{m-2}			$a_{n-2} - \sigma_2$	...				
. . .								
b_1								
b_0								
					$a_m - \sigma_{n-m}$	$b_{m-1} \times$ $\times \dfrac{a_m - \sigma_{n-m}}{b_m}$	...	$b_0 \dfrac{a_m - \sigma_{m-n}}{b_m}$
	$\underbrace{\dfrac{a_n}{b_m}}_{c_{n-m}}$	$\underbrace{\dfrac{a_{n-1}-\sigma_1}{b_m}}_{c_{n-m-1}}$	$\underbrace{\dfrac{a_{n-2}-\sigma_2}{b_m}}_{c_{n-m-2}}$	...	$\underbrace{\dfrac{a_m - \sigma_{n-m}}{b_m}}_{c_0}$	$\underbrace{a_{m-1} - \delta_{m-1}}_{d_{m-1}}$	...	$\underbrace{a_0 - \delta_0}_{d_0}$

Цей процес продовжують доти, поки не буде обчислено вільний член c_0 частки. Після цього знаходять коефіцієнти остачі як різниці між числом, що стоїть у першому та останніх заповнених рядках відповідного стовпця.

ПРИКЛАДИ РОЗВ'ЯЗУВАННЯ ЗАДАЧ

1. Встановити подільність многочлена

$$f(x) = x^{19} + x^{17} + x^{13} + x^{11} + x^7 + x^5 - 6x^3$$

на многочлен $g(x) = x^2 - 1$ в кільці $Z[x]$.

Розв'язання. Запишемо многочлен $f(x)$ у вигляді суми многочленів, виділивши, якщо це можливо, в кожному з них множник-многочлен $g(x)$:

$$f(x) = (x^{19} - x^{17}) + (2x^{17} - 2x^{15}) + (2x^{15} - 2x^{13}) + (3x^{13} - 3x^{11}) +$$
$$+ (4x^{11} - 4x^9) + (4x^9 - 4x^7) + (5x^7 - 5x^5) + (6x^5 - 6x^3) = x^{17}(x^2 - 1) +$$
$$+ 2x^{15}(x^2 - 1) + 2x^{13}(x^2 - 1) + 3x^{11}(x^2 - 1) + 4x^9(x^2 - 1) +$$
$$+ 4x^7(x^2 - 1) + 5x^5(x^2 - 1) + 6x^3(x^2 - 1).$$

Оскільки кожен з многочленів-доданків ділиться на многочлен $g(x)$ в кільці $Z[x]$, то многочлен $f(x)$ ділиться на $g(x)$ в $Z[x]$.

2. Знайти остачу від ділення многочлена

$$f(x) = (x-2)^{100} + (x-1)^{50} + 1$$

на многочлен $g(x) = x^2 - 3x + 2$ в кільці $R[x]$.

Розв'язання. До многочленів $f(x)$, $g(x)$ застосуємо в кільці $R[x]$ теорему про ділення з остачею. Тоді існують многочлени $s(x)$ і $r(x)$ такі, що

$$f(x) = g(x) \cdot s(x) + r(x) \text{ і } \deg r(x) < 2.$$

Остання нерівність означає, що $r(x) = ax + b$. Тому

$$(x-2)^{100} + (x-1)^{50} + 1 = (x^2 - 3x + 2)\, s(x) + ax + b.$$

Враховуючи те, що $g(1) = g(2) = 0$, підставимо $x = 1$ і $x = 2$ у здобуту рівність. Маємо систему рівнянь:

$$\begin{cases} a + b = 2, \\ 2a + b = 2 \end{cases} \quad \text{або} \quad \begin{cases} a = 0, \\ b = 2. \end{cases}$$

Отже, $r(x) = 2$.

3. Виконати ділення з остачею многочлена

$f(x) = 3x^5 + x^4 - 10x^3 + 12x^2 + 10x - 8$ на многочлен $g(x) = 3x^2 + x - 1$.

Розв'язання. Застосуємо описану вище табличну схему. В таблиці повинно бути 7 стовпців і 6 рядків. Маємо (табл. 17).

Таблиця 17

	3	1	−10	12	10	−8
3	3	1	−5			
1		0	0	0		
−1			−9	−3	3	
				15	5	−5
	1	0	−3	5	2	−3

Отже, при діленні $f(x)$ на $g(x)$ дістали частку $s(x) = x^3 - 3x + 5$ і остачу $r(x) = 2x - 3$.

Зауваження

1. Оскільки рядок, що містить тільки число 0, не впливає на обчислення, то його можна не писати. При цьому в таблиці залишиться незаповненим передостанній рядок.

2. Для спрощення в таблиці відділяють лініями тільки перший і останні рядки та перший і m останніх стовпців.

Задачі

21.1. Перевірити, чи ділиться:

а) $f(x) = (3x^2 - 2x - 1)(10x^3 + 10x - 20) + 2x^4 - 2$ на $g(x) = 5x^2 - 5$ у кільцях $Z[x]$ і $Q[x]$;

б) $f(x) = x^2 + x + \bar{1}$ на $g(x) = x - \bar{1}$ у кільці $Z_3[x]$;

в) $f(x) = x^{100} + x^{98} + x^{96} + \ldots + x^4 + x^2 + x - i$ на $g(x) = x^2 + 1$ у кільці $C[x]$.

21.2. Довести, що многочлен $f(x) = x^3 + 2$ не ділиться на жоден многочлен першого степеня в кільці $Z[x]$.

21.3. Довести, що многочлен $f(x) = x^3 + \bar{2}$ ділиться на деякий многочлен першого степеня в кільці $Z_3[x]$.

21.4. При яких значеннях a многочлен $f(x) = 3x^4 - 2x^2 - 5$ ділиться на многочлен $g(x) = x^2 - a$: а) в кільці $Z[x]$? б) в кільці $Q[x]$?

21.5. Довести, що при будь-якому натуральному n, кратному 3 многочлен $f(x) = x^n - 1$ ділиться на многочлен $g(x) = x^2 + x + 1$ у кільці $Z[x]$.

21.6. Знайти необхідні і достатні умови подільності таких многочленів:

а) $f(x) = x^3 + bx + c$ на $g(x) = x^2 + ax - 1$ в кільці $R[x]$;

б) $f(x) = x^3 + bx + c$ на $g(x) = x^2 + 1$ в кільці $Z[x]$;

в) $f(x) = x^4 + bx^2 + c$ на $g(x) = x^2 + ax + 1$ в кільці $Z[x]$.

21.7. Довести, що многочлен $f(x) = x^n - a^n$ ділиться на многочлен $g(x) = x - a$ над областю цілісності K при будь-якому натуральному n.

21.8. Перевірити справедливість твердження: «Довільний многочлен $f(x)$ з кільця $Z[x]$ ділиться з остачею на будь-який многочлен $g(x)$ з цього кільця, відмінний від нуль-многочлена».

21.9. Довести, що коли в кільці $K[x]$ над областю цілісності K можна виконати ділення з остачею многочлена $f(x)$ на $g(x)$, то частка і остача визначаються однозначно.

21.10. Довести, що в кільці $K[x]$ над областю цілісності K з одиницею можна виконати ділення з остачею довільного многочлена $f(x)$ на будь-який многочлен $g(x)$, старший коефіцієнт якого дорівнює одиниці.

21.11. Знайти остачу від ділення:

а) $f(x) = x^{10000} + x^{1000} + x^{100} + x^{10} + x - 1$ на $g(x) = ix - 1$ у кільці $(Z[i])[x]$;

б) $f(x) = x^{30} + x^{25} + x^{20} + x^{15} + x^{10} + x + 1$ на $g(x) = x^5 - 1$ у кільці $Z[x]$;

в) $f(x) = x^{1982} + x^{991} + 1$ на $g(x) = x^2 - 1$ у кільці $Z[x]$;

г) $f(x) = x^{1982} + x + 1$ на $g(x) = x^2 - (1+i)x + i$ в кільці $C[x]$;

д) $f(x) = x^{100} + x^{99} - 2x^{98} - 3x^3 + 2x + 5$ на $g(x) = x^2 + x - 2$ в кільці $Z[x]$.

21.12. Виконати ділення многочленів:

а) $f(x) = 4x^5 - 6x^3 + 2x^2 - 4$ на $g(x) = 2x^2 - 5x + 1$ в кільці $Q[x]$;

б) $f(x) = (2i + 3)x^3 - 4ix + i - 2$ на $g(x) = x^2 + i$ в кільці $C[x]$;

в) $f(x) = \bar{4}x^3 + \bar{2}x^2 - x + \bar{1}$ на $g(x) = \bar{2}x + \bar{3}$ в кільці $Z_5[x]$;

г) $f(x) = 10x^7 - 36x^6 + 13x^5 + 38x^4 - 6x^3 + 3x^2 - 20x - 13$ на $g(x) = 2x^2 - 4x - 3$ в кільці $R[x]$;

д) $f(x) = (\bar{2}x^3 + \bar{3})(x - \bar{2}) - x^2$ на $g(x) = (x + \bar{3})^2$ в кільці $Z_5[x]$;

е) $f(x) = \bar{3}x^7 + \bar{6}x^3 + \bar{3}x + \bar{6}$ на $g(x) = x^2 + \bar{6}x + \bar{5}$ у кільці $Z_7[x]$;

є) $f(x) = \frac{1}{2}x^6 + \frac{1}{8}x^5 - x^3 + x^2 - 1$ на $g(x) = x^3 - \frac{1}{8}x + 1$ у кільці $Q[x]$;

ж) $f(x) = ix^4 + (1+i)x + (1-i)$ на $g(x) = x^3 + (1+i)$ в кільці $C[x]$.

21.13. Можна вважати, що многочлени $f(x) = x^5 + 3x^4 + x^3 + 4x^2 - 3x - 1$ і $g(x) = x^2 + x + 1$ належать кільцям $Z[x]$ та $Z_5[x]$ залежно від того, як інтерпретувати їхні коефіцієнти. Довести, що в першому випадку $f(x)$ не ділиться на $g(x)$, а в другому — ділиться. Чи можлива реалізація оберненого варіанта?

21.14. Довести, що многочлен $f(x) = x^6 + x^3 + a$ не ділиться на многочлен $g(x) = x^3 + x + a$ в кільці $Q[x]$ при жодному значенні числа a.

21.15. При яких значеннях a і b многочлен $f(x) = x^3 + 2x^2 + ax + b$ ділиться на многочлен $g(x) = x^2 + x + ab$ в кільці $Q[x]$?

21.16. При діленні многочлена $f(x)$ на $g(x)$ в кільці $Z[x]$ дістали остачу $r(x) = 3x^2 - 4x + 1$. Знайти остачу від ділення $(f(x))^2$ на $g(x)$, якщо $\deg g = 5$.

21.17. При діленні $f(x)$ на $g(x)$ в кільці $R[x]$ дістали остачу 3, а при діленні $(f(x))^2$ на $(g(x))^2$ — остачу 9. Яка буде остача, якщо $f(x)$ ділити на $(g(x))^2$?

21.18. Остачі від ділення многочленів $f_1(x)$ і $f_2(x)$ на $g(x)$ в кільці $Q[x]$ відповідно дорівнюють $r_1(x) = -2x + \frac{2}{3}$ і $r_2(x) = x^2 + 3x - 1$. Знайти остачу від ділення многочлена $f(x) = 3f_1(x) + 2f_2(x)$ на $g(x)$.

21.19. При діленні $f(x)$ на $g(x)$ у кільці $C[x]$ дістали частку $s(x) = ix + 3 - 2i$ та остачу $r(x) = (i-1)x^2 + 2$. Знайти остачу від ділення $f(x)$ на $s(x)$.

21.20. Знайти найменший ідеал I кільця $Z[x]$, який містить:
а) многочлен $f(x) = 3x - 5$;
б) многочлени $f_1(x) = 2x - 1$ і $f_2(x) = 3x + 2$;
в) многочлени $f_1(x) = x^2 - 1$ і $f_2(x) = x^2 - 3x + 2$.

21.21. Чи є ідеалом в кільці $R[x]$ множина I всіх многочленів, у яких вільний член є парним числом?

21.22. Множина I містить число 0 і всі многочлени $f(x)$ з кільця $Z[x]$, які містять змінну x, не нижче другого степеня. Довести, що множина I є ідеалом кільця $Z[x]$. Чи є цей ідеал головним?

21.23. Довести, що множина I всіх многочленів кільця $Z[x]$, коефіцієнти яких діляться на число n, є головним ідеалом в $Z[x]$.

21.24. Довести, що множина I всіх многочленів кільця $Z[x]$, вільний член яких дорівнює парному числу, є ідеалом в $Z[x]$. Чи є цей ідеал головним?

§ 22. Ділення многочлена на двочлен $x - a$. Розклад многочлена за степенями двочлена $x - a$

Література

[1] — § 22, с. 231—235;
[2] — § 22, с. 234—239;
[3] — гл. 14, § 4, с. 481—482;
[5] — гл. VII, § 3, с. 266—268;
[6] — § 22, с. 144—145;
[7] — § 12, с. 71—72;
[8] — гл. 6, § 1, с. 243—244.

ТЕОРЕТИЧНІ ВІДОМОСТІ

У попередньому параграфі було наведено таблицю для виконання ділення з остачею многочлена $f(x)$ на многочлен $g(x)$ над полем P. Ця схема значно спрощується, якщо многочлен $g(x)$ є двочленом виду $g(x) = b_m x^m + b_0$. Справді, вона має вигляд (табл. 18). З другого по передостанній рядок цієї таблиці в кожному стовпці міститься не більш як одне число, відмінне від нуля. Наприклад, з другого по $(m+1)$-й стовпець — це a_n, a_{n-1}, ..., a_{n-m+1}.

Таблиця 18

	a_n	a_{n-1}	a_{n-2}	...	a_{n-m+1}	a_{n-m}	...	a_m	a_{m-1}	...	a_0
b_m	a_n	0	0		0	$b_0 \frac{a_n}{b_m}$					
0		a_{n-1}	0		0	0					
0			a_{n-2}		0	0					
⋮											
0					a_{n-m+1}	0					
b_0								$a_m - c_{n-m}$	0	...	$b_0 \frac{a_m - c_{n-m}}{b_m}$
	$\frac{a_n}{b_m}$	$\frac{a_{n-1}}{b_m}$	$\frac{a_{n-2}}{b_m}$	...	$\frac{a_{n-m+1}}{b_m}$	$\frac{a_{n-m} - c_{n-m}}{b_m}$	...	$\frac{a_m - c_{n-m}}{b_m}$	$a_{m-1} - b_{m-1}$	...	$a_0 - b_0$

У наступних стовпцях: $b_0 \frac{a_n}{b_m}$, $b_0 \frac{a_{n-1}}{b_m}$, ..., $b_0 \frac{a_{n-m+1}}{b_m}$, тобто добутки вільного члена b_0 дільника $g(x)$ на коефіцієнти частки c_{n-m}, c_{n-m+1}, ..., c_{n-2m+1} і т. д. Це означає, що в таблиці можна обмежитися тільки трьома рядками і заповнювати її в такій послідовності:

1) спочатку розіб'ємо коефіцієнти многочлена $f(x)$ у групи по m членів зліва направо (в останній групі може бути менше ніж m членів);

2) коефіцієнти b_m і b_0 записують у першому стовпці в першому і другому рядках;

3) кожен ряд першої групи (a_n, ..., a_{n-m+1}) ділять на старший член дільника b_m і записують у третій рядок під ним; у другому рядку з другої по $(m+1)$-у клітину можна не вписувати чисел;

4) вільний член b_0 послідовно множать на знайдені коефіцієнти частки і вписують у другий рядок, починаючи з $(m+2)$-ї клітини;

5) знаходять наступні коефіцієнти частки, і процес продовжують доти, поки не заповнять останню клітину таблиці в третьому рядку.

Якщо двочлен $g(x)$ має вигляд $g(x) = x^m + b_0$, то при обчисленні коефіцієнтів частки за наведеною табличною схемою не треба виконувати ділення чисел, тоді ця схема нагадує схему Горнера. При цьому число 1 можна також не писати в лівому верхньому кутку таблиці.

При діленні многочлена $f(x)$ на двочлен $g(x) = x - a$ описану схему можна спростити. Так, якщо усно обчислювати різницю коефіцієнтів a_i, $0 \leqslant i \leqslant n$, і добутків вільного члена $-a$ на знайдений коефіцієнт частки c_{i-1}, то в таблиці стає зайвим другий рядок. Тоді розглядувана таблична схема відрізняється від схеми Горнера тільки тим, що в першому стовпці міститься число $-a$ замість a.

Нехай $f(x)$ — деякий многочлен над полем P. Для будь-якого елемента a з поля P остача при діленні многочлена $f(x)$ на двочлен $x - a$ дорівнює $f(a)$.

Многочлен $f(x)$ ділиться на двочлен $x - a$ тоді і тільки тоді, коли остача дорівнює нулю.

Подамо многочлен $f(x)$ з кільця $P[x]$ у вигляді

$$f(x) = c_n(x-a)^n + c_{n-1}(x-a)^{n-1} + \ldots + c_1(x-a) + c_0,$$

де $c_0, c_1, \ldots, c_n \in P$ називається розкладом многочлена за степенями $x - a$. Коефіцієнти розкладу $c_0, c_1, \ldots, c_n$ можна знайти в результаті послідовного ділення $f(x)$ на $x - a$, потім здобутої першої частки на $x - a$ і т. д.

ПРИКЛАДИ РОЗВ'ЯЗУВАННЯ ЗАДАЧ

1. Виконати ділення многочлена $f(x) = 2x^7 + 4x^5 - x^4 - 6x^3 - x^2 + 3x - 2$ на двочлен $g(x) = 2x^3 - 1$ в кільці $R[x]$.

Розв'язання. Виконуємо ділення за описаною вище табличною схемою (табл. 19).

Таблиця 19

	2	2	0	4	−1	−6	−1	3	−2
−1					−1	0	−2	0	3
	1	0	2	0	−3	1	3	−5	

Отже, при діленні $f(x)$ на двочлен $g(x)$ дістали частку $s(x) = x^4 + 2x^2 - 3$ і остачу $r(x) = x^2 + 3x - 5$.

2. Розкласти многочлен

$$f(x) = 2x^7 + 4x^5 - x^4 - 6x^3 - x^2 + 3x - 2$$

за степенями двочлена $g(x) = x^2 + 1$ в кільці $Q[x]$.

Розв'язання. Щоб розв'язати задачу, треба знайти многочлени $h_3(x)$, $h_2(x)$, $h_1(x)$, $h_0(x)$ в кільці $Q[x]$ такі, що виконується рівність

$$f(x) = h_3(x)(x^2+1)^3 + h_2(x)(x^2+1)^2 + h_1(x)(x^2+1) + h_0(x)$$

і $\deg h_i < \deg g$ для всіх $0 \leqslant i \leqslant 3$. Із записаної рівності бачимо, що $h_0(x)$ є остача від ділення многочлена $f(x)$ на $x^2 + 1$, $h_1(x)$ є остача від ділення здобутої частки на $x^2 + 1$, $h_2(x)$ є остача від ділення нової частки на $x^2 + 1$ і $h_3(x)$ є остача від ділення останньої частки на многочлен $x^2 + 1$. Виконуємо послідовно ділення за описаною схемою (табл. 20). Отже,

$$f(x) = 2x(x^2+1)^3 + (-2x-1)(x^2+1)^2 + (-8x+1)(x^2+1) + 11x - 2.$$

3. Знайти остачу від ділення многочлена

$$f(x) = ix^4 + (3-2i)x^3 + (2i-4)x^2 + (3-3i)x + 3i + 2$$

на двочлен $g(x) = x + 1 - i$.

Таблиця 20

	2	0	4	−1	−6	−1	3	−2
1			2	0	2	−1	−8	0
	2	0	2	−1	−8	0	11	−2
1			2	0	0	−1		
	2	0	0	−1	−8	1		
1			2	0				
	2	0	−2	−1				
1								
	2	0						

$h_0(x) = 11x - 2$; $h_2(x) = -2x - 1$;
$h_1(x) = -8 + 1$; $h_3(x) = 2x$.

Розв'язання. Ділення виконуємо за спрощеною табличною схемою (табл. 21).

Таблиця 21

	i	$3-2i$	$2i-4$	$3-3i$	$3i+2$
$1-i$	i	$2-3i$	$-3+7i$	$-1-13i$	$16+15i$

Щоб знайти коефіцієнти частки і остачі, доцільно (незалежно від того, яку схему застосувати) виконати проміжні обчислення:

$$3 - 2i - i(1-i) = 3 - 2i - i - 1 = 2 - 3i,$$

$$2i - 4 - (1-i)(2-3i) = 2i - 4 - 2 + 3i + 2i + 3 = -3 + 7i,$$

$$3 - 3i - (1-i)(-3+7i) = 3 - 3i + 3 - 7i - 3i - 7 = -1 - 13i,$$

$$3i + 2 - (1-i)(-1-13i) = 3i + 2 + 1 + 13i - i + 13 = 16 + 15i.$$

Отже, остача дорівнює $16 + 15i$.

4. Довести, що многочлен

$$f(x) = (x + a + b)^{1983} - x^{1983} - a^{1983} - b^{1983}$$

ділиться на двочлени $g_1(x) = x + a$ і $g_2(x) = x + b$ в кільці $C[x]$.

Розв'язання. Знайдемо значення многочлена $f(x)$ при $x = -a$ і $x = -b$

$$f(-a) = b^{1983} + a^{1983} - a^{1983} - b^{1983} = 0,$$

$$f(-b) = a^{1983} + b^{1983} - a^{1983} - b^{1983} = 0.$$

За теоремою Безу многочлен ділиться на двочлени $g_1(x)$ і $g_2(x)$.

Задачі

22.1. Виконати ділення многочленів

а) $f(x) = 10x^4 - 23x^3 + 26x^2 - 9x - 2$ на $g(x) = 2x - 3$ в кільці $Z[x]$;

б) $f(x) = (2+2i)x^4 - 6x^3 + (2-4i)x^2 + (1+11i)x + 2 - 5i$ на $g(x) = (1-i)x + 3i$ в кільці $C[x]$;

в) $f(x) = 2x^5 + 12{,}5x^3 - 4x^2 + 5{,}5x - 2{,}5$ на $g(x) = 4x^2 + 1$ в кільці $Q[x]$;

г) $f(x) = -\bar{5}x^5 + \bar{5}x^5 - \bar{2}x^3 + \bar{3}x^2 - \bar{2}x + \bar{5}$ на $g(x) = \bar{6}x^3 + \bar{4}$ в кільці $Z_7[x]$;

д) $f(x) = (2+i)x^5 + 2ix^4 + (-2+6i)x^3 - 8x^2 + (2+3i)x + 1 - 6i$ на $g(x) = ix^2 - 3$ в кільці $C[x]$.

22.2. Знайти частку і остачу від ділення:

а) $f(x) = x^4 - 2x^3 + 4x^2 - 6x + 8$ на $g(x) = x - 1$ в кільці $Z[x]$;

б) $f(x) = 4x^4 + x^3$ на $g(x) = x + 1 + i$ в кільці $C[x]$;

в) $f(x) = \bar{6}x^6 + x^5 + \bar{1}$ на $g(x) = x + \bar{3}$ в кільці $Z_7[x]$;

г) $f(x) = (1+\sqrt{2})x^4 + \dfrac{\sqrt{2}}{1+\sqrt{2}}x^2 + 1$ на $g(x) = x - 1 + \sqrt{2}$ в кільці $Q(\sqrt{2})[x]$.

22.3. Знайти значення многочлена $f(x)$ з кільця $K[x]$ в точці $x = x_0$, якщо:

а) $f(x) = x^4 - 3x^3 + 6x^2 - 10x + 16$, $x_0 = 4$ і $K = \mathbf{Z}$;

б) $f(x) = x^5 + (1+2i)x^4 - (1+3i)x^2 + 7$, $x_0 = -2 - i$, $K = \mathbf{C}$;

в) $f(x) = x^5 + x^4 + \bar{3}x^2 + \bar{1}$, $x_0 = \bar{3}$, $K = Z_5$;

г) $f(x) = x^3 - (1+\sqrt{2})x^2 + (1+\sqrt{2})$, $x_0 = 1 - \sqrt{2}$, $K = Q(\sqrt{2})$.

22.4. Знайти такі значення a і b, при яких многочлен $f(x) = x^5 - a^2x^2 + bx + 1$ ділиться на двочлени $g_1(x) = x - 1$ і $g_2(x) = x + 1$ у кільці $R[x]$.

22.5. Довести, що многочлен $f(x) = x^n - a^n$ для кожного $n \in \mathbf{N}$ ділиться на двочлен $g(x) = x - a$ над будь-якою областю цілісності K з одиницею.

22.6. Довести, що многочлен $f(x) \in K[x]$ ділиться на $g(x) = x - a$ для довільного $a \in K$, якщо:

а) $f(x) = x^7 - x$ і $K = Z_7$;

б) $f(x) = x^{10} - x^5$ і $K = Z_5$;

в) $f(x) = x^p - x$ і $K = Z_p$.

22.7. Остачі від ділення многочлена $f(x)$ з кільця $Z[x]$ на $g_1(x) = x - 2$ і $g_2(x) = x - 1$ відповідно дорівнюють 1 та 2. Знайти остачу при діленні цього многочлена на $g(x) = (x-1)(x-2)$.

22.8. Остачі від ділення многочлена $f(x)$ з кільця $Z[x]$ на $g_1(x) = x - 1$, $g_2(x) = x - 2$, $g_3(x) = x + 1$ відповідно дорівнюють 3, 15 та 0. Знайти остачу від ділення $f(x)$ на $g(x) = x^3 - 2x^2 - x + 2$.

22.9. Многочлен $f(x)$ з кільця $C[x]$ ділиться на $g_1(x) = x + 1$; при діленні на $g_2(x) = x - 1$ цей многочлен дає остачу 2, а при діленні на $g_3(x) = x - i$ остачу $-i$. Знайти остачу від ділення многочлена $f(x)$ на $g(x) = (x^2 - 1)(x - i)$.

22.10. Знайти остачу від ділення многочлена $f(x) = x^{243} + x^{81} + x^{27} + x^9 + x^3 + x + 1$ на двочлени:

а) $g(x) = x + i$; б) $g(x) = x^2 + 1$.

22.11. Довести, що многочлен

$$f(x) = (\cos\alpha - x\sin\alpha)^n - \cos n\alpha + x\sin n\alpha$$

ділиться на $g_1(x) = x + i$ і $g_2(x) = x - i$ в кільці $C[x]$ для всіх $n \in \mathbf{N}$ і $\alpha \in \mathbf{R}$.

22.12. Довести, що многочлен $f(x) = x^n + a^n$ ділиться на двочлен $g(x) = x + a$ в $Z_2[x]$.

22.13. Довести, що многочлен $f(x) = (x+a)^n - x^n - a^n$ ділиться:

а) на $g(x) = x$ над областю цілісності K з одиницею;

б) на $g(x) = x + a$ над областю цілісності K з одиницею при непарному n;

в) на $g(x) = x + a$ в кільці $Z_2[x]$.

22.14. Довести, що при непарному n многочлен

$$f(x) = (x + a + b)^n - x^n - a^n - b^n$$

ділиться на $g_1(x) = x + a$ і $g_2(x) = x + b$ в кільці $R[x]$.

22.15. Довести, що при непарному n многочлен

$$f(x) = (x-a)^n + (a-b)^n + (b-x)^n$$

ділиться на $g_1(x) = x - a$ і $g_2(x) = x - b$ в кільці $R[x]$.

22.16. Довести, що многочлен $f(x)$, утворений з многочлена $h(y)$ заміною $y = x^n$, $n \in \mathbf{N}$, при діленні на двочлен $g(x) = x^n - a$ над областю цілісності K з одиницею дає остачу $f(a)$.

22.17. Знайти остачу від ділення многочлена $f(x) = x^4 - 2x^2 + 6$ на $g(x) = x^2 - 1$ в $Z[x]$.

22.18. Знайти остачу від ділення многочлена $f(x) = x^6 + \bar{2}x^3 + \bar{2}$ на $g(x) = x^3 + \bar{1}$ в кільці $Z_3[x]$.

22.19. Довести, що многочлен $f(x) = x^p - x + \bar{1}$ з кільця $Z_p[x]$, де p — просте число, не ділиться на двочлен $g(x) = x - \bar{a}$ при жодному $\bar{a} \in Z_p$.

22.20. Довести, що многочлен $f(x)$ не ділиться на многочлен $g(x)$ в кільці $K[x]$, якщо:

а) $f(x) = x^{1984} + x + 1$, $g(x) = x^2 - 1$ і $K = \mathbf{Z}$;

б) $f(x) = x^{2m} + \bar{2}x + \bar{2}$, $g(x) = x^2 + \bar{4}$ і $K = Z_5$;

в) $f(x) = x^3 - 6x^2 + 11x - 6$, $g(x) = x^2 - 5x + 4$ і $K = \mathbf{Z}$.

22.21. Визначити a і b так, щоб многочлен $f(x) = ax^4 + bx^3 + 1$ ділився на $g(x) = (x-1)^2$ в кільці $Z[x]$

22.22. Розкласти многочлен $f(x)$ за степенями двочлена $g(x) = x - a$, якщо:

а) $f(x) = x^4 - 2x^3 + 3x^2 - 5x + 1$, $a = 1$ в кільці $Q[x]$;

б) $f(x) = \bar{2}x^4 + x^3 + x^2 + \bar{2}$, $a = \bar{1}$ в кільці $Z_3[x]$;

в) $f(x) = x^5 - 3ix^3 - 4x^2 + 5ix - 1$, $a = -i$ в кільці $C[x]$.

22.23. Розкласти:

а) $f(x) = x^6 - 4x^5 - 7x^4 + x^3 + 2x^2 - x - 1$ за степенями двочлена $g(x) = x^2 - 1$ в кільці $Z[x]$;

б) $f(x) = x^7 + \bar{1}$ за степенями двочлена $g(x) = x^3 + \bar{2}$ в кільці $Z_5[x]$;

в) $f(x) = x^4 - 2x + i$ за степенями двочлена $g(x) = x^3 + i$ в кільці $C[x]$.

§ 23. Найбільший спільний дільник і найменше спільне кратне многочленів

Література

[1] — § 22, с. 238—243;
[2] — § 22, с. 242—247;
[3] — гл. 14, § 2, с. 470—471;
[5] — гл. IX, § 3, с. 323—333;
[6] — § 21, с. 137—143;
[7] — § 8, с. 55—60;
[8] — гл. 5, § 3, с. 226—229.

ТЕОРЕТИЧНІ ВІДОМОСТІ

Нехай $f(x)$ і $g(x)$ — многочлени над полем P. Якщо $f(x)$ і $g(x)$ діляться на многочлен $d(x)$ з кільця $P[x]$, то $d(x)$ називають їхнім **спільним дільником.**

Спільний дільник многочленів $f(x)$ і $g(x)$, який ділиться на кожний їхній спільний дільник, називають **найбільшим спільним дільником** многочленів $f(x)$, $g(x)$ і позначають символом (f, g).

Найбільший спільний дільник заданих многочленів визначається однозначно з точністю до сталого множника.

Для будь-яких двох многочленів $f(x)$ і $g(x)$ з кільця $P[x]$ (з яких хоча б один відмінний від 0) існує найбільший спільний дільник, який дорівнює останній відмінній від нуля остачі в алгоритмі Евкліда.

Найбільший спільний дільник $d(x)$ многочленів $f(x)$ і $g(x)$ з кільця $P[x]$ завжди можна подати у вигляді

$$d(x) = f(x)\,u(x) + g(x)\,v(x),$$

де $u(x)$ і $v(x)$ — деякі многочлени з кільця $P[x]$. Многочлени $f(x)$, $g(x) \in P[x]$ називаються **взаємно простими**, якщо кожен їхній спільний дільник є многочленом нульового степеня. При цьому пишуть $(f, g) = 1$.

Многочлени $f(x)$ і $g(x)$ з кільця $P[x]$ є взаємно простими тоді і тільки тоді, коли існують многочлени $u(x)$, $v(x) \in P[x]$ такі, що

$$f(x)\,u(x) + g(x)\,v(x) = 1.$$

Взаємно прості многочлени мають такі властивості:

1°. $\underset{f(x),g(x),h(x)\in P[x]}{\forall} [(f, g) = 1 \wedge (h, f) = 1 \Rightarrow (f, gh) = 1]$;

2°. $\underset{f(x),g(x),h(x)\in P[x]}{\forall} [f(x)\,g(x) \vdots h(x) \wedge (f, h) = 1 \Rightarrow g(x) \vdots h(x)]$;

3°. $\underset{f(x),g(x),h(x)\in P[x]}{\forall} [f(x) \vdots g(x) \wedge f(x) \vdots h(x) \wedge (g, h) = 1 \Rightarrow f(x) \vdots g(x)\,h(x)]$.

Спільним кратним многочленів $f(x)$, $g(x)$ з кільця $P[x]$ називають многочлен $s(x) \in P[x]$ такий, що $s(x)$ ділиться на $f(x)$ і $g(x)$. **Найменшим спільним кратним** многочленів $f(x)$ і $g(x)$ називається таке їхнє спільне кратне, на яке ділиться кожне спільне кратне цих многочленів.

Найменше спільне кратне многочленів $f(x)$ і $g(x)$ визначається однозначно з точністю до сталого множника і позначається через $[f, g]$.

Для довільних відмінних від нуля многочленів $f(x)$ і $g(x)$ з кільця $P[x]$ найменше спільне кратне існує в $P[x]$ і визначається за формулою

$$[f, g] = \frac{f(x)\,g(x)}{(f, g)}.$$

ПРИКЛАДИ РОЗВ'ЯЗУВАННЯ ЗАДАЧ

1. Знайти найбільший спільний дільник і найменше спільне кратне многочленів $f(x) = 3x^3 - 6x^2 + 5x - 10$ і $g(x) = 2x^3 - 4x^2 + 3x - 6$ в кільці $Q[x]$.

Розв'язання. Розглянемо многочлен $s(x) = 2f(x) - 3g(x) = x - 2$. З властивостей подільності та означення найбільшого спільного дільника многочленів маємо $(f(x), g(x)) = (s(x), g(x))$. Оскільки $g(2) = 0$, то за теоремою Безу $g(x) \vdots s(x)$. Тому

$$(f, g) = s(x) = x - 2.$$

Для обчислення найменшого спільного кратного $[f, g]$ цих многочленів використаємо формулу

$$[f, g] = \frac{f(x)\,g(x)}{(f, g)}.$$

Оскільки $g(x) = (2x^2 + 3)(x - 2)$, то

$$[f, g] = \frac{(3x^3 - 6x^2 + 5x - 10)(2x^2 + 3)(x - 2)}{x - 2} = (3x^3 - 6x^2 + 5x + 10)(2x^2 + 3).$$

2. Для многочленів $f(x) = x^4 + \bar{4}x^3 + \bar{4}x^2 + \bar{6}x + \bar{6}$ і $g(x) = x^3 - \bar{1}$ з кільця $Z_7[x]$ знайти їхній найбільший спільний дільник і многочлени $u(x)$ і $v(x)$ такі, що

$$f(x)\,u(x) + g(x)\,v(x) = (f, g).$$

Розв'язання. Застосуємо алгоритм Евкліда до многочленів $f(x)$ і $g(x)$ (табл. 22—24). Звідси

$$(f, g) = r_2(x) = x + \bar{6},$$

$$r_2(x) = g(x) - r_1(x)\,s_2(x) = g(x) - (f(x) - g(x)\,s_1(x))\,s_2(x) =$$

$$= f(x)(-s_2(x)) + g(x)(\bar{1} + s_1(x)\,s_2(x)).$$

Тому

$$u(x) = -s_2(x) = -\bar{2}x = \bar{5}x,$$

$$v(x) = \bar{1} + s_1(x)\,s_2(x) = \bar{1} + (x + \bar{4})\,\bar{2}x = \bar{2}x^2 + x + \bar{1}.$$

Таблиця 22

	$\bar{1}$	$\bar{4}$	$\bar{4}$	$\bar{6}$	$\bar{6}$	$f(x) = g(x)\,s_1(x) + r_1(x)$,
$-\bar{1}$				$-\bar{1}$	$-\bar{4}$	$s_1(x) = x + \bar{4}$,
	$\bar{1}$	$\bar{4}$	$\bar{4}$	$\bar{0}$	$\bar{3}$	$r_1(x) = \bar{4}x^2 + \bar{3}$;

Таблиця 23

$\bar{4}$	$\bar{1}$	$\bar{0}$	$\bar{0}$	$-\bar{1}$	$g(x) = r_1(x)\,s_2(x) + r_2(x)$,
$\bar{3}$			$\bar{6}$	$\bar{0}$	$s_2(x) = \bar{2}x$,
	$\bar{2}$	$\bar{0}$	$-\bar{6}$	$-\bar{1}$	$r_2(x) = -\bar{6}x - \bar{1} = x + \bar{6}$;

Таблиця 24

	$\bar{4}$	$\bar{0}$	$\bar{3}$	$r_1(x) = r_2(x)\,s_3(x)$,
$\bar{6}$	$\bar{4}$	$-\bar{3}$	$\bar{0}$	$s_3(x) = \bar{4}x - \bar{3}$.

3. Нехай $f(x)$, $g(x)$ і $h(x)$ — деякі многочлени з кільця $P[x]$ над полем P. Знайти всі многочлени $u(x)$ і $v(x)$ в кільці $P[x]$ такі, що

$$f(x)\,u(x) + g(x)\,v(x) = h(x), \tag{1}$$

коли деякі многочлени $u_0(x)$, $v_0(x)$, над полем P задовольняють цю рівність.

Розв'язання. Позначимо $(f, g) = d(x)$, $f_1(x) = \frac{f(x)}{d(x)}$ і $g_1(x) = \frac{g(x)}{d(x)}$. Тоді кожна пара многочленів

$$\begin{cases} u(x) = u_0(x) + g_1(x)\,s(x), \\ v(x) = v_0(x) - f_1(x)\,s(x), \end{cases} \tag{2}$$

де $s(x) \in P[x]$, також задовольняє рівність (1). Покажемо, що кожен розв'язок рівняння (1) у кільці $P[x]$ відносно $u(x)$ і $v(x)$ можна подати у вигляді (2). Справді, нехай $u_1(x)$ і $v_2(x)$ також є розв'язком рівняння (1), тобто

$$f(x)\,u_0(x) + g(x)\,v_0(x) = h(x),$$
$$f(x)\,u_1(x) + g(x)\,v_1(x) = h(x).$$

Тоді

$$f(x)\,(u_0(x) - u_1(x)) + g(x)\,(v_0(x) - v_1(x)) = 0,$$
$$f(x)\,(u_0(x) - u_1(x)) = -g(x)\,(v_0(x) - v_1(x)),$$
$$f_1(x)\,(u_0(x) - u_1(x)) = -g_1(x)\,(v_0(x) - v_1(x)).$$

Оскільки $(f_1, g_1) = 1$, то за властивістю взаємно простих многочленів в кільці $P[x]$ існує многочлен $\bar{s}(x)$ такий, що

$$\begin{cases} u_0(x) - u_1(x) = -g_1(x)\,\bar{s}(x), \\ v_0(x) - v_1(x) = f_1(x)\,\bar{s}(x). \end{cases}$$

Тому

$$\begin{cases} u_1(x) = u_0(x) + g_1(x)\,\bar{s}(x), \\ v_1(x) = v_0(x) - f_1(x)\,\bar{s}(x), \end{cases}$$

тобто будь-який розв'язок рівняння (1) можна подати у вигляді (2).
Таким чином, рівності (2) задають всі пари многочленів $u(x)$ і $v(x)$, які задовольняють рівність (1).

4. Розв'язати рівняння

$$u(x)\,(x^2 - 1) + v(x)\,(x^2 + 2x + 1) = x^3 + 1$$

відносно многочленів $u(x)$ і $v(x)$ у кільці $Q[x]$.
Розв'язання. Задане рівняння в кільці $Q[x]$ рівносильне рівнянням

$$u(x)\,(x-1)\,(x+1) + v(x)\,(x+1)^2 = (x+1)\,(x^2 - x + 1)$$

і

$$u(x)\,(x-1) + v(x)\,(x+1) = x^2 - x + 1.$$

Двочлени $g_1(x) = x - 1$ і $g_2(x) = x + 1$ є взаємно простими і

$$-\frac{1}{2}\,g_1(x) + \frac{1}{2}\,g_2(x) = 1.$$

Звідси

$$-\frac{1}{2}\,(x^2 - x + 1)\,g_1(x) + \frac{1}{2}\,(x^2 - x + 1)\,g_2(x) = x^2 - x + 1,$$

тобто одним з розв'язків останнього, а, отже, і заданого рівняння відносно $u(x)$ і $v(x)$ є многочлени

$$u_0(x) = -\frac{1}{2}\,(x^2 - x + 1),$$

$$v_0(x) = \frac{1}{2}\,(x^2 - x + 1).$$

Застосовуючи тепер формулу (2) з прикладу 3, маємо

$$u(x) = -\frac{1}{2}\,(x^2 - x + 1) + (x + 1)\,s(x)$$

$$v(x) = \frac{1}{2}\,(x^2 - x + 1) - (x - 1)\,s(x)$$

де $s(x) \in Q[x]$.

Задачі

23.1. Нехай $f(x)$ і $g(x)$ є многочлени над полем P, $s(x) = f(x) + g(x)$, $h(x) = f(x) - g(x)$. Довести, що $(f, g) = (s, h)$.

23.2. Нехай $f(x)$ і $g(x)$ — многочлени над полем P. Знайти необхідну і достатню умови, при яких многочлени $s(x) = a_{11}f(x) + a_{12}g(x)$ і $h(x) = a_{21}f(x) + a_{22}g(x)$ з кільця $P[x]$ мають той самий найбільший спільний дільник, що й многочлени $f(x)$ і $g(x)$.

23.3. Не застосовуючи алгоритм Евкліда, знайти найбільший спільний дільник таких многочленів:

а) $f(x) = x^3 + 3x^2 - 2$,
$g(x) = x^3 + 3x^2 - x - 3$;

б) $f(x) = x^4 + x^3 - 3x^2 - 2x - 2$,
$g(x) = -x^3 + 3x^2 + 2x + 2$;

в) $f(x) = x^4 + x^3 - 3x^2 - 2x - 1$,
$g(x) = x^3 + x^2 - 3x - 3$;

г) $f(x) = 2x^3 + x^2 + 4x + 2$,
$g(x) = 2x^3 + x^2 + 6x + 3$.

23.4. Довести, що многочлени $f(x) = a_nx^n + \ldots + a_1x + a_0$, де $a_0 \neq 0$ і $g(x) = a_nx^n + \ldots + a_1x$, є взаємно простими.

23.5. Користуючись алгоритмом Евкліда, знайти найбільший спільний дільник таких многочленів:

а) $f(x) = x^3 + x^2 - 4x - 6$,
$g(x) = x^3 + x^2 - 10x - 6$ в кільці $Q[x]$;

б) $f(x) = 3x^4 - 3x^3 + 4x^2 - x + 1$,
$g(x) = 2x^3 - x^2 + x + 1$ в кільці $Q[x]$;

в) $f(x) = x^4 + x^3 + x^2 + x + 1$,
$g(x) = 4x^3 + 3x^2 + 2x + 1$ в кільці $Q[x]$;

г) $f(x) = x^3 + \bar{3}x^2 + \bar{2}x + \bar{1}$,
$g(x) = x^3 + \bar{2}x^2 + x + \bar{2}$ в кільці $Z_5[x]$;

д) $f(x) = x^4 + 2ix^3 - 2x^2 - 2ix + 1$,
$g(x) = x^3 + (i+1)\,x^2 + ix$ в кільці $C[x]$.

23.6. Знайти найменше спільне кратне таких многочленів:

а) $f(x) = x^4 - 4x^3 + 4x^2 - 5x - 2$,
$g(x) = x^2 - x + 2$ в кільці $Q[x]$;

б) $f(x) = 2x^3 + 7x^2 + 4x - 3$,
$g(x) = x^3 + x^2 - 3x + 1$ в кільці $Q[x]$;

в) $f(x) = x^3 + \bar{6}x^2 + \bar{4}x + \bar{1}$,
$g(x) = x^3 + x^2 + \bar{3}x - \bar{4}$ в кільці $Z_7[x]$;
г) $f(x) = x^3 - x^2 + 3x - 3$,
$g(x) = x^4 + 2x^3 + 2x - 1$ в кільці $R[x]$;
д) $f(x) = x^4 + 2ix^3 - 2x^2 - 2ix + 1$,
$g(x) = x^3 + (i+1)x^2 + ix$ в кільці $C[x]$.

23.7. Визначити многочлени $u(x)$ і $v(x)$ так, щоб для многочленів $f(x)$ і $g(x)$ виконувалась рівність $f(x)u(x) + g(x)v(x) = (f, g)$, якщо:
а) $f(x) = x^3 + 5x^2 + 6x + 2$, $g(x) = x^2 + 6x + 5$ в кільці $Q[x]$;
б) $f(x) = x^3 + \bar{3}x^2 + \bar{2}x + \bar{1}$,
$g(x) = x^3 + \bar{2}x^2 + x + \bar{2}$ в кільці $Z_5[x]$;
в) $f(x) = 4x^4 - 2x^3 - 16x^2 + 5x + 9$,
$g(x) = 2x^3 - x^2 - 5x + 4$ в кільці $Q[x]$;
г) $f(x) = x^4 + 1$,
$g(x) = x^3 - 2ix - x$ в кільці $C[x]$.

23.8. Нехай P — деяке поле, $f(x)$ і $g(x)$ — многочлени з кільця $P[x]$. Довести, що найменший ідеал I в кільці $P[x]$, що містить многочлени $f(x)$ і $g(x)$, збігається з головним ідеалом, породженим многочленом (f, g).

23.9. Довести, що множина I всіх спільних кратних многочленів $f(x)$ і $g(x)$ з кільця $P[x]$ многочленів над полем P є ідеал. Яким многочленом породжується цей ідеал?

23.10. У кільці $P[x]$ многочленів над полем P знайти найменший ідеал I, який містить многочлени $f_1(x), f_2(x), \ldots, f_n(x)$.

23.11. Яким умовам повинні задовольняти многочлени $f(x)$, $g(x)$ і $h(x)$ над полем P, щоб рівняння $f(x)u(x) + g(x)v(x) = h(x)$ мало розв'язок у кільці $P[x]$ відносно $u(x)$ і $v(x)$?

23.12. Знайти множину всіх розв'язків рівняння

$$f(x)u(x) + g(x)v(x) = h(x)$$

в кільці $K[x]$, якщо:
а) $f(x) = x^2 - 1$,
$g(x) = x^2 - 2x + 1$,
$h(x) = x^3 - 1$ і $K = Q$;
б) $f(x) = x^3 - \bar{1}$,
$g(x) = x^2 + \bar{3}$,
$h(x) = x^3 - \bar{2}x^2 + x$ і $K = Z_5$;
в) $f(x) = x^2 + (2+i)x + 2i$,
$g(x) = x^2 - 4$,
$h(x) = x^2 + 2ix$ і $K = C$;
г) $f(x) = (x^2 + 1)^2$,
$g(x) = x + i$,
$h(x) = x^2 + (1+i)x + i$ і $K = C$.

23.13. Визначити найбільший спільний дільник многочленів:
а) $f(x) = x^4 + x^3 - 3x^2 - 4x - 1$,
$g(x) = x^3 + x^2 - x - 1$,
$h(x) = 2x^3 + 4x^2 + 2x$ в кільці $Q[x]$;

б) $f(x) = x^5 + x^4 + \bar{1}$,
$g(x) = x^4 + x^2 + \bar{1}$,
$h(x) = x^3 + \bar{1}$ в кільці $Z_2[x]$;
в) $f(x) = x^3 - x^2 + x - 1$,
$g(x) = x^3 - (2i+1)x^2 + (2i-1)x + 1$,
$h(x) = x^2 + (1+i)x + i$ в кільці $C[x]$.

23.14. З'ясувати, чи має розв'язок рівняння

$$f(x)u(x) + g(x)v(x) + h(x)w(x) = s(x)$$

в кільці $K[x]$, якщо:
а) $f(x) = x^4 + 2x^3 - 2x - 1$,
$g(x) = x^2 - 1$,
$h(x) = x^3 - x$,
$s(x) = x^3 - 3x^2 + 1$ і $K = Q$;
б) $f(x) = x^4 + 2x^2 + 1$,
$g(x) = x^3 - x^2 + x - 1$,
$h(x) = x^2 + (i+1)x + i$,
$s(x) = x^2 + (i-1)x - i$ і $K = C$.

§ 24. Незвідні многочлени над полем. Розклад многочленів на незвідні множники

Література

[1] — § 22, с. 243—247;
[2] — § 22, с. 247—252;
[3] — гл. 14, § 2, с. 471—474;
[5] — гл. IX, § 3, с. 333—339;
[6] — § 48, с. 290—295;
[7] — § 9, с. 60—64;
[8] — гл. 5, § 3, 4, с. 229—232.

ТЕОРЕТИЧНІ ВІДОМОСТІ

Нехай $f(x)$ — деякий многочлен над полем P. Многочлен $f(x)$ називається **незвідним** в $P[x]$ (або над полем P), якщо він не є константою і не має в $P[x]$ інших дільників, крім констант і многочленів виду $cf(x)$, де $c \in P \setminus \{0\}$.

Многочлен $f(x)$ називається **звідним** в $P[x]$ (над полем P), якщо $\deg f \geqslant 1$ і в кільці $P[x]$ існують такі многочлени $g(x)$, $s(x)$, що $f(x) = g(x)s(x)$, $\deg g \geqslant 1$ і $\deg s \geqslant 1$.

Незвідні над полем P многочлени мають такі найпростіші властивості:

1°. Многочлен першого степеня над будь-яким полем P є незвідним у кільці $P[x]$;

2°. Якщо многочлен $p(x)$ є незвідним над полем P, то для кожного $c \in P \setminus \{0\}$ многочлен $cp(x)$ також незвідний над P;

3°. Якщо многочлен $p(x)$ є незвідним над полем P, то для будь-якого многочлена $f(x)$ з кільця $P[x]$ $f(x) \vdots p(x)$ або $f(x)$ і $p(x)$ є взаємно прості;

4°. Якщо незвідний многочлен $p(x)$ над полем P ділиться на незвідний многочлен $q(x)$ з кільця $P[x]$, то ці многочлени відрізняються тільки сталим множником.

Будь-який многочлен ненульового степеня над полем P можна подати у вигляді добутку незвідних многочленів $p_k(x)$, $1 \leqslant k \leqslant l$, над полем P:

$$f(x) = p_1(x)p_2(x)\ldots p_l(x).$$

Такий розклад є єдиним з точністю до сталих множників і порядку нумерації многочленів $p_k(x)$.

Зображення многочлена $f(x)$ з кільця $P[x]$ у вигляді добутку

$$f(x) = [p_1(x)]^{k_1}[p_2(x)]^{k_2}\dots[p_m(x)]^{k_m},$$

де $p_1(x), p_2(x), \dots, p_m(x)$ — попарно взаємно прості і незвідні над полем P многочлени, називають **канонічним розкладом** многочлена $f(x)$ над полем P.

Канонічний розклад для будь-якого многочлена ненульового степеня $f(x)$ над полем P завжди існує і єдиний з точністю до сталих множників та порядку нумерації множників.

Якщо многочлени $f(x)$ і $g(x)$ розкладено в добуток незвідних множників над полем P, то їхній найбільший спільний дільник (f, g) дорівнює добутку всіх незвідних множників, які входять у розклад як $f(x)$, так і $g(x)$. Якщо таких спільних незвідних множників немає, то многочлени $f(x)$ і $g(x)$ є взаємно простими.

ПРИКЛАДИ РОЗВ'ЯЗУВАННЯ ЗАДАЧ

1. Чи є звідним у полі **Q** многочлен

$$f(x) = x^4 + 2x^3 - 3x^2 - 5x + 2?$$

Розв'язання. Нехай многочлен $f(x)$ є звідним у полі **Q**, тобто його можна розкласти в добуток не менше як двох многочленів ненульового степеня з кільця $Q[x]$. Щоб розкласти многочлен $f(x)$ на множники, застосуємо метод невизначених коефіцієнтів. При цьому досить розглянути два випадки можливого розкладу:

1) обидва множники мають степінь 2;
2) один множник має степінь 1, а другий 3.

Нехай

$$f(x) = (ax^2 + bx + c)(dx^2 + mx + n). \tag{1}$$

Тоді з рівності $x^4 + 2x^3 - 3x^2 - 5x + 2 = adx^4 + (am + bd)x^3 + (an + bm + cd)x^2 + (bn + cm)x + cn$ маємо

$$\begin{cases} ad = 1, \\ am + bd = 2, \\ an + bm + cd = -3, \\ bn + cm = -5, \\ cn = 2. \end{cases} \tag{2}$$

Розв'яжемо цю систему рівнянь у цілих числах. З першого знаходимо $a = d = 1$ або $a = d = -1$, з останнього $c = 1$, $n = 2$; $c = 2$, $n = 1$; $c = -2$, $n = -1$; $c = -1$, $n = -2$. Розглянемо кожен з восьми можливих варіантів. Якщо $a = d = 1$ і $c = 1$, $n = 2$, то система набирає вигляду

$$\begin{cases} m + b = 2, \\ bm = -6, \\ 2b + m = -5. \end{cases}$$

Ця система несумісна.

У кожному з решти варіантів несумісними також є системи рівнянь:

$$\begin{cases} m + b = 2, \\ bm = -6, \\ b + 2m = -5, \end{cases} \quad \begin{cases} m + b = 2, \\ bm = 0, \\ -2b - m = -5, \end{cases} \quad \begin{cases} m + b = 2, \\ bm = 0, \\ -2b - m = -5, \end{cases} \quad \begin{cases} m + b = -2, \\ bm = 0, \\ 2b + m = -5, \end{cases}$$

$$\begin{cases} m + b = -2, \\ bm = 0, \\ b + 2m = -5, \end{cases} \quad \begin{cases} m + b = -2, \\ bm = -6, \\ -b - 2m = -5, \end{cases} \quad \begin{cases} m + b = -2, \\ bm = -6, \\ -2b - m = -5. \end{cases}$$

Це означає, що система рівнянь (2) несумісна і многочлен $f(x)$ не розкладається в добуток двох многочленів другого степеня з цілими коефіцієнтами. Припустимо, що розклад (1) виконується при дробових числах a, b, c, d, m, n. Зведемо до найменшого спільного знаменника коефіцієнти многочленів $g_1(x) = ax^2 + bx + c$ і $g_2(x) = dx^2 + mx + n$ та винесемо за дужки ці знаменники і найбільші спільні дільники чисельників обох многочленів. Дістанемо розклад

$$f(x) = \frac{r}{s}(a_1x^2 + b_1x + c_1)(d_1x^2 + m_1x + n_1),$$

де $(r, s) = (a_1, b_1, c_1) = (d_1, m_1, n_1) = 1$. Оскільки коефіцієнти многочлена $f(x)$ є цілими числами, то всі коефіцієнти многочлена

$$g(x) = (a_1x^2 + b_1x + c_1)(d_1x^2 + m_1x + n_1)$$

мають ділитися на число s, а тому й на кожен його простий дільник p. Разом з тим, серед кожної трійки чисел a_1, b_1, c_1 та d_1, m_1, n_1 знайдуться числа, які не діляться на p. Тому серед коефіцієнтів a_1d_1, $a_1m_1 + b_1d_1$, $a_1n_1 + b_1m_1 + c_1d_1$, $b_1n_1 + c_1m_1$ і c_1n_1 многочлена $g(x)$ знайдеться такий, що не ділиться на p. Тому $s = 1$ і ми дістанемо розклад (1) з цілими коефіцієнтами, що неможливо.

Нехай

$$f(x) = (ax + b)(cx^3 + dx^2 + mx + n). \tag{3}$$

Тоді з рівності $x^4 + 2x^3 - 3x^2 - 5x + 2 = acx^4 + (ad + bc)x^3 + (am + bd)x^2 + (an + bm)x + bn$ маємо:

$$\begin{cases} ac = 1, \\ ad + bc = 2, \\ am + bd = -3, \\ an + bm = -5, \\ bn = 2. \end{cases} \tag{4}$$

Одним з розв'язків системи (4) є $a = c = n = 1$, $b = 2$, $d = 0$ і $m = -3$. Отже, $f(x) = (x + 2)(x^3 - 3x + 1)$, тобто многочлен $f(x)$ звідний у полі **Q**.

2. Довести, що многочлен $f(x) = \bar{2}x^2 + x + \bar{1}$ незвідний у полі Z_3.

Розв'язання. Якщо многочлен $f(x)$ є звідним у полі Z_3, то його можна подати у вигляді $f(x) = (\bar{a}x + \bar{b})(\bar{c}x + \bar{d})$, де $\bar{a}\bar{c} \neq 0$. Звідси $f(x) = \bar{a}\left(x + \frac{\bar{b}}{\bar{a}}\right)(\bar{c}x + \bar{d})$ і згідно з теоремою Безу многочлен $f(x)$ має коренем $x = -\frac{\bar{b}}{\bar{a}}$.

Проте $f(\bar{0}) = \bar{1}$, $f(\bar{1}) = \bar{1}$ і $f(\bar{2}) = \bar{2}$, тобто многочлен $f(x)$ не має коренів в Z_3. Отже, многочлен $f(x)$ незвідний у полі Z_3.

3. Довести, що фактор-кільце $P[x]/<p(x)>$ кільця многочленів $P[x]$ над полем P за ідеалом $<p(x)>$, породженим незвідним у полі P многочленом $p(x)$, є полем.

Розв'язання. Відомо, що елементи кільця $P[x]/I$ мають вигляд

$$A = f(x) + \{g(x)p(x) | g(x) \in P[x]\},$$

де $f(x)$ — представник класу A. З означення операції множення у фактор-кільці і того, що $P[x]$ є областю цілісності, випливає її комутативність. Клас $E = 1 + <p(x)>$ є одиницею в $P[x]/<p(x)>$.

Візьмемо тепер довільний елемент B фактор-кільця $P[x]/<p(x)>$ такий, що $B \neq <p(x)>$. Тоді у множині B існує многочлен $h(x)$, який не ділиться на многочлен $p(x)$, $B = h(x) + <p(x)>$ і за властивістю незвідних многочленів $h(x)$ і $p(x)$ є взаємно простими. Отже, в кільці $P[x]$ існують многочлени $u(x)$ і $v(x)$ такі, що

$$h(x)u(x) + p(x)v(x) = 1.$$

Звідси $h(x)u(x) = 1 - p(x)v(x)$. Тому оберненим елементом до B є $B^{-1} = u(x) + <p(x)>$.

Таким чином, фактор-кільце $P[x]/<p(x)>$ є полем.

4. Знайти найбільший спільний дільник і найменше спільне кратне многочленів

$$f(x) = (x-2)(x-3)^2(x+1)$$

і

$$g(x) = x^3 - 3x^2 - 2x + 6 \text{ з кільця } Q[x].$$

Розв'язання. Для многочлена $f(x)$ відомий канонічний розклад у полі Q. Щоб знайти найбільший спільний дільник і найменше спільне кратне даних многочленів, доцільно знайти канонічний розклад многочлена $g(x)$ у полі Q. Це можна зробити групуванням його членів і винесенням спільного множника:

$$g(x) = (x^3 - 3x^2) - (2x - 6) = x^2(x-3) - 2(x-3) = (x-3)(x^2-2).$$

Тепер за теоремою про знаходження найбільшого спільного дільника і найменшого спільного кратного многочленів, розкладених на незвідні у полі Q множники, маємо:

$$(f, g) = x - 3;$$

$$[f, g] = (x-2)(x^2-2)(x-3)^2(x+1).$$

Задачі

24.1. Довести, що многочлен

а) $f(x) = x^3 - 2$ незвідний у полі $\mathbf{Q}$;
б) $f(x) = x^2 + x + 1$ незвідний у полі $\mathbf{Q}$;
в) $f(x) = x^2 + x + \bar{1}$ незвідний у полі Z_5;
г) $f(x) = x^4 + \bar{1}$ незвідний у полі $\mathbf{Q}$;
д) $f(x) = x^4 + \bar{1}$ звідний у полі Z_5;
е) $f(x) = x^6 + x^3 + 1$ незвідний у полі $\mathbf{Q}$.

24.2. У кільці $Z_3[x]$ знайти всі многочлени другого степеня, які є незвідними у полі Z_3.

24.3. У кільці $Z_5[x]$ справджуються рівності:

$$x^2 + x + \bar{4} = (x + \bar{3})^2 \text{ і } x^2 + x + \bar{4} = (\bar{4}x + \bar{2})^2.$$

Чи не суперечать вони теоремі про розклад многочлена на незвідні множники у полі Z_5?

24.4. Довести, що кожен многочлен другого степеня над полем $\mathbf{C}$ є звідним у полі $\mathbf{C}$.

24.5. Многочлен $f(x) = x^2 + \bar{2}x + \bar{2}$ можна розглядати в кільцях $Z_5[x]$ і $Z_3[x]$. Він є звідним у полі Z_5 і незвідним у полі Z_3. Чи є такий многочлен, що належить обом кільцям і є звідним у полі Z_3, а незвідним у полі Z_5?

24.6. Довести, що в кільці $Z_p[x]$ при довільному простому p існують незвідні у полі Z_p многочлени як завгодно великого степеня.

24.7. Довести, що множина незвідних многочленів у будь-якому полі P є нескінченною.

24.8. Многочлен $f(x) = \bar{2}x^3 + \bar{3}x^2 + \bar{3}x + \bar{2}$ розкласти на незвідні в полі Z_5 множники, якщо відомо, що цей многочлен має два корені, які є протилежними елементами в полі Z_5.

24.9. Розкласти на незвідні множники в полі $\mathbf{Q}$ такі многочлени:

а) $f(x) = 2x^5 - x^4 - 6x^3 + 3x^2 + 4x - 2$;
б) $f(x) = 3x^5 + x^4 - 15x^3 - 5x^2 + 12x + 4$,

які мають по дві пари коренів, що відрізняються тільки знаком.

24.10. Розкласти на незвідні множники многочлен

$$f(x) = 2x^5 - x^4 - 2x^3 + x^2 - 4x + 2$$

в полях $\mathbf{Q}$, $\mathbf{R}$ і $\mathbf{C}$, якщо він має дві пари коренів у полі, які є протилежними числами.

24.11. Довести, що многочлен третього степеня звідний у полі $\mathbf{Q}$ тоді і тільки тоді, коли один з його коренів є раціональним числом.

24.12. Нехай многочлен $f(x)$ належить кільцям $Z_p[x]$ і $Z[x]$ залежно від інтерпретації його коефіцієнтів. Довести, що кожен незвідний у полі Z_p многочлен не можна розкласти на множники в кільці $Z[x]$.

24.13. Довести незвідність у кільці $Z[x]$ таких многочленів:

а) $f(x) = x^5 - x^2 + 1$;
б) $f(x) = x^5 + x^4 + x^3 + x^2 + 1$;
в) $f(x) = x^3 - x^2 + x + 1$.

24.14. Довести, що многочлен $f(x) = x^{2k} + x^k + 1$ є незвідним у полі $\mathbf{Q}$ при будь-якому $k \in \mathbf{N}$.

24.15. Чи є звідним многочлен $f(x) = x^4 + 4$ в таких полях: а) Z_5; б) $\mathbf{Q}$; в) $\mathbf{R}$; г) $\mathbf{C}$?

24.16. Розкласти на незвідні в полі P множники такі многочлени:

а) $f(x) = x^4 - 2x^3 - 27x^2 - 44x + 7$, якщо $P = \mathbf{Q}$;
б) $f(x) = x^4 - 6x^3 + 11x^2 - 6x + 1$, якщо $P = \mathbf{R}$;
в) $f(x) = 4x^4 + 4x^3 + 13x^2 + 6x + 9$, якщо $P = \mathbf{Q}$;
г) $f(x) = x^4 - 5x^3 - 8x^2 + 19x - 3$, якщо $P = \mathbf{Q}$;
д) $f(x) = (x^2 + x - 1)^2 + 3x(x^2 + x - 1) + 2x^2$, якщо $P = \mathbf{R}$;
е) $f(x) = x^2(x-3)^2 + 4x^2 - 12x + 4$, якщо $P = \mathbf{R}$;
є) $f(x) = (x+2)(x+3)(x+4)(x+5) + 1$, якщо $P = \mathbf{R}$;
ж) $f(x) = (x+a)(x+2a)(x+3a)(x+4a) + a^2$, якщо $P = \mathbf{Q}$, $a \in \mathbf{Q}$;
з) $f(x) = (x+1)(x+3)(x+9)(x+11) + 15$, якщо $P = \mathbf{Q}$;
і) $f(x) = x^4 - 10x^2 + 169$, якщо $P = \mathbf{R}$;
к) $f(x) = x^4 + x^2 + \bar{1}$, якщо $P = Z_3$;
л) $f(x) = x^8 + x^4 + 1$, якщо $P = \mathbf{Q}$;
м) $f(x) = x^8 - 1$, якщо $P = \mathbf{R}$;
н) $f(x) = x^9 - 1$, якщо $P = \mathbf{Q}$;
о) $f(x) = x^{12} - 1$, якщо $P = \mathbf{Q}$;
п) $f(x) = x^4 + 1$, якщо $P = \mathbf{C}$;
р) $f(x) = x^5 - x$, якщо $P = Z_5$.

24.17. Знайти найбільший спільний дільник і найменше спільне кратне таких многочленів:

а) $f(x) = (x-1)^2(x^2+1)(x^2-5x+6)$,
$g(x) = x^2 - x - 2$ з кільця $Z[x]$;
б) $f(x) = (x^2 - 2x + 3)^2(x^2 + 5x - 6)^2$,
$g(x) = (x^2 - 8x + 12)^2(x^3 - 1)$ з кільця $Q[x]$;
в) $f(x) = x^4 + 2x^3 - 2x - 1$,

$g(x) = (x+1)(x^2 - x - 2)$ з кільця $Q[x]$;

г) $f(x) = (x+1)^2 (x^2+1)(x^2-1)$,
$g(x) = (x-i)^2 (x+1)$ з кільця $\mathbf{C}[x]$;

д) $f(x) = x^5 - x$,
$g(x) = (x^2 + x + \bar{1})^2 (\bar{2}x + \bar{4})$ з кільця $Z_5[x]$;

е) $f(x) = x^9 - 1$,
$g(x) = x^{12} - 1$ з кільця $Q[x]$.

24.18. Чи є полем кільце $Q[x]/\langle x^2 - 1\rangle$?

24.19. У фактор-кільці $Q[x]/\langle x^2+1\rangle$ знайти елемент, обернений до класу $A = \{x + (x^2+1)s(x) \mid s(x) \in Q[x]\}$.

24.20. У фактор-кільці $Q[x]/\langle -x+1\rangle$ знайти елемент, обернений до класу A, одним з представників якого є многочлен $f(x) = x$.

24.21. У фактор-кільці $Q[x]/\langle x^2 - 4\rangle$ знайти елемент, обернений до класу A, одним з представників якого є такий многочлен:

а) $f(x) = x^2 - 5x + 6$; б) $f(x) = x^2 - 1$.

24.22. Довести, що фактор-кільце $R[x]/\langle x^2+1\rangle$ ізоморфне полю комплексних чисел $\mathbf{C}$.

§ 25. Похідна многочлена. Кратні корені многочлена. Виділення кратних множників многочлена

Література

[1] — § 22, с. 235; § 23, с. 247—262;
[2] — § 23, с. 252—267;
[3] — гл. 14, § 4, с. 479—484;
[5] — гл. IX, § 3, с. 340—343;
[6] — § 22, с. 145—147, § 48, с. 295—298;
[7] — § 10, 11, с. 64—70;
[8] — гл. 6, § 1, с. 243—257.

ТЕОРЕТИЧНІ ВІДОМОСТІ

Нехай $f(x) = a_n x^n + a_{n-1}x^{n-1} + \ldots + a_1 x + a_0$ — деякий многочлен над полем P.

Похідною многочлена $f(x)$ називають многочлен

$$f'(x) = na_n x^{n-1} + (n-1)a_{n-1}x^{n-2} + \ldots + 2a_2 x + a_1.$$

Вважають, що похідна многочлена нульового степеня і нуль-многочлена дорівнює нулю (нуль-многочлену).

Виконуються такі рівності:

1°. $\forall_{f(x),\, g(x) \in P[x]} \quad [f(x) + g(x)]' = f'(x) + g'(x)$;

2°. $\forall_{f(x),\, g(x) \in P[x]} \quad [f(x)\,g(x)]' = f'(x)\,g(x) + f(x)\,g'(x)$;

3°. $\forall_{f(x) \in P[x],\, c \in P} \quad [cf(x)]' = cf'(x)$;

4°. $\forall_{f(x) \in P[x],\, k \in \mathbf{N}} \quad \{[f(x)]^k\}' = k[f(x)]^{k-1} f'(x)$.

Якщо поле P має характеристику 0, то для кожного многочлена $f(x)$ з кільця $P[x]$ такого, що $\deg f \geqslant 1$, виконується рівність $\deg f' = \deg f - 1$.

Наведемо два означення кореня многочлена.

Елемент a поля P називають **коренем многочлена** $f(x)$ з кільця $P[x]$, якщо $f(a) = 0$.

Елемент a поля P називають **коренем многочлена** $f(x)$ з кільця $P[x]$, якщо $f(x)$ ділиться на $g(x) = x - a$.

Ці означення рівносильні над будь-яким полем P.

Елемент $a \in P$ називається **k-кратним коренем** (або коренем k-ї кратності) многочлена $f(x)$ з кільця $P[x]$, якщо $f(x)$ ділиться на $(x-a)^k$ і не ділиться на $(x-a)^{k+1}$. Корені кратності 1 називають **простими**, а корені, кратність яких більша 1, — **кратними**.

Для того щоб елемент a поля P характеристики 0 був коренем кратності k для многочлена $f(x)$ з кільця $P[x]$, необхідно і достатньо, щоб

$$f(a) = f'(a) = \ldots = f^{k-1}(a) = 0 \text{ і } f^k(a) \neq 0, \tag{1}$$

де через $f^m(x)$ позначено m-у похідну многочлена $f(x)$. Нехай $f(x) = [p_1(x)]^{k_1} \times [p_2(x)]^{k_2} \ldots [p_l(x)]^{k_l}$ — канонічний розклад многочлена $f(x)$ над полем P. Незвідний многочлен $p_i(x)$, $1 \leqslant i \leqslant l$, називають **множником кратності** k_i многочлена $f(x)$, якщо $f'(x)$ ділиться на $[p_i(x)]^{k_i}$, але не ділиться на $[p_i(x)]^{k_i+1}$.

Якщо незвідний над полем P характеристики 0 многочлен $p(x)$ є множником кратності $k \geqslant 2$ многочлена $f(x)$, то він є множником кратності $k-1$ для похідної $f'(x)$. Якщо $p(x)$ — множник першої кратності многочлена $f(x)$, то він не міститься в розкладі $f'(x)$ на незвідні множники. Для того щоб многочлен не мав кратних множників, необхідно і достатньо, щоб він був взаємно простим із своєю похідною.

Позначимо через $\varphi_1(x)$ добуток всіх незвідних множників першої кратності многочлена $f(x)$, через $\varphi_2(x)$ — добуток всіх незвідних множників другої кратності і т. д. Тоді

$$f(x) = \varphi_1(x)[\varphi_2(x)]^2 \ldots [\varphi_m(x)]^m,$$

або

$$f = \varphi_1 \varphi_2^2 \varphi_3^3 \ldots \varphi_m^m. \tag{1}$$

Якщо многочлен не має множників кратності $k < m$, то вважають, що $\varphi_k = 1$.

Подання многочлена у вигляді (1) називається **відокремленням кратних множників**. У будь-якого многочлена над полем P характеристики 0 можна відокремити кратні множники за допомогою скінченного числа раціональних дій над деякими многочленами.

ПРИКЛАДИ РОЗВ'ЯЗУВАННЯ ЗАДАЧ

1. Знайти значення похідних $f'(x)$, $f''(x)$, $f'''(x)$ та $f^{IV}(x)$ для многочлена $f(x) = ix^4 + (1-i)x^3 - (2+i)x^2 + 3x - 3 - 4i$ з кільця $C[x]$ при $x = 2i$ та розкласти многочлен за степенями двочлена $x - 2i$.

Розв'язання. І *спосіб*. Знайдемо похідні многочлена $f(x)$:

$$f'(x) = 4ix^3 + 3(1-i)x^2 - 2(2+i)x + 3,$$
$$f''(x) = 12ix^2 + 6(1-i)x - 2(2+i),$$
$$f'''(x) = 24ix + 6(1-i),$$
$$f^{IV}(x) = 24i.$$

Тоді

$$f'(2i) = 4i(2i)^3 + 3(1-i)(2i)^2 - 2(2+i)2i + 3 = 27 + 4i,$$
$$f''(2i) = 12i(2i)^2 + 6(1-i)2i - 2(2+i) = 8 - 38i,$$

$$f''(2i) = 24i\,(2i) + 6\,(1-i) = -42 - 6i,$$

$$f^{IV}(2i) = 24i.$$

Щоб знайти розклад многочлена $f(x)$ за степенями двочлена $x - 2i$, застосуємо формулу Тейлора, яка справджується для многочленів над полем характеристики 0:

$$f(x) = f(2i) + f'(2i)(x-2i) + \frac{f''(2i)}{2!}(x-2i)^2 + \frac{f'''(2i)}{3!}(x-2i)^3 + \frac{f^{IV}(2i)}{4!}(x-2i)^4.$$

Оскільки

$$f(2i) = i\,(2i)^4 + (1-i)(2i)^3 - (2+i)(2i)^2 + 3\,(2i) - 3 - 4i = -3 + 14i,$$

то

$$f(x) = i\,(x-2i)^4 + (-7-i)(x-2i)^3 + (4-19i)(x-2i)^2 + (27+4i)(x-2i) - 3 + 14i.$$

II *спосіб*. Знайдемо розклад многочлена $f(x)$ за степенями двочлена $x - 2i$ (див. § 22), застосувавши для знаходження його коефіцієнтів схему Горнера (табл. 25).

Таблиця 25

	i	$1-i$	$-2-i$	3	$-3-4i$
$2i$	i	$-1-i$	$-3i$	9	$-3+14i$
$2i$	i	$-3-i$	$2-9i$	$27+4i$	
$2i$	i	$-5-i$	$4-19i$		
$2i$	i	$-7-i$			
$2i$	i				

$$f(2i) = -3 + 14i; \qquad f'(2i) = 27 + 4i;$$

$$\frac{1}{2!}f''(2i) = 4 - 19i; \qquad \frac{1}{3!}f'''(2i) = -7 - i;$$

$$\frac{1}{4!}f^{IV}(2i) = i.$$

Отже,

$$f(x) = i\,(x-2i)^4 + (-7-i)(x-2i)^3 + (4-19i)(x-2i)^2 + (27+4i)(x-2i) - 3 + 14i,$$

$$f'(2i) = 27 + 4i, \quad f''(2i) = 8 - 38i, \quad f'''(2i) = -42 - 6i \text{ та } f^{IV}(2i) = 24i.$$

2. Знайти всі дійсні числа b, при яких многочлен $f(x) = x^5 - 5x^3 + b$ з кільця $R[x]$ має кратний корінь у полі R. Знайти цей корінь.

Розв'язання. Нехай α є кратним коренем заданого многочлена. Тоді $f(x)$ ділиться на $(x-\alpha)^2$, тобто існує многочлен $s(x) \in R[x]$ такий, що $f(x) = (x-\alpha)^2 \cdot s(x)$. Знайдемо його похідну:

$$f'(x) = 2(x-\alpha)s(x) + s'(x)(x-\alpha)^2.$$

Звідси $f'(\alpha) = 0$. Це означає, що число α задовольняє систему рівнянь

$$\begin{cases} \alpha^5 - 5\alpha^3 + b = 0, \\ 5\alpha^4 - 15\alpha^2 = 0. \end{cases}$$

Розв'язуючи друге рівняння, дістаємо

$$\alpha_1 = 0, \qquad \alpha_2 = -\sqrt{3}, \qquad \alpha_3 = \sqrt{3}.$$

Тому число b може набувати тільки одне із значень:

$$b_1 = 0, \qquad b_2 = -6\sqrt{3} \text{ або } b_3 = 6\sqrt{3}.$$

Таким чином, при $b = 0$ кратним коренем є число 0, при $b = -6\sqrt{3}$ — число $-\sqrt{3}$ і при $b = 6\sqrt{3}$ — число $\sqrt{3}$.

3. Трикратним коренем многочлена $f(x)$ з кільця $Q[x]$ є число 2. Якою є кратність цього кореня для многочлена

$$g(x) = f'(x)(x^2+3) + (x+3)f''(x)?$$

Розв'язання. Оскільки число 2 є трикратним коренем многочлена $f(x)$, то $f(2) = f'(2) = f''(2) = 0$ і $f'''(2) \neq 0$. Знайдемо $g(2)$:

$$g(2) = f'(2)(4+3) + (2+3)f''(2) = 0.$$

Отже, число 2 є коренем многочлена $g(x)$. Обчислимо похідну:

$$g'(x) = f''(x)(x^2+3) + 2xf'(x) + 3f''(x) + (x+3)f'''(x),$$

$$g'(2) = f''(2)(4+3) + 4f'(2) + 3f''(2) + 5f'''(2) = 5f'''(2) \neq 0.$$

Це означає, що число 2 є простим коренем многочлена $g(x)$.

4. Відокремити кратні множники многочлена

$$f(x) = x^4 - 2ix^3 - 2ix - 1.$$

Розв'язання. Щоб відокремити кратні множники многочлена $f(x)$, треба подати його у вигляді

$$f = \varphi_1\varphi_2^2\varphi_3^3 \dots \varphi_m^m,$$

де φ_i — добуток всіх незвідних множників i-ї кратності в канонічному розкладі многочлена $f(x)$ над полем C при всіх $1 \leqslant i \leqslant m$. Схему знаходження многочленів φ_i для всіх $1 \leqslant i \leqslant m$ подамо таблицею (табл. 26).

Таблиця 26

$f = \varphi_1\varphi_2^2\varphi_3^3 \dots \varphi_m^m$	$q_1 = \frac{f}{d_1} = \varphi_1\varphi_2\varphi_3 \dots \varphi_m$	$\varphi_1 = \frac{q_1}{q_2}$
$d_1 = (f, f') = \varphi_2\varphi_3^2 \dots \varphi_m^{m-1}$	$q_2 = \frac{d_1}{d_2}\varphi_2\varphi_3 \dots \varphi_m$	$\varphi_2 = \frac{q_2}{q_3}$
$d_2 = (d_1, d_1') = \varphi_3 \dots \varphi_m^{m-2}$	$q_3 = \frac{d_2}{d_3} = \varphi_3 \dots \varphi_m$	
. . . . .	. . . . .	. . . . .
$d_{m-1} = (d_{m-2}, d_{m-2}') = \varphi_m$	$q_m = \frac{d_{m-1}}{d_m} = \varphi_m$	$\varphi_m = q_m$
$d_m = 1$		

Знайдемо многочлени $d_1, d_2, \dots, d_m$ для многочлена $f(x)$. Застосуємо алгоритм Евкліда:

$$f'(x) = 4x^3 - 6ix^2 - 2i.$$

Оскільки найбільший спільний дільник многочленів ми визначаємо з точністю до сталого множника, то щоб уникнути дробових коефіцієнтів, помножимо результати проміжних обчислень на відповідний множник. Ділення виконуватимемо «кутом»:

(множимо на 2)
$$\begin{array}{r|l} x^4-2ix^3-2ix-1 & 4x^3-6ix^2-2i \\ \underline{-\,2x^4-4ix^3-4ix-2} & \overline{2x^3-3ix^2-i} \\ \underline{-\,2x^4-3ix^3-ix} & x+1 \\ -ix^3-3ix-2 & \\ \text{(множимо на } 2i\text{)} & \\ \underline{-\,2x^3-6x-4i} & \\ 2x^3-3ix-i & \\ \text{(ділимо на } 3i\text{)} & \\ \underline{-\,3ix^2+6x-3i} & \\ x^2-2ix-1 & \end{array}$$

(ділимо на 2)

$$\begin{array}{r|l} 2x^3-3ix^2-i & x^2-2ix-1 \\ \underline{-\,2x^3-4ix^2-2x} & \overline{2x+i} \\ ix^2+2x-i & \\ \underline{-\,ix^2+2x-i} & \\ 0 & \end{array}$$

Отже,

$$d_1 = x^2-2ix-1 = (x-i)^2$$

$$d_1' = 2x-2i = 2(x-i),$$

$$d_2 = x-i,$$

$$d_2' = 1,$$

$$d_3 = (d_2, d_2') = 1.$$

Обчислимо многочлени: q_1, q_2 і q_3:

$$q_1 = \frac{f}{d_1} = x^2+1; \qquad q_2 = \frac{d_1}{d_2} = x-i;$$

$$q_3 = \frac{d_2}{d_3} = x-i.$$

Тепер знайдемо множники φ_1, φ_2 і φ_3:

$$\varphi_1 = \frac{q_1}{q_2} = x+i, \qquad \varphi_2 = \frac{q_2}{q_3} = 1, \qquad \varphi_3 = q_3 = x-i.$$

Таким чином, маємо

$$f(x) = (x+i)(x-i)^3.$$

Задачі

25.1. Знайти похідну таких многочленів:
а) $f(x) = 9(x^2+x-1)^3(x^3-2)$ з кільця $Q[x]$;
б) $f(x) = 2i(ix^3-3x)((1+i)x^2-i)$ з кільця $C[x]$;
в) $f(x) = \bar{4}x^{10}+\bar{3}x^2(x+\bar{3})$ з кільця $Z_5[x]$.

25.2. Знайти $f'(2)$, якщо:
а) $f(x) = \bar{2}x^3(x^3+\bar{4})-(x+\bar{1})^2$ є многочлен з кільця $Z_5[x]$;
б) $f(x) = (\bar{5}x^8+\bar{8})^3(x-\bar{3})^2$ є многочлен з кільця $Z_{13}[x]$.

25.3. Довести, що різниця $\deg f - \deg f'$ для многочлена $f(x)$ з кільця $Z_p[x]$, де p — деяке просте число, може бути як завгодно великою.

25.4. Довести, що многочлен $f(x)$ з кільця $Z_p[x]$, степінь якого дорівнює $p-1$, не може бути похідною жодного многочлена з цього кільця.

25.5. Довести, що похідна p-го порядку від будь-якого многочлена $f(x)$ з кільця $Z_p[x]$ дорівнює 0.

25.6. Знайти многочлен шостого степеня $f(x)$ з кільця $Z_3[x]$, якщо $f'(x) = \bar{2}x+\bar{1}$ і $f(\bar{1}) = 1$.

25.7. Знайти многочлен $f(x)$ з кільця $Q[x]$, якщо $f''(x) = 24x+2$, $f(0) = 1$ і $f(1) = 5$.

25.8. Многочлен $f(x)$ з кільця $Q[x]$ при діленні на многочлен $g(x) = (x^2+1)^3$ дає остачу $r(x) = x^2-1$. Знайти остачу від ділення $f''(x)$ на многочлен $h(x) = x^2+1$.

25.9. Довести, що многочлен n-го степеня $f(x)$ над полем P характеристики 0 ділиться на свою похідну $f'(x)$ тоді і тільки тоді, коли $f(x) = a(x+b)^n$, де $a, b \in P$, $a \neq 0$ і $n \in \mathbf{N}$.

25.10. У кільці $Z_2[x]$ знайти всі многочлени $f(x)$ такі, що діляться на свою похідну і степінь яких не перевищує 3.

25.11. У кільці $Z_3[x]$ знайти число всіх многочленів третього степеня, які діляться на свою похідну.

25.12. Розкласти многочлен $f(x)$ за степенями двочлена $g(x) = x-a$ і знайти $f'(a)$, $f''(a)$, $f'''(a)$, $f^{IV}(a)$, якщо:
а) $f(x) = x^4-2x^3+3x^2-5x+1$ належить $Q[x]$ і $a = 1$;
б) $f(x) = x^5-3ix^3-4x^2+5ix-1$ належить $C[x]$ і $a = -i$;
в) $f(x) = (x-3)(x-2)(x+1)(x+4)+1$ належить $Q[x]$ і $a = -1$;
г) $f(x) = \bar{4}x^5+\bar{10}x^3-x+\bar{2}$ належить $Z_{11}[x]$ і $a = \bar{3}$;
д) $f(x) = \bar{2}x^4+x^3+x^2+\bar{2}$ належить $Z_3[x]$ і $a = \bar{1}$.

25.13. Многочлен четвертого степеня з кільця $C[x]$, старший коефіцієнт якого дорівнює $2i$, має число $1-i$ трикратним коренем, а при діленні на $x+i$ дає остачу $2-i$. Знайти цей многочлен.

25.14. Довести, що число -3 є простим коренем многочлена $f(x) = x^n+3^n$ з кільця $Q[x]$ при будь-якому непарному натуральному n.

25.15. Знайти кратність кореня:
а) $x = 3$ многочлена $f(x) = x^4-6x^3+10x^2-6x+9$ з кільця $Q[x]$;
б) $x = 2$ многочлена $f(x) = x^5+4x^4-7x^3-11x^2+4$ з кільця $Q[x]$;
в) $x = 1+i$ многочлена $f(x) = x^4-(3+4i)x^3+(3+3i)x^2+(8-2i)x-2-2i$ з кільця $C[x]$;
г) $x = \bar{3}$ многочлена $f(x) = x^6+\bar{2}x$ з кільця $Z_5[x]$.

25.16. Відмінне від нуля дійсне число a є трикратним коренем многочлена $f(x)$ з кільця $R[x]$. Знайти кратність кореня a для многочлена

$$g(x) = (x-a)f(x)+(x+a)f''(x).$$

25.17. При яких дійсних значеннях a мають кратні корені такі многочлени:

а) $f(x) = x^3 + x^2 + ax + 3$;
б) $f(x) = x^3 - 4x^2 - 3x + a$;
в) $f(x) = x^3 + 3x^2 + 3ax - 4$?

25.18. Многочлен $f(x) = x^3 + 5x^2 + 8x + a$ має кратний корінь. Знайти число a і розкласти многочлен на незвідні множники в полі Q.

25.19. При яких необхідних і достатніх умовах наступні многочлени з кільця $R[x]$ мають кратні корені:

а) $f(x) = x^3 + ax + b$;
б) $f(x) = x^4 + ax + b$;
в) $f(x) = x^5 + ax + b$;
г) $f(x) = x^5 + ax^3 + b$?

25.20. Чи мають кратні множники такі многочлени з кільця $C[x]$:

а) $f(x) = x^3 + 4x^2 + x - 6$;
б) $f(x) = x^3 + (3 - 2i)x^2 - (1 + 6i)x - 3$;
в) $f(x) = x^4 - 2x^3 - 3x^2 + 4x + 4$;
г) $f(x) = x^6 - 6x^4 - 4x^3 + 9x^2 + 12x + 4$;
д) $f(x) = x^4 + (1 - 3i)x^3 - (3 + 3i)x^2 - (3 - i)x + i$?

25.21. Відокремити кратні множники таких многочленів:

а) $f(x) = x^3 - 3x^2 + 4$;
б) $f(x) = x^4 + (4 - 8i)x^3 + (-18 - 24i)x^2 + (-44 + 8i)x + (-7 + 24i)$;
в) $f(x) = x^5 + 4x^4 + 7x^3 + 8x^2 + 5x + 2$;
г) $f(x) = x^5 - ix^4 + 5x^3 - ix^2 + 8x + 4i$;
д) $f(x) = x^5 + 5x^4 + (6 - i)x^3 - (4 + 6i)x^2 - (8 + 12i)x - 8i$;
е) $f(x) = x^6 + (-1 + 3i)x^5 + (6 - 3i)x^4 + (-6 + 10i)x^3 + (21 - 10i)x^2 - (21 + 9i)x + 9i$.

25.22. Довести, що кожний незвідний у полі Q многочлен не може мати кратних множників у кільці $P[x]$ для кожного числового поля P.

§ 26. Інтерполяційні многочлени. Поле раціональних дробів

Література

[1] — § 23, с. 250—251; § 24, с. 262—272;
[2] — § 23, с. 253—256, § 24, с. 267—278;
[5] — гл. X, § 1—3, с. 357—373;
[6] — § 24, с. 158; § 50, с. 305—311;
[8] — гл. 5, § 4, с. 233—242; гл. 6, § 1, с. 246—247.

ТЕОРЕТИЧНІ ВІДОМОСТІ

Нехай P — деяке поле, $a_1, a_2, \ldots, a_n, a_{n+1}$ — різні елементи поля P і $b_1, b_2, \ldots, b_n, b_{n+1}$ — довільні елементи поля P.

Існує один і тільки один многочлен $f(x)$ в кільці $P[x]$, степінь якого не перевищує n і який набуває в $(n+1)$-й точці $a_i \in P$ задані значення $b_i \in P$, $i = 1, 2, \ldots, n+1$.

Шуканий многочлен має вигляд

$$f(x) = \sum_{i=1}^{n+1} b_i \frac{(x-a_1)\ldots(x-a_{i-1})(x-a_{i+1})\ldots(x-a_{n+1})}{(a_i-a_1)\ldots(a_i-a_{i-1})(a_i-a_{i+1})\ldots(a_i-a_{n+1})}. \quad (1)$$

Многочлен (1) називають **інтерполяційним многочленом Лагранжа.**

Іноді доцільно многочлен $f(x)$ записувати у вигляді

$$f(x) = c_0 + c_1(x-a_1) + \ldots + c_n(x-a_1)(x-a_2)\ldots(x-a_n), \quad (2)$$

де коефіцієнти $c_0, c_1, \ldots, c_n$ визначаються послідовним підставленням значень $x = a_1, x = a_2, \ldots, x = a_{n+1}$. Многочлен (2) називають **інтерполяційним многочленом Ньютона.**

Для будь-якого поля P існує єдине (з точністю до ізоморфізму) поле $P[x]$, яке містить кільце $P[x]$ многочленів над полем P і кожен елемент якого можна подати як частку

$$\frac{f(x)}{g(x)}, \text{ де } f(x), g(x) \in P[x] \text{ і } g(x) \neq 0. \quad (3)$$

Зауважимо, що відповідно до загальної теорії елементом поля $P[x]$ є не кожна окрема частка (3), а клас часток, які дорівнюють одна одній.

Дві частки $\frac{f_1(x)}{g_1(x)} = \frac{f_2(x)}{g_2(x)}$ дорівнюють одна одній, якщо $f_1(x)g_2(x) = f_2(x) \times g_1(x)$. Як правило, раціональний дріб подають тією часткою $\frac{f(x)}{g(x)}$, для якої $(f, g) = 1$.

Нехай раціональні дроби задано нескоротними частками і старший коефіцієнт знаменника дорівнює 1.

Раціональний дріб $\frac{f(x)}{g(x)}$ **називається правильним,** якщо степінь $f(x)$ менше степеня $g(x)$. У противному разі раціональний дріб називається **неправильним.**

Елементарним дробом над полем P називається раціональний дріб виду $\frac{f(x)}{[g(x)]^k}$, де $g(x)$ — незвідний многочлен над полем P, $\deg f < \deg g$ і $k \in N$.

Якщо $\frac{f(x)}{g_1(x)g_2(x)\ldots g_m(x)}$ — правильний раціональний дріб над полем P і многочлени $g_1(x), g_2(x), \ldots, g_m(x)$ — попарно взаємно прості, то в кільці $P[x]$ існують многочлени $f_1(x), \ldots, f_m(x)$ такі, що

$$\frac{f(x)}{g_1(x)g_2(x)\ldots g_m(x)} = \frac{f_1(x)}{g_1(x)} + \frac{f_2(x)}{g_2(x)} + \ldots + \frac{f_m(x)}{g_m(x)}$$

і кожен з дробів у правій частині є правильним.

Правильний дріб над полем P виду $\frac{f(x)}{[g(x)]^k}$, де $g(x)$ — незвідний над P многочлен і $k \in N$, можна подати як суму елементарних дробів над цим полем

$$\frac{f(x)}{[g(x)]^k} = \frac{f_1(x)}{g(x)} + \frac{f_2(x)}{[g(x)]^2} + \ldots + \frac{f_k(x)}{[g(x)]^k}.$$

Правильний дріб над полем P можна подати як суму елементарних дробів над цим полем і до того єдиним способом.

Неправильний дріб $\frac{f(x)}{g(x)}$ можна подати як суму многочлена і правильного дробу.

ПРИКЛАДИ РОЗВ'ЯЗУВАННЯ ЗАДАЧ

1. Довести тотожність

$$a^2\frac{(x-b)(x-c)}{(a-b)(a-c)}+b^2\frac{(x-a)(x-c)}{(b-a)(b-c)}+c^2\frac{(x-b)(x-a)}{(c-b)(c-a)}=x^2,\ \text{де } a,\ b,\ c\in\mathbf{R}.$$

Розв'язання. Розглянемо многочлен

$$f(x)=a^2\frac{(x-b)(x-c)}{(a-b)(a-c)}+b^2\frac{(x-a)(x-c)}{(b-a)(b-c)}+c^2\frac{(x-b)(x-a)}{(c-b)(c-a)}.$$

Обчислимо його значення, якщо $x\in\{a,\ b,\ c\}$:

$$f(a)=a^2,\quad f(b)=b^2,\quad f(c)=c^2.$$

Це означає, що $f(x)$ є многочленом Лагранжа, степінь якого не вище 2. Многочлен $g(x)=x^2$ при $x\in\{a,\ b,\ c\}$ набуває значень:

$$g(a)=a^2,\quad g(b)=b^2,\quad g(c)=c^2.$$

Як відомо (див., наприклад, [2], § 23, теорема 3), над полем **R** існує тільки один многочлен, степінь якого не більше 2 і який при трьох різних дійсних числах a, b і c набуває значень a^2, b^2 і c^2. Це означає, що многочлени $f(x)$ і $g(x)$ дорівнюють один одному.

2. На координатній площині задано чотири точки $A(0;\ 1)$, $B(-1;\ 2)$, $C(1;\ 4)$ і $D(2;\ 2)$. Знайти многочлен третього степеня, графік якого проходить через ці точки.

Розв'язання. Складемо таблицю значень для шуканого многочлена $f(x)$ (табл. 27).

Таблиця 27

x	0	-1	1	2
$f(x)$	1	2	4	2

Щоб знайти коефіцієнти многочлена $f(x)$, застосуємо інтерполяційну формулу Ньютона:

$$f(x)=c_0+c_1x+c_2x(x+1)+c_3x(x+1)(x-1). \qquad (1)$$

Підставивши значення $x\in\{0,\ -1,\ 1,\ 2\}$, дістаємо

$$\begin{cases}1=c_0,\\ 2=c_0-c_1,\\ 4=c_0+c_1+2c_2,\\ 2=c_0+2c_1+6c_2+6c_3,\end{cases}\quad\text{або}\quad\begin{cases}c_0=1,\\ c_1=-1,\\ c_2=2,\\ c_3=-\frac{3}{2}.\end{cases}$$

Отже,

$$f(x)=-\frac{3}{2}x(x+1)(x-1)+2x(x+1)-x+1=-\frac{3}{2}x^3+2x^2+\frac{5}{2}x+1.$$

3. Розкласти на елементарні дроби над полем **Q** дріб

$$\frac{f(x)}{g(x)}=\frac{x^2+4x+3}{(x^2-4x+4)(x+3)^2}.$$

Розв'язання. Перевіримо, чи є даний дріб нескоротним. Для цього знайдемо найбільший спільний дільник його чисельника і знаменника. Розкладемо їх на незвідні множники в полі **Q**:

$$f(x)=x^2+4x+3=(x+1)(x+3),$$
$$g(x)=(x^2-4x+4)(x+3)^2=(x-2)^2(x+3)^2.$$

Звідси $(f,\ g)=x+3$. Це означає, що перш ніж розкласти заданий дріб на елементарні, треба замінити його нескоротним дробом, що дорівнює йому. Отже,

$$\frac{f(x)}{g(x)}=\frac{x+1}{(x-2)^2(x+3)}.$$

Шуканий розклад повинен мати такий вигляд (див., наприклад, [1], § 24, с. 269, теорема 1):

$$\frac{x+1}{(x-2)^2(x+3)}=\frac{A}{x-2}+\frac{B}{(x-2)^2}+\frac{C}{x+3},$$

де A, B, C — невизначені коефіцієнти. Отже, маємо

$$x+1=A(x-2)(x+3)+B(x+3)+C(x-2)^2.$$

Оскільки многочлени рівні між собою, то:

1) при $x=2$, $5B=3$, $B=\frac{3}{5}$.

2) при $x=-3$, $25C=-2$, $C=-\frac{2}{25}$.

3) $A+C=0$ і $A=\frac{2}{25}$.

Остаточно дістаємо

$$\frac{f(x)}{g(x)}=\frac{x+1}{(x-2)^2(x+3)}=\frac{2}{25(x-2)}+\frac{3}{5(x-2)^2}-\frac{2}{25(x+3)}.$$

4. Розкласти на елементарні дроби над полями **Q** і **R** дріб

$$\frac{f(x)}{g(x)}=\frac{x+3}{(x^3-2)(x+1)}.$$

Розв'язання. Спочатку розв'яжемо задачу в полі **Q**. Многочлен $g_1(x)=x^3-2$ у цьому полі незвідний. Тому заданий дріб є правильним і нескоротним. Шуканий розклад матиме вигляд:

$$\frac{x+3}{(x^3-2)(x+1)}=\frac{A}{x+1}+\frac{Bx^2+Cx+D}{x^3-2},$$

де A, B, C і D — невизначені коефіцієнти. Звідси

$$x+3=A(x^3-2)+(Bx^2+Cx+D)(x+1).$$

Прирівнюючи коефіцієнти многочленів при однакових степенях невідомого в лівій і правій частинах рівності, дістаємо систему рівнянь:

$$\begin{aligned}A+B&=0,\\ B+C&=0,\\ C+D&=1,\\ D-2A&=3.\end{aligned}$$

Звідси $A=-\frac{2}{3}$, $B=\frac{2}{3}$, $C=-\frac{2}{3}$, $D=\frac{5}{3}$, тобто шуканий розклад заданого дробу на елементарні дроби над полем **Q** має вигляд:

$$\frac{x+3}{(x^3-2)(x+1)}=-\frac{2}{3(x+1)}+\frac{2x^2-2x+5}{3(x^3-2)}.$$

Перший з доданків правої частини є елементарним дробом над полем **R**. Розкладемо на елементарні дроби другий доданок:

$$\frac{2x^2-2x+5}{x^3-2}=\frac{2x^2-2x+5}{\left(x-\sqrt[3]{2}\right)\left(x^2+\sqrt[3]{2}x+\sqrt[3]{4}\right)}=\frac{A_1}{x-\sqrt[3]{2}}+\frac{B_1x+C_1}{x^2+\sqrt[3]{2}x+\sqrt[3]{4}},$$

$$2x^2-2x+5=A_1\left(x^2+\sqrt[3]{2}x+\sqrt[3]{4}\right)+(B_1x+C_1)\left(x-\sqrt[3]{2}\right),$$

$$\begin{cases}A_1+B_1=2,\\ A_1\sqrt[3]{2}-B_1\sqrt[3]{2}+C_1=-2,\\ A_1\sqrt[3]{4}-C_1\sqrt[3]{2}=5.\end{cases}$$

Розв'язуючи цю систему, дістанемо:

$$A_1 = \frac{2}{3} + \frac{5}{12}\sqrt[3]{2} - \frac{1}{3}\sqrt[3]{4}, \quad B_1 = \frac{4}{3} - \frac{5}{12}\sqrt[3]{2} + \frac{1}{3}\sqrt[3]{4},$$

$$C_1 = -\frac{2}{3} + \frac{2}{3}\sqrt[3]{2} - \frac{5}{3}\sqrt[3]{4}.$$

Отже, розклад дробу $\frac{x+3}{(x^3-2)(x+1)}$ на елементарні дроби над полем **R** має вигляд:

$$\frac{x+3}{(x^3-2)(x+1)} = -\frac{2}{3(x+1)} + \frac{\frac{2}{3} + \frac{5}{12}\sqrt[3]{2} - \frac{1}{3}\sqrt[3]{4}}{x - \sqrt[3]{2}} +$$

$$+ \frac{\left(\frac{4}{3} - \frac{5}{12}\sqrt[3]{2} + \frac{1}{3}\sqrt[3]{4}\right)x - \frac{2}{3} + \frac{2}{3}\sqrt[3]{2} - \frac{5}{3}\sqrt[3]{4}}{x^2 + \sqrt[3]{2}x + \sqrt[3]{4}}.$$

Зауваження. Наведений приклад свідчить про те, що розклад дробу на елементарні дроби залежить від поля, над яким розглядається дріб.

Задачі

26.1. Скільки існує многочленів $f(x)$ першого та другого степенів над полем **R** таких, що $f(-1) = -1$ і $f(2) = 2$?

26.2. Чи може графік многочлена третього степеня над полем **R** мати з прямою $y = kx$ більше трьох спільних точок?

26.3. Довести, що графік многочлена степеня n перетинає будь-яку пряму не більш ніж в n точках.

26.4. Довести, що коли при будь-якому раціональному значенні змінної x многочлен $f(x)$ набуває раціональних значень, то всі коефіцієнти многочлена є раціональними числами.

26.5. Довести тотожності:

а) $a\frac{(x-b)(x-c)}{(a-b)(a-c)} + b\frac{(x-a)(x-c)}{(b-a)(b-c)} + c\frac{(x-a)(x-b)}{(c-a)(c-b)} = x$;

б) $\frac{(x-a)(x-b)(x-c)}{(d-a)(d-b)(d-c)} + \frac{(x-b)(x-c)(x-d)}{(a-b)(a-c)(a-d)} +$

$+ \frac{(x-a)(x-c)(x-d)}{(b-a)(b-c)(b-d)} + \frac{(x-a)(x-b)(x-d)}{(c-a)(c-b)(c-d)} = 1.$

26.6. Використовуючи формулу інтерполяційного многочлена Лагранжа, побудувати многочлени найменшого степеня $f(x) \in Q[x]$ за такими таблицями значень (табл. 28—30).

Таблиця 28

а)

x	−3	1	2
$f(x)$	22	2	7

Таблиця 29

б)

x	0	1	3	4
$f(x)$	2	1	1	2

26.7. Використовуючи інтерполяційну формулу Ньютона, побудувати многочлени найменшого степеня $f(x) \in Q[x]$ за такими таблицями значень (табл. 31—33).

Таблиця 30

в)

x	−2	−1	0	1	2
$f(x)$	−4	−2	0	2	4

Таблиця 31

а)

x	−1	0	1	2
$f(x)$	4	1	2	7

Таблиця 32

б)

x	0	1	2	3	4
$f(x)$	1	2	3	4	6

Таблиця 33

в)

x	0	1	2	...	n
$f(x)$	1	3	9	...	3^n

26.8. Знайти многочлени найменшого степеня $f(x) \in Q[x]$ за такими таблицями значень: (табл. 34—37).

Таблиця 34

а)

x	−1	0	1
$f(x)$	2	−1	2

Таблиця 35

б)

x	1	2	3	4
$f(x)$	4	3	2	1

Таблиця 36

в)

x	1	i	−1	$-i$
$f(x)$	i	1	$-i$	−1

, обчислити $f(2i)$ та $f(0)$.

Таблиця 37

г)

x	1	4	9	16
$f(x)$	1	2	3	4

, обчислити $f(3)$ та $f(2)$.

26.9. Відображення f поля Z_5 в себе задається так: $f(\bar{0}) = f(\bar{2}) = f(\bar{4}) = \bar{0}$ і $f(\bar{1}) = f(\bar{3}) = \bar{1}$. Задати це відображення за допомогою многочлена з кільця $Z_5[x]$ найменшого степеня.

26.10. Задати всі взаємно однозначні відображення поля Z_3 в себе за допомогою многочленів з кільця $Z_3[x]$, степінь яких не перевищує 2.

26.11. Довести, що для будь-якого простого числа p всі відображення поля Z_p в себе можна задати многочленами з кільця $Z_p[x]$, степінь яких не перевищує $p-1$.

26.12. У полі $R(x)$ знайти нескоротний дріб, який дорівнює таким дробам:

а) $\frac{x^2-4x+3}{x^2-5x+6}$; б) $\frac{3x^2-x-2}{x^6-1}$;

в) $\frac{x^8+x^4+1}{x^2+x+1}$; г) $\frac{x^2-x-1}{x^3-x^2-x-2}$.

26.13. Перевірити, чи є раціональний дріб $\frac{f(x)}{g(x)}$ елементарним над полем P, якщо:

а) $\frac{f(x)}{g(x)}=\frac{x^2-1}{x^3-2}$ і $P=\mathbf{Q}$;

б) $\frac{f(x)}{g(x)}=\frac{x^3-1}{(x^3+3)^2}$ і $P=\mathbf{Q}$;

в) $\frac{f(x)}{g(\lambda)}=\frac{5x+6}{x^4+2x^2+1}$ і $P=\mathbf{R}$;

г) $\frac{f(x)}{g(x)}=\frac{1}{x^2+x+1}$ і $P=\mathbf{R}$;

д) $\frac{f(x)}{g(x)}=\frac{x+i}{(x^2+2)^2}$ і $P=\mathbf{C}$;

е) $\frac{f(x)}{g(x)}=\frac{x^2+\bar{1}}{(x+\bar{3})^2}$ і $P=Z_5$.

26.14. Розкласти дріб $\frac{f(x)}{g(x)}$ на елементарні дроби над полем $\mathbf{R}$, якщо:

а) $\frac{f(x)}{g(x)}=\frac{x^2-5x+6}{(2x-1)(x^2-2x)}$;

б) $\frac{f(x)}{g(x)}=\frac{x^2}{(x+2)(x+3)}$;

в) $\frac{f(x)}{g(x)}=\frac{x^3+1}{(x^2+2x+1)^2}$;

г) $\frac{f(x)}{g(x)}=\frac{2x}{(x-1)(x^2+1)}$;

д) $\frac{f(x)}{g(x)}=\frac{x^2}{(x^2+x+2)^2}$;

е) $\frac{f(x)}{g(\lambda)}=\frac{x^3-1}{(x^2+x+1)^2(x^2+1)}$;

є) $\frac{f(x)}{g(x)}=\frac{x^4+2x^3-18x^2+54}{x^5+6x^4+9x^3}$;

ж) $\frac{f(x)}{g(x)}=\frac{x^2+3x+2}{(x^4+4)(x+2)}$;

з) $\frac{f(x)}{g(x)}=\frac{x^2}{x^4-4}$.

26.15. Розкласти дріб $\frac{f(x)}{g(x)}$ на елементарні дроби над полем $\mathbf{C}$, якщо:

а) $\frac{f(x)}{g(x)}=\frac{i}{(x-i)(x+2i)}$;

б) $\frac{f(x)}{g(x)}=\frac{2x}{(x-1)(x^2+1)}$;

в) $\frac{f(x)}{g(x)}=\frac{1}{(x^2-2x+2)(x-1+i)}$;

г) $\frac{f(x)}{g(x)}=\frac{x^2}{x^4-4}$.

26.16. Розкласти дріб $\frac{f(x)}{g(p)}$ на елементарні дроби над полем $\mathbf{Q}$, якщо:

а) $\frac{f(x)}{g(x)}=\frac{1}{x^4-2x}$; б) $\frac{f(x)}{g(x)}=\frac{x^2}{x^4-4}$; в) $\frac{f(x)}{g(x)}=\frac{1}{x^3+x}$.

26.17. Розкласти дріб $\frac{f(x)}{g(x)}$ на елементарні дроби над полем Z_5, якщо:

а) $\frac{f(x)}{g(x)}=\frac{\bar{1}}{x^3+x}$; б) $\frac{f(x)}{g(x)}=\frac{\bar{1}}{x^5-x}$; в) $\frac{f(x)}{g(x)}=\frac{x^2}{x^4-\bar{4}}$.

26.18. Розкласти дріб $\frac{f(x)}{g(x)}=\frac{\bar{1}}{x^p-x}$ на елементарні дроби над полем Z_p, де p — довільне просте число.

Розділ V. МНОГОЧЛЕНИ ВІД КІЛЬКОХ ЗМІННИХ

§ 27. Кільце многочленів від n змінних над областю цілісності. Розклад многочлена на добуток незвідних множників

Література

[1] — § 25, с. 272—288;
[2] — § 25, с. 279—297;
[3] — гл. 14, § 1, с. 485—493;
[5] — гл. XI, § 1, 2, с. 392—413;
[6] — § 61, с. 312—320;
[7] — § 21, с. 113—123;
[8] — гл. 5, § 2, с. 212—216.

ТЕОРЕТИЧНІ ВІДОМОСТІ

Кільцем многочленів $R[x_1, x_2, \ldots, x_{n-1}, x_n]$ від n змінних $x_1, x_2, \ldots, x_{n-1}, x_n$ над областю цілісності $\mathbf{R}$ називається кільце многочленів від змінної x_n над кільцем $R[x_1, x_2, \ldots, x_{n-1}]$.

Кільце многочленів $R[x_1, x_2, \ldots, x_n]$ над областю цілісності $\mathbf{R}$ є область цілісності, причому кожен елемент $f \in R[x_1, x_2, \ldots, x_n]$ можна подати як скінченну суму:

$$f=\sum_{i=1}^{m} a_i x_1^{k_{1i}} x_2^{k_{2i}} \ldots x_n^{k_{ni}}, \qquad (1)$$

де $a_i \in \mathbf{R}$, $k_{ij} \in \mathbf{Z}_+$, $i \in \{1, 2, \ldots, m\}$ та $j \in \{1, 2, \ldots, n\}$. Будь-який вираз виду (1) є елементом кільця $R[x_1, x_2, \ldots, x_n]$.

Елементи кільця $R[x_1, x_2, \ldots, x_n]$ називають **многочленами від n змінних над $\mathbf{R}$** і позначають $f(x_1, x_2, \ldots, x_n)$, $g(x_1, x_2, \ldots, x_n)$, ... Кожен доданок $a_i x_1^{k_{1i}} x_2^{k_{2i}} \ldots x_n^{k_{ni}}$ в сумі (1) називають **членом многочлена** $f(x_1, x_2, \ldots, x_n)$, елемент $a_i \in \mathbf{R}$ — **коефіцієнтом** цього члена. Два члени, які відрізняються тільки коефіцієнтами, називають **подібними**.

У подальшому вважатимемо, що в сумі (1) подібних членів немає. Така форма запису многочлена називається **канонічною** і кожен многочлен з кільця $R[x_1, x_2, \ldots, x_n]$ можна записати в такій формі тільки єдиним способом.

Степенем члена $ax_1^{k_1}x_2^{k_2}\ldots x_n^{k_n}$ многочлена називають суму $k_1+k_2+\ldots+k_n$. Число k_i, $i=1, 2, \ldots, n$, називають **степенем даного члена відносно** x_i

Найбільший із степенів членів називають **степенем многочлена**, а член з найбільшим степенем — **старшим членом многочлена**. Якщо всі члени многочлена мають степінь l, то кажуть, що це однорідний многочлен степеня l.

Нехай $ax_1^{k_1}x_2^{k_2}\dots x_n^{k_n}$ і $bx_1^{l_1}x_2^{l_2}\dots x_n^{l_n}$ — два члени многочлена $f(x_1, x_2, \dots, x_n)$. Вважають, що перший член вищий від другого, якщо $k_1 = l_1$, $k_2 = l_2$, $\dots$, $k_{t-1} = l_{t-1}$ і $k_t > l_t$. Відношення «бути вищим» на множині членів многочлена є лінійним строгим порядком, його називають **лексикографічним**.

Нехай члени многочлена $f(x_1, x_2, \dots, x_n)$ упорядковані лексикографічно. Тоді перший по порядку член називають **вищим членом** многочлена.

Вищий член добутку двох многочленів дорівнює добутку вищих членів цих многочленів.

Означення подільності многочленів, його властивості, поняття звідного та незвідного многочленів у кільці $P[x_1, x_2, \dots, x_n]$ залишаються тими самими, що й в кільці $P[x]$ (див. § 21, 24).

Будь-який многочлен $f(x_1, x_2, \dots, x_n)$ над полем P ненульового степеня можна подати у вигляді добутку многочленів, незвідних у полі P і при тому єдиним способом з точністю до сталих множників і порядку множників.

Кільце $P[x_1, x_2, \dots, x_n]$ не є кільцем головних ідеалів, а отже, воно не може бути евклідовим кільцем.

ПРИКЛАДИ РОЗВ'ЯЗУВАННЯ ЗАДАЧ

1. Подати многочлен

$$f(x, y, z) = (x + 2y)(z^2 - 1) + (y - z)^2 - (x + z)(y - 2)$$

у вигляді суми однорідних многочленів, кожен з яких упорядкований лексикографічно, і знайти його вищий член.

Розв'язання. Знайдемо канонічну форму заданого многочлена:

$$f(x, y, z) = xz^2 - x + 2yz^2 - 2y + y^2 - 2yz + z^2 - xy + 2x - zy + 2z = xz^2 + x + 2yz^2 - 2y + y^2 - 3yz + z^2 - xy + 2z.$$

Оскільки многочлен має члени першого, другого і третього степенів, то його можна подати у вигляді суми трьох однорідних многочленів:

$$f(x, y, z) = (xz^2 + 2yz^2) + (y^2 - 3yz + z^2 - xy) + (x - 2y + 2z).$$

Упорядкуємо кожен з однорідних многочленів-доданків лексикографічно:

$$f(x, y, z) = (xz^2 + 2yz^2) + (-xy + y^2 - 3yz + z^2) + (x - 2y + 2z).$$

Вищими членами кожного з доданків відповідно є xz^2, $-xy$ та x. Вищим серед них, а, отже, і вищим членом многочлена $f(x, y, z)$ є $-xy$.

2. Відображення множини $Z_3 \times Z_3$ в Z_3 задано табл. 38.

Таблиця 38

$(\bar0, \bar0)$	$(\bar0, \bar1)$	$(\bar0, \bar2)$	$(\bar1, \bar0)$	$(\bar1, \bar1)$	$(\bar1, \bar2)$	$(\bar2, \bar0)$	$(\bar2, \bar1)$	$(\bar2, \bar2)$
$\bar0$	$\bar2$	0	$\bar2$	$\bar0$	$\bar2$	$\bar0$	$\bar2$	$\bar0$

Знайти канонічну форму многочлена з кільця $Z_3[x, y]$, який задає це саме відображення.

Розв'язання. Позначимо: $x_1 = y_1 = \bar0$, $x_2 = y_2 = \bar1$, $x_3 = y_3 = \bar2$. У кільці $Z_3[x, y]$ розглянемо многочлен

$$f(x, y) = \bar2\frac{(x - x_2)(x - x_3)(y - y_1)(y - y_3)}{(x_1 - x_2)(x_1 - x_3)(y_2 - y_1)(y_2 - y_3)} + \bar2\frac{(x - x_1)(x - x_2)(y - y_2)(y - y_3)}{(x_2 - x_1)(x_2 - x_3)(y_1 - y_2)(y_1 - y_3)} +$$

$$+ \bar2\frac{(x - x_1)(x - x_3)(y - y_1)(y - y_2)}{(x_2 - x_1)(x_2 - x_3)(y_3 - y_1)(y_2 - y_3)} + \bar2\frac{(x - x_1)(x - x_2)(y - y_1)(y - y_3)}{(x_3 - x_1)(x_3 - x_2)(y_2 - y_1)(y_2 - y_3)}.$$

Оскільки

$$f(x_1, y_1) = f(x_1, y_3) = f(x_2, y_2) = f(x_3, y_1) = f(x_3, y_3) = \bar0,$$

$$f(x_1, y_2) = f(x_2, y_1) = f(x_2, y_3) = f(x_3, y_2) = \bar2,$$

то многочлен $f(x, y)$ є шуканим. Знайдемо його канонічну форму:

$$f(x, y) = \bar2\frac{(x - \bar1)(x - \bar2)(y - \bar2)y}{(-\bar1)(-\bar2)\bar1(-\bar1)} + \bar2\frac{x(x - \bar2)(y - \bar1)(y - \bar2)}{\bar1(-\bar1)(-\bar1)(-\bar2)} + \bar2\frac{x(x - \bar2)(y - \bar1)y}{\bar1(-\bar1)\bar2\cdot\bar1} + \bar2\frac{x(x - \bar1)y(y - \bar2)}{\bar2\cdot\bar1\cdot\bar1(-\bar1)} =$$

$$= \bar2(x + \bar2)(x + \bar1)y(y + \bar1) + \bar2x(x + \bar1)(y + \bar2)(y + \bar1) + \bar2xy(x + \bar1)(y + \bar2) + \bar2xy(x + \bar2)(y + \bar1) = (\bar2x^2y^2 + \bar2x^2y + y^2 + y) + (\bar2x^2y^2 + \bar2y^2x + x^2 + x) + (\bar2x^2y^2 + x^2y + \bar2xy^2 + xy) + (\bar2x^2y^2 + xy^2 + \bar2x^2y + xy) =$$

$$= \bar2x^2y^2 + \bar2x^2y + x^2 + \bar2xy^2 + \bar2xy + x + y^2 + y.$$

3. Розкласти у полі Q на незвідні множники такий многочлен:

$$f(x, y) = (x + y)^5 - x^5 - y^5.$$

Розв'язання. Розглянемо многочлен $f(x, y)$ як многочлен від змінної y над областю цілісності $Q[x]$. Тоді $f(x, 0) = f(x, -x) = 0$. Це означає, що $f(x, y)$ ділиться на многочлени $y - 0 = y$ та $y + x$. Розглядаючи $f(x, y)$ як многочлен від змінної x над областю цілісності $Q[y]$, маємо $f(0, y) = f(-y, y) = 0$, тобто заданий многочлен ділиться на $x - 0 = x$. Проте $f(x, y)$ є однорідним многочленом, тому його можна подати у вигляді

$$f(x, y) = xy(y + x)(ax^2 + bxy + cy^2),$$

де $a, b, c \in Q$ — невизначені коефіцієнти. Запишемо многочлен $f(x, y)$ у канонічній формі:

$$f(x, y) = 5x^4y + 10x^3y^2 + 10x^2y^3 + 5xy^4.$$

Прирівнюючи тепер коефіцієнти при x^4y і y^4x, знаходимо $a = 5$, $c = 5$. Якщо $x = y = 1$, то $a + b + c = 15$, $b = 5$. Тому $f(x, y) = 5xy(y + x)(x^2 + xy + y^2)$. Многочлен $g(x, y) = x^2 + xy + y^2$ є незвідним у полі Q. Справді, припустивши, що

$$x^2 + xy + y^2 = (m_1x + n_1y)(m_2x + n_2y)$$

для деяких $m_1, m_2, n_1, n_2 \in Q$, дістаємо систему рівнянь

$$\begin{cases} m_1m_2 = 1, \\ n_1n_2 = 1, \\ m_1n_2 + m_2n_1 = 1 \end{cases} \quad \text{або} \quad \begin{cases} m_1 = \dfrac{1}{m_2}, \\ n_1 = \dfrac{1}{n_2}, \\ \dfrac{n_2}{m_2} + \dfrac{m_2}{n_2} = 1, \end{cases}$$

яка у множині Q розв'язків не має.

Отже, шуканий розклад є

$$f(x, y) = 5xy(y + x)(x^2 + xy + y^2).$$

Задачі

27.1. Знайти канонічну форму таких многочленів:
а) $f(x, y) = (x-y)^2(x^2+xy+y^2)(x+2y)+x^2-1$;
б) $f(x, y) = (x-y)(y-z)(x-z)xyz$.

27.2. Довести, що множина всіх однорідних многочленів кільця $P[x_1, x_2, \ldots, x_n]$ многочленів над полем P є підкільцем.

27.3. Скільки членів може мати канонічна форма однорідного многочлена: а) другого степеня від двох змінних; б) другого степеня від трьох змінних; в) третього степеня від двох змінних; г) третього степеня від трьох змінних?

27.4. Довести, що однорідний многочлен степеня m, де $m>0$, від n змінних має в загальному вигляді $\frac{(m+n-1)!}{m!\,(n-1)!}$ членів.

27.5. Довести, що канонічна форма многочлена m-го степеня від n змінних має в загальному вигляді $\frac{(m+n)!}{n!m!}$ членів.

27.6. Скільки існує однорідних многочленів другого степеня від трьох змінних над полем: а) Z_2; б) Z_3?

27.7. Довести, що над полем Z_p існує p^6-1 однорідних многочленів другого степеня від трьох змінних.

27.8. Довести, що над полем Z_p існує $p^{\frac{(m+n-1)!}{m!(n-1)!}}-1$ однорідних многочленів m-го степеня від n змінних.

27.9. Упорядкувати лексикографічно і знайти вищий член таких многочленів:
а) $f(x, y, z) = 2x^3(y+z)-3y^2x^2(x^2+z^2)+5x^4yz^2$ з кільця $Z[x, y, z]$;
б) $f(x, y, z) = (\bar{2}x+\bar{3}y)^2z-x(y+z-\bar{3}xz)$ з кільця $Z_5[x, y, z]$;
в) $f(x, y, z, t) = (x+y)(z+y)+\bar{2}x(y+t+\bar{1})+(y+t)^3$ з кільця $Z_3[x, y, z, t]$.

27.10. Знайти два різних многочлени від двох змінних над полем Z_2, які визначають те саме відображення $Z_2 \times Z_2$ в Z_2, задане такими таблицями (табл. 39, 40).

Таблиця 39

а)

$(\bar{0}, \bar{0})$	$(\bar{0}, \bar{1})$	$(\bar{1}, \bar{0})$	$(\bar{1}, \bar{1})$
$\bar{1}$	$\bar{0}$	$\bar{0}$	$\bar{1}$

Таблиця 40

б)

$(\bar{0}, \bar{0})$	$(\bar{0}, \bar{1})$	$(\bar{1}, \bar{0})$	$(\bar{1}, \bar{1})$
$\bar{1}$	$\bar{0}$	$\bar{1}$	$\bar{0}$

27.11. Довести, що кожне відображення множини Z_p^n у множину Z_p можна подати многочленом від n змінних над полем Z_p.

27.12. Довести, що многочлен $f(x_1, x_2, \ldots, x_n)$ над областю цілісності K ділиться на многочлен $g(x_1, x_2, \ldots, x_n) = x_n - s(x_1, x_2, \ldots, x_{n-1})$ з цього самого кільця тоді і тільки тоді, коли $f(x_1, x_2, \ldots, x_{n-1}, s(x_1, x_2, \ldots, x_{n-1}))$ є нульовим многочленом.

27.13. Перевірити подільність многочлена $f(x, y, z, t) = (xy-zt)^5+(zx-yt)^5$ на многочлен $g(x, y, z, t) = (y+z)(x-t)$ у кільці $Z[x, y, z, t]$.

27.14. Довести, що многочлен $f(x, y, z) = (x+y+z)^n - x^n - y^n - z^n$ ділиться на многочлен $g(x, y, z) = (x+y)(y+z)(x+z)$ при будь-якому натуральному n.

27.15. Довести, що многочлен $f(x, y) = x^2+y^2-1$ незвідний у полі $\mathbf{Q}$.

27.16. Довести, що будь-який однорідний многочлен k-го степеня від двох змінних $f(x, y)$ над полем P можна за допомогою введення нової змінної подати у вигляді добутку двох многочленів, кожен з яких має одну змінну.

27.17. Застосовуючи заміну $x = ty$, розкласти на незвідні у полі P множники многочлен $f(x, y)$, якщо:
а) $f(x, y) = 9x^4-12x^3y-21x^2y^2-40xy^3-16y^4$ і $P=\mathbf{Q}$;
б) $f(x, y) = 4x^4+4x^3y+13x^2y^2+6xy^3+9y^4$ і $P=\mathbf{Q}$;
в) $f(x, y) = x^2+xy+y^2$ і $P=Z_3$;
г) $f(x, y) = x^4+\bar{4}y^4$ і $P=Z_5$;
д) $f(x, y) = (x^2-xy)^2+2x^2y^2-2xy^3+y^4$ і $P=\mathbf{Q}$.

27.18. Розкласти на незвідні у полі $\mathbf{Q}$ множники такі многочлени:
а) $f(x, y, z) = (x+y+z)^3-x^3-y^3-z^3$;
б) $f(a, b, c) = (b-c)(b+c)^2+(c-a)(c+a)^2+(a-b)(a+b)^2$;
в) $f(a, b, c) = a(b-c)^3+b(c-a)^3+c(a-b)^3$;
г) $f(x, y, z) = x(y^2-z^2)+y(z^2-x^2)+z(x^2-y^2)$;
д) $f(x, y, z) = (x+y+z)^4-(y+z)^4-(x+y)^4-(z+x)^4+x^4+y^4+z^4$;
е) $f(a, b, c) = (a-b)(a+b)^3+(b-c)(b+c)^3+(c-a)(c+a)^3$;
є) $f(x, y, z) = x^3y^2+y^3z^2+z^3x^2-x^2y^3-y^2z^3-z^2x^3$;
ж) $f(a, b, c) = a^4(b-c)+b^4(c-a)+c^4(a-b)$;
з) $f(x, y, z) = (x+y+z)^5-x^5-y^5-z^5$;
к) $f(x, y, z) = (y-z)^5+(z-x)^5+(x-y)^5$.

27.19. Довести, що многочлен $f(x, y, z) = (x+y+z)^{2n+1} - x^{2n+1} - y^{2n+1} - z^{2n+1}$ ділиться на многочлен $g(x, y, z) = (x+y+z)^3-x^3-y^3-z^3$ при будь-якому n, $n \in \mathbf{N}$.

27.20. Довести, що в кільці $P[x, y]$ многочленів від двох змінних над полем $\mathbf{P}$ не всі ідеали є головними.

27.21. Довести, що фактор-кільце $P[x, y]/\langle x-y\rangle$ ізоморфне кільцю $P[x]$.

§ 28. Симетричні многочлени

Література

[1] — § 26, с. 288—295;
[2] — § 26, с. 298—305;
[3] — гл. 14, § 2, с. 493—500;
[5] — гл. XI, § 3, с. 413—423;
[6] — § 52, с. 321—328;
[7] — § 22, с. 123—130;
[8] — гл. 6, § 2, с. 257—263;
[44] — § 1, 3, с. 8—19, 47—61; § 7, с. 115—137.

ТЕОРЕТИЧНІ ВІДОМОСТІ

Многочлен $f(x_1, x_2, \ldots, x_n)$ з кільця $P[x_1, x_2, \ldots, x_n]$ називають **симетричним відносно змінних** $x_1, x_2, \ldots, x_n$, якщо внаслідок довільної перестановки змінних $x_1, x_2, \ldots, x_n$ утворюється многочлен, який дорівнює заданому.

Симетричні многочлени мають такі властивості:

1°. Множина всіх симетричних многочленів від n змінних над полем P утворює область цілісності з одиницею;

2°. Якщо симетричний многочлен $f(x_1, x_2, \ldots, x_n)$ містить деякий член $ax_1^{l_1}x_2^{l_2}\ldots x_n^{l_n}$, то він містить і член, утворений з заданого, внаслідок будь-якої перестановки показників $l_1, l_2, \ldots, l_n$;

3°. Якщо $ax_1^{l_1}x_2^{l_2}\ldots x_n^{l_n}$ є вищий член симетричного многочлена, то $l_1 \geqslant l_2 \geqslant \ldots \geqslant l_n$.

Симетричні многочлени

$$\sigma_1 = x_1 + x_2 + \ldots + x_n,$$
$$\sigma_2 = x_1x_2 + x_1x_3 + \ldots + x_{n-1}x_n,$$
$$\ldots\ldots\ldots\ldots\ldots\ldots$$
$$\sigma_n = x_1x_2\ldots x_n$$

називають **елементарними симетричними многочленами.**

Будь-який симетричний многочлен $f(x_1, x_2, \ldots, x_n)$ від n змінних над полем P можна подати у вигляді многочлена від елементарних симетричних многочленів $\sigma_1, \sigma_2, \ldots, \sigma_n$ цих змінних, коефіцієнти якого належать тому самому полю P. Таке зображення є єдиним.

ПРИКЛАДИ РОЗВ'ЯЗУВАННЯ ЗАДАЧ

1. Виразити через елементарні симетричні многочлени такий многочлен:

$$f(x_1, x_2, x_3) = 3x_1^3 + 3x_2^3 + 3x_3^3 + 5x_1x_2x_3 + 2x_1^2 + 2x_2^2 + 2x_3^2.$$

Розв'язання. Заданий многочлен є сумою двох однорідних многочленів

$$f_1(x_1, x_2, x_3) = 3x_1^3 + 3x_2^3 + 3x_3^3 + 5x_1x_2x_3$$

і

$$f_2(x_1, x_2, x_3) = 2x_1^2 + 2x_2^2 + 2x_3^2$$

відповідно третього і другого степенів. Розв'яжемо цю задачу для кожного многочлена окремо.

Щоб виразити многочлен $f_1(x_1, x_2, x_3)$ через елементарні симетричні многочлени, застосуємо загальну схему і метод невизначених коефіцієнтів. Складемо таблицю (табл. 41).

При складанні всіх можливих систем показників вищого члена враховано, що: 1) сума показників у всіх змінних дорівнює степеню многочлена $f_1(x_1, x_2, x_3)$; 2) послідовність показників у змінних x_1, x_2, x_3 незростаюча.

Тому

$$f_1(x_1, x_2, x_3) = 3\sigma_1^3 + a\sigma_1\sigma_2 + b\sigma_3,$$

де a, b — невизначені коефіцієнти. Обчислення коефіцієнтів a і b подаємо у вигляді такої таблиці (табл. 42). Отже, $a = -9$, $b = 14$. Тоді

$$f_1(x_1, x_2, x_3) = 3\sigma_1^3 - 9\sigma_1\sigma_2 + 14\sigma_3.$$

Застосуємо тепер формули скороченого множення. Як відомо,

$$(x_1 + x_2 + x_3)^2 = x_1^2 + x_2^2 + x_3^2 + 2x_1x_2 + 2x_1x_3 + 2x_2x_3.$$

Звідси

$$x_1^2 + x_2^2 + x_3^2 = (x_1 + x_2 + x_3)^2 - 2(x_1x_2 + x_1x_3 + x_2x_3),$$

тому $f_2(x_1, x_2, x_3) = 2\sigma_1^2 - 4\sigma_2$.

Таблиця 41

Система показників вищого члена			Вищий член	Відповідний добуток елементарних симетричних многочленів
x_1	x_2	x_3		
3	0	0	$3x_1^3$	$3\sigma_1^{3-0}\sigma_2^{0-0}\sigma_3^0 = 3\sigma_1^3$
2	1	0	$ax_1^2x_2$	$a\sigma_1^{2-1}\sigma_2^{1-0}\sigma_3^0 = a\sigma_1\sigma_2$
1	1	1	$bx_1x_2x_3$	$b\sigma_1^{1-1}\sigma_2^{1-1}\sigma_3^1 = b\sigma_3$

Таблиця 42

x_1	x_2	x_3	σ_1	σ_2	σ_3	$f_1(x_1, x_2, x_3) = 3\sigma_1^3 + a\sigma_1\sigma_2 + b\sigma_3$
1	1	0	2	1	0	$6 = 24 + 2a$
1	1	−2	0	−3	−2	$-28 = -2b$

Остаточно маємо

$$f(x_1, x_2, x_3) = f_1(x_1, x_2, x_3) + f_2(x_1, x_2, x_3) =$$
$$= 3\sigma_1^3 - 9\sigma_1\sigma_2 + 14\sigma_3 + 2\sigma_1^2 - 4\sigma_2.$$

2. Знайти симетричний многочлен від n змінних з найменшим числом членів який містить член $x_1^2x_2^2$, і виразити його через елементарні симетричні многочлени.

Розв'язання. Позначимо шуканий многочлен через $o(x_1, x_2, \ldots, x_n)$. Згідно з означенням симетричного многочлена, многочлен $o(x_1, x_2, \ldots, x_n)$ разом з членом $x_1^2x_2^2x_3^0\ldots x_n^0$ містить усі члени, утворені із заданого переставлянням змінних[1]. Це означає, що

$$o(x_1, x_2, \ldots, x_n) = x_1^2x_2^2 + \ldots + x_1^2x_n^2 +$$
$$+ x_2^2x_3^2 + \ldots + x_2^2x_n^2 + \ldots + x_{n-1}^2x_n^2.$$

Складемо таблицю (табл. 43).

Таблиця 43

Система показників вищого члена						Вищий член	Відповідний добуток елементарних многочленів
x_1	x_2	x_3	x_4	...	x_n		
2	2	0	0	...	0	$x_1^2x_2^2$	$\sigma_1^{2-2}\sigma_2^{2-0} = \sigma_2^2$
2	1	1	0	...	0	$ax_1^2x_2x_3$	$a\sigma_1^{2-1}\sigma_2^{1-1}\sigma_3^1 = a\sigma_1\sigma_3$
1	1	1	1	...	0	$bx_1x_2x_3x_4$	$b\sigma_1^{1-1}\sigma_2^{1-1}\sigma_3^{1-1}\sigma_4^1 = b\sigma_4$

[1] Многочлен $o(x_1, x_2, \ldots, x_n)$ іноді позначають через $o(x_1^2x_2^2)$ і називають орбітою $x_1^2x_2^2$, або **моногенним многочленом, породженим членом** $x_1^2x_2^2$.

Звідси

$$\varphi(x_1, x_2, \ldots, x_n) = \sigma_2^2 + a\sigma_1\sigma_3 + b\sigma_4.$$

Покладемо $x_1 = x_2 = x_3 = 1$, $x_4 = x_5 = \ldots = x_n = 0$. Тоді $\sigma_1 = 3$, $\sigma_2 = 3$, $\sigma_3 = 1$, $\sigma_4 = 0 \cdot 1 \cdot 9 + 3a = 3$, тобто $a = -2$. Якщо $x_1 = x_2 = x_3 = x_4 = 1$ і $x_5 = \ldots = x_n = 0$, то $\sigma_1 = 4$, $\sigma_2 = 6$, $\sigma_3 = 3$, $\sigma_4 = 1 \cdot 1 \cdot 36 + 16a + b = 6$. Тому $b = 2$. Отже,

$$\varphi(x_1, x_2, \ldots, x_n) = \sigma_2^2 - 2\sigma_1\sigma_3 + 2\sigma_4.$$

3. Виразити многочлен $f(x, y) = x^6 + y^6$ через елементарні симетричні многочлени.

Розв'язання. Застосовуючи формули скороченого множення, дістаємо

$$f(x, y) = (x^2 + y^2)(x^4 - x^2y^2 + y^4) = ((x + y)^2 - 2xy) \times$$
$$\times ((x^2 + y^2)^2 - 3x^2y^2) = (\sigma_1^2 - 2\sigma_2)((\sigma_1^2 - 2\sigma_2)^2 - 3\sigma_2^2) =$$
$$= (\sigma_1^2 - 2\sigma_2)^3 - 3\sigma_2^2(\sigma_1^2 - 2\sigma_2) = \sigma_1^6 - 6\sigma_1^4\sigma_2 + 9\sigma_1^2\sigma_2^2 - 2\sigma_2^3.$$

Наведений приклад свідчить про те, що не завжди загальна схема процесу подання симетричного многочлена через елементарні є раціональною.

Задачі

28.1. Чи є симетричними такі многочлени:

а) $f(x_1, x_2, x_3) = x_1^2x_2 + x_1^2x_3 + x_2^2x_1 + x_2^2x_3 + x_1 + x_2 + x_3$;

б) $f(x_1, x_2, x_3) = 2x_1^3 + 2x_2^2 + 2x_3^2 + x_1x_2x_3 - 1$;

в) $f(x_1, x_2, x_3, x_4) = (x_1x_2 + x_3x_4)(x_1x_4 + x_2x_3)(x_1x_3 + x_2x_4)$;

г) $f(x_1, x_2, x_3) = (x_1 - x_2)(x_2 - x_3)(x_3 - x_1)$;

д) $f(x_1, x_2, \ldots, x_n) = x_1x_2 \ldots x_{n-1} + x_1x_2 \ldots x_{n-2}x_n + \ldots + x_2x_3 \ldots x_n$?

28.2. Доповнити задані многочлени найменшим числом нових членів так, щоб вони стали симетричними:

а) $f(x_1, x_2) = x_1^2 + 2x_2$;

б) $f(x_1, x_2, x_3) = x_1^3 + 2x_1x_2 + 2x_2x_3 + 5$;

в) $f(x_1, x_2, x_3) = (x_1 + x_2)^2 + 2x_1x_3 + x_1x_2x_3$.

28.3. Знайти вищий член таких многочленів:

а) $f(x_1, x_2) = 5\sigma_1^2\sigma_2\sigma_3$;

б) $f(x_1, x_2, x_3) = \sigma_1^2 + 2\sigma_2\sigma_3 - 3\sigma_3^2$.

28.4. Виразити через елементарні симетричні многочлени такі многочлени:

а) $f(x, y) = x^3y + y^3x + 2x^2 + 2y^2$;

б) $f(x, y) = 2x^4y - 5x^2y + 2xy^4 - 5xy^2$.

28.5. Нехай $s_n(x, y) = x^n + y^n$, де $n \in \mathbf{N}$. Довести, що для всіх $k > 2$ виконується рекурентне співвідношення

$$s_k = \sigma_1 s_{k-1} - \sigma_2 s_{k-2}.$$

28.6. При позначеннях задачі 28.5 перевірити справедливість таких рівностей:

а) $s_2 = \sigma_1^2 - 2\sigma_2$;

б) $s_3 = \sigma_1^3 - 3\sigma_1\sigma_2$;

в) $s_4 = \sigma_1^4 - 4\sigma_1^2\sigma_2 + 2\sigma_2^2$;

г) $s_5 = \sigma_1^5 - 5\sigma_1^3\sigma_2 + 5\sigma_1\sigma_2^2$;

д) $s_6 = \sigma_1^6 - 6\sigma_1^4\sigma_2 + 9\sigma_1^2\sigma_2^2 - 2\sigma_2^3$;

е) $s_7 = \sigma_1^7 - 7\sigma_1^5\sigma_2 + 14\sigma_1^3\sigma_2^2 - 7\sigma_1\sigma_2^3$.

28.7. Нехай $s_n(x, y, z) = x^n + y^n + z^n$, де $n \in \mathbf{N}$. Довести, що для всіх $k > 3$ виконується рекурентне співвідношення

$$s_k = \sigma_1 s_{k-1} - \sigma_2 s_{k-2} + \sigma_3 s_{k-3}.$$

28.8. При позначеннях задачі 28.7 перевірити справедливість таких рівностей:

а) $s_2 = \sigma_1^2 - 2\sigma_2$;

б) $s_3 = \sigma_1^3 - 3\sigma_1\sigma_2 + 3\sigma_3$;

в) $s_4 = \sigma_1^4 - 4\sigma_1^2\sigma_2 + 2\sigma_2^2 + 4\sigma_1\sigma_3$;

г) $s_5 = \sigma_1^5 - 5\sigma_1^3\sigma_2 + 5\sigma_1\sigma_2^2 + 5\sigma_1^2\sigma_3 - 5\sigma_2\sigma_3$;

д) $s_6 = \sigma_1^6 - 6\sigma_1^4\sigma_2 + 9\sigma_1^2\sigma_2^2 - 2\sigma_2^3 + 6\sigma_1^3\sigma_3 - 12\sigma_1\sigma_2\sigma_3 + 3\sigma_3^2$.

28.9. Виразити через елементарні симетричні многочлени такі многочлени:

а) $f(x_1, x_2, x_3) = x_1^3 + x_2^3 + x_3^3 - x_1 - x_2 - x_3$;

б) $f(x_1, x_2, x_3) = x_1^5x_2x_3 + x_2^5x_1x_3 + x_1x_2x_3^5 + 2x_1x_2x_3$;

в) $f(x_1, x_2, x_3) = x_1^4x_2^2 + x_2^4x_1^2 + x_3^4x_2^2 + x_3^4x_1^2 + x_1^4x_3^2 + x_2^4x_3^2$;

г) $f(x_1, x_2, x_3) = (x_1 - x_2)^2 + (x_1 - x_3)^2 + (x_2 - x_3)^2$;

д) $f(x_1, x_2, x_3) = (x_1 + x_2 - 5x_3)(x_2 + x_3 - 5x_1)(x_1 + x_3 - 5x_2)$;

е) $f(x_1, x_2, x_3) = (x_1^2 - x_2x_3)(x_2^2 - x_1x_3)(x_3^2 - x_1x_2)$.

28.10. Виразити через елементарні симетричні многочлени чисельник і знаменник раціонального дробу $\dfrac{f(x_1, \ldots, x_n)}{g(x_1, \ldots, x_n)}$ та знайти його значення, якщо:

а) $\dfrac{f(x_1, x_2)}{g(x_1, x_2)} = \dfrac{(x_1 - x_2)^4}{x_1 + x_2}$ і $\sigma_1 = 2$, $\sigma_2 = 1$;

б) $\dfrac{f(x_1, x_2, x_3)}{g(x_1, x_2, x_3)} = \dfrac{1}{x_2} + \dfrac{1}{x_3} + \dfrac{1}{x_1} + \dfrac{2}{x_1x_2} + \dfrac{2}{x_1x_3} + \dfrac{2}{x_2x_3}$ і $\sigma_1 = 0$, $\sigma_2 = 1$, $\sigma_3 = 2$;

в) $\dfrac{f(x_1, x_2)}{g(x_1, x_2)} = \dfrac{x_1^3 + x_2^3}{x_1^2 + x_2^2}$ і змінні x_1, x_2 набувають значень, що дорівнюють кореням рівняння $x^2 + x + 2 = 0$.

28.11. Виразити через елементарні симетричні многочлени такі орбіти многочленів:

а) $x_1^3x_3$ в кільці $P[x_1, x_2, x_3]$;

б) $x_1x_2x_3$ в кільці $P[x_1, x_2, x_3, x_4]$;

в) x_1^3 в кільці $P[x_1, x_2, \ldots, x_n]$.

28.12. Многочлен $f(x_1, x_2, \ldots, x_n)$, який змінює знак при перестановці будь-яких двох змінних, називається **антисиметричним**. Довести, що:

а) квадрат антисиметричного многочлена є симетричним многочленом;

б) добуток симетричного і антисиметричного многочленів є антисиметричним многочленом;

в) будь-який антисиметричний многочлен від двох змінних $f(x_1, x_2)$ можна подати у вигляді $f(x_1, x_2) = (x_1 - x_2) g(x_1, x_2)$, де $g(x_1, x_2)$ є симетричним многочленом;

г) будь-який антисиметричнй многочлен від трьох змінних $f(x_1, x_2, x_3)$ можна подати у вигляді $f(x_1, x_2, x_3) = (x_1 - x_2)(x_1 - x_3) \times (x_2 - x_3) g(x_1, x_2, x_3)$, де $g(x_1, x_2, x_3)$ є симетричним многочленом.

28.13. Довести, що коли симетричний многочлен $f(x_1, x_2)$ ділиться на $x_1 - x_2$, то він ділиться також на $(x_1 - x_2)^2$.

28.14. Довести, що коли симетричний многочлен $f(x_1, x_2, x_3)$ ділиться на $x_1 - x_2$, то він ділиться на многочлен $g(x_1, x_2, x_3) = (x_1 - x_2)^2 (x_1 - x_3)^2 (x_2 - x_3)^2$.

28.15. Довести, що будь-який многочлен від двох змінних є сумою деяких симетричного і антисиметричного многочленів.

§ 29. Застосування симетричних многочленів до розв'язування деяких задач з елементарної алгебри

Література

[2] — § 26, с. 305—309;
[6] — § 53, с. 328—334;
[44] — § 2, 4, с. 19—46, 62—89.

ПРИКЛАДИ РОЗВ'ЯЗУВАННЯ ЗАДАЧ

1. Розв'язати рівняння

$$\sqrt[3]{8+x} + \sqrt[3]{8-x} = 1.$$

Розв'язання. Зробимо заміну:

$$\sqrt[3]{8+x} = u, \quad \sqrt[3]{8-x} = v.$$

Тоді матимемо систему рівнянь

$$\begin{cases} u + v = 1, \\ u^3 + v^3 = 16. \end{cases}$$

Позначивши $u + v = \sigma_1$ і $uv = \sigma_2$, дістаємо

$$u^3 + v^3 = (u+v)\left((u+v)^2 - 3uv\right) = \sigma_1^3 - 3\sigma_1\sigma_2.$$

Система набуває вигляду

$$\begin{cases} \sigma_1 = 1, \\ \sigma_1^3 - 3\sigma_1\sigma_2 = 16 \end{cases} \quad \text{або} \quad \begin{cases} \sigma_1 = 1, \\ \sigma_2 = -5. \end{cases}$$

Повертаючись до змінних u і v, знаходимо

$$\begin{cases} u + v = 1, \\ uv = -5. \end{cases}$$

Розв'язками цієї системи є

$$\begin{cases} u_1 = \dfrac{1+\sqrt{21}}{2}, \\ v_1 = \dfrac{1-\sqrt{21}}{2} \end{cases} \quad \text{та} \quad \begin{cases} u_2 = \dfrac{1-\sqrt{21}}{2}, \\ v_2 = \dfrac{1+\sqrt{21}}{2}. \end{cases}$$

Враховуючи введену заміну, маємо сукупність рівнянь

$$\sqrt[3]{8+x} = \frac{1+\sqrt{21}}{2},$$

$$\sqrt[3]{8+x} = \frac{1-\sqrt{21}}{2},$$

її розв'язками є: $x_1 = 3\sqrt{21}$, $x_2 = -3\sqrt{21}$.

2. Розв'язати систему рівнянь

$$\begin{cases} x + y + z = 6, \\ xy + xz + yz = 5, \\ x^3 + y^3 + z^3 = 126. \end{cases}$$

Розв'язання. Ліва частина кожного з рівнянь системи є симетричним многочленом, а в перших двох рівняннях — навіть елементарним. Згідно з прикладом 1, § 27,

$$3x^3 + 3y^3 + 3z^3 + 5xyz = 3\sigma_1^3 - 9\sigma_1\sigma_2 + 14\sigma_3.$$

Отже, $x^3 + y^3 + z^3 = \sigma_1^3 - 3\sigma_1\sigma_2 + 3\sigma_3$. Тому маємо таку систему:

$$\begin{cases} \sigma_1 = 6, \\ \sigma_2 = 5, \\ \sigma_3 = 0 \end{cases} \quad \text{або} \quad \begin{cases} x + y + z = 6, \\ xy + xz + yz = 5, \\ xyz = 0. \end{cases}$$

Якщо

$$x = 0, \text{ то } \begin{cases} y + z = 6, \\ yz = 5. \end{cases}$$

Одним з розв'язків заданої системи рівнянь є: $x = 0$, $y = 1$, $z = 5$. Усі інші розв'язки дістаємо перестановкою чисел 0, 1, 5. Таким чином,

$$(x, y, z) \in \{(0, 1, 5), (0, 5, 1), (1, 0, 5), (1, 5, 0), (5, 0, 1), (5, 1, 0)\}.$$

3. Розкласти на множники найменшого степеня з раціональними коефіцієнтами многочлен

$$f(x, y, z) = 2x^2y^2 + 2x^2z^2 + 2y^2z^2 - x^4 - y^4 - z^4.$$

Розв'язання. Цей многочлен є симетричним. Виразимо його через елементарні симетричні многочлени (див. задачу 28, 8, в):

$$x^4 + y^4 + z^4 = \sigma_1^4 - 4\sigma_1^2\sigma_2 + 2\sigma_2^2 + 4\sigma_1\sigma_3.$$

Крім того,

$$x^2y^2 + x^2z^2 + y^2z^2 = (xy + xz + yz)^2 - 2x^2yz - 2xy^2z - 2xyz^2 = \sigma_2^2 - 2\sigma_1\sigma_3.$$

Тому

$$f(x, y, z) = 2\sigma_2^2 - 4\sigma_1\sigma_3 - \sigma_1^4 + 4\sigma_1^2\sigma_2 - 2\sigma_2^2 - 4\sigma_1\sigma_3 = \sigma_1\left(4\sigma_1\sigma_2 - \sigma_1^3 - 8\sigma_3\right).$$

Це означає, що многочлен $f(x, y, z)$ ділиться на многочлен

$$g_1(x, y, z) = x + y + z.$$

Оскільки заданий многочлен містить змінні x, y і z тільки в парному степені, то він не зміниться при заміні x на $-x$, y на $-y$ та z на $-z$. Це означає, що $f(x, y, z)$ ділиться також на многочлени:

$$g_2(x, y, z) = -x + y + z,$$
$$g_3(x, y, z) = x - y + z,$$
$$g_4(x, y, z) = x + y - z.$$

Враховуючи те, що многочлени $g_1(x, y, z)$, $g_2(x, y, z)$, $g_3(x, y, z)$ і $g_4(x, y, z)$ є попарно взаємно простими і $\deg f(x, y, z) = 4$, маємо

$$f(x, y, z) = k(x + y + z)(x + y - z)(x - y + z)(y + z - x).$$

Покладаючи тепер $x = y = z = 1$, дістаємо $3k = 3$ і $k = 1$.
Отже, шуканий розклад є

$$f(x, y, z) = (x + y + z)(x + y - z)(x - y + z)(y + z - x).$$

4. Скласти квадратне рівняння з коренями x_1 і x_2, якщо $x_1^3 + x_2^3 = 7$ і $x_1 + x_2 = 1$.

Розв'язання. Нехай шукане рівняння має вигляд $x^2 + ax + b = 0$. Згідно з теоремою Вієта, його корені задовольняють умови $x_1 + x_2 = -a$ і $x_1 x_2 = b$. Оскільки $x_1^3 + x_2^3 = \sigma_1^3 - 3\sigma_1\sigma_2$, то

$$\begin{cases} \sigma_1^3 - 3\sigma_1\sigma_2 = 7, \\ \sigma_1 = 1 \end{cases} \quad \text{і} \quad \begin{cases} \sigma_1 = 1, \\ \sigma_2 = -2. \end{cases}$$

Отже, $b = -2$, і шукане рівняння є

$$x^2 - x - 2 = 0.$$

5. Довести, що коли x, y, z — цілі числа і $x + y + z$ ділиться на 6, то число $x^3 + y^3 + z^3$ також ділиться на 6.

Розв'язання. Розглянемо многочлен $f(x, y, z) = x^3 + y^3 + z^3$. Згідно з прикладом 2, $x^3 + y^3 + z^3 = \sigma_1^3 - 3\sigma_1\sigma_2 + 3\sigma_3$. Число $\sigma_1 = x + y + z$ ділиться на 6 і тому є парним. Це означає, що хоча б одне з чисел x, y, z парне. Тому $\sigma_3 = xyz$ ділиться на 2, а $3\sigma_3$ ділиться на 6. Отже, $x^3 + y^3 + z^3$ ділиться на 6.

Задачі

29.1. У множині дійсних чисел розв'язати такі системи рівнянь:

а) $\begin{cases} x^3 + y^3 = 35, \\ x + y = 5; \end{cases}$

б) $\begin{cases} x^5 + y^5 = 33, \\ x + y = 3; \end{cases}$

в) $\begin{cases} x^2 + xy + y^2 = 49, \\ x^4 + x^2y^2 + y^4 = 931; \end{cases}$

г) $\begin{cases} x^3 + y^3 + xy(x + y) = 13, \\ x^2y^2(x^2 + y^2) = 468; \end{cases}$

д) $\begin{cases} (x - y)(x^2 - y^2) = 3, \\ (x + y)(x^2 + y^2) = 15; \end{cases}$

е) $\begin{cases} x + y + z = 1, \\ x^2 + y^2 + z^2 = 9, \\ x^3 + y^3 + z^3 = 1; \end{cases}$

є) $\begin{cases} x - y + z = 6, \\ x^2 + y^2 + z^2 = 14, \\ x^3 - y^3 + z^3 = 36. \end{cases}$

29.2. Розв'язати систему ірраціональних рівнянь:

а) $\begin{cases} \sqrt{x} + \sqrt{y} = 9, \\ \sqrt[3]{x} + \sqrt[3]{y} = 5; \end{cases}$

б) $\begin{cases} \sqrt{\frac{x}{y}} + \sqrt{\frac{y}{x}} = \frac{61}{\sqrt{xy}} + 1, \\ \sqrt[4]{x^3y} + \sqrt[4]{xy^3} = 78. \end{cases}$

29.3. Розв'язати такі рівняння:

а) $x + \sqrt{17 - x^2} + x\sqrt{17 - x^2} = 9;$

б) $x\frac{19 - x}{x + 1}\left(x + \frac{19 - x}{x + 1}\right) = 84;$

в) $\sqrt[3]{10 - x} - \sqrt[3]{3 - x} = 1;$

г) $\sqrt[4]{8 - x} + \sqrt[4]{89 + x} = 5;$

д) $\sqrt[4]{78 + \sqrt[3]{24 + \sqrt{x}}} - \sqrt[4]{84 - \sqrt[3]{30 - \sqrt{x}}} = 0.$

29.4. Розкласти на множники найменшого степеня з дійсними коефіцієнтами такі многочлени:

а) $f(x, y) = 10x^4 - 27x^3y - 110x^2y^2 - 27xy^3 + 10y^4;$

б) $f(x, y) = 6x^4 - 11x^3y - 18x^2y^2 - 11xy^3 + 6y^4;$

в) $f(x, y) = 2x^4 - x^3y + 3x^2y^2 - xy^3 + 2y^4;$

г) $f(x, y) = 18x^4 - 21x^3y - 94x^2y^2 - 21xy^3 + 18y^4.$

29.5. Подати у вигляді добутку такі многочлени:

а) $f(x, y, z) = (x + y)(x + z)(y + z) + xyz;$

б) $f(x, y, z) = x^3(y + z) + y^3(x + z) + z^3(x + y) + xyz(x + y + z);$

в) $f(x, y, z) = (x - y)^4 + (y - z)^4 + (x - z)^4;$

г) $f(x, y, z) = (x^2 + y^2 + z^2 + xy + xz + yz)^2 - (x + y + z)^2(x^2 + y^2 + z^2).$

29.6. Скоротити дріб

$$\frac{f(x, y, z)}{g(x, y, z)} = \frac{yz - x^2 + xz - y^2 + xy - z^2}{x(yz - x^2) + y(xz - y^2) + z(xy - z^2)}.$$

29.7. Скласти квадратне рівняння з коренями x_1^3 і x_2^3, якщо x_1, x_2 є коренями квадратного рівняння $x^2 - 4x + 3 = 0$.

29.8. Довести, що коли x_1, x_2 є коренями квадратного рівняння $x^2 - 6x + 1 = 0$, то сума $x_1^n + x_2^n$ є цілим числом при будь-якому натуральному n і при жодному з них не ділиться на 5.

29.9. Скласти кубічне рівняння, коренями якого є квадрати коренів рівняння

$$x^3 - 2x^2 + x - 12 = 0.$$

29.10. Довести такі тотожності:

а) $x^4 + y^4 + (x + y)^4 = 2(x^2 + xy + y^2)^2;$

б) $(x + y)^3 + 3xy(1 - x - y) - 1 = (x + y - 1)(x^2 + y^2 - xy + x + y + 1);$

в) $a(b + c)^2 + b(c + a)^2 + c(a + b)^2 = (b + c)(a + c)(a + b) + 4abc;$

г) $xyz(x + y + z)^3 - (yz + xz + xy)^3 = (x^2 - yz)(y^2 - xz)(z^2 - xy);$

д) $(xy + xz + yz)^2 + (x^2 - yz)^2 + (y^2 - xz)^2 + (z^2 - xy)^2 = (x^2 + y^2 + z^2)^2.$

29.11. Довести, що коли $x + y + z = 0$, то:

а) $x^4 + y^4 + z^4 = 2(xy + xz + yz)^2;$

б) $2(x^4 + y^4 + z^4) = (x^2 + y^2 + z^2)^2;$

в) $2(x^5 + y^5 + z^5) = 5xyz(x^2 + y^2 + z^2).$

29.12. Довести, що коли $xy + xz + yz = 0$, то $(x+y)^2(x+z)^2 \times (y+z)^2 + 2x^2y^2z^2 = x^4(y+z)^2 + y^4(x+z)^2 + z^4(x+y)^2$.

29.13. Довести, що коли $xy + xz + yz = 1$, то

$$\frac{x}{1-x^2} + \frac{y}{1-y^2} + \frac{z}{1-z^2} = \frac{4xyz}{(1-x^2)(1-y^2)(1-z^2)}.$$

29.14. Довести, що коли $x + y + z = 0$ і $xy + xz + yz = 0$, то виконується рівність

$$3(x^3y^3 + x^3z^3 + y^3z^3) = (x^3 + y^3 + z^3)^2.$$

§ 30. Результант двох многочленів. Виключення невідомих з системи двох рівнянь з двома невідомими

Література

[1] — § 27, с. 296—311;
[2] — § 27, с. 310—325;
[3] — гл. 15, § 3, с. 500—504;
[5] — гл. XI, § 5, с. 432—438;
[6] — § 54, с. 334—345;
[8] — гл. 6, § 2, с. 265—271.

ТЕОРЕТИЧНІ ВІДОМОСТІ

Нехай

$$f(x) = a_n x^n + a_{n-1}x^{n-1} + \ldots + a_1 x + a_0,$$
$$g(x) = b_m x^m + b_{m-1}x^{m-1} + \ldots + b_1 x + b_0$$

є многочленами над полем P, $a_n b_m \neq 0$ і $\alpha_1, \alpha_2, \ldots, \alpha_n$ — корені многочлена $f(x)$.

Результантом многочленів $f(x)$ і $g(x)$ називається вираз

$$R(f, g) = a_n^m g(\alpha_1) g(\alpha_2) \ldots g(\alpha_n).$$

Результант $R(f, g)$ є симетричним многочленом від $\alpha_1, \alpha_2, \ldots, \alpha_n$, тому результант довільних двох многочленів над полем P є елементом цього поля.

Нехай $\gamma_1, \gamma_2, \ldots, \gamma_m$ — корені многочлена $g(x)$. Тоді:

1°. $R(f, g) = a_n^m b_m^n \prod\limits_{\substack{1 \leqslant i \leqslant n \\ 1 \leqslant j \leqslant m}} (\alpha_i - \gamma_j)$;

2°. $R(g, f) = (-1)^{mn} R(f, g)$.

Для того щоб многочлени $f(x)$ і $g(x)$ мали спільний корінь, необхідно і достатньо, щоб їхній результант дорівнював нулю.

Результант многочленів $f(x)$ і $g(x)$ можна подати у формі Сільвестра:

$$R(f, g) = \begin{vmatrix} a_n & a_{n-1} & \ldots & a_1 & a_0 & 0 & \ldots & 0 \\ 0 & a_n & \ldots & a_2 & a_1 & a_0 & \ldots & 0 \\ \ldots & \ldots & \ldots & \ldots & \ldots & \ldots & \ldots & \ldots \\ 0 & 0 & \ldots & a_n & & & \ldots & a_0 \\ b_m & b_{m-1} & \ldots & b_1 & b_0 & & \ldots & 0 \\ \ldots & \ldots & \ldots & \ldots & \ldots & \ldots & \ldots & \ldots \\ 0 & 0 & \ldots & b_m & & & \ldots & b_0 \end{vmatrix} \begin{matrix} \\ \\ \\ \\ \} m \text{ рядків} \\ \\ \\ \\ \} n \text{ рядків} \end{matrix}$$

Дискримінантом $D(f)$ многочлена $f(x)$ називається вираз

$$D(f) = (-1)^{\frac{n(n-1)}{2}} a_n^{-1} R(f, f'),$$

де $R(f, f')$ — результант многочлена $f(x)$ і його похідної $f'(x)$.

При цьому справджується рівність

$$D(f) = a_n^{2n-2} \prod_{1 \leqslant i < j \leqslant n} (\alpha_i - \alpha_j)^2.$$

Многочлен $f(x)$ має кратний корінь тоді і тільки тоді, коли його дискримінант дорівнює нулю.

Нехай задано систему двох алгебраїчних рівнянь з двома невідомими, що мають коефіцієнти з поля P:

$$\begin{cases} f(x, y) = 0, \\ g(x, y) = 0. \end{cases}$$

Схема виключення невідомих з цієї системи така:

1) упорядковуємо многочлени $f(x, y)$ і $g(x, y)$ за спадними степенями однієї із змінних, наприклад, x;

2) складаємо результант $R(f, g)$, розглядаючи змінну y як параметр;

3) знаходимо всі корені результанта $\beta_1, \beta_2, \ldots, \beta_l$;

4) підставляємо в задану систему замість змінної y значення $\beta_1, \beta_2, \ldots, \beta_l$; дістаємо сукупність l систем двох рівнянь з одним невідомим x;

5) розв'язуємо цю сукупність систем рівнянь і складаємо відповідні пари розв'язків.

ПРИКЛАДИ РОЗВ'ЯЗУВАННЯ ЗАДАЧ

1. Обчислити результант $R(f, g)$ для многочленів

$$f(x) = x^2 - 3x + 6 \quad \text{і} \quad g(x) = x^3 + x^2 - x - 1.$$

Розв'язання. I *спосіб*. Заданий многочлен $f(x)$ має комплексні корені. Многочлен $g(x) = (x^2 - 1)(x + 1)$ має коренями числа -1 і 1. Оскільки

$$R(f, g) = (-1)^{3 \cdot 2} R(g, f) = R(g, f),$$

то

$$R(f, g) = f(-1) f(-1) f(1) = 10 \cdot 10 \cdot 4 = 400.$$

II *спосіб*. Нехай α_1, α_2 — корені многочлена $f(x)$. Тоді

$$R(f, g) = (\alpha_1^3 + \alpha_2^2 - \alpha_1 - 1)(\alpha_2^3 + \alpha_2^2 - \alpha_2 - 1) = (\alpha_1\alpha_2)^3 +$$
$$+ (\alpha_1\alpha_2)^2(\alpha_1 + \alpha_2) - \alpha_1\alpha_2(\alpha_1^2 + \alpha_2^2) - (\alpha_1^3 + \alpha_2^3) +$$
$$+ (\alpha_1\alpha_2)^2 - \alpha_1\alpha_2(\alpha_1 + \alpha_2) - (\alpha_1^2 + \alpha_2^2) + \alpha_1\alpha_2 + (\alpha_1 + \alpha_2) + 1.$$

За теоремою Вієта, $\alpha_1\alpha_2 = 6$ і $\alpha_1 + \alpha_2 = 3$. Тоді

$$\alpha_1^2 + \alpha_2^2 = (\alpha_1 + \alpha_2)^2 - 2\alpha_1\alpha_2 = 3 \quad \text{і}$$
$$\alpha_1^3 + \alpha_2^3 = (\alpha_1 + \alpha_2)((\alpha_1 + \alpha_2)^2 - 3\alpha_1\alpha_2) = -27.$$

Отже,

$$R(f, g) = 216 + 108 + 18 + 27 + 36 - 18 + 3 + 3 + 3 + 1 = 400.$$

III *спосіб*. Обчислимо результант $R(f, g)$ у формі Сільвестра:

$$R(f, g) = \begin{vmatrix} 1 & -3 & 6 & 0 & 0 \\ 0 & 1 & -3 & 6 & 0 \\ 0 & 0 & 1 & -3 & 6 \\ 1 & 1 & -1 & -1 & 0 \\ 0 & 1 & 1 & -1 & -1 \end{vmatrix} = \begin{vmatrix} 1 & -3 & 6 & 0 & 0 \\ 0 & 1 & -3 & 6 & 0 \\ 0 & 0 & 1 & -3 & 6 \\ 0 & 4 & -7 & -1 & 0 \\ 0 & 1 & 1 & -1 & -1 \end{vmatrix} =$$

$$= \begin{vmatrix} 1 & -3 & 6 & 0 \\ 6 & 7 & -9 & 0 \\ 4 & -7 & -1 & 0 \\ 1 & 1 & -1 & -1 \end{vmatrix} = - \begin{vmatrix} 1 & -3 & 6 \\ 6 & 7 & -9 \\ 4 & -7 & -1 \end{vmatrix} =$$

$$= -(-7 + 36 \cdot 3 - 36 \cdot 7 - 168 - 63 - 18) = 400.$$

Зауваження. Найбільш раціональний тут I спосіб. Проте, якщо важко знайти корені заданих многочленів, то доцільно застосувати II або III спосіб.

2. Довести, що многочлен

$$f(x) = x^4 - 2x^3 + (a+1)x^2 - 2ax + a$$

має кратний корінь при будь-якому $a \in \mathbf{C}$.

Розв'язання. Достатньою умовою існування кратного кореня многочлена е те, що дискримінант многочлена дорівнює нулю. Крім того, $D(f) = (-1)^{\frac{4\cdot 3}{2}} \times \times 1^{-1} \cdot R(f, f')$. Знайдемо похідну:

$$f'(x) = 4x^3 - 6x^2 + 2(a+1)x - 2a.$$

Тоді

$$R(f, f') = \begin{vmatrix} 1 & -2 & (a+1) & -2a & a & 0 & 0 \\ 0 & 1 & -2 & (a+1) & -2a & a & 0 \\ 0 & 0 & 1 & -2 & (a+1) & -2a & a \\ 4 & -6 & 2(a+1) & -2a & 0 & 0 & 0 \\ 0 & 4 & -6 & 2(a+1) & -2a & 0 & 0 \\ 0 & 0 & 4 & -6 & 2(a+1) & -2a & 0 \\ 0 & 0 & 0 & 4 & -6 & 2(a+1) & -2a \end{vmatrix} =$$

$$= \begin{vmatrix} 1 & -2 & (a+1) & -2a & a & 0 & 0 \\ 0 & 1 & -2 & (a+1) & -2a & a & 0 \\ 0 & 0 & 1 & -2 & (a+1) & -2a & a \\ 0 & 2 & -2(a+1) & 6a & -4a & 0 & 0 \\ 0 & 4 & -6 & 2(a+1) & -2a & 0 & 0 \\ 0 & 0 & 4 & -6 & 2(a+1) & -2a & 0 \\ 0 & 0 & 0 & 4 & -6 & 2(a+1) & -2a \end{vmatrix} =$$

$$= 2^4 \begin{vmatrix} 1 & -2 & (a+1) & -2a & a & 0 \\ 0 & 1 & -2 & (a+1) & -2a & a \\ 1 & -(a+1) & 3a & -2a & 0 & 0 \\ 2 & -3 & (a+1) & -a & 0 & 0 \\ 0 & 2 & -3 & (a+1) & -a & 0 \\ 0 & 1 & 0 & (a-2) & (1-a) & 0 \end{vmatrix} =$$

$$= 2^4 a \begin{vmatrix} 1 & -2 & (a+1) & -2a & a \\ 0 & (1-a) & (2a-1) & 0 & -a \\ 0 & 1 & (-a-1) & 3a & -2a \\ 0 & 2 & -3 & (a+1) & -a \\ 0 & 1 & 0 & (a-2) & (1-a) \end{vmatrix} =$$

$$= 2^4 a \begin{vmatrix} -a & 3a & -3a & a \\ 1 & (-a-1) & 3a & -2a \\ 0 & (2a-1) & (-5a+1) & 3a \\ 0 & (a+1) & -2(a+1) & (1+a) \end{vmatrix}.$$

Якщо $a = 0$, то $R(f, f') = 0$; якщо $a \neq 0$, то

$$R(f, f') = 2^4 \cdot a \begin{vmatrix} 0 & -a+2 & 3(a-1) & -2a+1 \\ 1 & -(a+1) & 3a & -2a \\ 0 & 2a-1 & (-5a+1) & 3a \\ 0 & a+1 & -2(a+1) & 1+a \end{vmatrix} =$$

$$= -2^4 a \begin{vmatrix} -a+2 & a-2 & -2a+1 \\ 2a-1 & -2a+1 & 3a \\ a+1 & -a-1 & 1+a \end{vmatrix} = 0.$$

Отже, при будь-яких $a \in \mathbf{C}$, $R(f, f') = 0$ і $D(f) = 0$. Тому многочлен $f(x)$ має кратний корінь.

3. Розв'язати систему рівнянь

$$\begin{cases} y^2 + x^2 - y - 3x = 0, \\ y^2 - 6xy - x^2 + 11y + 7x - 12 = 0. \end{cases}$$

Розв'язання. Застосуємо метод виключення невідомих. Для цього в лівих частинах рівнянь впорядкуємо многочлени за спадними степенями змінної y (можна взяти і змінну x):

$$\begin{cases} y^2 - y + x^2 - 3x = 0, \\ y^2 + (11 - 6x)y - x^2 + 7x - 12 = 0. \end{cases}$$

Складемо результант для цих многочленів і знайдемо його корені:

$$R(x) = \begin{vmatrix} 1 & -1 & x^2 - 3x & 0 \\ 0 & 1 & -1 & x^2 - 3x \\ 1 & 11 - 6x & -x^2 + 7x - 12 & 0 \\ 0 & 1 & 11 - 6x & -x^2 + 7x - 12 \end{vmatrix} =$$

$$= \begin{vmatrix} 1 & -1 & x^2 - 3x & 0 \\ 0 & 1 & -1 & x^2 - 3x \\ 0 & 12 - 6x & -2x^2 + 10x - 12 & 0 \\ 0 & 1 & 11 - 6x & -x^2 + 7x - 12 \end{vmatrix} =$$

$$= \begin{vmatrix} 1 & 0 & x^2 - 3x \\ 12 - 6x & -2x^2 + 4x & 0 \\ 1 & 12 - 6x & -x^2 + 7x - 12 \end{vmatrix} =$$

$$= 2(x-2) \begin{vmatrix} 1 & 0 & x^2 - 3x \\ -3 & -x & 0 \\ 1 & 12 - 6x & -x^2 + 7x - 12 \end{vmatrix} =$$

$$= 2(x-2) \begin{vmatrix} 1 & 0 & x^2 - 3x \\ -3 & -x & -x \\ 1 & 12 - 6x & -x^2 + x \end{vmatrix} = 2x(x-2) \begin{vmatrix} 1 & 0 & x - 3 \\ -3 & -x & -1 \\ 1 & 12 - 6x & -x + 1 \end{vmatrix} =$$

$$= 2x(x-2)(x^2 - x - 3(x-3)(12 - 6x) + x^2 - 3x + 12 - 6x) =$$

$$= 2x(x-2)(20x^2 - 100x + 120) = 40x(x-2)^2(x-3).$$

Отже, коренями результанта є 0, 2 і 3. Підставимо їх у задану систему замість змінної x.

а) Якщо $x = 0$, то матимемо систему з одним невідомим:

$$\begin{cases} y^2 - y = 0, \\ y^2 + 11y - 12 = 0. \end{cases}$$

Її розв'язком є $y = 1$. Це означає, що $x_1 = 0$, $y_1 = 1$ є розв'язком заданої системи.

б) Якщо $x = 2$, то дістаємо

$$\begin{cases} y^2 - y - 2 = 0, \\ y^2 - y - 2 = 0. \end{cases}$$

Розв'язками цієї системи є: $y = -1$, $y = 2$. Тоді розв'язками заданої системи є: $x_2 = 2$, $y_2 = -1$ і $x_3 = 2$, $y_3 = 2$.

в) Якщо $x = 3$, то система набуває вигляду

$$\begin{cases} y^2 - y = 0, \\ y^2 - 7y = 0. \end{cases}$$

Її розв'язком є $y = 0$. Отже, $x_4 = 3$, $y_4 = 0$ є розв'язком заданої системи. Таким чином, задана система рівнянь має розв'язки:

$$(x, y) \in \{(0, 1), (2, -1), (2, 2), (3, 0)\}.$$

Задачі

30.1. Обчислити результант $R(f, g)$ для таких пар многочленів:

а) $f(x) = 6x^2 + x - 2$, $g(x) = 3x^2 - 4x + 2$;

б) $f(x) = x^3 + 2x - 1$, $g(x) = x^2 - 2x - 3$;

в) $f(x) = 2x^3 + x^2 - 2x - 1$, $g(x) = 3x^3 - 4x^2 + 7$;

г) $f(x) = x^4 - 3x^2 - 4$, $g(x) = 3x^3 + x^2 + 3x - 1$;

д) $f(x) = 2x^2 + x - 2$, $g(x) = x^4 + 5x^2 + 4$;

е) $f(x) = x^2 - 2x + 2$, $g(x) = 2x^2 + x - 5$;

е) $f(x) = x^4 - 2x^2 + 3$, $g(x) = x^2 - x + 1$;

ж) $f(x) = 3x^3 + x - 1$, $g(x) = x^2 - 2x + 4$;

з) $f(x) = x^3 - 2x + 2$, $g(x) = x^2 + 2x + 2$;

к) $f(x) = x^3 + x^2 + x - 1$, $g(x) = x^3 - x - 1$;

л) $f(x) = x^3 + 2x^2 + x - 2$, $g(x) = x^2 - 2x + 3$;

м) $f(x) = x^3 + 2x^2 + 4x + 1$, $g(x) = 3x^2 + 4x + 4$.

30.2. Довести, що:

а) $R(f, g_1 \pm g_2) = R(f, g_1) \pm R(f, g_2)$, коли $\deg f = 1$;

б) $R(f, g_1 \cdot g_2) = R(f, g_1) \cdot R(f, g_2)$;

в) $R(f_1 \cdot f_2, g_1 \cdot g_2) = R(f_1, g_1) \cdot R(f_1, g_2) \cdot R(f_2, g_1) \cdot R(f_2, g_2)$.

30.3. При якому значенні λ мають спільний корінь такі многочлени:

а) $f(x) = 2x^2 + \lambda x - 3$, $g(x) = \lambda x^2 + x - 2$;

б) $f(x) = x^2 + \lambda$, $g(x) = x^3 - 3x^2 + \lambda x - 3$;

в) $f(x) = x^3 - 5x^2 + 4\lambda x - 4$, $g(x) = 3x^2 - 5\lambda x + 8$;

г) $f(x) = x^3 + \lambda x^2 + 2$, $g(x) = x^3 + 2\lambda x - 1$?

30.4. Обчислити дискримінант таких многочленів:

а) $f(x) = x^3 + 6x + 2$;

б) $f(x) = x^3 - 6ix + 4 - 4i$;

в) $f(x) = x^3 - 9x^2 + 21x - 5$;

г) $f(x) = x^4 - x^2 + 1$;

д) $f(x) = x^4 - (1 + 2i)x^3 - (4 - 2i)x^2 + (1 + 6i)x + 3$;

е) $f(x) = x^4 - x^3 - 3x^2 + x + 1$;

є) $f(x) = x^5 + 2$;

ж) $f(x) = x^n + a$, де $n \in \mathbf{N}$ і $a \in \mathbf{C}$.

30.5. Знаючи, що дискримінант многочлена

$$f(x) = a_5x^5 + a_4x^4 + a_3x^3 + a_2x^2 + a_1x + a_0$$

дорівнює нулю, знайти дискримінант многочлена

$$\varphi(x) = a_0x^5 + a_1x^4 + a_2x^3 + a_3x^2 + a_4x + a_5.$$

Результат узагальнити.

30.6. Довести, що дискримінант многочлена $f(x) = x^4 + ax^2 + bx + c$ дорівнює дискримінанту многочлена

$$g(x) = 8x^3 - 4ax^2 - 8cx - (b^2 - 4ac).$$

30.7. Довести, що:

а) $D((x - a) \cdot f(x)) = D(f(x)) \cdot |f(a)|^2$;

б) $D(f \cdot g) = D(f) \cdot D(g) \cdot [R(f, g)]^2$.

30.8. При якому значенні λ мають кратні корені такі многочлени:

а) $f(x) = 4x^3 - \lambda x + 1$;

б) $f(x) = x^3 - 3x^2 + \lambda^2$;

в) $f(x) = x^3 + (2 - 3i)x^2 - \lambda x - 2$?

30.9. Розв'язати такі системи рівнянь:

а) $\begin{cases} x^2 + 2y^2 = 17, \\ 6x^2 - xy - 12y^2 = 0; \end{cases}$

б) $\begin{cases} x^2 - y^2 - 3 = 0, \\ x^2 + xy - y - 3 = 0; \end{cases}$

в) $\begin{cases} y^2 - 5y + 4x - 4 = 0, \\ 2y^2 + y - x^2 + 1 = 0; \end{cases}$

г) $\begin{cases} x^2y - 2x^2 - xy - 4 = 0, \\ x^2y - 2x^2 + 2x + y - 2 = 0; \end{cases}$

д) $\begin{cases} 5x^2 - 5y^2 - 3x + 9y = 0, \\ 5x^3 + 5y^3 - 15x^2 - 13xy - y^2 = 0; \end{cases}$

е) $\begin{cases} (y - 1)x^2 + xy - 3 = 0, \\ (y - 1)x^2 - 2x + y - 1 = 0. \end{cases}$

Розділ VI. МНОГОЧЛЕНИ НАД ПОЛЕМ КОМПЛЕКСНИХ ЧИСЕЛ І НАД ПОЛЕМ ДІЙСНИХ ЧИСЕЛ

§ 31. Многочлени над полем комплексних чисел. Алгебраїчна замкненість поля комплексних чисел

Література

[1] — § 28, 29, с. 311—319;
[2] — § 28, § 29, с. 325—334;
[3] — гл. 16, § 1, с. 505—512;
[5] — гл. VII, § 2, с. 255—261; гл. VIII, § 3, с. 291—297; гл. IX, § 4, с. 343—347;

[6] — § 23, 24, с. 147—158;
[7] — § 13, с. 76—83;
[8] — гл. 6, § 3, с. 272—281.

ТЕОРЕТИЧНІ ВІДОМОСТІ

Нехай $f(x)$ — деякий многочлен над полем P. Якщо $\deg f \geqslant 1$, то існує розширення K поля P, в якому міститься деякий корінь многочлена $f(x)$. З цього твердження випливає, що для будь-якого многочлена $f(x) \in P[x]$ степеня $\deg f \geqslant 1$ існує таке розширення L поля P, що $f(x)$ можна подати в $L[x]$ у вигляді добутку лінійних множників.

Поле P називають **полем розкладу многочлена** $f(x)$, якщо $f(x)$ розкладається в $P[x]$, на лінійні множники. Поле P, яке є полем розкладу будь-якого многочлена $f(x) \in P[x]$, називають **алгебраїчно замкненим.**

Нехай $f(z) = a_n z^n + \ldots + a_1 z + a_0$ — многочлен ненульового степеня над полем $\mathbf{C}$ комплексних чисел, а M — як завгодно велике додатне дійсне число. Введемо позначення $N_1 = 1 + \frac{2A}{|a_n|}$, де A — найбільший з модулів коефіцієнтів $|a_{n-1}|, \ldots, |a_1|, |a_0|$. Тоді для будь-якого $z \in \mathbf{C}$, $|f(z)| > M$, як тільки $|z| > \max\left\{N_1, \sqrt[n]{\frac{2M}{|a_n|}}\right\}$. Многочлен $f(z)$ має тільки ті корені, модуль яких менший за число $N_0 = 1 + \frac{A}{|a_n|}$. Крім того, як тільки $|z| > N_0$, то модуль старшого члена многочлена $f(x)$ більше за модуль суми решти членів цього многочлена.

Кожен многочлен ненульового степеня з комплексними коефіцієнтами

$$f(z) = a_n z^n + \ldots + a_1 z + a_0$$

має хоча б один комплексний корінь. Звідси випливає, що незвідними над полем комплексних чисел є тільки многочлени першого степеня, а кожен многочлен n-го степеня ($n > 0$) над полем комплексних чисел єдиним способом (з точністю до порядку множників) розкладається над цим полем на лінійні множники:

$$f(z) = a_n (z - z_1)(z - z_2) \ldots (z - z_n),$$

де $z_1, z_2, \ldots, z_n$ — корені многочлена $f(z)$. Отже, поле $\mathbf{C}$ є алгебраїчно замкненим і для коренів многочлена $f(z)$ у полі $\mathbf{C}$ є справедливими формули Вієта:

$$z_1 + z_2 + \ldots + z_n = -\frac{a_{n-1}}{a_n},$$

$$z_1 z_2 + z_1 z_2 + \ldots + z_{n-1} z_n = \frac{a_{n-2}}{a_n},$$

$$\ldots\ldots\ldots\ldots\ldots\ldots$$

$$z_1 z_2 \ldots z_n = (-1)^n \frac{a_0}{a_n}.$$

ПРИКЛАДИ РОЗВ'ЯЗУВАННЯ ЗАДАЧ

1. Довести, що фактор-кільце $Q[x]/\langle x^2 - 2\rangle$ кільця $Q[x]$ за головним ідеалом $\langle x^2 - 2\rangle$ є полем розкладу многочлена $f(x) = x^2 - 2$ з кільця $Q[x]$.

Розв'язання. Многочлен $f(x) = x^2 - 2$ не має раціональних коренів і тому є незвідним над полем $\mathbf{Q}$. Ідеал $\langle f\rangle = \langle x^2 - 2\rangle$ відіграє роль нуля в фактор-кільці $Q[x]/\langle x^2 - 2\rangle$, а елементи останнього мають вигляд $a = g(x) + \langle f\rangle$, де $g(x) \in Q[x]$. Оскільки в кільці $Q[x]$ можна виконувати ділення многочленів з остачею, то вважатимемо, що $\deg g < 2$. Нехай $a = g(x) + \langle f\rangle \neq \langle f\rangle$. Тоді многочлени $f(x)$ і $g(x)$ є взаємно простими. Тому існують многочлени $u(x)$, $v(x) \in Q[x]$ такі, що $f(x)u(x) + g(x)v(x) = 1$. Звідси $g(x)v(x) = 1 - f(x)u(x)$, тому в кільці $Q[x]/\langle x^2 - 2\rangle$ виконується рівність $[g(x) + \langle f\rangle][v(x) + \langle f\rangle] = 1 + \langle f\rangle$. Це означає, що для елемента $a \in Q[x]/\langle x^2 - 2\rangle$ існує обернений елемент $a^{-1} = v(x) + \langle f\rangle$.

Отже, $Q[x]/\langle x^2 - 2\rangle$ є полем, яке містить поле $\overline{Q} = \left\{\frac{m}{n} + \langle f\rangle \;\middle|\; \frac{m}{n} \in Q\right\}$, ізоморфне $\mathbf{Q}$. Ототожнимо число $\frac{m}{n} \in \mathbf{Q}$ з класом $\frac{m}{n} + \langle f\rangle$.

Нехай $b = x + \langle f\rangle \in Q[x]/\langle x^2 - 2\rangle$.
Вважаючи, що $-2 = -2 + \langle f\rangle$, маємо: $f(b) = b^2 + \langle -2\rangle = [x + \langle f\rangle]^2 + [-2 + \langle f\rangle] = [x^2 + \langle f\rangle] + [-2 + \langle f\rangle] = x^2 - 2 + \langle f\rangle = \langle f\rangle$.
Аналогічно $f(-b) = f(-x + \langle f\rangle) = \langle f\rangle$. Це означає, що многочлен $f(x) = x^2 - 2$ має в полі $Q[x]/\langle x^2 - 2\rangle$ два корені: $x_1 = b$ і $x_2 = -b$. Тоді $f(x) = (x - b)(x + b)$ і поле $Q[x]/\langle x^2 - 2\rangle$ є полем розкладу многочлена $f(x) = x^2 - 2$.

2. Розкласти на незвідні над полем $\mathbf{C}$ множники многочлен

$$f(x) = (2i - 3)x^3 - 2 - 3i.$$

Розв'язання. Знайдемо корені многочлена $f(x)$:

$$(2i - 3)x^3 - 2 - 3i = 0, \quad x^3 = -i,$$

$$x_{1,\,2,\,3} = \sqrt[3]{-i} \text{ або } x_{1,\,2,\,3} = \cos\frac{\frac{3}{2}\pi + 2k\pi}{3} + i\sin\frac{\frac{3}{2}\pi + 2k\pi}{3}, \text{ де } k = 0, 1, 2.$$

Тому $x_1 = i$, $x_2 = -\frac{\sqrt{3}}{2} - \frac{1}{2}i$, $x_3 = \frac{\sqrt{3}}{2} - \frac{1}{2}i$.

Отже,
$$f(x) = (2i - 3)(x - i)\left(x + \frac{\sqrt{3}}{2} + \frac{1}{2}i\right)\left(x - \frac{\sqrt{3}}{2} + \frac{1}{2}i\right).$$

3. Знайти зведений многочлен за його коренями x_1^2, $x_1 x_2$ і x_2^2, якщо числа x_1 і x_2 є коренями рівняння

$$x^2 + (i + 2)x - i = 0.$$

Розв'язання. Нехай $f(x) = x^3 + ax^2 + bx + c$ — шуканий многочлен. За формулами Вієта маємо

$$\begin{cases} x_1^2 + x_1 x_2 + x_2^2 = -a, \\ x_1^3 x_2 + x_1^2 x_2^2 + x_1 x_2^3 = b, \\ x_1^3 x_2^3 = -c. \end{cases}$$

Проте $x_1 + x_2 = -i - 2$ і $x_1 x_2 = -i$. Тому

$$a = -(x_1 + x_2)^2 + x_1 x_2 = -(-i - 2)^2 - i = -3 - 5i,$$

$$b = x_1 x_2 (x_1^2 + x_1 x_2 + x_2^2) = x_1 x_2 [(x_1 + x_2)^2 - x_1 x_2] =$$
$$= -i[(i + 2)^2 + i] = -5 - 3i,$$
$$c = -(x_1 x_2)^3 = -i.$$

Отже,

$$f(x) = x^3 - (3 + 5i)x^2 - (5 + 3i)x - i.$$

Задачі

31.1. Довести, що $Q[x]/\langle x^2 - 3\rangle$ є полем розкладу многочлена $f(x) = x^2 - 3$.

31.2. Довести, що поля $Q[x]/\langle x^2 - 3\rangle$ і $Q(\sqrt{3})$ ізоморфні.

31.3. Чи є поле $Q(\sqrt[3]{2})$ полем розкладу многочлена $f(x) = x^3 - 2$?

31.4. Знайти мінімальне поле розкладу многочлена $f(x) = x^2 - 5$ з кільця $Q[x]$.

31.5. Знайти мінімальне поле розкладу многочлена $f(x) = x^4 - 1$ з кільця $Q[x]$.

31.6. Довести, що поле $R[x]/\langle x^2 + 1\rangle$ є алгебраїчно замкненим.

31.7. Чи є алгебраїчно замкненим поле $Q[x]/\langle x^2 + 1\rangle$?

31.8. Знайти додатне число m таке, що з нерівності $|z| > m$ випливають такі нерівності:

а) $|z^4 + 4z^3 - 4z^2 - 2| > 648$;

б) $|z^4 - 4z^3 + 2z + 6| > 8$;

в) $|4z^4 + z^3 - 2z^2 + 1 + i| > 512$;

г) $|f(z)| > |f(a)|$, якщо $f(z) = 2z^5 - z^4 + z^3 - (2 + i)z^2 + iz - (3 + 2i)$ та $a = i$.

31.9. Чи може число $3 - 4i$ бути коренем таких многочленів:

а) $f(z) = 2iz^5 + 3z^4 - (1 + i)z^2 + (2 - 3i)z - 4i$,

б) $f(z) = z^4 - 6z^3 + 5z^2 + iz - 3 + 4i$?

31.10. Розкласти многочлен $f(x)$ на незвідні над полем C множники:

а) $f(x) = 5x^2 + 2x + 10$;

б) $f(x) = x^2 - (1 + i)x + i$;

в) $f(x) = x^4 - 6x^3 + 11x^2 - 6x + 1$;

г) $f(x) = x^4 - 10x^2 + 169$;

д) $f(x) = x^8 - 1$;

е) $f(x) = x^4 + 8x^3 + 8x - 1$.

31.11. Знайти многочлен найменшого степеня, в якого:

а) число i є подвійним коренем, а $1 - i$ — простим;

б) число 2 є подвійним коренем, а $2i$, $3 + i$, $3 - i$ — простими коренями;

в) число $-2i$ є потрійним коренем, а -3 — простим.

31.12. Знайти суму квадратів коренів многочлена

$$f(x) = x^3 + 3x^2 - 7x + 1.$$

31.13. Знайти суму кубів коренів многочлена

$$f(x) = x^3 + 2x^2 + x - 3.$$

31.14. Довести, що коли комплексні числа $\alpha_1, \alpha_2, \ldots, \alpha_n$ задовольняють умови

$$\alpha_1 + \alpha_2 + \ldots + \alpha_n = -a_{n-1},$$
$$\alpha_1\alpha_2 + \ldots + \alpha_{n-1}\alpha_n = a_{n-2},$$
$$\ldots\ldots\ldots\ldots\ldots$$
$$\alpha_1\alpha_2 \ldots \alpha_n = (-1)^n a_0,$$

то ці числа є коренями многочлена

$$f(z) = z^n + a_{n-1}z^{n-1} + \ldots + a_1 z + a_0.$$

31.15. Знайти зведені многочлени, в яких:

а) корені дорівнюють $y_1 = x_2x_3$, $y_2 = x_1x_3$, $y_3 = x_1x_2$, а x_1, x_2, x_3 є коренями многочлена $f(x) = x^3 - 2x - 5$;

б) корені дорівнюють $y_1 = \frac{x_1}{x_2x_3}$, $y_2 = \frac{x_2}{x_1x_3}$, $y_3 = \frac{x_3}{x_1x_2}$, а x_1, x_2, x_3 є коренями многочлена $f(x) = -2x^3 + x^2 + 2x + 3$.

31.16. Довести, що всі корені наступних многочленів є дійсними числами:

а) $f(x) = x^3 + 3x - 1$;

б) $f(x) = x^3 + 7x^2 + 25x + 1$.

31.17. Корені многочлена $f(x)$ утворюють арифметичну прогресію. Знайти цей многочлен і його корені, якщо:

а) $f(x) = x^3 + 6x^2 + 5x + r$,

б) $f(x) = x^3 - 18x^2 + qx + 24$.

31.18. Один з коренів многочлена

$$f(x) = x^3 - 7x^2 + 14x + r$$

вдвоє більший за другий. Знайти $f(x)$ і його корені.

31.19. За формулами Вієта знайти зведений многочлен $f(x)$ найменшого степеня, якщо його похідна має прості корені 2 та $1 - i$, двократні корені i, а 1 є коренем многочлена $f(x)$.

31.20. Довести, що рівність $ab = c$ є необхідною і достатньою умовою того, щоб серед коренів рівняння

$$x^3 + ax^2 + bx + c = 0, \quad c \neq 0,$$

були два протилежні числа.

31.21. Розв'язати рівняння $x^3 - 3\sqrt{3}x^2 + 7x - \sqrt{3} = 0$, якщо один з його коренів більше від другого на $\sqrt{2}$.

31.22. Розв'язати рівняння $8x^3 + 4x^2 - 34x + 15 = 0$, якщо два його корені x_1 і x_2 задовольняють рівняння $2x_1 - 4x_2 = 1$.

31.23. Корені рівняння $x^3 - 6x^2 + px + q = 0$ задовольняють співвідношення $x_1 : x_2 : x_3 = 1 : 2 : 3$. Знайти ці корені та коефіцієнти p і q.

§ 32. Многочлени над полем дійсних чисел

Література

[1] — § 29, с. 320—323;
[2] — § 29, с. 334—337;
[3] — гл. 16, § 2, с. 513—514;
[5] — гл. IX, § 5, с. 347—350;
[6] — § 24, с. 159—161;
[7] — § 14, с. 84—86;
[8] — гл. 6, § 4, с. 282—283.

ТЕОРЕТИЧНІ ВІДОМОСТІ

Нехай $f(z) = a_n z^n + a_{n-1}z^{n-1} + \ldots + a_1 z + a_0$ — многочлен з дійсними коефіцієнтами. Якщо комплексне число z_0 є коренем многочлена $f(z)$, то спряжене комплексне число $\bar{z}_0$ також є коренем цього многочлена. Крім того, якщо комплексне число z_0 є коренем k-ї кратності многочлена $f(z)$, то спряжене комплексне число $\bar{z}_0$ також є коренем многочлена тієї самої кратності.

Кожен многочлен з дійсними коефіцієнтами, степінь якого більше 2, є звідним над полем дійсних чисел.

Кожен многочлен $f(z)$ з дійсними коефіцієнтами єдиним способом розкладається над полем **R** у добуток лінійних множників і квадратних тричленів:

$$f(z) = a_n (z - z_1)^{k_1} \dots (z - z_l)^{k_l} (z^2 + p_{l+1} z + g_{l+1})^{k_l+1} \dots (z^2 + p_m z + g_m)^{k_m}.$$

ПРИКЛАДИ РОЗВ'ЯЗУВАННЯ ЗАДАЧ

1. Розв'язати рівняння

$$x^4 - x^3 + x^2 + 9x - 10 = 0,$$

якщо один з його коренів дорівнює $1 - 2i$.

Розв'язання. Задане рівняння має дійсні коефіцієнти. Тому число $1 + 2i$ також є його коренем, а многочлен

$$f(x) = x^4 - x^3 + x^2 + 9x - 10$$

ділиться на квадратний тричлен $x^2 - 2x + 5$.

Виконаємо ділення «кутом»

$$\begin{array}{r|l} x^4 - x^3 + x^2 + 9x - 10 & x^2 - 2x + 5 \\ \underline{x^4 - 2x^3 + 5x^2} & \hline x^2 + x - 2 \\ -x^3 - 4x^2 + 9x & \\ \underline{x^3 - 2x^2 + 5x} & \\ -2x^2 + 4x - 10 & \\ \underline{-2x^2 + 4x - 10} & \\ 0 & \end{array}$$

Щоб знайти інші корені заданого рівняння, розв'язуємо рівняння $x^2 + x - 2 = 0$. Маємо $x = -2$, $x = 1$. Отже,

$$x_1 = 1 - 2i,\ x_2 = 1 + 2i,\ x_3 = -2,\ x_4 = 1.$$

2. Знайти многочлен найменшого степеня з дійсними коефіцієнтами і старшим коефіцієнтом, що дорівнює 5, якщо цей многочлен має потрійний корінь $1 - i$ і простий корінь 2.

Розв'язання. Оскільки шуканий многочлен $f(x)$ має потрійний корінь $1 + i$, то його розклад на незвідні множники над полем **C** має вигляд: $f(x) = 5(x - 1 + i)^3 (x - 1 - i)^3 (x - 2)$.

Звідси

$$f(x) = 5(x^2 - 2x + 2)^3 (x - 2).$$

Задачі

32.1. Розв'язати такі рівняння:

а) $x^4 + x^3 - x^2 - 10x - 12 = 0$, якщо $x_1 = -1 + i\sqrt{3}$;
б) $x^4 - x^3 + x^2 + 4x + 10 = 0$, якщо $x_1 = -1 + i$;
в) $x^4 - x^3 - 11x^2 + 31x - 20 = 0$, якщо $x_1 = 2 + i$;
г) $x^4 - 10x^3 + 36x^2 - 58x + 35 = 0$, якщо $x_1 = 2 - i$.

32.2. Число $-3 + i$ є коренем рівняння з дійсними коефіцієнтами $x^3 + x^2 + ax + b = 0$. Знайти числа a і b та два інших корені рівняння.

32.3. Довести, що коли зведений многочлен з дійсними коефіцієнтами має тільки уявні корені, то його можна подати у вигляді суми квадратів двох многочленів з дійсними коефіцієнтами.

32.4. Довести, що многочлен

$$f(x) = a_n x^n + \dots + a_1 x + a_0$$

з дійсними коефіцієнтами має суто уявні корені тоді і тільки тоді, коли многочлени

$$g_1(y) = a_0 - a_2 y^2 + a_4 y^4 - \dots$$

і

$$g_2(y) = a_1 - a_3 y^2 + a_5 y^4 - \dots$$

мають спільний дійсний корінь.

32.5. Чи мають суто уявні корені такі многочлени з дійсними коефіцієнтами:

а) $f(x) = x^4 - 4x^3 + 3x^2 - 8x + 2$;
б) $f(x) = x^4 + 2x^3 + x^2 + 11x + 3$;
в) $f(x) = x^4 + x^3 - 4x^2 + 3x - 21$;
г) $f(x) = x^5 + 3x^3 - x^2 + 4x + 4$?

32.6. Многочлен $f(x) = x^4 - 2x^3 + 6x^2 - 18x + a$ має суто уявний корінь. Знайти дійсне число a і всі корені цього многочлена.

32.7. Зведений многочлен четвертого степеня з дійсними коефіцієнтами має всі уявні корені. Довести, що цей многочлен можна подати у вигляді суми квадратів зведеного квадратного тричлена і многочлена першого степеня з дійсними коефіцієнтами.

32.8. Довести, що многочлен

$$f(x) = x^4 + 2x^3 + 4x^2 + 3x + 3$$

не має дійсних коренів.

32.9. Довести, що при дійсних a, b і c рівняння

$$x^8 + a^2 x^6 + b^2 x^4 + c^2 x^2 = 0$$

не має дійсних коренів, відмінних від нуля.

32.10. Розкласти наступні многочлени на незвідні над полем **R** множники:

а) $f(x) = x^4 + 4x^3 + 2x^2 + 20x + 25$;
б) $f(x) = x^4 + 2x^3 + 4x^2 + 3x + 1$;
в) $f(x) = x^4 + x^3 + x^2 + x + 1$;
г) $f(x) = x^4 - 2x^3 + x^2 + 3$;
д) $f(x) = x^6 + x^5 + x^4 + 2x^3 + x^2 + x + 1$.

32.11. Чи мають дійсні корені такі многочлени:

а) $f(x) = 2x^6 + x^4 + x^2 + 1$,
б) $f(x) = 4x^5 + 2x^4 + 3x^2 + 1$?

32.12. Чи має многочлен $f(x) = 2x^3 - 3x^2 + 4x - 1$ корінь з проміжку $[4, 10]$?

32.13. Довести, що многочлен

$$f(x) = 6x^5 - 4x^3 + 2x^2 + 3x - 1$$

при всіх $x \geqslant 2$ набуває тільки додатних значень.

§ 33. Рівняння третього і четвертого степенів

Література

[2] — § 30, с. 337—348;
[3] — гл. 16, § 3, с. 515—521;
[5] — гл. VIII, § 2, с. 284—291;
[6] — § 38, с. 233—240.

ТЕОРЕТИЧНІ ВІДОМОСТІ

Нехай $x^3+a_2x^2+a_1x+a_0=0$ — рівняння третього степеня з комплексними коефіцієнтами. За допомогою підстановки $x=y-\frac{a_2}{3}$ зведемо його до виду

$$x^3+px+q=0. \tag{1}$$

Число $D=\frac{q^2}{4}+\frac{p^3}{27}$ називають **дискримінантом рівняння** (1). Корені цього рівняння знаходять за формулою

$$x=\sqrt[3]{-\frac{q}{2}+\sqrt{D}}+\sqrt[3]{-\frac{q}{2}-\sqrt{D}},$$

яка називається **формулою Кардано.**

Якщо $u_1=\sqrt[3]{-\frac{q}{2}+\sqrt{D}}$ і $v_1=\sqrt[3]{-\frac{q}{2}-\sqrt{D}}$ є тими значеннями кубічних коренів, при яких $x_1=u_1+v_1$ є коренем рівняння (1), то решту коренів цього рівняння обчислюють так:

$$x_2=-\frac{1}{2}(u_1+v_1)+\frac{i\sqrt{3}}{2}(u_1-v_1),$$

$$x_3=-\frac{1}{2}(u_1+v_1)-\frac{i\sqrt{3}}{2}(u_1-v_1).$$

Числа u_1 і v_1 знаходять з умови $u_1v_1=-\frac{p}{3}$.

Якщо коефіцієнти p і q рівняння (1) є дійсними числами, то:

а) при $D>0$ рівняння має один дійсний і два комплексних спряжених корені;

б) при $D=0$ рівняння має три дійсних корені, два з яких дорівнюють один одному;

в) при $D<0$ рівняння має три дійсних різних корені.

Рівняння четвертого степеня

$$x^4+a_3x^3+a_2x^2+a_1x+a_0=0 \tag{2}$$

в результаті введення допоміжної змінної t запишемо у вигляді

$$\left(x^2+\frac{a_3x}{2}+\frac{t}{2}\right)^2=\left(\frac{a_3^2}{4}-a_2+t\right)x^2+\left(\frac{a_3t}{2}-a_1\right)x+\frac{t^2}{4}-a_0.$$

Значення змінної t беруть таке, щоб у правій частині рівності утворювався квадрат деякого двочлена $ax+b$. Для цього розв'язують допоміжне кубічне рівняння

$$t^3-a_2t^2+(a_3a_1-4a_0)t-(a_3^2a_0-4a_2a_0+a_0^2)=0, \tag{3}$$

яке називають **кубічною резольвентою рівняння** (2).

Якщо t_0 — один з коренів рівняння (3), то рівняння (2) рівносильне сукупності рівнянь:

$$\left[\begin{array}{l} x^2+\frac{a_3}{2}x+\frac{t_0}{2}=ax+b, \\ x^2+\frac{a_3}{2}x+\frac{t_0}{2}=-(ax+b). \end{array}\right.$$

ПРИКЛАДИ РОЗВ'ЯЗУВАННЯ ЗАДАЧ

1. Розв'язати рівняння $ix^3-3ix+2=0$.

Розв'язання. Зведемо це рівняння до виду (1). Для цього помножимо обидві його частини на $-i$. Матимемо

$$x^3+3x-2i=0.$$

Тут $p=3$, $q=-2i$ і $D=0$. Тоді $\sqrt[3]{-\frac{q}{2}+\sqrt{D}}=\sqrt[3]{i}$. Нехай $u_1=-i$. Оскільки $u_1v_1=-1$, то $v_1=-i$. Звідси $x_1=-2i$, $x_2=i$, $x_3=i$.

2. При якому значенні дійсного числа a рівняння

$$y^3+3y^2+3\left(1+\sqrt[3]{a}\right)y+2a+3\sqrt[3]{a}+1=0$$

має три дійсних різних корені?

Розв'язання. Введемо заміну $y=x-1$. Матимемо

$$(x-1)^3+3(x-1)^2+3\left(1+\sqrt[3]{a}\right)(x-1)+2a+3\sqrt[3]{a}+1=0,$$

$$x^3+3\sqrt[3]{a}x+2a=0.$$

Дискримінант цього рівняння $D=a^2+a$. Розв'яжемо нерівність $D<0$, знаходимо $a^2+a<0$ і $-1<a<0$.

Отже, задане рівняння має 3 дійсних і різних корені тоді, коли $-1<a<0$.

3. Розв'язати рівняння $x^4-2x^3+6x^2-2x+5=0$.

Розв'язання. Застосуємо метод Феррарі. Залишимо в лівій частині рівняння перші два доданки, а решту перенесемо в праву частину:

$$x^4-2x^3=-6x^2+2x-5.$$

У лівій частині виділимо повний квадрат, додавши до обох частин вираз x^2. Матимемо

$$(x^2-x)^2=-5x^2+2x-5.$$

Доповнимо ліву частину цього рівняння до повного квадрата, ввівши нову змінну t:

$$(x^2-x)^2+2t(x^2-x)+t^2=2t(x^2-x)-5x^2+2x+t^2-5,$$

$$(x^2-x+t)^2=(2t-5)x^2+(2-2t)x+t^2-5.$$

Виберемо t так, щоб у правій частині рівняння був теж повний квадрат. При цьому дискримінант квадратного тричлена відносно змінної x має дорівнювати нулю:

$$(1-t)^2-(t^2-5)(2t-5)=0,$$

$$1-2t+t^2-2t^3+5t^2+10t-25=0,$$

$$t^3-3t^2-4t+12=0.$$

Знайдемо один з коренів останнього рівняння. У цьому разі можна не застосовувати формулу Кардано. Тоді

$$t^2(t-3)-4(t-3)=0,$$

$$(t-3)(t^2-4)=0.$$

Одним з коренів останнього рівняння є $t_1 = 3$. Отже, маємо

$$(x^2 - x + 3)^2 = x^2 - 4x + 4,$$
$$(x^2 - x + 3)^2 - (x - 2)^2 = 0,$$
$$(x^2 - 2x + 5)(x^2 + 1) = 0.$$

Останнє рівняння рівносильне сукупності рівнянь:

$$\begin{cases} x^2 - 2x + 5 = 0, \\ x^2 + 1 = 0. \end{cases}$$

Розв'язуючи її, знаходимо

$$x_{1,2} = \pm i,\ x_{3,4} = 1 \pm 2i.$$

Зауваження. Задане рівняння можна розв'язати за допомогою заміни $x = y + \frac{1}{2}$. Тоді здобуте рівняння не міститиме змінну y в третьому степені. Тому в лівій частині рівняння залишають тільки y^4 і знову вводять змінну t.

Задачі

33.1. Обчислити дискримінант таких рівнянь:

а) $x^3 - 9x - 4 = 0$; г) $x^3 + x^2 - x - \frac{2}{27} = 0$;

б) $x^3 - 4x + 1 = 0$; д) $x^3 - 6ix + 4(1 - i) = 0$;

в) $x^3 - ix = 0$; е) $x^3 - 3ix^2 + 4 = 0$.

33.2. Розв'язати такі рівняння:

а) $x^3 - 3x + 2 = 0$; д) $x^3 - 6x^2 + 4x - 1 = 0$;

б) $x^3 + 3x - 2i = 0$; е) $x^3 - 2x^2 + x - 3 = 0$;

в) $x^3 - 24x - 56 = 0$; є) $x^3 + 6ix + 4 + 4i = 0$;

г) $2x^3 - 3x^2 + 1 = 0$; ж) $x^3 + 3\sqrt[3]{6}x + 7i = 0$.

33.3. При яких дійсних значеннях a рівняння $ax^3 - 3x + 2a = 0$ має один дійсний і два комплексних корені?

33.4. При яких дійсних значеннях a рівняння $ax^3 + (a - 1)x + a - 1 = 0$ має кратний корінь? Знайти його.

33.5. Довести, що корені рівняння $x^3 + 3ax^2 - 3a^3 = 0$ є дійсними при будь-якому дійсному значенні числа a.

33.6. Які корені залежно від значення числа a має рівняння з дійсними коефіцієнтами $x^3 - 3x^2 - ax + 2a^2 - 3a - 4 = 0$?

33.7. Довести, що при $a \geqslant 0$ і довільному дійсному b рівняння $x^3 + ax + b = 0$ має тільки один дійсний корінь.

33.8. Довести, що при довільному дійсному c рівняння $x^3 - x^2 + x + c = 0$ має тільки один дійсний корінь.

33.9. Довести, що будь-яке кубічне рівняння з дійсними коефіцієнтами і від'ємним дискримінантом можна за допомогою заміни $x = my + n$ звести до вигляду $ay^3 - 3by^2 - 3ay + b = 0$, де a, b — дійсні числа.

33.10. Звести до вигляду $ay^3 - 3by^2 - 3ay + b = 0$, де a, b — дійсні числа, такі рівняння:

а) $x^3 + 6x^2 + 6x - 8 = 0$;

б) $x^3 - 3x^2 - 4x + 1 = 0$;

в) $x^3 + 4x^2 + x - \frac{16}{3} = 0$.

33.11. Довести, що кубічне рівняння з дійсними коефіцієнтами $ay^3 - 3by^2 - 3ay + b = 0$ має корені $y_1 = \operatorname{tg}\frac{\varphi}{3}$, $y_2 = \operatorname{tg}\frac{\varphi + 2\pi}{3}$, $y_3 = \operatorname{tg}\frac{\varphi + 4\pi}{3}$, де кут φ визначається з умови

$$\sin\varphi = \frac{b}{\sqrt{a^2 + b^2}},$$

$$\cos\varphi = \frac{a}{\sqrt{a^2 + b^2}}.$$

33.12. Застосовуючи формули із задачі 33.11, розв'язати такі рівняння:

а) $y^3 - 3y^2 - 3y + 1 = 0$;

б) $y^3 - 3\sqrt{3}y^2 - 3y + \sqrt{3} = 0$;

в) $y^3 + 3y^2 - 3y - 1 = 0$;

г) $y^3 + 6y^2 - 3y - 2 = 0$.

33.13. Знайти корені рівняння $ax^3 + bx^2 + cx + d = 0$, якщо його коефіцієнти задовольняють умову $ad = bc$.

33.14. Коефіцієнти членів кубічного рівняння, розміщених у порядку спадання степенів невідомого, утворюють геометричну прогресію. Довести, що корені цього рівняння також утворюють геометричну прогресію із знаменником t.

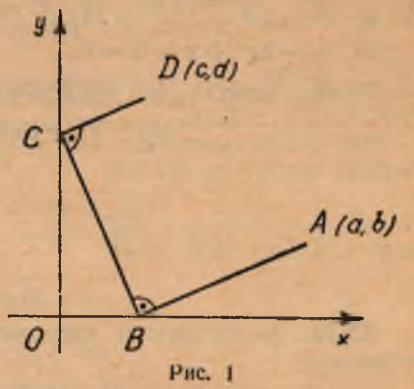


Рис. 1

33.15. Точки A, B, C, D побудовано так, що $\angle ABC = \angle BCD = \frac{\pi}{2}$ (рис. 1). Координати точок A і D є коефіцієнтами кубічного рівняння з дійсними коефіцієнтами

$$ax^3 + bx^2 + cx + d = 0.$$

Довести, що число $x_0 = \frac{x_B - b}{a}$, де x_B — абсциса точки B, є дійсним коренем цього кубічного рівняння.

33.16. За умовою попередньої задачі описати геометрично області, в яких знаходяться точки A і D, якщо кубічне рівняння з дійсними коефіцієнтами $ax^3 + bx^2 + cx + d = 0$, має: а) три дійсних різних корені; б) два дійсних різних корені; в) тільки один дійсний корінь.

33.17. Розв'язати графічно такі рівняння:

а) $4x^3 + 11x^2 + 14x + 6 = 0$;

б) $4x^3 + 6x^2 + 2x - 3 = 0$;

в) $2x^3 + 5x^2 - x - 2 = 0$;

г) $2x^3 + 4x^2 - 5x + 3 = 0$;

д) $2x^3 + 5x^2 - x - 1 = 0$.

33.18. Розв'язати такі рівняння четвертого степеня:

а) $x^4 + 3x^2 + 2x + 3 = 0$;

б) $x^4 + x^3 + 6x^2 + 2x + 8 = 0$;

в) $x^4 - 6x^3 + 6x^2 + 27x - 56 = 0$;
г) $9x^4 + 6x^3 - 3x^2 + 4x - 1 = 0$;
д) $4x^4 - 4x^3 - 6x^2 + 2x + 1 = 0$.

33.19. Довести, що многочлен з дійсними коефіцієнтами

$$f(x) = x^4 + a_3x^3 + a_2x^2 + a_1x + a_0$$

можна подати у вигляді $f(x) = (x^2 + px + q)^2 + r^2$ тоді і тільки тоді, коли

$$a_3^3 - 4a_2a_3 + 8a_1 = 0.$$

33.20. Застосовуючи твердження задачі 33.19, розв'язати такі рівняння:
а) $x^4 + 4x^3 + 11x^2 + 14x + 10 = 0$;
б) $x^4 - 2x^3 + x - 2 = 0$.

33.21. Довести, що многочлен з дійсними коефіцієнтами

$$f(x) = x^4 + a_3x^3 + a_2x^2 + a_1x + a_0$$

можна подати у вигляді

$$f(x) = (x^2 + px + q)^2 + (rx)^2$$

тоді і тільки тоді, коли

$$a_1^2 = a_0a_3^2.$$

33.22. Застосовуючи твердження задачі 33.21, розв'язати такі рівняння:
а) $x^4 - 2\sqrt{2}x^3 + 5x^2 - 4\sqrt{2}x + 4 = 0$;
б) $x^4 + 6x^3 + 9x^2 + 12x + 4 = 0$.

§ 34. Відокремлення дійсних коренів многочлена

Література

[1] — § 30, с. 323—336;
[2] — § 31, с. 348—363;
[3] — гл. 16, § 4, с. 521—525;
[6] — § 39—41, с. 241—259;
[7] — § 15, 16, с. 86—97;
[8] — гл. 6, § 4, с. 283—290.

ТЕОРЕТИЧНІ ВІДОМОСТІ

Нехай $f(z) = a_nz^n + a_{n-1}z^{n-1} + \ldots + a_1z + a_0$ — многочлен з комплексними коефіцієнтами, $A = \max\{|a_{n-1}|, \ldots, |a_1|, |a_0|\}$ і $N_0 = 1 + \frac{A}{|a_n|}$. Тоді всі корені многочлена $f(z)$ лежатимуть всередині круга з центром у початку координат і радіусом N_0. Якщо многочлен $f(z)$ має дійсні корені, то вони знаходяться в інтервалі $]-N_0;\ N_0[$.

Одним з методів знаходження верхньої межі додатних коренів многочлена з дійсними коефіцієнтами є метод **Ньютона**. В основі цього методу лежить той факт, що коли при $x = M$ многочлен $f(x)$ має додатне значення, а всі його похідні — невід'ємні, то число M є верхньою межею додатних коренів многочлена.

Якщо N_0, N_1, N_2 і N_3 — верхні межі відповідно додатних коренів многочленів з дійсними коефіцієнтами $f(x)$, $y^nf\left(\frac{1}{y}\right)$, $f(-y)$ і $y^nf\left(-\frac{1}{y}\right)$, то додатні корені многочлена $f(x)$ знаходяться в проміжку $\left]\frac{1}{N_1};\ N_0\right[$, а від'ємні — в проміжку $\left]-N_2;\ -\frac{1}{N_3}\right[$.

Нехай $c_1, c_2, \ldots, c_m$ — деяка впорядкована послідовність дійсних чисел. Кількість пар сусідніх чисел цієї послідовності, які мають протилежні знаки, називають **кількістю змін знаків даної послідовності**.

Правило Декарта: *число додатних коренів многочлена з дійсними коефіцієнтами $f(x) = a_nx^n + a_{n-1}x^{n-1} + \ldots + a_1x + a_0$ дорівнює або на парне число менше кількості змін знаків у послідовності його коефіцієнтів.* Це правило за допомогою заміни $x = -y$ можна застосувати для оцінки кількості від'ємних коренів многочлена $f(x)$.

Задача відокремлення дійсних коренів многочлена $f(x)$ полягає в знаходженні тих інтервалів, у кожному з яких лежить тільки один корінь. Відокремити корені многочлена $f(x)$, який не має кратних коренів, можна **методом Штурма**. При цьому для многочлена $f(x)$ будують насамперед **ряд Штурма:**

$$f(x),\ f'(x),\ F_1(x),\ F_2(x),\ \ldots,\ F_{m-1}(x),\ F_m.$$

Щоб знайти многочлени $F_i(x)$, $1 \leqslant i \leqslant m$, застосовують алгоритм, аналогічний алгоритму Евкліда:

$$f(x) = f'(x)\,\Phi_1(x) - F_1(x),$$
$$f'(x) = F_1(x)\,\Phi_2(x) - F_2(x),$$
$$F_1(x) = F_2(x)\,\Phi_3(x) - F_3(x),$$
$$\ldots\ldots\ldots\ldots\ldots$$
$$F_{m-2}(x) = F_{m-1}(x)\,\Phi_m(x) - F_m,$$
$$F_{m-1}(x) = F_m\,\Phi_{m+1}(x).$$

Відмінність цього алгоритму від алгоритму Евкліда полягає тільки в тому, що всі остачі $r_k(x)$ беруть з протилежними знаками, тобто $F_k(x) = -r_k(x)$.

Після цього застосовують **теорему Штурма:**

Якщо a і b — довільні дійсні числа, які не є коренями многочлена $f(x)$, то число p дійсних коренів многочлена $f(x)$ в інтервалі $]a;\ b[$ дорівнює $p = s(a) - s(b)$, де $s(a)$ і $s(b)$ — кількість змін знаків у ряді Штурма відповідно при $x = a$ і $x = b$.

ПРИКЛАДИ РОЗВ'ЯЗУВАННЯ ЗАДАЧ

1. Знайти кільце, в якому знаходяться всі корені рівняння

$$5x^7 + 3x^3 + 10x^2 - 2 = 0.$$

Розв'язання. Маємо $A = \max\{3,\ 10,\ 2\} = 10$ і $|a_n| = 5$. Тому $N_0 = 1 + \frac{10}{5} = 3$. Це означає, що всі корені x_i, $1 \leqslant i \leqslant 7$, заданого рівняння задовольняють нерівність $|x_i| < 3$.

Введемо заміну $x = \frac{1}{y}$. Маємо

$$-2y^7 + 10y^5 + 3y^4 + 5 = 0.$$

Тут $A = 10$, $|a_n| = 2$ і $N_0 = 1 + \frac{10}{2} = 6$. Тому корені y_i, $1 \leqslant i \leqslant 7$, задовольняють нерівність $|y_i| < 6$. Виконуючи обернену заміну $y = \frac{1}{x}$, дістаємо $\frac{1}{|x_i|} < 6$, тобто $|x_i| > \frac{1}{6}$.

Отже, всі корені заданого рівняння лежать всередині кільця з центром у початку координат, радіусом зовнішнього кола 3, а внутрішнього $\frac{1}{6}$ (рис. 2).

2. Знайти верхню межу від'ємних коренів многочлена

$$f(x) = x^5 - 8x^3 - 5x^2 + 6x - 3.$$

Розв'язання. Введемо заміну $x = -\frac{1}{y}$. Тоді

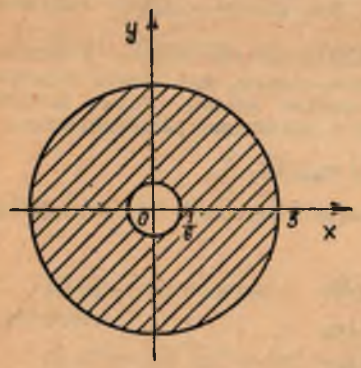


Рис. 2

$$f\left(-\frac{1}{y}\right) = -\frac{1}{y^5} + \frac{8}{y^3} - \frac{5}{y^2} - \frac{6}{y} - 3.$$

Розглянемо многочлен

$$g(y) = -y^5 f\left(-\frac{1}{y}\right) =$$

$$= 3y^5 + 6y^4 + 5y^3 - 8y^2 + 1,$$

який має ті самі корені, що й многочлен $f\left(-\frac{1}{y}\right)$.

Щоб знайти верхню межу його додатних коренів, застосуємо метод Ньютона. Знайдемо всі похідні многочлена $g(y)$:

$$g(y) = 3y^5 + 6y^4 + 5y^3 - 8y^2 + 1,$$
$$g^{I}(y) = 15y^4 + 24y^3 + 15y^2 - 16y,$$
$$g^{II}(y) = 60y^3 + 72y^2 + 30y - 16,$$
$$g^{III}(y) = 180y^2 + 144y + 30,$$
$$g^{IV}(y) = 360y + 144,$$
$$g^{V}(y) = 360.$$

Неважко перевірити, що число 1 є верхньою межею додатних коренів многочлена $g(y)$. Тоді число -1 є верхньою межею від'ємних коренів заданого многочлена.

3. Відокремити дійсні корені многочлена

$$f(x) = x^4 - 2x^2 + 4x - 1.$$

Розв'язання. Для цього многочлена $A = 4$, $|a_n| = 1$, $N_0 = 5$. Тому його дійсні корені знаходяться в інтервалі $]-5; 5[$.

Складемо ряд Штурма (многочлени ряду знаходитимемо з точністю до сталого множника).

$$f'(x) = 4x^3 - 4x + 4 = 4(x^3 - x + 1);$$

$$\begin{array}{r|l} x^4 - 2x^2 + 4x - 1 & x^3 - x + 1 \\ \hline -\,x^4 - x^2 + x & x \\ \hline -x^2 + 3x - 1 & \end{array} \quad \Longrightarrow \quad F_1(x) = x^2 - 3x + 1;$$

$$\begin{array}{r|l} x^3 - x + 1 & x^2 - 3x + 1 \\ \hline -\,x^3 - 3x^2 + x & x + 3 \\ \hline 3x^2 - 2x + 1 & \\ -\,3x^2 - 9x + 3 & \\ \hline 7x - 2 & \end{array} \quad \Longrightarrow \quad F_2(x) = -7x + 2;$$

$$\begin{array}{r|l} x^2 - 3x + 1 & -7x + 2 \\ \hline -\,7x^2 - 21x + 7 & -x + \frac{19}{7} \\ \hline -\,7x^2 - 2x & \\ \hline -19x + 7 & \\ -19x + \frac{38}{7} & \\ \hline \frac{11}{7} & \end{array} \quad \Longrightarrow \quad F_3 = -1.$$

Таким чином, ряд Штурма утворюють многочлени:

$$x^4 - 2x^2 + 4x - 1,\ x^3 - x + 1,\ x^2 - 3x + 1,\ -7x + 2,\ -1.$$

Складемо таблицю (табл. 44).

Таблиця 44

x_0 \ Знак	$f(x_0)$	$f'(x_0)$	$F_1(x_0)$	$F_2(x_0)$	F_3	Кількість змін знаків
-5	$+$	$-$	$+$	$+$	$-$	3
5	$+$	$+$	$-$	$-$	$-$	1
0	$-$	$+$	$+$	$+$	$-$	2

Отже, заданий многочлен має два дійсних корені, один з яких від'ємний і знаходиться в інтервалі $]-5; 0[$, а другий — додатний і знаходиться в інтервалі $]0; 5[$.

Задачі

34.1. Знайти на комплексній площині кільце, в якому знаходяться всі комплексні корені таких рівнянь:

а) $x^{1982} - 4x^{24} + 4x^3 - 7x^2 + 1 = 0$;
б) $x^6 - x^5 + x^4 - x^3 + x + 7 = 0$;
в) $x^{12} + x^{11} - 5x^6 + 6x^2 - 6 = 0$;
г) $2x^5 + 6x^4 + x^3 - x^2 - 54x + 27 = 0$.

34.2. Знайти методом Ньютона верхню межу додатних коренів таких многочленів:

а) $f(x) = 2x^3 - 3x^2 + 5$;
б) $f(x) = x^4 - 8x + 1$;
в) $f(x) = (x-2)^6 + (x-1)^3$;
г) $f(x) = -2x^4 + 6x^3 - 7x + 3$.

34.3. Знайти методом Ньютона нижню межу додатних коренів таких многочленів:

а) $f(x) = 5x^4 - 3x^3 + x^2 + 1$;
б) $f(x) = 4x^4 - 12x^2 + 8x - 1$;
в) $f(x) = x^5 + 6x^4 - 11x^3 - 11x^2 + 6x + 1$.

34.4. Знайти число змін знаків у коефіцієнтах таких многочленів:

а) $f(x) = 5x^7 - 2x^6 + 3x^5 - x^4 + 6x^3 + 2x^2 - x + 1$;
б) $f(x) = 12x^4 - x^3 - 3x^2 + 2x + 4$;
в) $f(x) = 19x^5 - 2x^3 + x - 1$;
г) $f(x) = (x-1)^{100}$.

34.5. Оцінити за правилом Декарта число додатних і від'ємних коренів таких многочленів:

а) $f(x) = x^4 - 2x^3 - 7x^2 - 8x + 1$;
б) $f(x) = 2x^3 - 3x^2 + x - 1$;
в) $f(x) = x^5 - 5x^3 - 10x^2 + 2$;
г) $f(x) = x^6 + x^5 - 12x^4 - 13x^3 - 27x^2 - 14x - 14$,
д) $f(x) = x^3 - 12x - 4$.

34.6. Знайти межі доданих та від'ємних коренів таких многочленів

а) $f(x) = -3x^4 + 5x^3 + 9x^2 - x + 1$;
б) $f(x) = x^5 + 5x^3 - 7x + 2$;
в) $f(x) = 3x^4 - 12x^3 + 8x^2 + 2x + 4$;
г) $f(x) = -2x^7 + 3x^5 - x^3 + x - 1$;
д) $f(x) = x^3 - 12x - 4$.

34.7. Знайти число дійсних коренів многочленів:

а) $f(x) = x^4 - 2x^3 - 6x^2 + 4x + 4$ на проміжку $[2; 4]$;
б) $f(x) = x^4 + 3x^3 - 4x - 1$ на проміжку $[0; 2]$;
в) $f(x) = x^4 - 2x^3 - 4$ на проміжку $[-3; 5]$;
г) $f(x) = x^7 + 5x^2 - 10$ на проміжку $[1; 3]$.

34.8. Відокремити дійсні корені таких многочленів:

а) $f(x) = 2x^3 - 5x - 1$;
б) $f(x) = -8x^3 + 16x - 2$;
в) $f(x) = x^3 + 6x - 2$;
г) $f(x) = x^4 - 4x^3 - 12x + 9$;
д) $f(x) = 2x^5 - 10x^3 + 10x^2 - 2$;
е) $f(x) = x^4 - 4x + 1$;
є) $f(x) = x^4 - 2x^3 + 3x^2 - 2x + 2$.

Розділ VII. МНОГОЧЛЕНИ НАД ПОЛЕМ РАЦІОНАЛЬНИХ ЧИСЕЛ І АЛГЕБРАЇЧНІ ЧИСЛА

§ 35. Цілі і раціональні корені многочлена з цілими коефіцієнтами. Критерій незвідності Ейзенштейна

Література

[1] — § 31, с. 337—343;
[2] — § 32, с. 363—369;
[3] — гл. 17, § 1, с. 526—528;
[5] — гл. IX, § 6, с. 350—355;
[6] — § 56, 57, с. 350—358;
[7] — § 17, 18, с. 97—104.

ТЕОРЕТИЧНІ ВІДОМОСТІ

Нехай $f(x) = a_n x^n + a_{n-1}x^{n-1} + \ldots + a_1 x + a_0$ — многочлен з цілими коефіцієнтами.

Якщо нескоротний дріб $\frac{p}{q}$ є коренем многочлена $f(x)$, то p є дільником вільного члена a_0, а q — дільником старшого коефіцієнта a_n цього многочлена.

Якщо $a_n = 1$, то всі раціональні корені многочлена $f(x)$ є цілими числами. Оскільки многочлени $f(x)$ і $a_n^{n-1} f(x)$ мають однакові корені, то знаходження раціональних коренів многочлена $f(x)$ можна за допомогою заміни $y = xa_n$ звести до відшукання цілих коренів многочлена

$$a_n^{n-1} f(x) = g(y) = y^n + a_{n-1}y^{n-1} + a_{n-2}a_n y^{n-2} + \ldots + a_1 a_n^{n-2} y + a_0 a_n^{n-1}.$$

Існують інші необхідні умови для того, щоб раціональне число було коренем многочлена з цілими коефіцієнтами. Зокрема, щоб нескоротний дріб $\frac{p}{q}$ був раціональним коренем многочлена $f(x)$, необхідно, щоб при довільному цілому k число $f(k)$ ділилося на $p - qk$, де $p - qk \neq 0$. Така умова на практиці найчастіше використовується для $k = \pm 1$, при цьому числа $\frac{f(1)}{p-q}$ і $\frac{f(-1)}{p+q}$ мають бути цілими.

Многочлен $f(x)$ з цілими коефіцієнтами є звідним у полі Q раціональних чисел тоді і тільки тоді, коли існують многочлени $f_1(x)$ і $f_2(x)$ ненульового степеня з цілими коефіцієнтами такі, що $f(x) = f_1(x) f_2(x)$, тобто коли многочлен $f(x)$ є звідним у кільці Z.

Критерій Ейзенштейна незвідності многочлена з цілими коефіцієнтами:
Якщо коефіцієнти $a_0, a_1, \ldots, a_{n-1}$ многочлена $f(x)$ в кільця $Z[x]$ діляться на деяке просте число p, причому a_0 не ділиться на p^2, а старший коефіцієнт a_n не ділиться на p, то многочлен $f(x)$ незвідний у полі раціональних чисел.

Отже, у кільці многочленів над полем раціональних чисел є многочлени довільного степеня, які незвідні у полі Q.

ПРИКЛАДИ РОЗВ'ЯЗУВАННЯ ЗАДАЧ

1. Розв'язати рівняння

$$24x^5 + 10x^4 - x^3 - 19x^2 - 5x + 6 = 0.$$

Розв'язання. Знайдемо спочатку раціональні корені цього рівняння (якщо вони є). Раціональними коренями тут можуть бути такі числа:

$$\pm 1;\ \pm 2;\ \pm 3;\ \pm 6;\ \pm\tfrac{1}{2};\ \pm\tfrac{3}{2};\ \pm\tfrac{1}{3};\ \pm\tfrac{2}{3};\ \pm\tfrac{1}{4};\ \pm\tfrac{3}{4};\ \pm\tfrac{1}{6};\ \pm\tfrac{1}{8};\ \pm\tfrac{3}{8};\ \pm\tfrac{1}{12};\ \pm\tfrac{1}{24}. \quad (1)$$

Знайдемо межі дійсних коренів заданого рівняння. Оскільки $A = 19$ і $a_n = 24$, то $N_0 = 1 + \frac{19}{24} = 1\frac{19}{24}$. Отже, всі дійсні корені знаходяться в інтервалі $\left]-1\frac{19}{24};\ 1\frac{19}{24}\right[$. Серед чисел ряду (1) у цей інтервал входять такі числа:

$$\pm 1;\ \pm\tfrac{1}{2};\ \pm\tfrac{3}{2};\ \pm\tfrac{1}{3};\ \pm\tfrac{2}{3};\ \pm\tfrac{1}{4};\ \pm\tfrac{3}{4};\ \pm\tfrac{1}{6};\ \pm\tfrac{1}{8};\ \pm\tfrac{3}{8};\ \pm\tfrac{1}{12};\ \pm\tfrac{1}{24}. \quad (2)$$

Для заданого рівняння маємо: $f(1) = 15$ і $f(-1) = -21$. Поставимо умову, щоб числа $\frac{15}{p-q}$ і $-\frac{21}{p+q}$ були цілими. Тоді залишаться числа

$$\pm\tfrac{1}{2};\ -\tfrac{3}{2};\ -\tfrac{2}{3};\ -\tfrac{1}{4};\ \tfrac{3}{4};\ \tfrac{1}{6}. \quad (3)$$

Оскільки «кандидатів» на корені ще багато, то знаходимо $f(-2) = -660$ і перевіряємо, для якого з чисел ряду (3) дріб $\frac{-660}{p+2q}$ є цілим числом. Цю умову задовольняють тільки числа

$$\pm\frac{1}{2};\ -\frac{3}{2};\ -\frac{2}{3};\ \frac{3}{4}.$$

Застосуємо схему Горнера для перевірки того, яке з останніх чисел є коренем заданого рівняння (табл. 45).

Таблиця 45

	24	10	−1	−19	−5	6
$\frac{1}{2}$	24	22	10	−14	−12	0
$\frac{1}{2}$	24	34	27	$-\frac{1}{2}$	$-12\frac{1}{4}$	
$-\frac{1}{2}$	24	10	5	$-16\frac{1}{2}$	$-3\frac{1}{4}$	
$-\frac{3}{2}$	24	−14	31	$-59\frac{1}{2}$	$77\frac{1}{4}$	
$-\frac{2}{3}$	24	6	6	−18	0	
$-\frac{2}{3}$	24	−10	$\frac{38}{3}$	$-26\frac{4}{9}$		
$\frac{3}{4}$	24	24	24	0		

У схемі виділено коефіцієнти повних часток. Отже, задане рівняння має три раціональних корені: $-\frac{2}{3};\ \frac{1}{2}$ і $\frac{3}{4}$. Решту коренів рівняння знайдемо, прирівнюючи останню частку до нуля. Матимемо

$$24x^2 + 24x + 24 = 0,$$
$$x^2 + x + 1 = 0.$$

У цьому рівнянні комплексні корені $\frac{-1 \pm \sqrt{3}i}{2}$. Тому задане рівняння має п'ять різних коренів:

$$-\frac{2}{3},\ \frac{1}{2},\ \frac{3}{4},\ \frac{-1-i\sqrt{3}}{2},\ \frac{-1+i\sqrt{3}}{2}.$$

2. Розкласти на незвідні у полі Q множники многочлен

$$f(x) = x^6 - x^5 + 2x^3 - 2x^2 + 6x - 6.$$

Розв'язання. Згрупуємо в цьому многочлені по два члени, що стоять поряд, і винесемо спільні множники за дужки. Тоді

$$f(x) = x^5(x-1) + 2x^2(x-1) + 6(x-1) = (x-1)(x^5 + 2x^2 + 6).$$

Многочлен $g(x) = x^5 + 2x^2 + 6$ є незвідним у полі Q за критерієм Ейзенштейна (простим дільником є число 2). Отже, дістали шуканий розклад.

3. Довести, що многочлен

$$f(x) = x^6 - 2x^3 + 3x^2 - 6x + 7$$

є незвідним у полі Q.

Розв'язання. До заданого многочлена безпосередньо застосувати критерій Ейзенштейна не можна. Зробимо заміну $x = y + 1$. Маємо

$f(y+1) = g(y) = (y+1)^6 - 2(y+1)^3 + 3(y+1)^2 - 6(y+1) + 7 = y^6 + 6y^5 + 15y^4 + 20y^3 + 15y^2 + 6y + 1 - 2y^3 - 6y^2 - 6y - 2 + 3y^2 + 6y + 3 - 6y - 6 + 7 = y^6 + 6y^5 + 15y^4 + 18y^3 + 12y^2 + 3.$

Усі коефіцієнти многочлена $g(y)$, крім старшого, діляться на 3, а вільний член не ділиться на 9. Це означає, що многочлен $g(y)$ є незвідним у полі Q. Отже, многочлен $f(x)$ також є незвідним у полі Q.

4. Чи є звідним у полі Q многочлен

$$f(x) = x^3 - 6x^2 + 12x - 4?$$

Розв'язання. Подамо заданий многочлен у вигляді $f(x) = (x-2)^3 + 4$. Зробимо заміну: $y = x - 2$. Тоді $f(y+2) = g(y) = y^3 + 4$. Оскільки кубічний многочлен $g(y)$ не має раціональних коренів, то він є незвідним у полі Q. Отже, многочлен $f(x)$ також незвідний у полі Q.

Задачі

35.1. Розв'язати такі рівняння:

а) $x^4 - 4x^3 - 13x^2 + 28x + 12 = 0$;
б) $x^3 - 2x^2 - 3x + 10 = 0$;
в) $x^4 - x^3 - 22x^2 + 16x + 96 = 0$;
г) $2x^3 - 5x^2 + 6x - 2 = 0$;
д) $12x^3 - x^2 + 2x - 1 = 0$;
е) $10x^3 - 3x^2 - 2x + 1 = 0$;
є) $2x^3 + 3x^2 + 6x - 4 = 0$;
ж) $x^4 + 4x^3 - 2x^2 - 12x + 9 = 0$;
з) $x^3 - (a+b+c)x^2 + (ab+ac+bc)x - abc = 0$;
к) $x^3 - (3a-1)x^2 + (2a^2 - 3a)x + 2a^2 = 0$;
л) $x^3 - 2x^2 - (a^2 - a - 1)x + (a^2 - a) = 0$;
м) $x^3 - (2a+1)x^2 + (a^2 + 2a - b^2)x + (b^2 - a^2) = 0$.

35.2. Знайти раціональні корені таких рівнянь:

а) $x^3 - x^2 - \frac{8}{x^3 - x^2} = 2$;
б) $2x^3 - 3x^2 + 4x - 5 = 0$;
в) $\frac{16}{x^3 + 3x^2 - x + 5} - \frac{5}{x^3 + 3x^2 - x + 2} = 1$;
г) $x^3 - (p^2 - p + 7)x - 3(p^2 - p - 2) = 0$, якщо $p = \sqrt[3]{2}$;
д) $(2x^2 + 3x - 1)^2 - 5x^2(2x^2 + 3x - 1) + 5x^4 - x = 0$.

35.3. Розкласти на незвідні у полі Q множники такі многочлени:

а) $f(x) = x^4 + x^3 - 6x^2 - 7x - 7$;
б) $f(x) = x^4 - x^3 - 6x^2 + 8x - 2$;
в) $f(x) = 6x^4 - 13x^3 + 12x^2 - 13x + 6$;
г) $f(x) = 9x^4 - 15x^3 + 28x^2 - 20x + 16$;
д) $f(x) = (x+3)^4 + (x+5)^4 - 16$;
е) $f(x) = (x+1)^6 - 9(x+1)^3 + 20$.

35.4. Довести, що незвідними у полі **Q** є такі многочлени:

а) $f(x) = x^3 - 3x^2 + 1$;

б) $f(x) = x^6 + 2$;

в) $f(x) = x^5 + 5x + 9$;

г) $f(x) = x^4 + x^3 + x^2 + x + 1$;

д) $f(x) = x^6 + x^5 + x^4 + x^3 + x^2 + x + 1$;

е) $f(x) = x^{p-1} + x^{p-2} + \ldots + x + 1$, де p — просте число.

35.5. Дослідити на звідність у полі **Q** такі многочлени:

а) $f(x) = x^4 + x^3 - 10x^2 + x + 1$;

б) $f(x) = (5 - x)^4 + (2 - x)^4 - 17$;

в) $f(x) = x^3 + x^2 - 1$;

г) $f(x) = x^4 + 2x + 3$.

35.6. Довести, що коли многочлен $f(x)$ можна розглядати як елемент кілець $Z[x]$ і $Z_m[x]$, залежно від інтерпретації його коефіцієнтів, і $f(x)$ є незвідним у кільці $Z_m[x]$, то він незвідний також у кільці $Z[x]$.

35.7. Довести незвідність у кільці $Z[x]$ таких многочленів:

а) $f(x) = x^5 + x^2 + 1$;

б) $f(x) = x^5 + x^4 + x^2 + x + 1$;

в) $f(x) = x^6 + x^4 + x^2 + x + 1$;

г) $f(x) = 5x^3 + x - 1$;

д) $f(x) = 2x^3 - 3x + 5$.

§ 36. Алгебраїчні і трансцендентні числа. Будова простого алгебраїчного розширення поля

Література

[1] — § 32, 33, с. 344—360;
[2] — § 33, с. 370—374;
[3] — гл. 17, § 2, с. 528—531;
[4] — гл. VI, § 1, с. 316—320; § 5, с. 327—332;
[5] — гл. X, § 5, 6, с. 380—391;
[6] — § 58, с. 358—363;
[8] — гл. 9, § 1, с. 420—424.

ТЕОРЕТИЧНІ ВІДОМОСТІ

Нехай P — деяке числове поле. **Число** α називають **алгебраїчним відносно поля** P, якщо воно є коренем деякого многочлена над полем P. Число, яке не є алгебраїчним відносно поля P, називають **трансцендентним відносно** P. Зокрема, алгебраїчні і трансцендентні числа відносно поля раціональних чисел **Q** називають відповідно просто **алгебраїчними і трансцендентними.**

Якщо α є алгебраїчним числом відносно поля P, то в кільці $P[x]$ існує єдиний незвідний зведений многочлен[1] $f(x)$, який має α своїм коренем, а його степінь n є найменшим серед степенів усіх многочленів з коренем α. При цьому многочлен $f(x)$ називають **мінімальним многочленом** числа α, а його степінь n — **степенем алгебраїчного числа** α відносно поля P.

Мінімальне розширення поля P, яке містить число $\alpha \notin P$, називають **простим розширенням поля** P, утвореним приєднанням числа α, і позначають через $P(\alpha)$. Якщо α є алгебраїчним (трансцендентним) відносно поля P, то $P(\alpha)$ називають **простим алгебраїчним (трансцендентним) розширенням.**

[1] Многочлен називають **зведеним**, якщо його старший коефіцієнт дорівнює одиниці.

Поле $P(\alpha)$, утворене з поля P приєднанням кореня α незвідного у полі P многочлена n-го степеня

$$f(x) = x^n + a_{n-1}x^{n-1} + \ldots + a_1x + a_0,$$

складається з усіх чисел виду

$$\beta = c_0 + c_1\alpha + c_2\alpha^2 + \ldots + c_{n-1}\alpha^{n-1},$$

де $c_0, c_1, \ldots, c_{n-1} \in P$.

Нехай F — деяке підполе поля P. Тоді P можна розглядати як векторний простір над полем F. При цьому розширення P поля F називають **скінченним**, якщо P є скінченно-вимірним векторним простором над F. При цьому розмірність простору P називають **степенем розширення** P над полем F.

Просте алгебраїчне розширення $P(\alpha)$ є скінченним розширенням поля P, а степінь розширення $P(\alpha)$ над полем P дорівнює степеню числа α відносно P.

Розширення P поля F, утворене за допомогою кількох послідовно виконаних простих алгебраїчних розширень, називають складеним алгебраїчним розширенням. **Розширення** P поля F називають **алгебраїчним**, якщо всі його елементи є алгебраїчними відносно поля F.

Будь-яке скінченне розширення поля P є його алгебраїчним та складеним розширенням. Кожне складене алгебраїчне розширення поля P є простим розширенням цього поля.

ПРИКЛАДИ РОЗВ'ЯЗУВАННЯ ЗАДАЧ

1. Довести, що число $\alpha = \sqrt{2 - \sqrt[3]{1 + \sqrt{3}}}$ є алгебраїчним, і знайти його мінімальний многочлен.

Розв'язання. Позбавимося радикалів у правій частині заданої рівності. Для цього послідовно піднесемо обидві частини рівності до четвертого, третього і другого степенів. Матимемо:

$$\alpha^4 = 2 - \sqrt[3]{1 + \sqrt{3}},$$

$$\alpha^4 - 2 = -\sqrt[3]{1 + \sqrt{3}},$$

$$(\alpha^4 - 2)^3 = -1 - \sqrt{3},$$

$$(\alpha^4 - 2)^3 + 1 = -\sqrt{3},$$

$$((\alpha^4 - 2)^3 + 1)^2 = 3.$$

Остання рівність означає, що число α є коренем многочлена $f(x) = ((x^4 - 2)^3 + 1)^2 - 3$ з раціональними коефіцієнтами, тобто α є алгебраїчним числом. Знайдемо канонічну форму многочлена $f(x)$:

$$f(x) = (x^{12} - 6x^8 + 12x^4 - 7)^2 - 3 = x^{24} - 12x^{20} + 60x^{16} - 158x^{12} + 228x^8 - 168x^4 + 46.$$

Оскільки всі коефіцієнти многочлена $f(x)$, крім старшого, діляться на 2, а вільний член 46 не ділиться на 4, то, за критерієм Ейзенштейна, многочлен $f(x)$ є незвідним у полі Q. Отже, $f(x)$ є мінімальним многочленом алгебраїчного числа α.

2. Знайти алгебраїчне число, приєднанням якого до поля Q можна дістати складене алгебраїчне розширення $Q(\sqrt{2})(\sqrt{3})$.

Розв'язання. Число $\alpha = \sqrt{3}$ є алгебраїчним над полем $Q(\sqrt{2})$ і його мінімальний многочлен $f(x) = x^2 - 3$. Тому всі числа з поля $Q(\sqrt{2})(\sqrt{3})$

запишемо у вигляді $\beta = c_0 + c_1\sqrt{2}$, де $c_0, c_1 \in Q(\sqrt{2})$. Оскільки всі числа в поля $Q(\sqrt{2})$ можна подати у вигляді $a + b\sqrt{2}$, де $a, b \in \mathbf{Q}$, то

$$\beta = (a_0 + b_0\sqrt{2}) + (a_1 + b_1\sqrt{2})\sqrt{3} = a_0 + b_0\sqrt{2} + a_1\sqrt{3} + b_1\sqrt{6}, \qquad (1)$$

де $a_0, b_0, a_1, b_1 \in \mathbf{Q}$.

Якщо $a_0 = b_1 = 0$ і $b_0 = a_1 = 1$, то дістанемо $\gamma = \sqrt{2} + \sqrt{3} \in Q(\sqrt{2})(\sqrt{3})$. Тому $Q(\sqrt{2} + \sqrt{3}) \subset Q(\sqrt{2})(\sqrt{3})$. Число γ є алгебраїчним і $f(x) = x_4 - 10x^2 + 1$ — його мінімальний многочлен. Це означає, що $Q(\gamma)$ є простим алгебраїчним розширенням і його елементи мають вигляд

$$d_0 + d_1\gamma + d_2\gamma^2 + d_3\gamma^3, \qquad (2)$$

де $d_0, d_1, d_2, d_3 \in \mathbf{Q}$.

Покажемо, що кожне число вигляду (1) можна подати у вигляді (2).

Маємо $\gamma^2 = 5 + 2\sqrt{6}$ і $\sqrt{6} = \frac{1}{2}(\gamma^2 - 5)$. Застосовуючи тепер формулу $(x+y)^3 = x^3 + y^3 + 3xy(x+y)$, знаходимо

$$\gamma^3 = 2\sqrt{2} + 3\sqrt{3} + 3\sqrt{6}(\sqrt{2} + \sqrt{3}) = 2\gamma + \sqrt{3} + \frac{3}{2}\gamma(\gamma^2 - 5).$$

Звідси $\sqrt{3} = \frac{11}{2}\gamma - \frac{1}{2}\gamma^3$ і $\sqrt{2} = \frac{1}{2}\gamma^3 - \frac{9}{2}\gamma$. Тому

$$\beta = a_0 + b_0\left(\frac{1}{2}\gamma^3 - \frac{9}{2}\gamma\right) + a_1\left(-\frac{1}{2}\gamma^3 + \frac{11}{2}\gamma\right) + b_1\frac{1}{2}(\gamma^2 - 5) = \left(a_0 - \frac{5}{2}b_1\right) +$$

$$+ \left(\frac{11}{2}a_1 - \frac{9}{2}b_0\right)\gamma + \frac{1}{2}b_1\gamma^2 + \left(\frac{1}{2}b_0 - \frac{1}{2}a_1\right)\gamma^3.$$

Отже, $\beta \in Q(\gamma)$, тобто

$$Q(\sqrt{2})(\sqrt{3}) \subset Q(\sqrt{2} + \sqrt{3})$$

і

$$Q(\sqrt{2})(\sqrt{3}) = Q(\sqrt{2} + \sqrt{3}).$$

3. Знайти степінь розширення **C** (поля комплексних чисел) над полем **R**.
Розв'язання. Векторний простір **C** над полем **R** має розмірність 2. Справді, числа 1 та i утворюють лінійно незалежну систему і кожне комплексне число має вигляд $a \cdot 1 + bi$, де $a, b \in \mathbf{R}$. Тому розширення **C** над полем **R** має степінь 2.

Задачі

36.1. Довести, що число α є алгебраїчним, і знайти його мінімальний многочлен, якщо:

а) $\alpha = \sqrt{2 + \sqrt{3}}$;
б) $\alpha = 1 + \sqrt{3 - \sqrt{5}}$;
в) $\alpha = \sqrt{13 - \sqrt{15}}$;
г) $\alpha + \sqrt[3]{2} + 1 = 0$;
д) $\alpha = \sqrt{5} - \sqrt[3]{3}$;
е) $\alpha = \sqrt[3]{2 + \sqrt{7}}$;
є) $\alpha = 1 + \sqrt{\sqrt[3]{6} + 1}$;
ж) $\alpha = i\sqrt{3} + 1$.

36.2. Знайти алгебраїчне число, приєднанням якого до поля **Q** можна дістати складене алгебраїчне розширення:

а) $Q(\sqrt{2})(\sqrt{5})$;
б) $Q(\sqrt{3})(\sqrt{4})$;
в) $Q(\sqrt{5})(\sqrt{7})$;
г) $Q(\sqrt{p})(\sqrt{q})$, де p, q — прості числа;
д) $Q(\sqrt{2})(\sqrt{3})(\sqrt{6})$;
е) $Q(\sqrt{2})(\sqrt{3})(\sqrt{5})$.

36.3. Знайти базис векторного простору P над полем **Q**, якщо:

а) $P = Q(\sqrt[3]{3})$;
б) $P = Q(\sqrt{2} + \sqrt{3})$;
в) $P = Q(\sqrt{3})(\sqrt{5})$;
г) $P = Q(\sqrt{2})(i)$;
д) $P = Q(\sqrt{2})(\sqrt{3})(\sqrt{5})$.

36.4. Довести, що поле дійсних чисел **R** не є скінченним розширенням поля **Q**.

36.5 Довести, що розширення P числового поля F, яке має третій степінь, не має інших підполів, крім F і P.

36.6. Довести, що розширення P числового поля F, яке має простий степінь, не має підполів, відмінних від F і P.

36.7. Довести, що множина всіх алгебраїчних чисел є зчисленною.

36.8. Довести, що множина всіх трансцендентних чисел є незчисленною.

36.9. Довести, що множина всіх алгебраїчних чисел є полем.

36.10. Алгебраїчне число називають цілим, якщо воно є коренем зведеного многочлена з цілими коефіцієнтами. Чи утворюють цілі алгебраїчні числа поле?

§ 37. Позбавлення від алгебраїчної ірраціональності в знаменнику дробу

Література

[1] — § 26, с. 294; § 32, с. 347—348;
[2] — § 26, с. 305—307; § 33, с. 374;
[3] — гл. 17, § 2, с. 532;
[7] — § 23, с. 130—133.

ТЕОРЕТИЧНІ ВІДОМОСТІ

Основні методи розв'язування задач на позбавлення від ірраціональності в знаменнику дробу грунтуються на таких фактах.

1. Якщо $f(x)$ — многочлен від однієї змінної над полем P з коренями $\alpha_1, \alpha_2, \ldots, \alpha_n$ (які можуть не належати P), то будь-який симетричний многочлен $g(x_1, x_2, \ldots, x_n)$ над полем P при $x_1 = \alpha_1, x_2 = \alpha_2, \ldots, x_n = \alpha_n$ набуває значення, яке є елементом поля P.

2. Поле $P(\alpha)$, утворене з числового поля P приєднанням кореня α, незвідного у полі P многочлена n-го степеня

$$f(x) = x^n + a_{n-1}x^{n-1} + \ldots + a_1x + a_0,$$

складається з усіх чисел виду

$$\alpha = c_0 + c_1\alpha + c_2\alpha^2 + \ldots + c_{n-1}\alpha^{n-1},$$

де $c_0, c_1, \ldots, c_{n-1}$ — довільні числа з поля P.

Крім цього, при розв'язуванні таких задач застосовуються формули скороченого множення:

$$x^n - y^n = (x-y)(x^{n-1} + x^{n-2}y + \ldots + y^{n-1}),$$
$$x^{2k+1} + y^{2k+1} = (x+y)(x^{2k} - x^{2k-1}y + \ldots + y^{2k}).$$

ПРИКЛАДИ РОЗВ'ЯЗУВАННЯ ЗАДАЧ

1. Позбавитися від ірраціональності в знаменнику дробу $\frac{1}{1-\omega_1}$, де ω_1 — один з коренів рівняння $x^3 - x - 1 = 0$.

Розв'язання. Нехай ω_2 і ω_3 — решта коренів заданого рівняння. Тоді

$$\frac{1}{1-\omega_1} = \frac{(1-\omega_2)(1-\omega_3)}{(1-\omega_1)(1-\omega_2)(1-\omega_3)} =$$
$$= \frac{1-\omega_2-\omega_3+\omega_2\omega_3}{1-\omega_1-\omega_2-\omega_3+\omega_1\omega_2+\omega_1\omega_3+\omega_2\omega_3-\omega_1\omega_2\omega_3}.$$

Згідно з теоремою Вієта,

$$\omega_1+\omega_2+\omega_3 = 0,\ \omega_1\omega_2+\omega_1\omega_3+\omega_2\omega_3 = -1 \text{ і } \omega_1\omega_2\omega_3 = 1.$$

Тому $\frac{1}{1-\omega_1} = \frac{1-(\omega_2+\omega_3)+\omega_2\omega_3}{-1} = -1+(\omega_2+\omega_3)-\omega_2\omega_3$, причому ω_2 і ω_3 є коренями рівняння $\frac{x^3-x-1}{x-\omega_1} = 0$.

Знайдемо його ліву частину. Виконаємо ділення многочленів у лівій частині за схемою Горнера (табл. 46).

Таблиця 46

	1	0	−1	−1
ω_1	1	ω_1	ω_1^2-1	0

Звідси $x^2 + \omega_1 x + \omega_1^2 - 1 = 0$. Це означає, що $\omega_2+\omega_3 = -\omega_1$ і $\omega_2\omega_3 = \omega_1^2 - 1$.

Отже, $\frac{1}{1-\omega_1} = -1-\omega_1-(\omega_1^2-1) = -\omega_1^2-\omega_1$.

2. Позбавитися від ірраціональності в знаменнику дробу

$$\frac{1}{\sqrt[3]{49}-\sqrt[3]{7}+3}.$$

Розв'язання. Заданий дріб є значенням раціонального дробу $\frac{f(x)}{g(x)} = \frac{1}{x^2-x+3}$ при $x = \sqrt[3]{7}$, яке є коренем незвідного у полі Q многочлена $h(x) = x^3 - 7$. Многочлени $g(x)$ і $h(x)$ взаємно прості. Знайдемо лінійне зображення їхнього найбільшого спільного дільника (див. приклад 2, § 23).

Ділення многочленів виконаємо «кутом»:

$$\begin{array}{r|l} x^3-7 & x^2-x+3 \\ \hline x^3-x^2+3x & x+1 \\ \hline x^2-3x-7 & \\ x^2-x+3 & \\ \hline -2x-10 & \end{array};$$

$$x^3 - 7 = (x^2-x+3)(x+1) - 2x - 10,$$

або

$$h(x) = g(x)(x+1) - (2x+10)$$
$$2x + 10 = -h(x) + g(x)(x+1);$$

і

$$\begin{array}{r|l} x^2-x+3 & -2x-10 \\ \hline x^2+5x & -\frac{1}{2}x+3 \\ \hline -6x+3 & \\ -6x-30 & \\ \hline 33 & \end{array};$$

$$x^2 - x + 3 = (-2x-10)\left(-\frac{1}{2}x+3\right) + 33$$

або

$$g(x) = -(2x+10)\left(-\frac{1}{2}x+3\right) + 33.$$

Звідси

$$33 = g(x) + (2x+10)\left(-\frac{1}{2}x+3\right) = g(x) + (-h(x) +$$
$$+ g(x)(x+1))\left(-\frac{1}{2}x+3\right) = g(x)\left(1+(x+1)\left(-\frac{1}{2}x+3\right)\right) +$$
$$+ h(x)\left(\frac{1}{2}x-3\right) = g(x)\left(-\frac{1}{2}x^2+\frac{5}{2}x+4\right) + h(x)\left(\frac{1}{2}x-3\right).$$

Оскільки $h\left(\sqrt[3]{7}\right) = 0$, то

$$33 = g\left(\sqrt[3]{7}\right)\cdot\left(-\frac{1}{2}\sqrt[3]{49}+\frac{5}{2}\sqrt[3]{7}+4\right),$$

$$\frac{1}{g\left(\sqrt[3]{7}\right)} = \frac{1}{\sqrt[3]{49}-\sqrt[3]{7}+3} = \frac{-\sqrt[3]{49}+5\sqrt[3]{7}+8}{66}.$$

3. Позбавитися від ірраціональності в знаменнику дробу $\frac{1}{\sqrt[3]{5}+\sqrt[5]{3}}$.

Розв'язання. I *спосіб*. Застосуємо формулу скороченого множення:

$$x^{15} - y^{15} = (x+y)(x^{14}y - x^{13}y^2 + x^{12}y^3 - x^{11}y^4 + x^{10}y^5 -$$
$$- x^9y^6 + x^8y^7 - x^7y^8 + x^6y^9 - x^5y^{10} + x^4y^{11} - x^3y^{12} + x^2y^{13} - xy^{14}).$$

Тоді

$$\frac{1}{\sqrt[3]{5}+\sqrt[5]{3}} = \frac{1}{3152}\left(5^4\sqrt[3]{25}\sqrt[5]{3} - 5^4\sqrt[3]{5}\sqrt[5]{9} + 5^4\sqrt[5]{27} -\right.$$
$$- 5^3\sqrt[3]{25}\sqrt[5]{81} + 5^3\sqrt[3]{5} - 5^3\sqrt[3]{5} + 5^2\sqrt[3]{25}\cdot 3\sqrt[5]{9} - 5^2\sqrt[3]{5}\cdot 3\sqrt[5]{27} +$$
$$\left. + 5^2\sqrt[5]{81} - 5\sqrt[3]{25}\cdot 3^2 + 5\sqrt[3]{5}\cdot 3^2\sqrt[5]{3} - 5\cdot 3^2\sqrt[5]{9} + \sqrt[3]{25}\cdot 3^2\sqrt[5]{27} -\right.$$

$$-\sqrt[3]{5}\cdot 3^2\sqrt[5]{81}+3^3\Big)=\frac{1}{3152}\Big(625\sqrt[5]{3}\sqrt[3]{25}-625\sqrt[3]{5}\sqrt[5]{9}+625\sqrt[5]{27}-$$
$$-125\sqrt[3]{25}\sqrt[5]{81}+375\sqrt[3]{5}-375\sqrt[5]{3}+75\sqrt[3]{25}\sqrt[5]{9}-$$
$$-75\sqrt[3]{5}\sqrt[5]{27}+75\sqrt[5]{81}-45\sqrt[3]{25}+45\sqrt[3]{5}\sqrt[5]{3}-45\sqrt[5]{9}+$$
$$+9\sqrt[3]{25}\sqrt[5]{27}-9\sqrt[3]{5}\sqrt[5]{81}+27\Big).$$

II спосіб. Якщо в знаменнику дробу є кілька радикалів, то їх можна поступово позбуватися одним із розглянутих вище способів (див. приклади 1 і 2) Позбавимося від ірраціональності $\sqrt[3]{5}$. Число $x=\sqrt[3]{5}$ є коренем многочлена $h(x)=x^3-5$. Многочлени $h(x)$ і $g(x)=x+\sqrt[5]{3}$ є взаємно простими і $h(x)=$ $=g(x)(x^2-\sqrt[5]{3}\,x+\sqrt[5]{9})-\sqrt[5]{27}-5$. Тому

$$g\left(\sqrt[3]{5}\right)\left(\sqrt[3]{25}-\sqrt[5]{3}\sqrt[3]{5}+\sqrt[5]{9}\right)=5+\sqrt[5]{27}$$

$$\frac{1}{\sqrt[3]{5}+\sqrt[5]{3}}=\frac{\sqrt[3]{25}-\sqrt[5]{3}\sqrt[3]{5}+\sqrt[5]{9}}{5+\sqrt[5]{27}}.$$

Число $y=\sqrt[5]{27}$ є коренем многочлена $h_1(y)=y^5-27$, многочлени $h_1(y)$ та $g_1(y)=y+5$ є взаємно простими і

$$y^5-27=(y-5)(y^4-5y^3+25y^2-125y+625)-3152.$$

Звідси

$$g_1\left(\sqrt[5]{27}\right)=\frac{3152}{9\sqrt[5]{9}-15\sqrt[5]{81}+75\sqrt[5]{3}-125\sqrt[5]{27}+625}.$$

Отже,

$$\frac{1}{\sqrt[3]{5}+\sqrt[5]{3}}=\frac{1}{3152}\left(\sqrt[3]{25}-\sqrt[5]{3}\sqrt[3]{5}+\sqrt[5]{9}\right)\left(9\sqrt[5]{9}-15\sqrt[5]{81}+75\sqrt[5]{3}-\right.$$
$$\left.-125\sqrt[5]{27}+625\right)$$

Виконавши множення, ми побачимо, що результат однаковий.

4. Позбавитися від ірраціональності в знаменнику дробу

$$\frac{1}{\sqrt{3}+\sqrt{5}+\sqrt{7}}.$$

Розв'язання. Введемо позначення: $x=\sqrt{3}$, $y=\sqrt{5}$, $z=\sqrt{7}$. Тоді дріб набуває вигляду $\frac{1}{x+y+z}=\frac{1}{\sigma_1}$, де σ_1 — елементарний симетричний многочлен від трьох змінних. Складемо вираз із степеневих сум $s_n(x, y, z)$ (див. задачі 28.7 28.8) з парними індексами n так, щоб у ньому був множником многочлен σ_1. Оскільки $s_2=\sigma_1^2-2\sigma_2$ і $s_4=\sigma_1^4-4\sigma_1^2\sigma_2+2\sigma_2^2+4\sigma_1\sigma_3$, то

$$\sigma_2^2=\sigma_1^4-4\sigma_1^2\sigma_2+4\sigma_2^2,$$

$$s_2^2-2s_4=\sigma_1(4\sigma_1\sigma_2-\sigma_1^3-8\sigma_3).$$

Зв'дси

$$\sigma_1=\frac{s_2^2-2s_4}{4\sigma_1\sigma_2-\sigma_1^3-8\sigma_3}.$$

Враховуючи те, що $s_2=15$ і $s_4=83$, маємо

$$\frac{1}{\sqrt{3}+\sqrt{5}+\sqrt{7}}=\frac{1}{59}(4(\sqrt{3}+\sqrt{5}+\sqrt{7})(\sqrt{15}+\sqrt{21}+\sqrt{35})-$$
$$-(\sqrt{3}+\sqrt{5}+\sqrt{7})^3-8\sqrt{105}).$$

Задачі

37.1. Позбавитися від ірраціональності в знаменнику дробу:

а) $\frac{1}{\omega}$, де $\omega^2+\omega-1=0$;

б) $\frac{\omega}{\omega+1}$, де $\omega^3-2\omega-3=0$;

в) $\frac{\omega}{1+\omega^2}$, де $\omega^4-4\omega-2=0$;

г) $\frac{\omega}{\omega^3+5}$, де $\omega^3-8\omega+2=0$;

д) $\frac{1}{\omega^2-\omega}$, де $\omega^4-5=0$.

37.2. Позбавитися від ірраціональності в знаменнику дробу:

а) $\frac{7}{1-\sqrt[4]{2}+\sqrt[4]{2}}$;

б) $\frac{\sqrt[3]{2}}{\sqrt[3]{4}+2\sqrt[3]{2}}$;

в) $\frac{1}{1+\sqrt[3]{2}+\sqrt[3]{4}}$;

г) $\frac{2}{\sqrt[3]{49}-\sqrt[3]{7}+3}$;

д) $\frac{1}{\sqrt[4]{27}-2\sqrt[4]{9}+\sqrt[4]{3}-1}$.

37.3. Позбавитися від ірраціональності в знаменнику дробу:

а) $\frac{1}{\sqrt[3]{6}-\sqrt[3]{5}}$;

б) $\frac{1}{\sqrt[5]{3}-\sqrt[5]{2}}$;

в) $\frac{1}{\sqrt[8]{3}+\sqrt[8]{2}}$;

г) $\frac{1}{\sqrt[9]{5}+\sqrt[9]{3}}$.

37.4. Позбавитися від ірраціональності в знаменнику дробу:

а) $\frac{1}{\sqrt{a}+\sqrt{b}+\sqrt{c}}$;

б) $\frac{1}{\sqrt[3]{2}+\sqrt[3]{3}+\sqrt[3]{5}}$;

в) $\frac{1}{\sqrt[3]{a}+\sqrt[3]{b}+\sqrt[3]{c}}$;

г) $\frac{1}{\sqrt[4]{a}+\sqrt[4]{b}+\sqrt[4]{c}}$.

37.5. Позбавитися від ірраціональності в таких співвідношеннях:

а) $\sqrt[3]{a}+\sqrt[3]{a^2}+b=0$;

б) $p\sqrt[3]{a^2}+q\sqrt[3]{a}+r=0$;

в) $\sqrt{a}+\sqrt{b}-\sqrt[4]{a^2+b^2}=0$.

Розділ I

§ 1

1.1. а) $q=4$, $r=7$; б) $q=0$, $r=31$; в) $q=-5$, $r=24$; г) $q=-1$, $r=100$ д) $q=-4$, $r=7$; е) $q=0$, $r=31$; є) $q=1$, $r=100$; ж) $q=5$, $r=24$.

1.2. а) $b=47$, $q=2$; $b=94$, $q=1$; б) $b=111$, $q=1$; в) $b_1=288$, $q_1=1$; $b_2=144$, $q_2=2$; $b_3=77$, $q_3=4$; $b_4=28$, $q_4=11$; $b_5=11$, $q_5=28$; г) $b=481$, $q=1$; $b=37$, $q=13$; д) $b=26$, $q=1$; $b=13$, $q=2$; е) За b можна взяти довільне ціле число таке, що $|b|>14$, $q=0$.

1.3. а) $b=25$, $r=21$; $b=26$, $r=7$; б) таких b і r не існує; в) $b=17$, $r=16$; г) b — довільне ціле число, причому $|b|>57$, $r=57$; д) $b=108$, $r=59$; е) $b=1$, $r=0$.

1.4 а) $2k$, $k\in\mathbf{Z}$; б) $3k$, $k\in\mathbf{Z}$; в) $8k$, $k\in\mathbf{Z}$; г) $7k+3$, $k\in\mathbf{Z}$; д) $4k+1$, $k\in\mathbf{Z}$; е) $2k+1$, $k\in\mathbf{Z}$; є) $3k+r$, $r=1,2$, $k\in\mathbf{Z}$; ж) $6k+r$, $r=1,5$ $k\in\mathbf{Z}$.

1.7. Розглянути різницю $\dfrac{mq+np}{m-p}-\dfrac{mn-pq}{m-p}$ і показати, що вона є цілим числом.

1.9. б) Розкласти $11^{10}-1$ на множники: $(11-1)(11^9+11^8+\ldots+11+1)$; в) $2222^{5555}+5555^{2222}=(2222^{5555}+4^{5555})+(5555^{2222}-4^{2222})-(4^{5555}-4^{2222})$. Розглянути кожен вираз у круглих дужках, використавши той факт, що сума однакових непарних степенів ділиться на суму основ, а різниця будь-яких однакових цілих степенів ділиться на різницю основ.

§ 2

2.1. Прості числа: 127, 919, 1033, 1657, 2647, 3163, 3623, 3631, 3767, 3769.

2.2. а) 2, 3, 5, 7, 11, 13, 17, 19, 23, 29, 31, 37, 41, 43, 47, 53, 59, 61, 67, 71, 73, 79, 83, 89, 97; б) 101, 103, 107, 109, 113, 127, 131, 137, 139, 149; в) 151, 157, 163, 167, 173, 179, 181, 191, 193, 197, 199; г) 557, 563, 569, 571, 577, 587, 593, 599; д) 1259, 1277, 1279, 1283, 1289, 1291, 1297; е) 2309, 2311, 2333, 2339, 2341, 2347; є) 2551, 2557, 2579, 2591, 2593; ж) 4327, 4337, 4339, 4349.

2.3. а) $2^5\cdot 5$; б) $2^3\cdot 3^2\cdot 7$; в) $7\cdot 11\cdot 13$; г) 1009; д) $29\cdot 61$; е) $2^3\cdot 3^2\cdot 5^2$; є) $53\cdot 67$; ж) $2^8\cdot 3^5\cdot 11^3$; з) $2^3\cdot 3^3\cdot 5^4\cdot 7^3\cdot 11^2\cdot 17\cdot 23\cdot 37$.

2.5. а) $13\cdot 61$; б) $2^3\cdot 3\cdot 31$; в) $2^2\cdot 31\cdot 127$; г) Позначити число 7^4 через x і розкласти число a на лінійні множники $(x-2)(x+3)$. Після спрощень дістаємо $a=2^2\cdot 601\cdot 2399$; д) $13\cdot 61\cdot 37\cdot 73\cdot 181$; е) $293\cdot 3413$; є) $13\cdot 4561$.

2.6. а) $p=2$; б) $p=3$; в) $p=3$; г) $p=3$; д) $p=3$; е) $p=3$. Числа 3, 5 і 7 є єдиною трійкою простих чисел-близнят (прості числа p і $p+2$ називають простими числами-близнятами); є) $p=3$. Якщо $p=3k+1$ або $p=3k+2$, то число $8p^2+1$ є складеним. Якщо $p=3k$, то $k=1$ і $p=3$. Тоді $8p^2+1=73$ і $8p^2+2p+1=79$; ж) $p=3$.

2.8. $p=13$. Розглянути рівняння $2p+1=(2x+1)^3$.

2.9. а) Якщо p — парне, то $p+10$ — складене, якщо p — непарне, то $p+5$ — складене; в) Якщо $2^n=3q+1$, то $2^n-1=3q$ — складене число, оскільки $n>2$; якщо $2^n=3q+2$, то $2^n+1=3q+3$ — складене число.

2.10. Усі натуральні числа містяться серед чисел виду $30k\pm s$, де k — ціле число, а $s=0,1,2,\ldots,15$. З них простими можуть бути числа виду $p=30k\pm 1$, $30k\pm 7$, $30k\pm 11$, $30k\pm 13$. Розглянути всі можливі випадки.

2.11. а), б) Використати метод математичної індукції;

в) $p_1p_2\ldots p_{k-1}=p_sq$ $(s>k,\ q>1)$, звідки $p_s\leqslant p_1p_2\ldots p_{k-1}$ і $p_s<p_1p_2\ldots p_k$. Тоді $p_{k+1}<p_1p_2\ldots p_k$;

г) Нехай p_k — найбільше просте число, що не перевищує $n > 2$. Канонічний розклад числа $t = p_1 p_2 \dots p_{k-1}$ містить тільки прості числа, більші за n. Отже, $t > n$, а тому $p_1 p_2 \dots p_k > n$.

2.13. Якщо n складене, то $n = ab$, $a > 1$, $b > 1$. Тоді $2^n - 1 = 2^{ab} - 1 = (2^a)^b - 1$ — складене.

2.14. Якщо n має хоч один непарний дільник $d > 1$,

то

$$2^n + 1 = (2^{\frac{n}{d}} + 1)(2^{\frac{n}{d}(d-1)} - 2^{\frac{n}{d}(d-2)} + \dots - 2^{\frac{n}{d}} + 1),$$

де обидва множники більші від 1, оскільки $n \geqslant 3$, $d \geqslant 3$. Тоді число $2^n + 1$ було б складеним, що суперечить умові. Отже, $n = 2^k$.

2.15. Використати рівність $p^2 - q^2 = (p - 1)(p + 1) - (q - 1)(q + 1)$.

2.16. 5. Використати задачу 2.6, е).

2.18. Якщо $n = 1$, то покласти $x = 3$; якщо $n \geqslant 2$, то покласти $x = n^2$.

2.19. а) $n = 2$, $n = 8$, б) $n = 3$.

2.20. Нехай p — простий дільник $n! - 1$. Оскільки $p \leqslant n! - 1$, то $p < n!$. Крім того, $n!$ не $\vdots p$, звідки $n < p$. Отже, $n < p < n!$ (З доведеного випливає, що множина простих чисел нескінченна.)

2.21. $(n + 1)! + 2$, $(n + 1)! + 3$, $\dots$, $(n + 1)! + (n + 1)$.

2.22. а) Припустимо, що множина простих чисел виду $3k + 2$ скінченна. Нехай це числа $p_1 < p_2 < \dots < p_s$. Розглянемо число $t = 3p_1 p_2 \dots p_s + 2$. Зрозуміло, що це число виду $3k + 2$. Оскільки $t > p_s$ і $t > 1$, то t складене. Отже, воно ділиться хоча б на одне просте число. На 3 воно не ділиться. Зрозуміло також, що всі прості дільники числа t не є виду $3k + 1$. Отже, число t ділиться хоча б на один простий дільник виду $3k + 2$. Оскільки всі такі прості числа знаходяться серед чисел $p_1, p_2, \dots, p_s$, то t ділиться на одне з них. Тоді з рівності $t = 3p_1 p_2 \dots p_s + 2$ випливає, що на це число поділиться й число 2. Дістали суперечність.

§ 3

3.1. а) 0; б) 7; в) 21; г) 13; д) 2; е) 17; є) 55; ж) 41; з) 71; к) 420; н) 1.

3.2. а) 13; б) 23; в) 119; г) 23; д) 7; е) 21; є) 2; ж) 33; з) 17; к) 12; м) 1.

3.3. а) 2; б) 0; в) 2520; г) 99671; д) 138600; е) 3276; є) 1116; ж) 67818; з) $n(n + 1)$.

3.4. а) 88200; б) 36036; в) 2940; г) $\frac{1}{2}n(n + 1)(n + 2)$ при n парному і $n(n + 1)(n + 2)$ при n непарному; д) 4 582 198; е) 4 272.

3.5. а) $3 = 5 \cdot 21 - 2 \cdot 51$; б) $2 = 20 \cdot (-26) + 3 \cdot 174$; в) $29 = -6 \cdot 899 + 11 \cdot 493$; г) $17 = -10 \cdot 1445 + 23 \cdot 629$; д) $43 = -4 \cdot 903 + 5 \cdot 731$; е) $47 = 2 \cdot 1786 - 5 \cdot 705$; є) $6 = -135 \cdot 822 + 64 \cdot 1734$; ж) $1 = 17 \cdot 4373 + 90 \cdot (-826)$; з) $17 = 45 \cdot (-3791) + 52 \cdot 3281$.

3.6. Див. приклад 3, § 3.

3.7. а) $a = 30$, $b = 120$; $a = 60$, $b = 90$ і навпаки; б) $a = 24$, $b = 120$ і навпаки; в) $a = 2$, $b = 10$ і навпаки; г) $a = 20$, $b = 420$; $a = 60$, $b = 140$ і навпаки; д) $a = 4$, $b = 180$; $a = 20$, $b = 36$ і навпаки; е) $a = 495$, $b = 315$ і навпаки; є) $a = 140$, $b = 252$ і навпаки; ж) $a = 4$, $b = 24$; $a = 8$, $b = 12$ і навпаки; з) $a = 4$, $b = 12$ і навпаки; к) $a = 24$, $b = 2496$; $a = 192$, $b = 312$ і навпаки; л) $a = 552$, $b = 115$; $a = 435$, $b = 232$ і навпаки; м) $a = 75$, $b = 195$ і навпаки; н) не існує.

3.10. а) $a^d - 1$, де $d = (m, n)$; б) 13, якщо $(a - 5) \vdots 13$; 1, якщо $(a - 5)$ не $\vdots 13$. Скористатися рівністю $4(a^2 + 1) = (2a + 3)(2a - 3) + 13$; в) 7.

3.12. а) Групуючи доданки, показати послідовно, що це число ділиться на 271 і на 7, і використати співвідношення $(7, 271) = 1$, $7 \cdot 271 = 1897$; б) покласти $n + 1 = a^3$ і показати, що $(a^3 - 1)a^3(a^3 + 1)$ ділиться на 7, 8 і 9;

в) Застосувати індукцію (за числом n, починаючи з $n = 0$);

д) Розглянути різницю $(a^{2k} + 1) - (a + 1)$.

§ 4

4.1. а) 12 і 168; б) 9 і 217; в) 24 і 1170; г) 8 і 624; д) 30 і 2418; е) 8 і 1440; є) 12 і 1960; ж) 24 і 2808; з) 16 і 2340; к) 30 і 3844; л) 8 і 3096; м) 24 і 8736.

4.2. а) 1, 2, 4, 8, 3, 6, 12, 24; б) 1, 5, 25, 2, 10, 50; в) 1, 5, 25, 2, 10, 50, 4, 20, 100; г) 1, 2, 4, 8, 3, 6, 12, 24, 9, 18, 36, 72, 5, 10, 20, 40, 15, 30, 60, 120, 45, 90, 180, 360; д) 1, 5, 25, 125, 3, 15, 75, 375.

4.3. а) 20; б) 1, якщо $\tau(n) = 1$; p, якщо $\tau(n) = 2$; p^2, якщо $\tau(n) = 3$; p^3 або pq, якщо $\tau(n) = 4$; p^4, якщо $\tau(n) = 5$; p^5 або p^2q, якщо $\tau(n) = 6$, де скрізь p і q — різні прості числа; в) 675; г) 200; д) 192; е) 192; є) 180; ж) 45 360; з) 18; к) $2^6 3^5 5^4$; л) 120; м) $3^3 5^4$; н) 1 400.

4.4. а) $m = 2^k$, де k — довільне натуральне число.

4.5. а) 28; б) 160 або 169; в) 280.

4.9. а) 16; б) 30; в) 40; г) 80; д) 200; е) 500; є) 192; ж) 400; з) 320.

4.10. а) 8; б) 12; в) 24; г) 40; д) 66; е) 20; є) 2.

4.12. а) $x = 16, 24, 20, 30, 15$; б) $x = 36, 28, 13, 26, 21, 42$; в) розв'язків немає; г) $x = 2$ при $p = 2$; $x = p$, $x = 2p$ при $p > 2$; д) $x = 2^{k+1}$; $2^k \cdot 3$; $2^{k-1} \cdot 5$; $2^{k-2} \cdot 15$ при $k \geqslant 2$; $x = 15$ при $k = 3$; е) $x = 2^k$, $k \in \mathbb{N}$; є) $x = 2^k \cdot 3^l$, $k, l \in \mathbb{N}$; ж) розв'язків немає; з) $x = 5^k$, $k \in \mathbb{N}$; к) $x = 3^k$, $k \in \mathbb{N}$ л) $x = 2^k \cdot s$, де k, $s \in \mathbb{N}$ і $(s, 6) = 1$; м) $x = 3$.

4.13. а) 7875; б) 143; в) 14 161; г) 741 125; д) 343; е) 67 375; є) 143, 183, 225, 244, 248; ж) при $p \neq 3$ розв'язків немає, при $p = 3$ за k можна взяти будь-яке натуральне число, відмінне від 1.

4.15. а) 2; б) -3; в) -1; г) 2; д) 4; е) 3; є) 5; ж) 4; з) -2; к) -3; л) 2.

4.16. а) 0,14; б) 0,86; в) 0,5; г) 0,6; д) 0,5; е) 0,15; є) 0,4; ж) $\frac{5}{7}$.

4.17. а) $[2,3x] = 3$, тоді $2,3x - \alpha = 3$ або $2,3x = 3 + \alpha$, де $0 < \alpha < 1$. Отже, $3 < 2,3x < 4$, тоді $\frac{3}{2,3} < x < \frac{4}{2,3}$. Остаточно маємо $x \in \left[\frac{30}{23}; \frac{40}{23}\right[$; б) $x \in \left[\frac{50}{32}; \frac{60}{32}\right[$; в) $x = \frac{m + \alpha}{a}$, де $0 < \alpha < 1$; г) $x = 7$; д) $x \in [\sqrt{2}; \sqrt{3}[$; е) $x = 1$; є) $x = 0$; $1\frac{1}{3}$; $2\frac{1}{3}$; ж) $x = 0; 1$; з) $x \in \varnothing$; к) $x \in [my; (m - 1)(y + 1)[$, де y — ціле число, причому $y < m - 1$.

4.18. а) Нехай $x = [x] + r$ і $y = [y] + s$, де $0 \leqslant r < 1$ і $0 \leqslant s < 1$. Тоді $x + y = [x] + [y] + (r + s)$. Якщо $0 \leqslant r + s < 1$, то $[x + y] = [x] + [y]$. Якщо $1 \leqslant r + s < 2$, то $[x + y] > [x] + [y]$. Отже, $[x + y] \geqslant [x] + [y]$; в) якщо $p = 4k + 1$, то $\left[\frac{p}{4}\right] = k = \frac{p - 1}{4}$; якщо $p = 4k + 3$, то $\left[\frac{p}{4}\right] = k = \frac{p - 3}{4}$; г) $a = mq + r$, де $0 \leqslant r < m$. Тоді $\frac{a}{m} = q + \frac{r}{m}$, де $0 \leqslant \frac{r}{m} < 1$, звідки $q = \left[\frac{a}{m}\right]$ і тому $\left[\frac{a}{m}\right] = \frac{a - r}{m}$; з) використати твердження з п. а) цієї задачі; к) розглянути випадки $m = 4k + 1$, і $m = 4k + 3$.

4.19. а) 48; б) 98; в) 832; г) 13 589.

4.20. а) $2^3 \cdot 3^4 \cdot 5 \cdot 7 \cdot 11$; б) $2^{16} \cdot 3^8 \cdot 5^3 \cdot 7^2 \cdot 11 \cdot 13 \cdot 17$; в) $2^{38} \cdot 3^{18} \cdot 5^9 \times 7^5 \cdot 11^3 \cdot 13^3 \cdot 17^2 \cdot 19^2 \cdot 23 \cdot 29 \cdot 31 \cdot 37$; г) $2^{71} \cdot 3^{35} \cdot 5^{18} \cdot 7^{11} \cdot 11^6 \cdot 13^5 \cdot 17^4 \times 19^3 \cdot 23^3 \cdot 29^2 \cdot 31^2 \cdot 37^2 \cdot 41 \cdot 43 \cdot 47 \cdot 53 \cdot 59 \cdot 61 \cdot 67 \cdot 71 \cdot 73$; д) $2^2 \cdot 11 \cdot 13 \times 17 \cdot 19$.

4.21. а) 12; б) 28; в) 494.

4.24. а) $\left[\frac{10^7}{786}\right] - \left[\frac{10^6}{786}\right] = 11450$;

б) $999 - \left[\frac{999}{5}\right] - \left[\frac{999}{7}\right] + \left[\frac{\left[\frac{999}{5}\right]}{7}\right] = 686$;

в) $100 - \left[\frac{100}{2}\right] - \left[\frac{100}{3}\right] + \left[\frac{100}{6}\right] = 33$;

г) 1378; д) 5634; е) 393.
4.25. 30.

§ 5

5.1. а) $[1; 3, 1, 1, 2]$, $\frac{P_k}{Q_k} = \frac{1}{1}, \frac{4}{3}, \frac{5}{4}, \frac{9}{7}, \frac{23}{18}$;

б) $[1; 1, 8, 2]$, $\frac{P_k}{Q_k} = \frac{1}{1}, \frac{2}{1}, \frac{17}{9}, \frac{36}{19}$;

в) $[2; 1, 1, 4, 2]$, $\frac{P_k}{Q_k} = \frac{2}{1}, \frac{3}{1}, \frac{5}{2}, \frac{23}{9}, \frac{51}{20}$;

г) $[-2; 1, 1, 2, 1, 5]$, $\frac{P_k}{Q_k} = -\frac{2}{1}, -\frac{1}{1}, -\frac{3}{2}, -\frac{7}{5}, -\frac{10}{7}, -\frac{57}{40}$;

д) $[-2; 2, 1, 3, 1, 1, 4, 3]$, $\frac{P_k}{Q_k} = -\frac{2}{1}, -\frac{3}{2}, \frac{-5}{3}, \frac{-18}{11}, \frac{-23}{14}, \frac{-41}{25}, \frac{-187}{114}, \frac{602}{367}$;

е) $[-6; 1, 1, 28]$, $\frac{P_k}{Q_k} = -\frac{6}{1}, -\frac{5}{1}, -\frac{11}{2}, -\frac{313}{57}$;

є) $[3; 1, 1, 1, 4, 10]$, $\frac{P_k}{Q_k} = \frac{3}{1}, \frac{4}{1}, \frac{7}{2}, \frac{11}{3}, \frac{51}{14}, \frac{521}{143}$;

ж) $[-1; 1, 1, 1, 1, 1, 1, 2, 6]$, $\frac{P_k}{Q_k} = \frac{-1}{1}, \frac{0}{1}, -\frac{1}{2}, -\frac{1}{3}, -\frac{2}{5}, -\frac{3}{8}, -\frac{5}{13}, -\frac{13}{34}, -\frac{83}{217}$;

з) $[-1; 2, 2, 1, 1, 6, 2]$, $\frac{P_k}{Q_k} = -\frac{1}{1}, -\frac{1}{2}, -\frac{3}{5}, -\frac{4}{7}, -\frac{7}{12}, -\frac{46}{79}, -\frac{99}{170}$;

к) $[0; 2, 1, 2]$, $\frac{P_k}{Q_k} = \frac{0}{1}, \frac{1}{2}, \frac{1}{3}, \frac{3}{8}$;

л) $[-1; 1, 1, 4, 1, 1, 1, 10]$, $\frac{P_k}{Q_k} = -\frac{1}{1}, \frac{0}{1}, -\frac{1}{2}, -\frac{4}{9}, -\frac{5}{11}, -\frac{9}{20}, -\frac{14}{31}, -\frac{149}{330}$.

5.2. а) $\frac{20}{31}$; б) $\frac{131}{583}$; в) $\frac{7}{23}$; г) $\frac{97}{113}$; д) $\frac{17}{83}$; е) $\frac{359}{113}$; є) $\frac{883}{271}$; ж) $\frac{73}{1201}$; з) $-\frac{234}{195}$; к) $-\frac{271}{100}$; л) $\frac{2}{3}$.

5.3. а) $\frac{105}{38}$; б) $\frac{245}{83}$; в) $\frac{64}{25}$; г) $\frac{73}{43}$; д) $\frac{99}{464}$; е) $-1\frac{11}{50}$; є) $-2\frac{11}{39}$; ж) $-4\frac{25}{41}$; з) $\frac{2633}{1810}$; к) $\frac{a^5 + 4a^3 + 3a}{a^4 + 3a^2}$; л) $\frac{a^3b^2 + 4a^2b + 3a}{a^2b^2 + 3ab + 1}$

5.4. Використати те, що

$$\frac{a}{(a, b)} = P_n, \quad \frac{b}{(a, b)} = Q_n, \quad P_nQ_{n-1} - P_{n-1}Q_n = (-1)^n.$$

5.6. а) $\frac{29}{37} \approx \frac{7}{9}$ $(+0{,}01) = 0{,}78$. Знак похибки «+», оскільки $\frac{P_4}{Q_4} < \frac{a}{b}$; б) $\frac{648}{385} \approx \frac{69}{41}$ $(+0{,}0003) \approx 1{,}6830$; в) $\frac{571}{359} \approx \frac{35}{22}$ $(-0{,}0005) \approx 1{,}5909$. Знак похибки «—», оскільки $\frac{P_5}{Q_5} > \frac{a}{b}$.

5.7. а) $\frac{85}{31}$ з надвишком; б) $\frac{277}{101}$ з недостачею.

5.8. а) $x = \left[\frac{73}{30}\right] = 2$; б) $x = 2$.

5.9. $[1; 1, 1, 4, 3]$. Розкласти $\frac{14}{9}$ в ланцюговий дріб.

5.10. $q_2 = 3$.

5.11. Замінити дріб $\frac{587}{113}$ підхідним дробом з похибкою, яка не перевищує 0,001. $\frac{587}{113} = [5; 5, 7, 3]$. Підхідні дроби:

$$\frac{P_0}{Q_0} = \frac{5}{1}, \quad \frac{P_1}{Q_1} = \frac{26}{5}, \quad \frac{P_2}{Q_2} = \frac{187}{36}, \quad \frac{P_3}{Q_3} = \frac{587}{113}.$$

Якщо взяти дріб $\frac{26}{5}$, то похибка становитиме $\frac{1}{5 \cdot 36} = \frac{1}{180} \approx 0{,}006$. Оскільки $0{,}006 > 0{,}001$, то дріб $\frac{26}{5}$ не підходить. Беремо дріб $\frac{187}{36}$. Знаходимо похибку $\frac{1}{36 \cdot 113} = \frac{1}{4068} \approx 0{,}0003 < 0{,}001$. Отже, можна побудувати передачу за допомогою валів з кількістю зубців 187 і 36, що технічно можливо. а) 22 і 7; б) 163 і 51.

5.12. а) $x = -8360 - 117t$, $y = 2717 + 38t$, $t \in \mathbf{Z}$;
б) $x = -2 + 4t$, $y = -4 + 7t$, $t \in \mathbf{Z}$;
в) $x = -125 - 114t$, $y = 45 + 41t$, $t \in \mathbf{Z}$;
г) $x = 1 - 9t$, $y = 39 + 49t$, $t \in \mathbf{Z}$;
д) $x = 9 + 31t$, $y = 2 - 12t$, $t \in \mathbf{Z}$;
е) $x = 75 + 23t$, $y = -120 - 37t$, $t \in \mathbf{Z}$;
є) $x = 4 + 17t$, $y = -11 - 53t$, $t \in \mathbf{Z}$;
ж) $x = -15 - 39t$, $y = -25 - 64t$, $t \in \mathbf{Z}$;
з) $x = -15 + 37t$, $y = 18 - 43t$, $t \in \mathbf{Z}$;
к) $x = 1270 + 359t$, $y = -2020 - 571t$, $t \in \mathbf{Z}$.

5.13. а) Розв'язків немає; б) $x = 4 + 42t$, $y = 23t$, $t \in \mathbf{N}$; в) $x = 3$, $y = 5$.

5.14. 56 і 44.

5.15. 19 дощок 11 см завширшки і 7 дощок 13 см завширшки або 6 дощок 11 см завширшки і 18 дощок 13 см завширшки.

5.16. 2 мішки по 60 кг і 4 мішки по 80 кг.

5.17. $3 - 5t$ білетів по 30 коп. і $28 + 3t$ білетів по 50 коп., де $-9 \leqslant t \leqslant 0$.

5.18. Горобців — 9, горлиць — 10, голубів — 11.

5.19. (0, 18, 8); (1, 16, 9); (2, 14, 10), (3, 12, 11); (4, 10, 12); (5, 8, 13); (6, 6, 14); (7, 4, 15); (8, 2, 16); (9, 0, 17).

5.20. а) $[1; (2)]$; б) $[1; (1, 2)]$; в) $[2, (4)]$; г) $[2; (2, 4)]$; д) $[2; (1, 1, 1, 4)]$; е) $[2; [1, 4)]$; є) $[3; (6)]$; ж) $[3; (3, 6)]$; з) $[3; (2, 6)]$; к) $[3; (1, 1, 1, 1, 6)]$; л) $[5; (3, 2, 3, 10)]$; м) $[5; (2, 10)]$; н) $[7; (1, 2, 7, 2, 1, 14)]$.

5.21. а) $[(2)]$; б) $[(1, 2)]$; в) $[1; (2, 2, 2, 1, 12, 1)]$; г) $[2; (1)]$; д) $[1; (1, 1, 4, 1)]$; е) $[2; (18, 2)]$; є) $[1; 7, (1, 6)]$; ж) $[-5; 2, (3, 5, 3, 1, 1, 10, 1, 1)]$; з) $[3; (3, 1, 1, 10, 1, 1, 3, 5)]$; к) $[2; 7, (2, 6)]$; л) $[0; 14, (8, 1, 2, 1, 8, 13)]$; м) $[1; 1, 1, (2, 2, 1, 12, 1, 2)]$; н) $]2; 1, 4, (5, 3)]$.

5.22. а) $\frac{\sqrt{3}+1}{2}$; б) $\frac{\sqrt{13}-1}{2}$; в) $\frac{\sqrt{29}-1}{2}$; г) $\sqrt{5}-2$; д) $\frac{\sqrt{53}-7}{2}$;

е) $1+\sqrt{1,(6)}$; є) $\sqrt{33}-2{,}5$; ж) $\frac{\sqrt{21}-3}{2}$; з) $\frac{\sqrt{3}-1}{2}$; к) $2(\sqrt{2}-1)$;

л) $1+\sqrt{3}$; м) $\frac{\sqrt{15}}{3}$; н) $\frac{\sqrt{2}+3}{6}$.

5.23. а) $\frac{\sqrt{37}-3}{4}$; б) $\frac{\sqrt{7925}-69}{14}$; в) $\frac{5\sqrt{13}-13}{3}$; г) $\frac{\sqrt{101}-1}{4}$;

д) $\frac{\sqrt{37}-1}{3}$; е) $\frac{\sqrt{37}+3}{4}$; є) $\frac{5\sqrt{2}}{2}$; ж) $\frac{2(\sqrt{14}+2)}{5}$; з) $\frac{25-\sqrt{61}}{4}$;

к) $\frac{29+\sqrt{21}}{10}$; л) $\frac{138-\sqrt{5}}{79}$; м) $\frac{18+\sqrt{506}}{28}$; н) $\frac{4\sqrt{95}-18}{13}$.

5.24. а) $x^2-102=0$; б) $x^2-92=0$; в) $x^2-x-4=0$; г) $10x^2-17x-5=0$; д) $19x^2-37x-11=0$; е) $2x^2-15x+26=0$; є) $16x^2-32x+13=0$.

5.25. а) $x=\sqrt{q^2+1}$; б) $x=\sqrt{q^2+2}$.

5.26 а) $[q;(2q)]$; б) $[q^2;(q,2q^2)]$; в) $[q;(1,q-1,1,2q)]$; г) $[q^3;(q^2,2q^3)]$.

5.27 а) $\frac{587}{103}=[5;1,2,3,10]\approx 5{,}7\ (+0{,}0002)$;

б) $3{,}14159=[3;7,15,1,25,1,7,4]\approx\frac{355}{113}\ (+0{,}000004)$;

в) $\frac{2}{3}\ (+0{,}07)=\frac{-1+\sqrt{5}}{2}$; г) $\frac{2}{37}\ (+0{,}00005)=\frac{2-\sqrt{3}}{5}$.

5.28 а) $x_1\approx\frac{349}{73}\ (-0{,}0001)\approx 4{,}7808$, $x_2\approx\frac{155}{57}\ (-0{,}0001)\approx 2{,}7192$;

б) $x_1\approx-\frac{29}{40}\ (-0{,}0001)\approx -0{,}7250$, $x_2\approx-\frac{331}{40}\ (-0{,}0001)\approx -8{,}2750$;

в) $x_1\approx-\frac{211}{80}\ (-0{,}0001)\approx -2{,}6375$, $x_2\approx\frac{311}{301}\ (-0{,}0001)\approx 1{,}0332$;

г) $x_1\approx\frac{593}{130}\ (-0{,}0001)\approx 4{,}5615$, $x_2\approx\frac{57}{130}\ (+0{,}0001)\approx 0{,}4384$;

д) $x_1\approx-\frac{251}{125}\ (+0{,}0001)\approx -2{,}008$, $x_2\approx-\frac{449}{140}\ (+0{,}0001)\approx -3{,}2071$.

5.29. $\frac{P_0}{Q_0}=\frac{1}{1}$, $\frac{P_1}{Q_1}=\frac{4}{3}$, $\frac{P_2}{Q_2}=\frac{5}{4}$, $\frac{P_3}{Q_3}=\frac{29}{23}$.

5.30. $\frac{65}{28}$.

5.31. а) $[5;(2,10)]\approx\frac{241}{44}$; б) $[7;(1,2,7,2,1,14)]\approx\frac{530}{69}$;

в) $[2;(1,4,1,1)]\approx\frac{271}{96}$; г) $[(1;12,1,1,1,2,1,1)]\approx\frac{109}{101}$.

5.32. а) Через x позначити дріб $\frac{1}{[(b,a)]}$. Тоді $[(a,b)]=a+x$ і треба довести, що $x(a+x)=\frac{a}{b}$. Оскільки $x=\frac{1}{b+\frac{1}{a+x}}$, то в результаті перетворень маємо $x^2+ax-\frac{a}{b}=0$, тобто $x(a+x)=\frac{a}{b}$;

в) Показати, що $\frac{a^4+3a^2+1}{a^3+2a}=[a;a,a,a]$. Якщо дріб $[a;a,a,a]$ обчислити, то дістанемо $\frac{a^4+3a^2+1}{a^3+2a}$, що свідчить про нескоротність останнього;

г) якщо $(P_n,P_{n-1})=d$, то $P_n=q_nP_{n-1}+P_{n-2}$, звідки $(P_{n-1},P_{n-2})=d$. При $n=2$ маємо $d=(P_1,P_0)=(q_1q_0+1,q_0)=1$. Твердження $(Q_n,Q_{n-1})=1$ доводять аналогічно; д) використати результати задачі 5.32, г); е) застосувати

формули $P_k=q_kP_{k-1}+P_{k-2}$ і $Q_k=q_kQ_{k-1}+Q_{k-2}$ при $k=n+2$ і $k=n+1$; є) використати індукцію за числом n; ж) використати індукцію за числом n і співвідношення $Q_n=q_nQ_{n-1}+Q_{n-2}\geqslant 2Q_{n-2}$;

л) Знак різниці

$$\alpha-\frac{P_n+P_{n+1}}{Q_n+Q_{n+1}}=\frac{q_{n+2}P_{n+1}+P_n}{q_{n+2}Q_{n+1}+Q_n}-\frac{P_n+P_{n+1}}{Q_n+Q_{n+1}}=$$

$$=\frac{(-1)^n(q_{n+2}-1)}{(q_{n+2}Q_{n+1}+Q_n)(Q_n+Q_{n+1})}$$

залежить від парності n; $\frac{P_n+P_{n+1}}{Q_n+Q_{n+1}}<\alpha$ при $n=2k$, $\alpha<\frac{P_n+P_{n+1}}{Q_n+Q_{n+1}}$ при $n=2k+1$. Дріб $\frac{P_n+P_{n+1}}{Q_n+Q_{n+1}}$ лежить між α і $\frac{P_n}{Q_n}$. Тоді

$$\left|\alpha-\frac{P_n}{Q_n}\right|>\left|\frac{P_n+P_{n+1}}{Q_n+Q_{n+1}}-\frac{P_n}{Q_n}\right|=\frac{1}{Q_n(Q_n+Q_{n+1})}.$$

Зауваження. Встановлена нерівність дає нижню границю для $\left|\alpha-\frac{P_n}{Q_n}\right|$ і, отже, доповнює відому нерівність

$$\left|\alpha-\frac{P_n}{Q_n}\right|<\frac{1}{Q_nQ_{n+1}};$$

м) Твердження випливає з рівності

$$\frac{(q_n+m)P_{n-1}+P_{n-2}}{(q_n+m)Q_{n-1}+Q_{n-2}}-\frac{q_nP_{n-1}+P_{n-2}}{q_nQ_{n-1}+Q_{n-2}}=(-1)^{n-2}\cdot m\cdot\frac{1}{A},$$

де $A>0$ — добуток знаменників підхідних дробів;

5.33. а) $\frac{ab+\sqrt{a^2b^2+4ab}}{2b}=[(a,b)]$;

б) маємо рівняння $bx^2-abx-a=0$ (див. задачу 5.32, а)). Сума коренів цього рівняння дорівнює a, звідки $x_2=a-[(a,b)]=-\frac{1}{[(b,a)]}$;

в) оскільки $x=[a;(b,c)]=a+\frac{1}{[(b,c)]}$, то $[(b,c)]=\frac{1}{x-a}$. Число $[(b,c)]$ є коренем рівняння $cx^2-bcx-b=0$ (див. задачу 5.33, б)). Отже, другий корінь можна знайти з умови $\frac{1}{x-a}=-\frac{1}{[(c,b)]}$, звідки $x=a-[(c,b)]$;

г) $\frac{\alpha}{\beta}=\frac{ab+1}{bc+1}$. Числа x і y задовольняють умову

$$(bc+1)x^2-(abc+a+c-b)x-(ab+1)=0,$$
$$(ab+1)y^2-(abc+a+c-b)y-(bc+1)=0,$$

звідки $\frac{x}{y}=\frac{ab+1}{bc+1}$, отже $\frac{\alpha}{\beta}=\frac{x}{y}$;

д) Якщо $\sqrt{m}=[q_0;q_1,q_2,\ldots]$, то $q_0+\sqrt{m}=[2q_0;q_1,q_2,\ldots]>1$ і $-1<q_0-\sqrt{m}<0$. Отже, $q_0+\sqrt{m}$ виражається чистим періодичним ланцюговим дробом, тобто $q_0+\sqrt{m}=[(2q_0;q_1,q_2,\ldots,q_n)]$. Тоді $\sqrt{m}=[q_0;(q_1,q_2,\ldots,q_n)]$.

5.34. а) $\alpha=\frac{10\sqrt{2}+P_{k-1}}{3\sqrt{2}+Q_{k-1}}$, $\frac{P_k}{Q_k}=[3;3]$, $\frac{P_{k-1}}{Q_{k-1}}=\frac{3}{1}$,

$$\alpha = \frac{10\sqrt{2}+3}{3\sqrt{2}+1} = \frac{57-\sqrt{2}}{17};$$

б) $\alpha = [2;\ 1,\ 5,\ 2,\ 1,\ (2,\ 1)] = \dfrac{51+4\sqrt{3}}{23}$.

5.35. Якщо $x = [a;\ a,\ a,\ \ldots] = [a,\ x]$, то $x = \dfrac{a+\sqrt{a^2+4}}{2}$.

§ 6

6.1. а) 64; б) 159; в) 596; г) 1205; д) 1429; е) 1874.
6.2. а) XXVI; б) CXII; в) MCMLXXX.
6.3. а) 10^9; б) 10^{12}; в) 10^{15}.
6.4. а) $11\,000_2$; б) $10\,001\,111_2$; в) $101\,011_2$; г) 111_2; д) $2\,255\,025_7$; е) $3(10)94\,913_{12}$; є) $30\,413_7$; ж) $190\,000_{12}$; з) 56_7 і остача 202_7; к) $(10)\,94_{12}$ і 87_{12} в остачі; л) $2{,}4_8$.
6.5. а) $100\,001_2$; б) 11, $11\,101_2$; в) 100 000, $11\,001_2$; г) 0, 1337_8; д) 11, 14_8.
6.6. а) 1_8; б) 1_6; в) 1_8; г) 1_5; д) 1_5; е) 1_8; є) 1_3; ж) 1_7; з) 1_7; к) 1_8; л) 1_4; м) 1_8; н) 1_6.
6.7. а) 39; б) 205; в) 229; г) 2617; д) 704; е) 8387; є) 1668; ж) 1523; з) 6871; к) 5669; л) 42 923.
6.8. а) 0,875; б) 0,75; в) 25,9365; г) 287,388671875; д) 0,044921875.
6.9. а) $4\,(10)\,2\,(11)_{12}$; б) $230\,578_9$; в) $11\,202\,102\,120\,100_3$; г) $367\,341_8$; д) $10\,001\,000\,110\,110\,111\,101\,100_2$; е) $2\,121\,311_5$; є) 4126_8.
6.10. а) $11\,111\,111\,010_2 = 221\,0122_3 = 31\,132_5$ б) $1\,010\,111\,000\,010_2 = 10\,211\,012_3 = 42\,121_5$; в) 2061_7; г) $1\,653\,212_7$; д) $55\,173_8$; е) $42\,167_8$.
6.11. а) 4; б) 5; в) 9; г) 9; д) 5; е) 9; є) 7; ж) 6; з) 5.
6.12. а) 5; б) 8; в) 6; г) 7; д) 7; е) 7; є) 7; ж) 9; з) 6; к) будь-яка основа g, $g \geqslant 2$.
6.14. а) $\underbrace{(100\ldots01)}_{2^k-1}{}_2$; б) $\underbrace{(11\ldots11}_{p}\underbrace{00\ldots00)}_{p-1}{}_2$.
6.15. $x = 2$, $y = 4$.
6.16. а) $7243 \cdot 29 = 210\,047$.
6.17. 153 846.
6.18. $x_1 = 0$, $y_1 = 8$; $x_2 = 8$, $y_2 = 0$.
6.19. 361.
6.21. $(xyz)_{10} = 150$, $g = 15$.
6.22. $63_{10} = 77_8 = 333_4 = 111\,111_2$.

Розділ II

§ 7

7.1. Усі множини, крім множин з) і м). Усі кільця з одиницями. Кільця б), г), е), ж) містять одиницю при $m = \pm 1$. Дільники одиниці: а) 1, —1; б) 1, —1 при $m = \pm 1$; в) $\pm(3+2\sqrt{2})^n$, де $n \in \mathbf{Z}$; д) 1, —1, i, $-i$; е) 1, —1, i, $-i$ при $m = \pm 1$; є) 1, —1; ж) 1, —1 при $m = \pm 1$; к) 1, —1; л) усі ненульові елементи; н) 1, —1, $\dfrac{1 \pm i\sqrt{3}}{2}$, $\dfrac{-1 \pm i\sqrt{3}}{2}$.

7.4. Усі множини, крім а), є кільцями. Усі кільця, крім є), ж), л), містять одиничний елемент. Дільники одиниці: б) такі матриці A, що $|A| = \pm 1$; в), г), д) будь-яка невироджена матриця; є) $\begin{pmatrix}1&0\\0&1\end{pmatrix}$, $\begin{pmatrix}-1&0\\0&-1\end{pmatrix}$; з) будь-яка ненульова матриця; к) $\begin{pmatrix}1&0\\0&1\end{pmatrix}$ і $\begin{pmatrix}-1&0\\0&-1\end{pmatrix}$; м) будь-яка ненульова матриця;

н) будь-яка ненульова матриця. Дільники нуля мають б) — е), це вироджені ненульові матриці. Комутативними є кільця є) — н).

7.5. Усі множини є кільцями. Всі кільця, крім б) — д), є комутативними і містять одиницю. Дільники одиниці: а) $\begin{pmatrix}1&0\\0&1\end{pmatrix}$, $\begin{pmatrix}-1&0\\0&-1\end{pmatrix}$, $\begin{pmatrix}\frac12&-\frac32\\\frac12&\frac12\end{pmatrix}$, $\begin{pmatrix}\frac12&\frac32\\-\frac12&\frac12\end{pmatrix}$, $\begin{pmatrix}-\frac12&-\frac32\\\frac12&-\frac12\end{pmatrix}$, $\begin{pmatrix}-\frac12&\frac32\\-\frac12&-\frac12\end{pmatrix}$; е) будь-яка ненульова матриця; є) $\begin{pmatrix}1&0\\0&1\end{pmatrix}$ і $\begin{pmatrix}-1&0\\0&-1\end{pmatrix}$; ж) $\begin{pmatrix}1&0\\0&1\end{pmatrix}$, $\begin{pmatrix}-1&0\\0&-1\end{pmatrix}$, $\begin{pmatrix}-1&0\\0&1\end{pmatrix}$, $\begin{pmatrix}1&0\\0&-1\end{pmatrix}$; з) $\begin{pmatrix}1&b\\0&1\end{pmatrix}$ або $\begin{pmatrix}-1&b\\0&-1\end{pmatrix}$, де b — довільне ціле число; к) матриці виду $\begin{pmatrix}1&b&c\\0&1&b\\0&0&1\end{pmatrix}$, $\begin{pmatrix}-1&b&c\\0&-1&b\\0&0&-1\end{pmatrix}$. Дільники нуля: а) немає; б) — д) усі ненульові матриці; е) немає; є) матриці виду $\begin{pmatrix}a&a\\a&a\end{pmatrix}$ і $\begin{pmatrix}a&-a\\-a&a\end{pmatrix}$, де $a \neq 0$; ж) матриці виду $\begin{pmatrix}a&0\\0&0\end{pmatrix}$ і $\begin{pmatrix}0&0\\0&b\end{pmatrix}$, де $a,\ b \neq 0$; з) довільна матриця виду $\begin{pmatrix}0&b\\0&0\end{pmatrix}$, $b \neq 0$; к) матриці виду

$$\begin{pmatrix}0&b&c\\0&0&b\\0&0&0\end{pmatrix}, \text{ де } b^2+c^2 \neq 0.$$

7.6. Кільцем є тільки а).
7.7. Не утворюють кільце множини з пп. б), д). Усі кільця комутативні. Дільники одиниці: а) усі елементи (одиницею в цьому кільці є пара (0, 0); в) немає одиниці; г) (1, 1), (1, —1), (—1, 1), (—1, —1) (одиницею тут є (1, 1); е) — ж) (1, 0), (—1, 0); (одиниця тут (1, 0)). Дільники нуля: а) усі пари, крім нульової (1, 1) і одиничної (0, 0); в) усі пари, крім нульової (0, 0); г) $(a,\ 0)$, $(0,\ b)$, де $a,\ b \neq 0$; е) $(a,\ a)$, $(a,\ -a)$, де $a \neq 0$; є), ж) дільників нуля немає.

7.10. Областями цілісності є *7.1*: а), б) при $m = 1$; в), г) при $m = 1$; д), е) при $m = 1$; є), ж) при $m = 1$; к), л), н); *7.4*: є), з), к), м), н); *7.5*: а), е); *7.7*: є), ж). Полями є *7.1*: л); *7.4*: з), м), н); *7.5*: е).
7.11. Дільниками нуля є вирази виду $a + ae$, $a \neq 0$.
7.12. Дільниками нуля є вирази виду be, $b \neq 0$.

§ 8

8.1. а) Двосторонні ідеали; б) двосторонній ідеал; в) лівий ідеал; г) правий ідеал; д) двосторонній ідеал; е) двосторонній ідеал; є) двосторонній ідеал; ж) двосторонній ідеал; з) двосторонній ідеал; к) двосторонній ідеал; л) двосторонній ідеал.
8.2. а) Правий ідеал; б) правий ідеал; в) лівий ідеал; г) двосторонній ідеал; д) не є ідеалом при $a \neq 0$; е) не є ідеалом при $a \neq 0$ і $b \neq 0$; є) двосторонній ідеал; ж) не є ідеалом при $a \neq 0$; з) не є ідеалом при $a \neq 0$.
8.5. а) $\langle 1 \rangle = \mathbf{Z}$; б) $\langle 6 \rangle$; в) $\langle 6 \rangle$; г) $\langle 3 \rangle$; д) $\langle 6 \rangle$; е) $\langle 18 \rangle$; є) $\langle 2 \rangle$; ж) $\langle 20 \rangle$; з) $\langle 40 \rangle$; к) $\langle 1 \rangle = \mathbf{Z}$; л) $\langle 35 \rangle$; м) $\langle 35 \rangle$.
8.8. а) $\langle 1 \rangle = \mathbf{Z}$; б) $\langle 2 \rangle$; в) $\langle 3 \rangle$; г) $\langle 1 \rangle = \mathbf{Z}$; д) $\langle 2 \rangle$; е) $\langle 1 \rangle = \mathbf{Z}$; є) $\langle 2 \rangle$.

8.10. Використати задачу 8.3, в); $a \equiv b \pmod 0$ тоді і тільки тоді, коли числа a і b дорівнюють одне одному.

8.11. Для фактор-кільця $Z_2 = Z/\langle 2\rangle$ маємо табл. 47, 48. Дільників нуля в Z_2 немає; $\bar{1}^{-1} = \bar{1}$.

Таблиця 47

+	$\bar{0}$	$\bar{1}$
$\bar{0}$	$\bar{0}$	$\bar{1}$
$\bar{1}$	$\bar{1}$	$\bar{0}$

Таблиця 48

×	$\bar{0}$	$\bar{1}$
$\bar{0}$	$\bar{0}$	$\bar{0}$
$\bar{1}$	$\bar{0}$	$\bar{0}$

Для Z_3 — табл. 49, 50.

Таблиця 49

+	$\bar{0}$	$\bar{1}$	$\bar{2}$
$\bar{0}$	$\bar{0}$	$\bar{1}$	$\bar{2}$
$\bar{1}$	$\bar{1}$	$\bar{2}$	$\bar{0}$
$\bar{2}$	$\bar{2}$	$\bar{0}$	$\bar{1}$

Таблиця 50

×	$\bar{0}$	$\bar{1}$	$\bar{2}$
$\bar{0}$	$\bar{0}$	$\bar{0}$	$\bar{0}$
$\bar{1}$	$\bar{0}$	$\bar{1}$	$\bar{2}$
$\bar{2}$	$\bar{0}$	$\bar{2}$	$\bar{1}$

Дільників нуля в Z_3 немає; $\bar{1}^{-1} = \bar{1}$; $\bar{2}^{-1} = \bar{2}$.

Для Z_4 — табл. 51, 52.

Таблиця 51

+	$\bar{0}$	$\bar{1}$	$\bar{2}$	$\bar{3}$
$\bar{0}$	$\bar{0}$	$\bar{1}$	$\bar{2}$	$\bar{3}$
$\bar{1}$	$\bar{1}$	$\bar{2}$	$\bar{3}$	$\bar{0}$
$\bar{2}$	$\bar{2}$	$\bar{3}$	$\bar{0}$	$\bar{1}$
$\bar{3}$	$\bar{3}$	$\bar{0}$	$\bar{1}$	$\bar{2}$

Таблиця 52

×	$\bar{0}$	$\bar{1}$	$\bar{2}$	$\bar{3}$
$\bar{0}$	$\bar{0}$	$\bar{0}$	$\bar{0}$	$\bar{0}$
$\bar{1}$	$\bar{0}$	$\bar{1}$	$\bar{2}$	$\bar{3}$
$\bar{2}$	$\bar{0}$	$\bar{2}$	$\bar{0}$	$\bar{2}$
$\bar{3}$	$\bar{0}$	$\bar{3}$	$\bar{2}$	$\bar{1}$

Дільник нуля $\bar{2}$; $\bar{1}^{-1} = \bar{1}$, $\bar{3}^{-1} = \bar{3}$.

Для Z_5 — табл. 53, 54.

Таблиця 53

+	$\bar{0}$	$\bar{1}$	$\bar{2}$	$\bar{3}$	$\bar{4}$
$\bar{0}$	$\bar{0}$	$\bar{1}$	$\bar{2}$	$\bar{3}$	$\bar{4}$
$\bar{1}$	$\bar{1}$	$\bar{2}$	$\bar{3}$	$\bar{4}$	$\bar{0}$
$\bar{2}$	$\bar{2}$	$\bar{3}$	$\bar{4}$	$\bar{0}$	$\bar{1}$
$\bar{3}$	$\bar{3}$	$\bar{4}$	$\bar{0}$	$\bar{1}$	$\bar{2}$
$\bar{4}$	$\bar{4}$	$\bar{0}$	$\bar{1}$	$\bar{2}$	$\bar{3}$

Таблиця 54

×	$\bar{0}$	$\bar{1}$	$\bar{2}$	$\bar{3}$	$\bar{4}$
$\bar{0}$	$\bar{0}$	$\bar{0}$	$\bar{0}$	$\bar{0}$	$\bar{0}$
$\bar{1}$	$\bar{0}$	$\bar{1}$	$\bar{2}$	$\bar{3}$	$\bar{4}$
$\bar{2}$	$\bar{0}$	$\bar{2}$	$\bar{4}$	$\bar{1}$	$\bar{3}$
$\bar{3}$	$\bar{0}$	$\bar{3}$	$\bar{1}$	$\bar{4}$	$\bar{2}$
$\bar{4}$	$\bar{0}$	$\bar{4}$	$\bar{3}$	$\bar{2}$	$\bar{1}$

Дільників нуля в Z_5 немає; $\bar{1}^{-1} = \bar{1}$, $\bar{2}^{-1} = \bar{3}$, $\bar{3}^{-1} = \bar{2}$, $\bar{4}^{-1} = \bar{4}$.

8.12. Z_2, Z_3 і Z_5.

8.14. а) $\bar{2}$, $\bar{4}$, $\bar{6}$; б) $\bar{3}$, $\bar{6}$; в) $\bar{2}$, $\bar{4}$, $\bar{5}$, $\bar{6}$, $\bar{8}$; г) $\bar{2}$, $\bar{3}$, $\bar{4}$, $\bar{6}$, $\bar{8}$, $\bar{9}$, $\bar{10}$; д) $\bar{2}$, $\bar{4}$, $\bar{6}$, $\bar{7}$, $\bar{8}$, $\bar{10}$, $\bar{12}$; е) $\bar{3}$, $\bar{5}$, $\bar{6}$, $\bar{9}$, $\bar{10}$, $\bar{12}$; є) $\bar{2}$, $\bar{4}$, $\bar{6}$, $\bar{8}$, $\bar{10}$, $\bar{12}$, $\bar{14}$.

8.15. а) $\bar{1}^{-1} = \bar{1}$, $\bar{2}^{-1} = \bar{4}$, $\bar{3}^{-1} = \bar{5}$, $\bar{4}^{-1} = \bar{2}$, $\bar{5}^{-1} = \bar{3}$, $\bar{6}^{-1} = \bar{6}$; б) $\bar{1}^{-1} = \bar{1}$, $\bar{3}^{-1} = \bar{3}$, $\bar{5}^{-1} = \bar{5}$, $\bar{7}^{-1} = \bar{7}$; в) $\bar{1}^{-1} = \bar{1}$, $\bar{2}^{-1} = \bar{5}$, $\bar{4}^{-1} = \bar{7}$, $\bar{5}^{-1} = \bar{2}$, $\bar{7}^{-1} = \bar{4}$, $\bar{8}^{-1} = \bar{8}$; г) $\bar{1}^{-1} = \bar{1}$, $\bar{3}^{-1} = \bar{7}$, $\bar{7}^{-1} = \bar{3}$, $\bar{9}^{-1} = \bar{9}$; д) $\bar{1}^{-1} = \bar{1}$, $\bar{2}^{-1} = \bar{6}$, $\bar{3}^{-1} = \bar{4}$, $\bar{4}^{-1} = 3$, $\bar{5}^{-1} = \bar{9}$, $\bar{6}^{-1} = \bar{2}$, $\bar{7}^{-1} = \bar{8}$, $\bar{8}^{-1} = \bar{7}$, $\bar{9}^{-1} = \bar{5}$, $\bar{10}^{-1} = \bar{10}$; е) $\bar{1}^{-1} = \bar{1}$; $\bar{5}^{-1} = \bar{5}$, $\bar{7}^{-1} = \bar{7}$, $\bar{11}^{-1} = \bar{11}$; є) $\bar{1}^{-1} = \bar{1}$, $\bar{2}^{-1} = \bar{7}$, $\bar{3}^{-1} = \bar{9}$, $\bar{4}^{-1} = \bar{10}$, $\bar{5}^{-1} = \bar{8}$, $\bar{6}^{-1} = \bar{11}$, $\bar{7}^{-1} = \bar{2}$, $\bar{8}^{-1} = \bar{5}$, $\bar{9}^{-1} = \bar{3}$, $\bar{10}^{-1} = \bar{4}$, $\bar{11}^{-1} = \bar{6}$, $\bar{12}^{-1} = \bar{12}$; ж) $\bar{1}^{-1} = \bar{1}$, $\bar{3}^{-1} = \bar{5}$, $\bar{5}^{-1} = \bar{3}$, $\bar{9}^{-1} = \bar{11}$, $\bar{11}^{-1} = \bar{9}$, $\bar{13}^{-1} = \bar{13}$; з) $\bar{1}^{-1} = \bar{1}$, $\bar{2}^{-1} = \bar{8}$, $\bar{4}^{-1} = \bar{4}$, $\bar{7}^{-1} = \bar{13}$, $\bar{8}^{-1} = \bar{2}$, $\bar{11}^{-1} = \bar{11}$, $\bar{13}^{-1} = \bar{7}$, $\bar{14}^{-1} = \bar{14}$; к) $\bar{1}^{-1} = \bar{1}$, $\bar{3}^{-1} = \bar{11}$, $\bar{5}^{-1} = \bar{13}$, $\bar{7}^{-1} = \bar{7}$, $\bar{9}^{-1} = \bar{9}$, $\bar{11}^{-1} = \bar{3}$, $\bar{13}^{-1} = \bar{5}$, $\bar{15}^{-1} = \bar{15}$.

8.16. а) $Z[i]/\langle 2\rangle = \{\bar{0}, \bar{1}, \bar{i}, \overline{1+i}\}$, де $\bar{0} = 0 + \langle 2\rangle = \{2k + 2si \mid k, s \in \mathbf{Z}\}$, $\bar{1} = 1 + \langle 2\rangle = \{2k + 1 + 2si \mid k, s \in \mathbf{Z}\}$, $\bar{i} = i + \langle 2\rangle = \{2k + (2s + 1)i \mid k, s \in \mathbf{Z}\}$, $\overline{1+i} = 1 + i + \langle 2\rangle = \{2k + 1 + (2s + 1)i \mid k, s \in \mathbf{Z}\}$. Таблиці додавання і множення (табл. 55, 56).

Таблиця 55

+	$\bar{0}$	$\bar{1}$	$\bar{i}$	$\overline{1+i}$
$\bar{0}$	$\bar{0}$	$\bar{1}$	$\bar{i}$	$\overline{1+i}$
$\bar{1}$	$\bar{1}$	$\bar{0}$	$\overline{1+i}$	$\bar{i}$
$\bar{i}$	$\bar{i}$	$\overline{1+i}$	$\bar{0}$	$\bar{1}$
$\overline{1+i}$	$\overline{1+i}$	$\bar{i}$	$\bar{1}$	$\bar{0}$

Таблиця 56

×	$\bar{0}$	$\bar{1}$	$\bar{i}$	$\overline{1+i}$
$\bar{0}$	$\bar{0}$	$\bar{0}$	$\bar{0}$	$\bar{0}$
$\bar{1}$	$\bar{0}$	$\bar{1}$	$\bar{i}$	$\overline{1+i}$
$\bar{i}$	$\bar{0}$	$\bar{i}$	$\bar{1}$	$\overline{1+i}$
$\overline{1+i}$	$\bar{0}$	$\overline{1+i}$	$\overline{1+i}$	$\bar{0}$

Дільник нуля $\overline{1+i}$; $\bar{1}^{-1} = \bar{1}$, $\bar{i}^{-1} = \bar{i}$. б) $Z[i]/\langle 3\rangle = \{\bar{0}, \bar{1}, \bar{2}, \bar{i}, \overline{2i}, \overline{1+i}, \overline{1+2i}, \overline{2+i}, \overline{2+2i}\}$, де

$$\bar{0} = 0 + \langle 3\rangle = \{3k + 3si \mid k, s \in \mathbf{Z}\},$$
$$\bar{1} = 1 + \langle 3\rangle = \{3k + 1 + 3si \mid k, s \in \mathbf{Z}\},$$
$$\bar{2} = 2 + \langle 3\rangle = \{3k + 2 + 3si \mid k, s \in \mathbf{Z}\},$$
$$\bar{i} = i + \langle 3\rangle = \{3k + (3s + 1)i \mid k, s \in \mathbf{Z}\},$$
$$\overline{2i} = 2i + \langle 3\rangle = \{3k + (3s + 2)i \mid k, s \in \mathbf{Z}\},$$
$$\overline{1+i} = 1 + i + \langle 3\rangle = \{3k + 1 + (3s + 1)i \mid k, s \in \mathbf{Z}\},$$
$$\overline{1+2i} = 1 + 2i + \langle 3\rangle = \{3k + 1 + (3s + 2)i \mid k, s \in \mathbf{Z}\},$$
$$\overline{2+i} = 2 + i + \langle 3\rangle = \{3k + 2 + (3s + 1)i \mid k, s \in \mathbf{Z}\},$$
$$\overline{2+2i} = 2 + 2i + \langle 3\rangle = \{3k + 2 + (3s + 2)i \mid k, s \in \mathbf{Z}\}.$$

Таблиці додавання і множення для елементів $Z[i]/\langle 3\rangle$ (табл. 57, 58).

Таблиця 57

$+$	$\bar{0}$	$\bar{1}$	$\bar{2}$	$\bar{i}$	$\overline{2i}$	$\overline{1+i}$	$\overline{1+2i}$	$\overline{2+i}$	$\overline{2+2i}$
$\bar{0}$	$\bar{0}$	$\bar{1}$	$\bar{2}$	$\bar{i}$	$\overline{2i}$	$\overline{1+i}$	$\overline{1+2i}$	$\overline{2+i}$	$\overline{2+2i}$
$\bar{1}$	$\bar{1}$	$\bar{2}$	$\bar{0}$	$\overline{1+i}$	$\overline{1+2i}$	$\overline{2+i}$	$\overline{2+2i}$	$\bar{i}$	$\overline{2i}$
$\bar{2}$	$\bar{2}$	$\bar{0}$	$\bar{1}$	$\overline{2+i}$	$\overline{2+2i}$	$\bar{i}$	$\overline{2i}$	$\overline{1+i}$	$\overline{1+2i}$
$\bar{i}$	$\bar{i}$	$\overline{1+i}$	$\overline{2+i}$	$\overline{2i}$	$\bar{0}$	$\overline{1+2i}$	$\bar{1}$	$\overline{2+2i}$	$\bar{2}$
$\overline{2i}$	$\overline{2i}$	$\overline{1+2i}$	$\overline{2+2i}$	$\bar{0}$	$\bar{i}$	$\bar{1}$	$\overline{1+i}$	$\bar{2}$	$\overline{2+i}$
$\overline{1+i}$	$\overline{1+i}$	$\overline{2+i}$	$\bar{i}$	$\overline{1+2i}$	$\bar{1}$	$\overline{2+2i}$	$\bar{2}$	$\overline{2i}$	$\bar{0}$
$\overline{1+2i}$	$\overline{1+2i}$	$\overline{2+2i}$	$\overline{2i}$	$\bar{1}$	$\overline{1+i}$	$\bar{2}$	$\overline{2+i}$	$\bar{0}$	$\bar{i}$
$\overline{2+i}$	$\overline{2+i}$	$\bar{i}$	$\overline{1+i}$	$\overline{2+2i}$	$\bar{2}$	$\overline{2i}$	$\bar{0}$	$\overline{1+2i}$	$\bar{1}$
$\overline{2+2i}$	$\overline{2+2i}$	$\overline{2i}$	$\overline{1+2i}$	$\bar{2}$	$\overline{2+i}$	$\bar{0}$	$\bar{i}$	$\bar{1}$	$\overline{1+i}$

Таблиця 58

$\times$	$\bar{0}$	$\bar{1}$	$\bar{2}$	$\bar{i}$	$\overline{2i}$	$\overline{1+i}$	$\overline{1+2i}$	$\overline{2+i}$	$\overline{2+2i}$
$\bar{0}$	$\bar{0}$	$\bar{0}$	$\bar{0}$	$\bar{0}$	$\bar{0}$	$\bar{0}$	$\bar{0}$	$\bar{0}$	$\bar{0}$
$\bar{1}$	$\bar{0}$	$\bar{1}$	$\bar{2}$	$\bar{i}$	$\overline{2i}$	$\overline{1+i}$	$\overline{1+2i}$	$\overline{2+i}$	$\overline{2+2i}$
$\bar{2}$	$\bar{0}$	$\bar{2}$	$\bar{1}$	$\overline{2i}$	$\bar{i}$	$\overline{2+2i}$	$\overline{2+i}$	$\overline{1+2i}$	$\overline{1+i}$
$\bar{i}$	$\bar{0}$	$\bar{i}$	$\overline{2i}$	$\bar{2}$	$\bar{1}$	$\overline{2+i}$	$\overline{1+i}$	$\overline{2+2i}$	$\overline{1+2i}$
$\overline{2i}$	$\bar{0}$	$\overline{2i}$	$\bar{i}$	$\bar{1}$	$\bar{2}$	$\overline{1+2i}$	$\overline{2+2i}$	$\overline{1+i}$	$\overline{2+i}$
$\overline{1+i}$	$\bar{0}$	$\overline{1+i}$	$\overline{2+2i}$	$\overline{2+i}$	$\overline{1+2i}$	$\overline{2i}$	$\bar{2}$	$\bar{1}$	$\bar{i}$
$\overline{1+2i}$	$\bar{0}$	$\overline{1+2i}$	$\overline{2+i}$	$\overline{1+i}$	$\overline{2+2i}$	$\bar{2}$	$\bar{i}$	$\overline{2i}$	$\bar{1}$
$\overline{2+i}$	$\bar{0}$	$\overline{2+i}$	$\overline{1+2i}$	$\overline{2+2i}$	$\overline{1+i}$	$\bar{1}$	$\overline{2i}$	$\bar{i}$	$\bar{2}$
$\overline{2+2i}$	$\bar{0}$	$\overline{2+2i}$	$\overline{1+i}$	$\overline{1+2i}$	$\overline{2+i}$	$\bar{i}$	$\bar{1}$	$\bar{2}$	$\overline{2i}$

Дільників нуля немає; $\bar{1}^{-1}=\bar{1}$, $\bar{2}^{-1}=\bar{2}$, $\bar{i}^{-1}=\overline{2i}$, $\overline{2i}^{-1}=\bar{i}$, $\overline{1+i}^{-1}=\overline{2+i}$, $\overline{1+2i}^{-1}=\overline{2+2i}$, $\overline{2+i}^{-1}=\overline{1+i}$, $\overline{2+2i}^{-1}=\overline{1+2i}$; в) $\langle 2i\rangle=\langle 2\rangle$; г) $\langle -3i\rangle=\langle 3\rangle$; д) $\langle i\rangle=Z[i]$ і тому $Z[i]/\langle i\rangle=\{Z[i]\}=\{\bar{0}\}$.

8.17. а) 16 елементів; дільники нуля; $\bar{2}$, $\overline{2i}$, $\overline{1+i}$, $\overline{2+2i}$, $\overline{3+i}$, $\overline{3+3i}$; $\bar{i}^{-1}=\overline{3i}$, $\overline{3i}^{-1}=\bar{i}$, $\overline{1+2i}^{-1}=\overline{1+2i}$;

б) 25 елементів; дільники нуля: $\overline{1+2i}$, $\overline{1+3i}$, $\overline{2+i}$, $\overline{2+4i}$, $\overline{3+i}$, $\overline{3+4i}$, $\overline{4+2i}$, $\overline{4+3i}$; $\bar{2}^{-1}=\bar{3}$, $\overline{4i}^{-1}=\bar{i}$, $\overline{3+2i}^{-1}=\overline{1+i}$;

в) 36 елементів; дільники нуля; $\bar{2}$, $\bar{3}$, $\bar{4}$, $\overline{2i}$, $\overline{3i}$, $\overline{4i}$, $\overline{1+i}$, $\overline{1+3i}$, $\overline{1+5i}$, $\overline{2+2i}$, $\overline{2+4i}$, $\overline{3+i}$, $\overline{3+3i}$, $\overline{3+5i}$, $\overline{4+2i}$, $\overline{4+4i}$, $\overline{5+i}$, $\overline{5+3i}$, $\overline{5+5i}$; $\overline{2+5i}^{-1}=\overline{2+3i}$, $\overline{4+i}^{-1}=\overline{2+i}$.

8.18. $Z[\sqrt{3}]/2Z[\sqrt{3}]=\{\bar{0},\ \bar{1},\ \overline{\sqrt{3}},\ \overline{1+\sqrt{3}}\}$, де $\bar{0}=0+2Z[\sqrt{3}]=\{2k+2s\sqrt{3}\mid k,\ s\in\mathbf{Z}\}$, $\bar{1}=1+2Z[\sqrt{3}]=\{2k+1+2s\sqrt{3}\mid k,\ s\in\mathbf{Z}\}$, $\overline{\sqrt{3}}=\sqrt{3}+2Z[\sqrt{3}]=\{2k+(2s+1)\sqrt{3}\mid k,\ s\in\mathbf{Z}\}$, $\overline{1+3}=1+\sqrt{3}+2Z[\sqrt{3}]=\{2k+1+(2s+1)\sqrt{3}\mid k,\ s\in\mathbf{Z}\}$.

Таблиці додавання і множення (табл. 59, 60).

Дільник нуля $\overline{1+\sqrt{3}}$; $\bar{1}^{-1}=\bar{1}$, $\overline{\sqrt{3}}^{-1}=\overline{\sqrt{3}}$.

Таблиця 59

$+$	$\bar{0}$	$\bar{1}$	$\overline{\sqrt{3}}$	$\overline{1+\sqrt{3}}$
$\bar{0}$	$\bar{0}$	$\bar{1}$	$\overline{\sqrt{3}}$	$\overline{1+\sqrt{3}}$
$\bar{1}$	$\bar{1}$	$\bar{0}$	$\overline{1+\sqrt{3}}$	$\overline{\sqrt{3}}$
$\overline{\sqrt{3}}$	$\overline{\sqrt{3}}$	$\overline{1+\sqrt{3}}$	$\bar{0}$	$\bar{1}$
$\overline{1+\sqrt{3}}$	$\overline{1+\sqrt{3}}$	$\overline{\sqrt{3}}$	$\bar{1}$	$\bar{0}$

Таблиця 60

$\times$	$\bar{0}$	$\bar{1}$	$\overline{\sqrt{3}}$	$\overline{1+\sqrt{3}}$
$\bar{0}$	$\bar{0}$	$\bar{0}$	$\bar{0}$	$\bar{0}$
$\bar{1}$	$\bar{0}$	$\bar{1}$	$\overline{\sqrt{3}}$	$\overline{1+\sqrt{3}}$
$\overline{\sqrt{3}}$	$\bar{0}$	$\overline{\sqrt{3}}$	$\bar{1}$	$\overline{1+\sqrt{3}}$
$\overline{1+\sqrt{3}}$	$\bar{0}$	$\overline{1+\sqrt{3}}$	$\overline{1+\sqrt{3}}$	$\bar{0}$

§ 9

9.3. Оскільки в довільному полі P є тільки два ідеали $\{0\}$ і P, а ядро $\operatorname{Ker}\varphi$ гомоморфізму φ двох полів P і P_1 повинно бути ідеалом в полі P, то при гомоморфному відображенні поля P на поле P_1 ці поля ізоморфні.

Зауваження. Якщо розглядати відображення поля в поле, то можливий ще очевидний гомоморфізм поля P в поле P_1:

$\psi(a)=0_1$ для будь-якого $a\in P$.

9.4. Використати задачу 8.4, з).

9.6. $\operatorname{Ker}\varphi=\left\{\begin{pmatrix}a & a\\ a & a\end{pmatrix}\,\middle|\, a\in\mathbf{Z}\right\}$.

9.7. $\operatorname{Ker}\varphi=3\mathbf{Z}$.

9.8. $\operatorname{Ker}\varphi=\left\{\begin{pmatrix}0 & 0\\ 0 & b\end{pmatrix}\,\middle|\, b\in\mathbf{Q}\right\}$.

9.9. $\operatorname{Ker}\varphi=\{f\in K\mid f(1)=0\}$.

9.12. 1) Кільце класів лишків Z_4; 2) поле із задачі 7.3, г); 3) 0, 1, a, $a+1$ при $1+1=0$, $a^2=a$, $a(a+1)=0$, $(a+1)^2=a+1$; 4) 0, 1, a, $a+1$ при $1+1=0$, $a^2=0$, $(a+1)^2=1$, $a(a+1)=a$. Усі кільця комутативні.

9.13. Кільце складається з елементів $\{ma\}$; $m=0,\ 1,\ \ldots,\ pq-1$. Елемент a можна вибрати так, що виконуватиметься один з чотирьох випадків: а) $a^2=a$ (кільце, ізоморфне кільцю класів лишків; 2) $a^2=0$ (нульове множення); 3) $a^2=pa$; 4) $a^2=qa$.

§ 10

10.14. а) 1; б) 10; в) 3; г) 15; д) $((m, n, s), (k, t, f))$; е) $[(m, n, s), (k, t, f)]$.

10.15. а) $(4+3i, 3+i) \sim 1+2i$, $[4+3i, 3+i] \sim \frac{(4+i)(3+i)}{1-2i} \sim 7-i$;
б) $(6+i, 5+7i) \sim 6+i$, $[6+i, 5+7i] \sim 5+7i$;
в) $(8+12i, 10+4i) \sim 2$; $[8+12i, 10+4i] \sim 16+76i$;
г) $(5-5i, 7-i) \sim 3+i$; $[5-5i, 7-i] \sim -5+15i$;
д) $(11-3i, 3+7i) \sim 1+i$, $[11-3i, 3+7i] \sim 61+7i$;
е) $(5+6i, 6+5i) \sim 1$; $[5+6i, 6+5i] \sim 61$;
є) $(7+3i, 5+2i) \sim 1$; $[7+3i, 5+2i] \sim 29+29i$.

10.16. а) $(7+\sqrt{2}, -5-5\sqrt{2}) \sim 1$; $[7+\sqrt{2}, -5-5\sqrt{2}] \sim 45+40\sqrt{2}$; б) $(5+2\sqrt{2}, 6-\sqrt{2}) \sim 5+2\sqrt{2}$; $[5+2\sqrt{2}, 6-2\sqrt{2}] \sim 26+7\sqrt{2}$.

10.17. Для задачі 10.15: а) $d = 1+2i = (4+3i)\cdot 1 + (3+i)(-1)$; б) $d = 6+i = (6+i)\cdot 1 + (5+7i)\cdot 0$; в) $d = 2 = (8+12i)(-1-3i) + (10+4i)\times(-1+4i)$;
г) $d = 3+i = (7-i)(-1) + (5-5i)(1+i)$;
д) $d = 1+i = (11-3i)(1-2i) + (3+7i)(1+i)$;
е) $d = 1 = (5+6i)(-6) + (6+5i)(6+i)$;
є) $d = 1 = (7+3i)(-2) + (5+2i)\cdot 3$.

Для задачі 10.16: а) $d = 1 = (7+\sqrt{2})(-4+2\sqrt{2}) + (-5-5\sqrt{2})(9-7\sqrt{2})$; б) $d = 5+2\sqrt{2} = (5+2\sqrt{2})\cdot 1 + (6-\sqrt{2})\cdot 0$.

10.18. а) Нехай z — ціле гауссове число і $\mathrm{Nr}(z) = p$ — просте число. Якщо $z = xy$, де $x, y \in Z[i]$, то $p = \mathrm{Nr}(z) = \mathrm{Nr}(x)\cdot\mathrm{Nr}(y)$. Оскільки $\mathrm{Nr}(x)$ і $\mathrm{Nr}(y)$ — натуральні числа і p — просте число, то або $\mathrm{Nr}(x) = 1$, або $\mathrm{Nr}(y) = 1$, тобто одне з чисел x або y є дільником одиниці в $Z[i]$. Це означає, що z є просте ціле гауссове число.

10.19. Показати, що $2 = 2^{\frac{1}{2}}2^{\frac{1}{2}} = 2^{\frac{1}{2}}2^{\frac{1}{4}}2^{\frac{1}{4}} = 2^{\frac{1}{2}}2^{\frac{1}{4}}2^{\frac{1}{8}}2^{\frac{1}{8}} = \ldots$

10.20. Знайти елементи, які неоднозначно розкладаються на прості множники, довівши простоту множників та їхню неасоційованість: а) $4 = 2\cdot 2 = (1+\sqrt{3}i)(1-\sqrt{3}i)$; б) $6 = 2\cdot 3 = (1+\sqrt{5}i)(1-\sqrt{5}i)$; в) $18 = 2\cdot 3\cdot 3 = (1+\sqrt{17}i)(1-\sqrt{17}i)$; г) $20 = 2\cdot 2\cdot 5 = (1+\sqrt{19}i)(1-\sqrt{19}i)$.

10.21. Використати норму $\mathrm{Nr}(a+b\sqrt{3}i) = a^2+3b^2$.

10.22. Використати норму $\mathrm{Nr}(a+bi) = a^2+b^2$.

10.24. а) $5 = (2+i)(2-i)$; б) $5-5i = (1-i)(2-i)(2+i)$; в) $3+i = (1+i)(2-i)$; г) $-90+180i = 3^2(1+i)^2(2+i)^2(2-i)$; д) $-182-126i = 7(1+i)^3(2+i)^3$; е) $7+8i = 7+8i$; є) $41 = (4+5i)(4-5i)$.

Розділ III

§ 11

11.1. а) 216 і 21, 134 і 214; б) 135 і 225, 106 і 181, 167 і 452; в) 217 і 241.

11.2. а) 137, 620; б) 201; в) 234, 634.

11.4. а) $-38 \equiv -3 \pmod 7$; б) $53 \equiv 5 \pmod 8$; в) $a+2 \equiv 0 \pmod 5$; г) $a^2 - b^2 \equiv 0 \pmod{(a-b)}$; д) $-73 \equiv r \pmod 8$; $0 \leqslant r < 8$; е) $20 \equiv 389 \pmod{41}$; є) $219 \not\equiv 129 \pmod 7$.

11.5. а) $n \equiv 0 \pmod 2$; б) $n \equiv 1 \pmod 2$; в) $n \equiv 1 \pmod 4$; г) $n \equiv 3 \pmod 5$; д) $n \equiv -2 \pmod 7$; е) $n \equiv -3 \pmod 8$.

11.6. а) — д) Показати, що в заданій конгруенції різниця частин ділиться на модуль; е), є) показати, що ліва частина заданої конгруенції ділиться на кожен множник модуля; ж), з) показати, що обидві частини заданої конгруенції закінчуються однаковими цифрами; к) оскільки $11\cdot 31 - 1 = 340 = 5\cdot 68$ і $2^5 \equiv -1 \pmod{11}$, то $(2^5)^{68} = 2^{340} = 2^{11\cdot 31-1} \equiv 1 \pmod{11}$. Оскільки $2^5 \equiv 1 \pmod{31}$, то $(2^5)^{68} = 2^{11\cdot 31-1} \equiv 1 \pmod{31}$. Тоді $2^{11\cdot 31-1} \equiv 1 \pmod{11\cdot 31}$. Звідси $2^{11\cdot 31} \equiv 2 \pmod{11\cdot 31}$; л) $3^{14} = (3^3)^4 3^2 = 27^4\cdot 3^2 \equiv (-2)^4 3^2 = 144 \equiv -1 \pmod{29}$.

11.7. а) — з), м) Показати, що обидві частини заданої конгруенції мають з модулем різні найбільші спільні дільники.

11.8. а) Використати формулу розкладу бінома:

$$(a+b)^p = a^p + C_p^1 a^{p-1}b + C_p^2 a^{p-2}b^2 + \ldots + C_p^{p-1}ab^{p-1} + b^p.$$

У правій частині цієї формули всі члени, крім a^p і b^p, діляться на p.

б) $C_p^k = \frac{(p-1)(p-2)\ldots(p-k)}{1\cdot 2\ldots k}$. Тоді $p-1 \equiv -1 \pmod p$; $p-2 \equiv -2 \pmod p$, $\ldots$, $p-k \equiv -k \pmod p$.

Помножаючи почленно ці конгруенції, дістаємо:

$$(p-1)(p-2)\ldots(p-k) \equiv (-1)^k 1\cdot 2\ldots k \pmod p.$$

Оскільки $k!$ і p взаємно прості і кожна частина конгруенції ділиться на $k!$, то $\frac{(p-1)(p-2)\ldots(p-k)}{k!} \equiv (-1)^k \pmod p$;

г) Оскільки $a = b + p^n t$, $t \in \mathbf{Z}$, то при піднесенні цієї рівності до степеня p дістанемо $a^p = b^p + p^{n+1}q$, $q \in \mathbf{Z}$, тобто $a^p \equiv b^p \pmod{p^{n+1}}$;

д) З чисел $1, 2, 3, \ldots, \frac{p-1}{2}, \frac{p+1}{2}, \ldots, p-2, p-1$ складемо $\frac{p-1}{2}$ конгруенцій:

$$1 \equiv -(p-1) \pmod p,$$
$$2 \equiv -(p-2) \pmod p,$$
$$\ldots\ldots\ldots\ldots$$
$$\frac{p-1}{2} \equiv -\frac{p+1}{2} \pmod p.$$

Тепер піднесемо кожну з цих конгруенцій до степеня $2k+1$ і результати додамо; е) з конгруенції $p \equiv p+2 \equiv 1 \pmod 2$ дістаємо конгруенцію $p^{p+2} + (p+2)^p \equiv 0 \pmod 2$, з конгруенції $p \equiv -1 \pmod{p+1}$ і $p+2 \equiv 1 \pmod{p+1}$ маємо $p^{p+2} + (p+2)^p \equiv 0 \pmod{p+1}$. Тоді $p^{p+2} + (p+2)^p \equiv 0 \pmod{2p+2}$;

є) усі задані числа, крім нуля, мають вигляд $\pm\frac{p-n}{2}$, $n = 1, 2, \ldots, p-2$. Конгруенції

$$\pm\frac{p-n}{2} \equiv 0 \pmod p, \quad \frac{p-n_1}{2} \pm \frac{p-n_2}{2} \equiv 0 \pmod p$$

призводять до неправильних конгруенцій

$$n \equiv p \pmod d, \quad n_1 \equiv \pm n_2 \pmod p.$$

11.9. а) 1; б) 1; в) 4; г) 0; д) 1; е) 1); є) 0; ж) 0; з) 1; к) 12; л) 3; м) 1; н) 71. Остача дорівнюватиме 36.

11.10. б) Нехай $11a + 2b \vdots 9$. Тоді $11a + 2b \equiv 0 \pmod 9$. Домножимо цю конгруенцію на 12. Матимемо $132a + 34b \equiv 0 \pmod{19}$. Звідси $18a + 5b \equiv 0 \pmod{19}$, тобто $18a + 5b \vdots 19$.

11.12. Застосувати метод доведення «від супротивного». в) Нехай x_0, y_0, z_0 — розв'язок рівняння $24^x + 36^y = 61^z$. Тоді $24^{x_0} + 36^{y_0} = 61^{z_0}$. Якщо числа рівні, то вони конгруентні за будь-яким модулем. Отже, $(-1)^{x_0} + 1^{y_0} \equiv 1^{z_0} \pmod 5$. Звідси $(-1)^{x_0} \equiv 0 \pmod 5$, що неможливо.

11.14. а) k, l, m — будь-які; б) k, l, m одночасно парні або непарні; в) k, $l+1$, m одночасно парні або непарні.

11.15. а) 2; б) 9; в) 7; г) 3.

11.16. а) 88; б) 67; в) 24; г) 9; д) 27; е) 36; є) оскільки $9^{10} \equiv 1 \pmod{100}$, то $9^{10q+r} \equiv 9^r \pmod{100}$. Оскільки $9^9 \equiv 9 \pmod{10}$, то $9^{9^9} \equiv 9^9 \equiv 89 \pmod{100}$. Шуканими цифрами є 8 і 9; ж) оскільки $7^4 = 2401 \equiv 1 \pmod{100}$, то і $7^{100} \equiv 1 \pmod{100}$, звідки $7^{9^{99}} \equiv 7^{100q+89} \equiv 7^{89} \pmod{100}$. Проте $7^{88} \equiv 1 \pmod{100}$, тому $7^{89} \equiv 7 \pmod{100}$. Отже, шуканими цифрами є 0 і 7.

11.17. а) $2^{25} + 1 = 2^{32} + 1$, $2^{32} = (2^8)^4 = (256^2)^2 = 65536^2 \equiv 154^2 \equiv 23716 \equiv -1 \pmod{641}$. Отже, $2^{32} + 1 \equiv 0 \pmod{641}$. Справді, $2^{32} + 1 = 4\,294\,967\,297 = 641 \cdot 6\,700\,417$;

б) Це твердження рівносильне твердженню, що числа 2^{2^n}, $n = 2, 3, \ldots$ закінчуються цифрою 6. Застосуємо метод математичної індукції. При $k = 2$ маємо $2^{2^2} = 16 \equiv 6 \pmod{10}$. Припустимо, що $2^{2^k} \equiv 6 \pmod{10}$ і доведемо, що $2^{2^{k+1}} \equiv 6 \pmod{10}$. Оскільки $(2^{2^k})^2 = 2^{2 \cdot 2^k} = 2^{2^{k+1}}$, то при піднесенні до квадрата конгруенції $2^{2^k} \equiv 6 \pmod{10}$ дістанемо $2^{2^{k+1}} \equiv 36 \equiv 6 \pmod{10}$, що й треба було довести.

§ 12

12.1. а) 6; б) 27 і -3; в) 8; г) 65 і -2; д) 1; е) 7; є) 14 і -1; ж) 667 і -114; з) 55 і -1; к) 1; л) 14 і -3; м) 501 і -2; н) 37 і -14.

12.2. 0, 1, 2, ..., $m-1$, якщо m — модуль.

12.3. $0, \pm 1, \pm 2, \ldots, \pm\frac{m-1}{2}$, якщо m — непарне число; $0, \pm 1, \pm 2, \ldots, \pm\left(\frac{m}{2}-1\right), \frac{m}{2}$ або $0, \pm 1, \pm 2, \ldots, \pm\left(\frac{m}{2}-1\right), -\frac{m}{2}$, якщо m — парне число.

12.4. 1, 2, ..., m, якщо m — модуль.

12.5 0, -1, $-2, \ldots, -(m-1)$, якщо m — модуль.

12.6. $-1, -2, \ldots, -m$, якщо m — модуль.

12.7. Наприклад: а) 3; б) 0, 5; в) 3, 4, 5; г) 0, 9, 10, -1; д) 0, 1, 2, 3, 100, е) 36, 1, 2, 3, 4, 5; є) 7, 8, 9, 10, 11, 12, 13; ж) 0, ± 1, ± 2, ± 3, 12; з) 0, -1, -2, -3, -4, -5, -6, -7, 1; к) 10, ± 1, ± 2, ± 3, ± 4, 5; л) 3, 2, 4, 5, 6, 7, 8, 9, 10, 11, 12, 13; м) -3, -4, -5, -6, -7, -8, -9, -10, -11, -12, -13, -14; -15, -16, -17; н) 20, ± 1, ± 2, ± 3, ± 4, ± 5, ± 6, ± 7, ± 8, ± 9, -10.

12.8. Використати відповіді до задач 12.2—12.7, виключивши у відповідних повних системах числа, не взаємно прості з модулем.

12.9. а), б), г), д), ж), з), к) — так; в), е), є) — ні.

12.10. а), в), г), д) — так; б), е) — ні.

12.13. а) $K_1^{(6)} = K_1^{(48)} \cup K_7^{(48)} \cup K_{13}^{(48)} \cup K_{19}^{(48)} \cup K_{25}^{(48)} \cup K_{31}^{(48)} \cup K_{37}^{(48)} \cup K_{43}^{(48)}$; $K_3^{(6)} = K_3^{(48)} \cup K_9^{(48)} \cup K_{15}^{(48)} \cup K_{21}^{(48)} \cup K_{27}^{(48)} \cup K_{33}^{(48)} \cup K_{39}^{(48)} \cup K_{45}^{(48)}$; $K_5^{(6)} = K_5^{(48)} \cup K_{11}^{(48)} \cup K_{17}^{(48)} \cup K_{23}^{(48)} \cup K_{29}^{(48)} \cup K_{35}^{(48)} \cup K_{41}^{(48)} \cup K_{47}^{(48)}$.

12.14. а) $K_2^{(3)}$; б) $K_3^{(4)}$; в) $K_2^{(5)}$; г) $K_3^{(7)}$; д) $K_7^{(8)}$; е) $K_2^{(9)}$; є) $K_3^{(10)}$; ж) $K_9^{(11)}$; з) $K_{15}^{(61)}$; к) не існує, оскільки $(198, 501) = 3 \neq 1$; л) $K_{472}^{(501)}$; м) $K_{1453}^{(1498)}$; $K_{98}^{(1693)}$.

§ 13

13.1. г), з) Теорема Ейлера не справджується.

13.2. г), л) Мала теорема Ферма не справджується.

13.3. а) 7; б) 1; в) 22; г) 5; д) 96; е) 29; є) 19; ж) 1; з) 1; к) 1.

13.4. а) 2; б) 1, 4, 1, 4; в) 13; г) 7; д) 14; е) 14; є) 65; ж) 49.

13.5. а) 21; б) 22; в) 64; г) 21; д) 375.

13.6. а) 2; б) 6; в) 1; г) 5; д) 2; е) 0; є) 2; ж) 2; з) 70; к) 7.

13.7. а) 01; б) 67; в) 31; г) 97; д) 01; е) 61; є) 61; ж) 97; з) 76; к) 92; л) 84.

13.12. а) 0, якщо $a \vdots 5$ і 1, якщо не ділиться на 5; б) $\frac{1+m}{2}$; в) $\frac{1+m}{2}$, якщо $m = 4k-1$ і $\frac{3m+1}{4}$, якщо $m = 4k+1$.

§ 14

14.1. а) $x \equiv 2 \pmod 3$; б) розв'язків немає; в) $x \equiv 2 \pmod 5$; г) $x \equiv 5 \pmod 7$; д) $x \equiv 4, 9 \pmod{10}$; е) $x \equiv 3 \pmod 7$; є) $x \equiv 8 \pmod{11}$; ж) $x \equiv 2, 5, 8, 11 \pmod{12}$.

14.2. а) $x \equiv 3 \pmod{13}$; б) розв'язків немає; в) $x \equiv 3, 10 \pmod{14}$; г) $x \equiv 2 \pmod{27}$; д) $x \equiv 6 \pmod{23}$; е) $x \equiv 3 \pmod{37}$; є) $x \equiv 11 \pmod{41}$; ж) $x \equiv 38 \pmod{51}$.

14.3. а) $x \equiv 4 \pmod{13}$; б) $x \equiv 3 \pmod{12}$; в) $x \equiv 10 \pmod{12}$; г) $x \equiv 14 \pmod{19}$; д) $x \equiv 13 \pmod{34}$; е) Розв'язків немає; є) $x \equiv 3 \pmod{22}$; ж) $x \equiv 1, 14, 27 \pmod{39}$.

14.4. а) $x \equiv 9 \pmod{98}$; б) $x \equiv 28 \pmod{119}$; в) розв'язків немає; г) $x \equiv 11 \pmod{169}$; д) $x \equiv 73 \pmod{177}$; е) $x \equiv 29 \pmod{201}$; є) $x \equiv 29, 138, 247 \pmod{327}$; ж) $x \equiv 17, 96, 175, 254, 333 \pmod{395}$; з) $x \equiv 153, 461, 769 \pmod{924}$; к) $x \equiv 1630 \pmod{2413}$; л) $x \equiv 200, 751, 1302, 1853, 2404 \pmod{2755}$; м) розв'язків немає.

14.5. а) $x \equiv 3 \pmod{23}$; б) $x \equiv 11 \pmod{24}$; в) $x \equiv 11 \pmod{24}$; г) $x \equiv 23 \pmod{30}$; д) розв'язків немає; е) $x = 2, 7, 12, 17, 22, 27 \pmod{30}$; є) $x \equiv 2 \pmod{41}$; ж) $x \equiv 21 \pmod{50}$.

14.7. а) $x \equiv a + b \pmod{ab}$; б) $x \equiv (a-b)^{\varphi(ab)-1} \pmod{ab}$; в) $x \equiv (a-b)(a+b)^{\varphi(ab)-1} \pmod{ab}$; г) $x \equiv (a-b) \pmod{ab}$; д) $x \equiv \frac{1+p}{2} \pmod p$; е) $x \equiv m-1 \pmod m$; є) $x \equiv a \pmod m$; ж) $x \equiv a^{p-2} \pmod p$.

14.8. а) Будь-яка конгруенція виду $ax \equiv b \pmod{15}$, де $(a, 15) = 1$; б) $ax \equiv b \pmod{15}$, $(a, 15) = 3$, $b \vdots 3$ або $(a, 15) = 5$, $b \vdots 5$; в) такої конгруенції скласти не можна.

14.9. а) $x = 2 + 3t$, $y = -2t$, $t \in \mathbf{Z}$; б) $x = 2 + 3t$, $y = 2 + 4t$, $t \in \mathbf{Z}$; в) $x = 3 + 4t$, $y = 1 - 3t$, $t \in \mathbf{Z}$; г) $x = 3 + 4t$, $y = -3 - 5t$, $t \in \mathbf{Z}$; д) $x = 7 + 8t$, $y = -2 - 3t$, $t \in \mathbf{Z}$; е) $x = -3 + 13t$, $y = 4 - 17t$, $t \in \mathbf{Z}$; є) $x = -7 + 15t$, $y = 12 - 23t$, $t \in \mathbf{Z}$; ж) $x = -1 + 16t$, $y = -8 + 17t$, $t \in \mathbf{Z}$; з) $x = 1 + 4t$, $y = 2 + 13t$, $t \in \mathbf{Z}$; к) розв'язків немає; л) $x = 20 + 21t$, $y = 23 + 25t$, $t \in \mathbf{Z}$; м) $x = 47 + 105t$, $y = 21 + 47t$, $t \in \mathbf{Z}$; н) $x = 94 + 111t$, $y = 39 + 47t$, $t \in \mathbf{Z}$.

14.10. а) $x \equiv 18 \pmod{35}$; б) розв'язків немає; в) $x \equiv 12 \pmod{35}$; г) $x \equiv 105 \pmod{225}$; д) $x \equiv 170b_1 + 52b_2 \pmod{221}$; е) $x \equiv 100 \pmod{143}$, $y \equiv -111 \pmod{143}$; є) $x \equiv 1 \pmod 5$; $y \equiv 2 \pmod 5$; ж) розв'язків немає.

14.11. а) $x \equiv 91 \pmod{120}$; б) $x \equiv 59 \pmod{60}$; в) $x \equiv 33 \pmod{90}$; г) $x \equiv 86 \pmod{315}$; д) $x \equiv 256 \pmod{1547}$; е) розв'язків немає; є) $x \equiv 47 \pmod{420}$; ж) $x \equiv 49 \pmod{420}$; з) $x \equiv 125 \pmod{1496}$; к) $x \equiv 11151b_1 + 11800b_2 + 16875b_3 \pmod{39325}$; л) $x \equiv 8479 \pmod{15015}$.

14.12. а) $x \equiv 17 \pmod{90}$; б) $x \equiv 4 \pmod{105}$; в) розв'язків немає; г) $x \equiv 299 \pmod{385}$; д) розв'язків немає; е) $x \equiv 9573 \pmod{13923}$; є) $x \equiv 85056 \pmod{130169}$.

14.13. Абсциси точок такі: $x \equiv 291 \pmod{819}$. Ординати знаходять за допомогою рівнянь прямих.

14.14. а) $a \equiv 5 \pmod 6$; б) $a \equiv 0 \pmod 4$; в) $a \equiv 1 \pmod 7$; г) $a \equiv 1 \pmod 6$.

14.15. Необхідно і достатньо, щоб $7 - 3 = 4 \not\equiv 0 \pmod{(6, m)}$. Якщо, наприклад, $(6, m) = 3$, то можна взяти $m = 15$.

14.16. 19.

14.18. а) 7; б) 2; в) 2; г) 19; д) 7; е) 8.

14.20. а), б) через 12 точок.

14.21. $r = \sqrt{a^2 + b^2}$.

14.22. $c \mid (a, b)$.

14.23. 5 вересня. Задача зводиться до розв'язування невизначеного рівняння $12x + 31y = 8$, $1 \leqslant x \leqslant 31$ (або $1 \leqslant y \leqslant 12$). Оскільки $(12, 31) = 1$, то таке рівняння з обмеженнями на x і y має єдиний розв'язок.

14.24. 2 і 4 або 6 і 1.

14.25. Можливі вісім варіантів: 2 і 39, 9 і 34, 16 і 29, 23 і 24, 30 і 19, 37 і 14, 44 і 9, 51 і 4. Найкращим є перший, бо в ньому треба зробити найменшу кількість стикувань труб.

14.26. Можливі 10 варіантів: 3 і 28, 8 і 25, 13 і 22, 18 і 19, 23 і 16, 28 і 13, 33 і 10, 38 і 7, 43 і 4, 48 і 1.

§ 15

15.1. а) $x^3 + 2x^2 + 3 \equiv 0 \pmod{11}$; б) $x^3 + 18x^2 + 4x - 17 \equiv 0 \pmod{59}$; в) $x^6 + 4x^5 + 22x^4 + 76x^3 + 70x^2 + 52x + 39 \equiv 0 \pmod{101}$; г) $x^n + a_1x^{n-1}h + \ldots + a_nh \equiv 0 \pmod{m}$, де h задовольняє умову $a_0h \equiv 1 \pmod{m}$.

15.2. а) $2x^3 + 3 \equiv 0 \pmod 5$; б) $3x^4 + 2x^3 + 3x^2 + 2x \equiv 0 \pmod 5$; в) $3x^2 + x - 2 \equiv 0 \pmod 7$; г) $5x^6 + x^5 + 5x^4 + 3x^2 + 3x + 4 \equiv 0 \pmod 7$; д) $6x^8 + 7x^5 + 3x^4 + 3x^3 + x^2 + 3 \equiv 0 \pmod{11}$.

15.3. а) $x \equiv 2 \pmod 3$; б) розв'язків немає; в) $x \equiv 1, 2 \pmod 3$; г) $x \equiv 1 \pmod 3$; д) $x \equiv 1 \pmod 3$; е) $x \equiv 4 \pmod 5$; є) $x \equiv 3 \pmod 5$; ж) $x \equiv 2 \pmod 5$; з) розв'язків немає; к) $x \equiv 1 \pmod 5$; л) $x \equiv 1, 2 \pmod 5$.

15.4. а) $x \equiv 2 \pmod 7$; б) $x \equiv 4 \pmod 7$; в) $x \equiv 1, 2, 3, 4, 5, 6 \pmod 7$; г) $x \equiv 4, 5 \pmod 7$; д) $x \equiv 4 \pmod{11}$; е) розв'язків немає; є) $x \equiv 7, 9 \pmod{11}$; ж) $x \equiv 12 \pmod{13}$; з) $x \equiv 7, 13 \pmod{23}$.

15.5. а) Випробовуючи лишки $0, \pm1, \pm2$, знаходимо перший розв'язок $x_1 \equiv 4 \pmod 5$. Запишемо тотожну конгруенцію

$$f(x) \equiv (x - 4) f_1(x) \pmod 5. \qquad (1)$$

Знаходимо $f_1(x)$ як частку від ділення $f(x)$ на $x - 4$ і визначаємо його корені за модулем 5:

$$f_1(x) = x^2 + 8x + 32 \equiv x^2 + 3x + 2 \equiv 0 \pmod 5.$$

Ця конгруенція має розв'язок $x_2 \equiv 3 \pmod 5$, отже

$$f_1(x) \equiv (x - 3) f_2(x) \pmod 5. \qquad (2)$$

Знаходимо $f_2(x)$ як частку від ділення $f_1(x)$ на $x - 3$ і його корені за модулем 5:

$$f_2(x) = x + 11 \equiv 0 \pmod 5.$$

Розв'язуючи цю конгруенцію, дістаємо $x \equiv 4 \pmod 5$, отже

$$f_2(x) \equiv x - 4 \pmod 5. \qquad (3)$$

З конгруенцій (1) — (3) маємо

$$f(x) \equiv (x - 3)(x - 4)^2 \pmod 5.$$

Зауважимо, що розв'язок $x \equiv 4 \pmod 5$ є двократним.

Конгруенція $(x - 3)(x - 4)^2 \equiv 0 \pmod 5$ є еквівалентною заданій. Ліва частина її і є розкладом на лінійні множники функції $f(x) = x^3 + 4x^2 - 3$ за модулем 5;

б) $(x - 1)(x - 2)^2 \equiv 0 \pmod 5$;
в) $(x - 1)(x - 2)(x - 3)(x - 4) \equiv 0 \pmod 5$;
г) $3(x - 1)(x - 2)(x - 3) \equiv 0 \pmod 5$;
д) $(x - 1)(x - 2)(x - 3)(x - 6) \equiv 0 \pmod 7$;
е) $5(x - 1)(x - 3)(x - 5) \equiv 0 \pmod 7$;
є) $6(x - 1)(x - 2)(x - 9) \equiv 0 \pmod{11}$;
ж) $(x - 2)(x - 3)(x - 9) \equiv 0 \pmod{17}$;
з) $(x - 1)(x - 13)(x - 21) \equiv 0 \pmod{23}$;
к) $(x - 2)^2(x - 11)(x - 28) \equiv 0 \pmod{29}$;
л) $(x - 17)(x - 28)(x - 30) \equiv 0 \pmod{31}$.

15.6. б) — е) Використати теорему Вільсона; є) треба почленно перемножити конгруенції $a \equiv a^p \pmod p$ і $(p - 1)! \equiv -1 \pmod p$.

15.7. а) $x \equiv 1, 2, 4, 5 \pmod 6$; б) $x \equiv 1 \pmod 6$; в) $x \equiv 2 \pmod{10}$; г) $x \equiv 0, 4, 6 \pmod{10}$; д) $x \equiv 7 \pmod{10}$; е) $x \equiv 9 \pmod{15}$; є) $x \equiv 11 \pmod{15}$; ж) $x \equiv 2, 5, 11 \pmod{15}$; з) $x \equiv 4 \pmod{21}$; к) розв'язків немає; л) $x \equiv 0, 14, 20, 34 \pmod{35}$; м) $x = 2, 7, 24, 29 \pmod{55}$.

15.8. а) $x \equiv 2, 5, 11, 17, 20, 26 \pmod{30}$; б) $x \equiv 3, 26, 28, 49, 63, 73, 84, 94 \pmod{105}$.

15.9. а) $x \equiv 21 \pmod{25}$; б) $x \equiv 16 \pmod{25}$;
в) $x \equiv 2, 3 \pmod{25}$; г) $x \equiv 13 \pmod{25}$;
д) $x \equiv 17 \pmod{49}$; е) $x \equiv 18, 33 \pmod{49}$;
є) $x \equiv 2, 9, 16, 23, 30, 33, 37, 44 \pmod{49}$;
ж) $x \equiv 8 \pmod{49}$; з) розв'язків немає.

15.10. а) $x \equiv 8 \pmod{27}$; б) $x \equiv 19 \pmod{27}$;
в) $x \equiv 22 \pmod{27}$; г) $x \equiv 16 \pmod{27}$;
д) $x \equiv 22, 53 \pmod{64}$; е) $x \equiv 61 \pmod{125}$;
є) $x \equiv 113 \pmod{125}$; ж) $x \equiv 84 \pmod{125}$;
з) $x \equiv 19 \pmod{125}$; к) $x \equiv 43, 123, 168, 248, 293, 373, 418, 498, 543, 623 \pmod{625}$.

15.11. а) Розв'язків немає; б) $x \equiv 2 \pmod{12}$;
в) $x \equiv 4, 13 \pmod{18}$; г) $x \equiv 12 \pmod{40}$;
д) $x \equiv 6, 33, 42 \pmod{45}$; е) $x \equiv 42 \pmod{45}$;
є) $x \equiv 6, 24, 42 \pmod{45}$; ж) $x \equiv 12, 24, 37, 49 \pmod{50}$;
з) $x \equiv 13 \pmod{63}$; к) $x \equiv 8, 44, 58 \pmod{63}$;
л) $x \equiv 32, 82, 132 \pmod{175}$; м) $x \equiv 36, 136 \pmod{175}$;
н) $x \equiv 22, 76, 122, 176 \pmod{225}$.

15.12. Необхідно і достатньо, щоб $p \equiv 1 \pmod n$ і $a^{\frac{p-1}{n}} \equiv 1 \pmod p$.

15.13. а) $x \equiv 1, 2, 4 \pmod 7$; б) $x \equiv 2, 6, 7, 10 \pmod{11}$; в) конгруенція має лише два розв'язки $x \equiv 2, 9 \pmod{11}$.

15.14. а) 6; б) $p - 1$; в) 8; г) $\varphi(m)$; д) $\frac{p-1}{2}$; е) $\frac{p-1}{2}$.

15.16. Оскільки 103 — просте число і $103 \equiv 1 \pmod 2$, то дана конгруенція має лише два розв'язки. Оскільки ж числа 31 і -31 задовольняють її і $31 \not\equiv -31 \pmod{103}$, то маємо такі два розв'язки: $x \equiv 31, 72 \pmod{103}$.

15.19. $x \equiv 3, 13 \pmod{20}$.

§ 16

16.1. а) $x^2 \equiv 4 \pmod 5$, $x \equiv 2, 3 \pmod 5$;
б) $(6x - 1)^2 \equiv 1 \pmod 5$, $x \equiv 0, 2 \pmod 5$;
в) $(2x + 2)^2 \equiv 1 \pmod 5$, $x \equiv 1, 2 \pmod 5$;
г) $(2x - 2)^2 \equiv 0 \pmod 7$, $x \equiv 1 \pmod 7$;
д) $(2x - 1)^2 \equiv 3 \pmod 7$, розв'язків немає;
е) $(3x + 1)^2 \equiv 4 \pmod 7$, $x \equiv 5, 6 \pmod 7$;
є) $(x - 5)^2 \equiv 1 \pmod{11}$, $x \equiv 4, 6 \pmod{11}$;
ж) $(10x + 7)^2 \equiv 4 \pmod{13}$, $x \equiv 1, 8 \pmod{13}$;
з) $(x - 3)^2 \equiv 0 \pmod{13}$, $x \equiv 3 \pmod{13}$.

16.2. а) $(x + 1)^2 \equiv 4 \pmod{10}$, $x \equiv 1, 7 \pmod{10}$;
б) $(x + 6)^2 \equiv 9 \pmod{15}$, $x \equiv 6, 12 \pmod{15}$;
в) $(6x + 7)^2 \equiv 4 \pmod{17}$, $x \equiv 2, 7 \pmod{17}$;
г) $(x - 4)^2 \equiv 13 \pmod{17}$, $x \equiv 12, 13 \pmod{17}$;
д) $(x - 1)^2 \equiv 17 \pmod{19}$, $x \equiv 7, 14 \pmod{19}$;
е) $(x - 5)^2 \equiv 5 \pmod{19}$, $x \equiv 14, 15 \pmod{19}$;
є) $(x + 6)^2 \equiv 8 \pmod{23}$, $x \equiv 4, 7 \pmod{23}$;
ж) $(2x - 5)^2 \equiv -39 \pmod{96}$, $x \equiv 13, 16 \pmod{24}$;
з) $(6x + 2)^2 \equiv 5 \pmod{44}$, розв'язків немає.

16.3. а) $a \equiv 1, 4 \pmod 5$; б) $a \equiv 1, 2, 4 \pmod 7$;
в) $a \equiv 1, 3, 4, 5, 9 \pmod{11}$; г) $a \equiv 1, 3, 4, 9, 10, 12 \pmod{13}$;
д) $a \equiv 1, 2, 4, 8, 9, 13, 15, 16 \pmod{17}$; е) $a \equiv 1, 2, 3, 4, 6, 8, 9, 12, 13, 16, 18 \pmod{23}$; є) $a \equiv 1, 3, 4, 7, 9, 10, 11, 12, 16, 21, 25, 26, 27, 28, 30, 33, 34, 36 \pmod{37}$;

ж) $a \equiv 1, 4, 6, 7, 9, 10, 11, 13, 15, 16, 17, 24, 25, 28, 29, 36, 37, 38, 40, 42, 43, 44, 46, 47, 49, 52 \pmod{53}$.

16.4. а) $x \equiv 3, 4 \pmod 7$; б) $x \equiv 2, 5 \pmod 7$; в) розв'язків немає.

16.5. а) -1; б) 1; в) 1; г) 1; д) -1; е) -1; є) -1; ж) -1; з) 1.

16.6. а) -1; б) 1; в) -1; г) -1; д) -1; е) 1; є) -1; ж) 1; з) 1.

16.7. а) 0; б) 2; в) 0; г) 0; д) 0; е) 2; є) 0; ж) 0; з) 0; к) 0.

16.8. а) $x \equiv 1 \pmod 3$; б) $x \equiv 1, 4 \pmod 5$;
в) $x \equiv 1, 2, 4 \pmod 7$; г) $x \equiv 1, 3, 4, 5, 9 \pmod{11}$;
д) $x \equiv 1, 2, 4, 8 \pmod{15}$; е) $x \equiv 7, 11, 13, 14 \pmod{15}$.

16.10. а) $x \equiv 66, 245 \pmod{311}$; б) $x \equiv 12, 35 \pmod{47}$;
в) $x \equiv 6, 23 \pmod{29}$; г) $x \equiv 15, 22 \pmod{37}$.

16.11. а) Ні; б) так; в) ні; г) так.

16.12. а) $x \equiv \pm 2 + 5q$, $y = 2 \pm 16q + 20q^2$, $q \in \mathbf{Z}$; б) розв'язків немає; в) розв'язків немає; г) $x = 8 + 11q$, $y = -1 + 6q + 11q^2$ або $x = 2 + 11q$, $y = -1 - 6q + 11q^2$, $q \in \mathbf{Z}$; д) $x = 10 + 13q$ або $x \equiv 11 - 13q$, $y = 13q^2 - 1$, $q \in \mathbf{Z}$.

16.14. а) $x \equiv 3, 5, 11, 13 \pmod{16}$;
б) $x \equiv 7, 9, 23, 25 \pmod{32}$;
в) $x \equiv 5, 11, 21, 27 \pmod{32}$;
г) $x \equiv 13, 19, 45, 51 \pmod{64}$;
д) $x \equiv 11, 21, 43, 53 \pmod{64}$;
е) $x \equiv 31, 33, 95, 97 \pmod{128}$;
є) $x \equiv 29, 35, 93, 99 \pmod{128}$;
ж) $x \equiv 41, 87, 169, 215 \pmod{256}$.

16.15. а) $x \equiv 13, 14 \pmod{27}$; б) $x \equiv 53, 72 \pmod{125}$;
в) $x \equiv 116, 127 \pmod{243}$; г) $x \equiv 1, 2, 177, 226 \pmod{400}$.

§ 17

17.1. а) 4; б) 2; в) 2; г) 6; д) 2; е) 4; є) 8; ж) 4; з) 10; к) не існує; л) 6; м) 18; н) 18.

17.2. а) клас K_1 має порядок 1; клас $K_{10} - 2$; класи K_3, K_4, K_5, $K_9 - 5$, класи K_2, K_6, K_7, $K_8 - 10$; б) клас K_1 має порядок 1; клас $K_{18} - 2$; класи K_7, $K_{11} - 3$; K_8, $K_{12} - 6$; класи K_4, K_5, K_6, K_9, K_{16}, $K_{17} - 9$; класи K_2, K_3, K_{10}; K_{13}, K_{14}, $K_{15} - 18$; в) клас K_1 має порядок 1; класи K_8, K_{13}, $K_{20} - 2$; класи K_4, $K_{16} - 3$; класи K_2, K_5, K_{10}, K_{11}, K_{18}, $K_{19} - 6$.

17.3. а) 12, 3 і 2; б) 8, 8 і 4; в) 10, 10, 2 і 5; г) 6, 2 і 12; д) 5, 10, 2 і 10.

17.4. а) 30; б) 2.

17.5. а) 2, 6, 7, 8; б) 2, 6, 7, 11; в) не існує; г) 2, 3, 10, 13, 14, 15; д) 3, 5, 10, 12, 17, 19, 24, 26, 38, 40, 45, 47; е) 2, 5, 11, 14, 20, 23, 29, 32, 38, 41, 47, 50, 56, 59, 65, 68, 74, 77.

17.6. а) 2, 3; б) 2, 5; в) 6, 2; г) 8, 3; д) 12, 2.

17.7. а) 3; б) 3; в) 5; г) 6; д) 2; е) 27; є) 5; ж) 7; з) 7; к) 3; л) 3; м) 2.

17.8. 2, 8, 10, 11, 14, 15, 18, 19, 21, 26, 27.

17.9. $x \equiv 1, 2, 4, 8, 9, 13, 15, 16 \pmod{17}$.

17.10. 5, 6, 9, 13, 22. **17.12.** 28.

17.13. а) x — довільне натуральне число; б) $P_8(5) = 2$, тому $x = 2n$, $n \in \mathbf{N}$;
в) $x = 6n$, $n \in \mathbf{N}$; г) $x = 20n$, $n \in \mathbf{N}$;
д) $x = 14n$, $n \in \mathbf{N}$; е) $x = 21n$, $n \in \mathbf{N}$.

17.14. $x \equiv 108 \pmod{131}$.

17.15. а) Оскільки $P_9(4) = 3$, то задана конгруенція має розв'язки тільки при $b \equiv 1, 4, 7 \pmod 9$; б) оскільки $P_9(5) = \varphi(9) = 6$, то задана конгруенція має розв'язки при умові, що $(b, 9) = 1$.

17.16. д) Використати результат задачі 17.16, г), н) дослідити конгруенцію $(a^k - 1)(a^k + 1) \equiv 0 \pmod p$.

17.17. б) Довести за індукцією, що $P_{2^\alpha}(a) \leqslant 2^{\alpha-2}$, де a — непарне натуральне число, $\alpha \geqslant 3$.

17.18. а) Нехай число $2^{2^n} + 1$ має простий дільник p. Тоді $2^{2^n} + 1 \equiv 0 \pmod p$, тобто $2^{2^n} \equiv -1 \pmod p$. Звідси $2^{2^{n+1}} \equiv 1 \pmod p$. Це означає, що $P_p(2) = 2^{n+1}$. Тоді $p - 1 \vdots 2^{n+1}$, тобто $p \equiv 1 \pmod{2^{n+1}}$. Оскільки конгруенція справджується при всіх $n > 1$, зокрема $p \equiv 1 \pmod{2^3}$, то $p = 8t + 1$.

За критерієм Ейлера про квадратичні лишки

$$2^{\frac{p-1}{2}} \equiv \left(\frac{2}{p}\right) \pmod p.$$

Проте $\left(\frac{2}{p}\right) = (-1)^{\frac{p^2-1}{8}} = (-1)^{\frac{(8t+1)^2-1}{8}} = 1$. Отже, $2^{\frac{p-1}{2}} \equiv 1 \pmod p$. Звідси $\frac{p-1}{2} \vdots 2^{n+1}$ і тому $p - 1 \vdots 2^{n+2}$ або $p \equiv 1 \pmod{2^{n+2}}$. Це означає, що $p = 1 + k \cdot 2^{n+2}$;

в) якщо q — просте непарне число і $a^p \equiv 1 \pmod q$, то $\delta = P_q(a) = 1$ або p. При $\delta = 1$ маємо $a \equiv 1 \pmod q$, а при $\delta = p$ маємо $q - 1 = 2px$, $x \in \mathbf{N}$;

г) якщо q — просте непарне число і $a^p + 1 \equiv 0 \pmod q$, то $a^{2p} \equiv 1 \pmod q$. Тому $\delta = P_q(a)$ є одним з чисел 1, 2, p або $2p$. Випадки $\delta = 1$ і $\delta = p$ неможливі. При $\delta = 2$ маємо: $a^2 \equiv 1 \pmod q$, $a + 1 \equiv 0 \pmod q$. При $\delta = 2p$ маємо: $q - 1 = 2px$, $x \in \mathbf{N}$.

д) Використати результат задачі 17.18, а), поклавши $a = 2$, і провести доведення методом від супротивного.

17.19. в) Очевидно, що $P_{a^m-1}(a) = m$ і тому $\varphi(a^m - 1) \vdots m$; є) використати результати задач 17.19, г) — 17.19, е).

§ 18

18.1. а), б), г), е), є), ж) — див. таблиці індексів за відповідними модулями в додатку; в) табл. 61, 62; д) табл. 63, 64.

18.2. Табл. 65, 66.

Таблиця 61

N	0	1	2	3	4
0		0	3	1	2

Таблиця 62

I	0	1	2	3	4
0	1	3	4	2	

Таблиця 63

N	0	1	2	3	4	5	6
0		0	4	5	2	1	3

Таблиця 64

I	0	1	2	3	4	5	6
0	1	5	4	6	2	3	

Таблиця 65

N	0	1	2	3	4	5	6	7	8	9
0		0	11	—	4	1	—	14	15	—
1	12	17	—	16	7	—	8	3	—	6
2	5	—	10	13	—	2	9			

18.5. а) $x \equiv 13 \pmod{17}$; б) $x \equiv 8 \pmod{27}$. Використати відповідь до задачі 18.2; в) $x \equiv 31 \pmod{37}$;
г) $x \equiv 30 \pmod{73}$; д) $x \equiv 32 \pmod{79}$;
е) $x \equiv 74 \pmod{79}$; є) $x \equiv 44 \pmod{83}$;
ж) $x \equiv 51 \pmod{97}$; з) $x \equiv 30 \pmod{221}$.
Оскільки $221 = 13 \cdot 17$, то слід розглянути систему конгруенцій

$$\begin{cases} 37x \equiv 5 \pmod{13}, \\ 37x \equiv 5 \pmod{17}. \end{cases}$$

Таблиця 66

l	0	1	2	3	4	5	6	7	8	9
0		5	25	17	4	20	19	14	16	26
1	22	2	10	23	7	8				
2										

18.6. а) $x \equiv 7,\ 10 \pmod{17}$; б) $x \equiv 8,\ 19 \pmod{27}$. Використати відповідь до задачі 18.2; в) $x \equiv 10,\ 43 \pmod{53}$;
г) $x \equiv 27,\ 34 \pmod{61}$; д) $x \equiv 27,\ 40 \pmod{67}$;
е) $x \equiv 21,\ 46 \pmod{67}$; є) $x \equiv 14,\ 57 \pmod{71}$;
ж) $x \equiv 17,\ 66 \pmod{83}$; з) $x \equiv 2,\ 7 \pmod{11}$;
к) $x \equiv 5,\ 20 \pmod{43}$; л) $x \equiv 3,\ 31 \pmod{47}$;
м) $x \equiv 1634,\ 1847 \pmod{59^2}$; н) $x \equiv 253,\ 4076 \pmod{73^2}$.
18.8. а) 3; б) 4; в) 0; г) 1; д) 0; е) 10; є) 0; ж) 7; з) 3; к) 1; л) 0.
18.9. а) $x \equiv 4,\ 33 \pmod{37}$; б) $x \equiv 17 \pmod{41}$;
в) розв'язків немає; г) $x \equiv 2,\ 18,\ 23,\ 39 \pmod{41}$;
д) $x \equiv 7 \pmod{43}$; е) розв'язків немає;
є) $x \equiv 17 \pmod{67}$; ж) $x \equiv 8,\ 28,\ 31,\ 36,\ 39,\ 59 \pmod{67}$;
з) $x \equiv 30,\ 53 \pmod{83}$; к) розв'язків немає.
18.10. а) $x \equiv 3,\ 5,\ 6 \pmod{7}$; б) $x \equiv 2,\ 3,\ 10,\ 11 \pmod{13}$;
в) $x \equiv 10,\ 13 \pmod{23}$; г) розв'язків немає;
д) $x \equiv 11,\ 27,\ 36 \pmod{37}$; е) $x \equiv 25,\ 30,\ 31,\ 36 \pmod{61}$;
є) $x \equiv 17 \pmod{73}$; ж) $x \equiv 12,\ 23,\ 35,\ 38,\ 50,\ 61 \pmod{73}$;
з) $x \equiv 17,\ 63,\ 66 \pmod{73}$; к) $x \equiv 3,\ 24,\ 46 \pmod{73}$;
л) $x \equiv 6,\ 14,\ 20,\ 59,\ 65,\ 73 \pmod{79}$.
18.11. а) $x \equiv 10 \pmod{29}$; б) $x \equiv 29 \pmod{31}$;
в) $x \equiv 24 \pmod{37}$; г) $x \equiv 14 \pmod{41}$;
д) $x \equiv 24 \pmod{47}$; е) $x \equiv 34 \pmod{53}$;
є) $x \equiv 47 \pmod{71}$.
18.12. а) 4; б) 16; в) не існує; г) 29; д) 30; е) 17; є) 2; ж) 16; з) не існує; к) 23; л) 2; м) не існує.
18.13. а) Розв'язків немає; б) $x \equiv 27 \pmod{30}$;
в) $x \equiv 11 \pmod{28}$; г) $x \equiv 27 \pmod{30}$;
д) $x \equiv 2,\ 5,\ 8,\ \ldots,\ 56,\ 59 \pmod{60}$; е) $x \equiv 3,\ 7,\ 11,\ \ldots,\ 55,\ 59 \pmod{60}$.
18.14. а) $x \equiv 38 \pmod{66}$; б) $x \equiv 3 \pmod{72}$; в) $x \equiv 3,\ 16,\ 29,\ 42,\ 55,\ 68 \pmod{78}$; г) $x \equiv 5,\ 46 \pmod{82}$.
18.15. а) 2; б) 11; в) 7; г) 5; д) 23; е) 13; є) 138. Оскільки $1739 = 37 \cdot 47$, то $P_{1739}(10) = [P_{37}(10), P_{47}(10)] = [3, 46] = 138$; ж) 84. Оскільки $4331 = 61 \cdot 71$, то $P_{4331}(32) = [P_{61}(32), P_{71}(32)] = [12, 7] = 84$.
18.16. а) 26; б) 62; в) 7; г) 16.
18.17. а), в), г), е), є) — є; б), д), ж) — не є.
18.18. а) $x \equiv 7,\ 57 \pmod{100}$; б) розв'язків немає.
18.19. а) 15, 17; 19; 20; б) 15; 18; 19; в) 15; 17; 19; г) 18; д) жодне; е) 15, 19.
18.20. а) 7; 37; б) 3; 5; 12; 18; 19; 20; 26; 28; 29; 30; 33; 34; в) 3; 27; 41; 52; г) 2; 6; 7; 10; 17; 18; 26; 30; 31; 35; 43; 44; 51; 54; 55; 59.

§ 19

19.1. а) Ті і тільки ті цілі числа, в яких остання цифра парна; б), е) ті і тільки ті цілі числа, в яких сума цифр ділиться на 3 (на 9); в), к), м) ті і тільки ті цілі числа, в яких на 4 (на 25, на 50) ділиться двоцифрове число, утворене їхніми останніми двома цифрами; г) ті і тільки ті цілі числа, які закінчуються 0 або 5; д), ж), з) ті і тільки ті цілі числа, в яких різниця між числом, записаним останніми трьома цифрами, і числом, записаним рештою цифр заданого числа (або навпаки), ділиться на 7 (на 11, на 13); є) ті і тільки ті цілі числа, які закінчуються 0; л) ті і тільки ті цілі числа, в яких сума трицифрових

б) $f(x) = g(x)(3+2i)x + (2-7i)x + (-2+i)$;
в) $f(x) = g(x)(2x^2 + 3x) + 1$;
г) $s(x) = 5x^5 - 8x^4 - 2x^3 + 3x^2 + 6,\ r(x) = 4x + 5$;
д) $s(x) = 3x^5 + 3x^4 + 2x^3 + x^2 + 5x + 3,\ r(x) = 3x + 3$;
е) $6;$ і)
19.6. а) $\frac{1}{8}x^3 + \frac{1}{8}x^2 + \frac{1}{64}x - \frac{71}{64},\ r(x) = \frac{449}{512}x^2 - \frac{71}{512}x + \frac{7}{64}$;
19.7. а) 4.
19.8. а) 19; б) $r(x) = 2x + 1 - i$.
19.11. а), б), в), $= 0$.
неправильно.
19.12. а) Помилки не $4x + 1)^2$.
вильно; б) помилки не виявл.
дулем 11 — виявлено.
19.13. а) 16; б) 18; в) 28; г) 3, $\in Z[x]$; б) $I = Z[x]$;
19.14. а) 6; б) 2; в) 6; г) 42; д) 16;
м) 104. Конгруенція $10^x \equiv 1 \pmod{53 \cdot 73}$ рів.

$$\begin{cases} 10^x \equiv 1 \pmod{53}, \\ 10^x \equiv 1 \pmod{73}. \end{cases}$$

Розв'язуючи кожну з цих конгруенцій індексуванням, дістаємо

$$\begin{cases} x \equiv 0 \pmod{13}, \\ x \equiv 0 \pmod{8}. \end{cases}$$

звідси $x \equiv 0 \pmod{104}$. Отже, $P_{53 \cdot 73}(10) = 104$.
19.15. а) 2; 6; б) 2; 2; в) 2; 1; г) 4; 2; д) 2; 1; е) 2; 2; є) 1; 18; ж) 4; 16; з) 2; 18; к) 2; 22; л) 4; 48; м) 3; 13.
19.16. а) $b = 11$, 33 або 99; б) $b = 27,\ 37,\ 111,\ 333$ або 999.
19.17. а) 0, (736842105263157894); б) 0, (748251). Використати рівність $\frac{107}{143} = \frac{4}{11} + \frac{5}{13}$; в) 63; 22.

19.18. а) Показати, що $\frac{1}{n-1} + \frac{1}{n} + \frac{1}{n+1} = \frac{3n^2 - 1}{n(n^2 - 1)}$, і розглянути випадки, коли n — парне, n — непарне; в) конгруенція $10^x \equiv 1 \pmod{pq}$ рівносильна системі

$$\begin{cases} 10^x \equiv 1 \pmod{p}, \\ 10^x \equiv 1 \pmod{q} \end{cases} \quad \text{або} \quad \begin{cases} x\,(\text{ind } 10)_p \equiv 0 \pmod{p-1}, \\ x\,(\text{ind } 10)_q \equiv 0 \pmod{q-1}, \end{cases}$$

або

$$\begin{cases} x \equiv 0 \left(\mod \frac{p-1}{d}\right), \\ x \equiv 0 \left(\mod \frac{q-1}{\delta}\right). \end{cases}$$

Звідси

$$x \equiv 0 \left(\mod \left[\frac{p-1}{d}, \frac{q-1}{\delta}\right]\right) \text{ і } P_{pq}(10) = \left[\frac{p-1}{d}, \frac{q-1}{\delta}\right];$$

г) Розглянемо будь-який період, який містить цифри $z_1, z_2, \ldots, z_k$ і утворюється при перетворенні дробу $\frac{n}{m}$ у десятковий, а також систему $r_0, r_1, \ldots, r_{k-1}$ усіх остач, що утворюються при нумерації їх по порядку, починаючи з $n = r_0$. Оскільки при діленні r_1 на m дістанемо в частці z_2 і остачу r_2 і т. д., то періоди дробів $\frac{r_0}{m}, \frac{r_1}{m}, \ldots, \frac{r_{k-1}}{m}$ відрізнятимуться один від одного круговою перестановкою цифр; період для другого дробу почнеться з z_2, для третього — з z_3 і т. д. Якщо 10 — первісний корінь за модулем m, то $k = \varphi(m)$ і числа r_i вичер-

Таблиця 66

l	0	1	2	3	4	5	6	7	8	9
0		5	25	17	4	20	19	14	16	
1	22	2	10	23	7	8				
2										

18.6. а) $x \equiv 7,\ 10 \pmod{17}$; б) $x \equiv 8,\ 19 \pmod{}$ задачі 18.2; в) $x \equiv 10,\ 43 \pmod{53}$;
г) $x \equiv 27,\ 34 \pmod{61}$; д) $x \equiv 27,$ [illegible] Ньютона і наслідок з теореми Ферма про
е) $x \equiv 21,\ 46 \pmod{67}$; є) $x =$
ж) $x \equiv 17,\ 66 \pmod{83}$.
к) $x \equiv 5,\ 20 \pmod{} = -1,\ c = 6$;
м) $x \equiv 16^{2} = 5,\ c = 7$.
18.8. а) $a = 6,\ g_1(x) = x^2 + 3x + 1,\ g_2(x) = -x^2 - 3x - 1$;

б) $a = 3,\ g_1(x) = \bar{2}x + \bar{2},\ g_2(x) = \bar{3}x + \bar{3};\ a = 2,\ g_1(x) = \bar{2}x + \bar{3},\ g_2(x) = \bar{3}x + \bar{2}$;

в) $a = 4,\ g_1(x) = 3x^2 - 2x + 2,\ g_2(x) = -3x^2 + 2x - 2$.

20.7. $a = 6,\ b = 2$.

20.8. $a = -8,\ b = 18,\ g_1(x) = x^2 - 4x + 1,\ g_2(x) = -x^2 + 4x - 1;\ a = 8,\ b = 14,\ g_1(x) = x^2 + 4x - 1,\ g_2(x) = -x^2 - 4x + 1$.

20.9. Так, якщо $a \in \mathbf{Z}$. Тоді $g(x) = 2x^2 - 3ax + a^2$.

20.10. $a^2 = 4b + 4(c + 1)$.

20.11. $a = 3,\ b = -7,\ c = 4$.

20.12. Ні.

20.14. а) $f(x) = (x^2 + 3)^2 + (2x)^2$;
б) $f(x) = (x^2 + 6x - 13)^2 + (2x - 14)^2$.

20.15. а) Так; б) ні; в) так; г) так; д) ні; е) ні.

20.16. в) Застосувати наслідок з теореми Ферма та показати, що $g(x)$ є нуль-многочленом і $f(x) = g(x) \cdot h(x)$, де $h(x) \in \mathbf{Z}_5[x]$.

20.22. а) 0; б) -1; в) $\bar{1}$.

20.23. $2^{k-1}s^k$.

20.24. Показати, що многочлен $f(x)$ не зміниться при заміні x на $-x$.

20.25. Розглянути многочлен $h(x) = (1 + 5x^2 + x^3)^k$, коефіцієнти якого при парних степенях змінної x дорівнюють відповідним коефіцієнтам многочлена $f(x)$.

20.26. а) $a \in \{8,\ 12\}$; б) $a = 1$.

§ 21

21.1. а) У кільці $Z[x]$ многочлен $f(x)$ не ділиться на $g(x)$, а в кільці $Q[x]$ — ділиться; б) ділиться; в) ні.

21.3. $f(x) = (x + \bar{2})(x^2 + x + \bar{1})$.

21.4. а) $a = -1$; б) $a \in \left\{-1,\ \frac{5}{3}\right\}$.

21.5. Взяти до уваги, що $x^3 - 1 = (x - 1)(x^2 + x + 1)$.

21.6. а) $b = -1 - a^2,\ a = c$;
б) $b = 1,\ c = 0$;
в) якщо $a = 0$, то $b = c + 1$ і $c \in \mathbf{Z}$; якщо $a \in \mathbf{Z} \setminus \{0\}$, то $b = 2 - a^2$ і $c = 1$.

21.8. Твердження хибне.

21.11. а) $r = 1 - i$; б) $r = 7$; в) $r(x) = x + 2$;
г) $r(x) = (2 + i)x + (1 - i)$; д) $r(x) = -7x + 11$.

21.12. а) $f(x) = g(x)\left(2x^3 + 5x^2 + \frac{17}{2}x + \frac{79}{4}\right) + \frac{361}{4}x - \frac{95}{4}$;

б) $f(x) = g(x)(3 + 2i)x + (2 - 7i)x + (-2 + i)$;
в) $f(x) = g(x)(\bar{2}x^2 + \bar{3}x) + \bar{1}$;
г) $s(x) = 5x^5 - 8x^4 - 2x^3 + 3x^2 + 6,\ r(x) = 4x + 5$;
ґ) $s(x) = 3x^5 + 3x^4 + 2x^3 + x^2 + 5x + 3,\ r(x) = 3x + 3$;
е) $s(x) = \frac{1}{8}x^3 + \frac{1}{8}x^2 + \frac{1}{64}x - \frac{71}{64},\ r(x) = \frac{449}{512}x^2 - \frac{71}{512}x + \frac{7}{64}$;
ж) $s(x) = ix,\ r(x) = 2x + 1 - i$.

21.13. Ні.

21.15. $a = 1,\ b = 0$.

21.16. $r_1(x) = (3x^2 - 4x + 1)^2$.

21.17. $r = 3$.

21.18. $r(x) = 2x^2$.

21.19. $r = -11 + 13i$.

21.20. а) $I = \{(3x - 5)f(x) \mid f(x) \in \mathbf{Z}[x]\}$; б) $I = Z[x]$;
в) $I = \{(x - 1)f(x) \mid f(x) \in Z[x]\}$.

21.23. $I = \{nf(x) \mid f(x) \in Z[x]\}$.

21.24. Ні.

§ 22

22.1. а) $s(x) = 5x^3 - 4x^2 + 7x + 6,\ r(x) = 16$;
б) $s(x) = 2ix^3 + (3 - i)x - 2,\ r(x) = 2 + i$;
в) $s(x) = 0{,}5x^3 + 3x - 1,\ r(x) = 2{,}5x - 1{,}5$;
г) $s(x) = \bar{5}x^3 + \bar{2}x^2 + \bar{1},\ r(x) = \bar{3}x^2 - \bar{2}x + \bar{1}$;
д) $s(x) = (1 - 2i)x^3 + 2x^2 - ix + 2i,\ r(x) = 2x + 1$.

22.2. а) $s(x) = x^3 - x^2 + 3x - 3,\ r(x) = 5$;
б) $s(x) = 4x^3 - (3 + 4i)x^2 + (-1 + 7i)x + 8 - 6i,\ r(x) = -14 + 2i$;
в) $s(x) = \bar{6}x^5 + \bar{4}x^4 + \bar{2}x^3 + x^2 + \bar{4}x + \bar{2},\ r(x) = \bar{2}$;
г) $s(x) = (1 + \sqrt{2})x^3 - x^2 + x + 1 - \sqrt{2},\ r(x) = 4 - 2\sqrt{2}$.

22.3. а) 136; б) $-1 - 46i$; в) $\bar{2}$; г) $9 - 5\sqrt{2}$.

22.4. $a = 1,\ b = -1$.

22.7. $r(x) = -x + 3$.

22.8. $r(x) = 3{,}5x^2 + 1{,}5x - 2$.

22.9. $r(x) = (0{,}5 + i)x^2 + x + 0{,}5 - i$.

22.10. а) 1; б) 1.

22.17. 5.

22.18. $\bar{1}$.

22.19. Застосувати задачу 22.6, в) і теорему Безу.

22.21. $a = 3,\ b = -4$.

22.22. а) $f(x) = (x - 1)^4 + 2(x - 1)^3 + 3(x - 1)^2 - (x - 1) - 2$;
б) $f(x) = \bar{2}(x - \bar{1})^4 + (x - \bar{1})^2 + (x - \bar{1})$;
в) $f(x) = (x + i)^5 - 5i(x + i)^4 - (3i + 10)(x + i)^3 + (-13 + 10i)(x + i)^2 + (22i + 5)(x + i) + 11 - i$.

22.23. а) $f(x) = (x^2 - 1)^3 - 4(x + 1)(x^2 - 1)^2 - (7x + 9)(x^2 - 1) - 4x - 5$;
б) $f(x) = x(x^3 + \bar{2})^2 + x(x^3 + \bar{2}) + \bar{4}x$;
в) $f(x) = (x^3 + i)^2 - 2i(x^3 + i) - 2x + i - 1$.

§ 23

23.2. $a_{11}a_{22} - a_{12}a_{21} \neq 0$.

23.3. а) $(f, g) = x + 1$; б) $(f, g) = 1$; в) $(f, g) = 1$; г) $(f, g) = 2x + 1$.

23.5. а) $(f, g) = x - 3$; б) $(f, g) = x^2 - x + 1$; в) $(f, g) = 1$;
г) $(f, g) = x + \bar{3}$; д) $(f, g) = x^2 + (1 + i)x + i$.

23.6. а) $[f, g] = x^4 - 4x^3 + 4x^2 - 5x - 2$;
б) $[f, g] = (2x^3 + 7x^2 + 4x - 3)(x - 1)$;
в) $[f, g] = (x^3 + \bar{6}x^2 + \bar{4}x + \bar{1})(x^3 + x^2 + \bar{3}x - \bar{4}) : (x + \bar{2})$;
г) $[f, g] = (x^3 - x^2 + 3x - 3)(x^4 + 2x^3 + 2x - 1)$;
д) $[f, g] = x^5 + 2ix^4 - 2x^3 - 2ix^2 + x$.

23.7. а) $u(x) = 1,\ v(x) = -x + 1$;

б) $u(x) = -x - \bar{1}$, $v(x) = x + \bar{2}$;

в) $u(x) = -\frac{x-1}{3}$, $v(x) = \frac{2x^2 - 2x - 3}{2}$;

г) $u(x) = -\frac{1}{9}(3x^2 + 10ix - 17)$, $v(x) = \frac{1}{28}(18x^3 + 57ix^2 - 159x - 78i)$.

23.8. Використати те, що

$$I = \{f(x)\,u(x) + g(x)\,v(x) \mid u(x),\ v(x) \in P[x]\}.$$

23.9. Ідеал I породжується многочленом $[f, g]$.

23.10. Ідеал I породжується найбільшим спільним дільником многочленів $f_1(x)$, $f_2(x)$, . . ., $f_n(x)$.

23.11. Многочлен $h(x)$ має ділитися на найбільший спільний дільник многочленів $f(x)$ і $g(x)$.

23.12. а) $u(x) = \frac{1}{2}(x^2 + x + 1) + (x - 1)\,s(x)$, $v(x) = -\frac{1}{2}(x^2 + x + 1) - (x + 1)\,s(x)$, де $s(x) \in Q[x]$;

б) $u(x) = \frac{x^2 + \bar{4}x}{\bar{3}} + (x + \bar{2})\,s(x)$, $v(x) = \frac{\bar{4}x + \bar{1}}{3}(x^2 + \bar{4}x) - (x^2 + x + \bar{1})\,s(x)$, де $s(x) \in Z_5[x]$;

в) рівняння розв'язків не має;

г) $u(x) = x + 1 + s(x)$, $v(x) = -x^4 + (i - 1)x^3 + (i - 1)x^2 + ix + i + 1 - (x - i)^2(x + i)\,s(x)$, де $s(x) \in C[x]$.

23.13. а) $(f, g, h) = x + 1$; б) $(f, g, h) = \bar{1}$; в) $(f, g, h) = x^2 + (i + 1)x + i$.

23.14. а) Рівняння розв'язків не має, оскільки многочлен $s(x)$ не ділиться на многочлен (f, g, h); б) рівняння має розв'язок, $s(x)$ ділиться на многочлен (f, g, h).

§ 24

24.2. $f_1(x) = x^2 + \bar{1}$, $f_2(x) = x^2 + x + \bar{2}$, $f_3(x) = x^2 + \bar{2}x + \bar{2}$.

24.5. Так (наприклад, $f(x) = x^2 + \bar{2}$).

24.8. $f(x) = (\bar{2}x + \bar{3})(x + \bar{1})(x + \bar{4})$.

24.9. а) $f(x) = (x - 1)(x + 1)(x^2 - 2)(2x - 1)$;

б) $f(x) = (x^2 - 1)(x^2 - 4)(3x + 1)$.

24.10. $f(x) = (x^2 + 1)(x^2 - 2)(2x - 1) = (x^2 + 1)(x - \sqrt{2})(x + \sqrt{2})(2x - 1) = (x - i)(x + i)(x - \sqrt{2})(x + \sqrt{2})(2x - 1)$.

24.15. а) $f(x) = (x + \bar{1})(x + \bar{2})(x + \bar{3})(x + \bar{4})$; б) незвідний;

в) $f(x) = (x^2 - \sqrt{2}x + 2)(x^2 + \sqrt{2}x + 2)$; г) звідний.

24.16. а) $f(x) = (x^2 - 7x + 1)(x^2 + 5x + 7)$;

б) $f(x) = \left(x - \frac{3 - \sqrt{5}}{2}\right)^2 \left(x - \frac{3 + \sqrt{5}}{2}\right)^2$;

в) $f(x) = (2x^2 + x + 3)^2$;

г) $f(x) = (x^2 - 6x + 1)(x^2 + x - 3)$;

д) $f(x) = \left(x - \frac{-1 - \sqrt{2}}{2}\right)\left(x - \frac{-1 + \sqrt{2}}{2}\right)\left(x - \frac{-3 + \sqrt{13}}{2}\right) \times \left(x - \frac{-3 - \sqrt{13}}{2}\right)$;

е) $f(x) = (x - 1)^2(x - 2)^2$;

є) $f(x) = \left(x - \frac{-7 - \sqrt{5}}{2}\right)^2 \left(x - \frac{-7 + \sqrt{5}}{2}\right)^2$;

ж) $f(x) = (x^2 + 5ax + 5a^2)^2$;

з) $f(x) = (x^2 + 12x + 26)(x^2 + 12x + 12)$;

і) $f(x) = (x^2 - 18)(x^2 + 8)$;

к) $f(x) = (x + \bar{1})^2(x + \bar{2})^2$;

л) незвідний;

м) $f(x) = (x - 1)(x + 1)(x^2 + 1)(x^4 + 1)$;

н) $f(x) = (x - 1)(x^2 + x + 1)(x^6 + x^3 + 1)$;

о) $f(x) = (x - 1)(x + 1)(x^2 + 1)(x^8 + x^4 + 1)$;

п) $f(x) = \left(x - \frac{\sqrt{2} - \sqrt{2}i}{2}\right)\left(x - \frac{\sqrt{2} + \sqrt{2}i}{2}\right)\left(x + \frac{\sqrt{2} + \sqrt{2}i}{2}\right) \times \left(x + \frac{\sqrt{2} - \sqrt{2}i}{2}\right)$;

р) $f(x) = x(x - \bar{1})(x - \bar{2})(x - \bar{3})(x - \bar{4})$.

24.17. а) $(f, g) = x^2 - x - 2$, $[f, g] = (x - 1)^2(x^2 + 1)(x^2 - 5x + 6)$;

б) $(f, g) = x - 1$, $[f, g] = (x^2 - 2x + 3)^2(x + 6)^2(x - 1)^2(x - 2)^2(x - 6)^2(x^2 + x + 1)$;

в) $(f, g) = (x + 1)^2$, $[f, g] = (x + 1)^3(x - 1)(x - 2)$;

г) $(f, g) = (x - i)(x + 1)$, $[f, g] = (x + 1)^3(x^2 + 1)(x - 1)(x - i)$;

д) $(f, g) = x + \bar{2}$, $[f, g] = x(x + \bar{1})(x + \bar{3})(x + \bar{4})(x^2 + x + \bar{1})^2$;

е) $(f, g) = x - 1$, $[f, g] = (x^{12} - 1)(x^2 + x + 1)(x^6 + x^3 + 1)$.

24.18. Ні.

24.19. $A^{-1} = \{-x + (x^2 + 1)\,s(x) \mid s(x) \in Q[x]\}$.

24.20. $A^{-1} = \{1 + (-x + 1)\,s(x) \mid s(x) \in Q[x]\} = A$.

24.21. а) Оберненого елемента не існує;

б) $A^{-1} = \left\{\frac{1}{3} + (x^2 + 4)\,s(x) \mid s(x) \in Q[x]\right\}$.

24.22. Ізоморфізмом є відображення

$$f(\{g(x) + x^2 + 1)\,s(x) \mid s(x) \in R[x]\}) = g(i).$$

§ 25

25.1. а) $f'(x) = 27(x^2 + x - 1)^2(2x + 1)(x^3 - 2) + 27x^2(x^2 + x - 1)^3$;

б) $f'(x) = 6i(3ix^2 - 1)((i + 1)x^2 - i) + 4x(-1 + i)(ix^3 - 3x)$;

в) $f'(x) = x(x + \bar{3}) + \bar{3}x^2$.

25.2. а) $\bar{4}$; б) $\bar{9}$.

25.6. $f(x) = \bar{2}x^6 + x^3 + x^2 + x + \bar{2}$.

25.7. $f(x) = 4x^3 + x^2 - x + 1$.

25.8. 2.

25.10. Усі, крім $f_1(x) = \bar{1}$, $f_2(x) = x^2$, $f_3(x) = x^2 + \bar{1}$, $f_4(x) = x^3 + x^2 + x$.

25.11. 54.

25.12. а) $f(x) = (x - 1)^4 + 2(x - 1)^3 + 3(x - 1)^2 - (x - 1) - 2$, $f'(1) = -1$, $f''(1) = 6$, $f'''(1) = 12$, $f^{IV}(1) = 24$;

б) $f(x) = (x + i)^5 - 5i(x + i)^4 - (3i + 10)(x + i)^3 + (10i - 13)(x + i)^2 + (5 + 22i)(x + i) + 11 - i$, $f'(-i) = 22i + 5$, $f''(-i) = 20i - 26$, $f'''(-i) = -60 - 18i$, $f^{IV}(-i) = -120i$, $f^{V}(-i) = 120$;

в) $f(x) = (x + 1)^4 - 4(x + 1)^3 - 9(x + 1)^2 + 36(x + 1) + 1$, $f'(-1) = 36$, $f''(-1) = -18$, $f'''(-1) = -24$, $f^{IV}(-1) = 24$;

г) $f(x) = \bar{4}(x - \bar{3})^5 + \bar{5}(x - \bar{3})^4 + \bar{7}(x - \bar{3})^3 + \bar{4}(x - \bar{3})^2 + \bar{8}(x - \bar{3}) + \bar{9}$, $f'(\bar{3}) = \bar{8}$, $f''(\bar{3}) = \bar{8}$, $f'''(\bar{3}) = \bar{9}$, $f^{IV}(\bar{3}) = \bar{10}$, $f^{V}(\bar{3}) = \bar{7}$;

д) $f(x) = \bar{2}(x - \bar{1})^4 + (x - \bar{1})^2 + (x - \bar{1})$, $f'(\bar{1}) = \bar{1}$, $f''(\bar{1}) = \bar{2}$, $f'''(\bar{1}) = \bar{0}$, $f^{IV}(\bar{1}) = \bar{0}$.

25.13. $f(x) = 2i(x^4 + (5i - 2)x^3 + (9i - 9)x^2 + (14 - 4i)x + (6i - 2))$.

25.15. а) 2; б) 1; в) 0; г) 5.

25.16. 1.

25.17. а) $a = -5$; б) $a \in \left\{-\frac{14}{27}, 18\right\}$; в) $a = 0$.

25.18. Якщо $a = 4$, то $f(x) = (x + 2)^2(x + 1)$. Якщо $a = \frac{102}{27}$, то $f(x) = \left(x + \frac{4}{3}\right)^2\left(x + \frac{7}{3}\right)$.

25.19. а) $4a^3 + 27b^2 = 0$; б) $27a^4 = 256b^3$;
в) $256a^5 + 3125b^4 = 0$; г) $3125b^3 + 108a^5 = 0$.
25.20. а) Не має; б) має; в) має; г) має; д) має.
25.21. а) $f(x) = (x-2)^2(x+1)$; б) $f(x) = (x+(1-2i))^4$;
в) $f(x) = (x^2+x+1)^2(x+2)$; г) $f(x) = (x+i)^3(x-2i)^2$;
д) $f(x) = (x+2)^3(x^2-x-i)$; е) $f(x) = (x-i)^3(x+3i)^2(x-1)$.

§ 26

26.1. Існує єдиний многочлен першого степеня $f(x) = x$, який задовольняє умову задачі. Кожен многочлен $f(x) = (4c-1)x^2 - (6+3c)x - 7c$ при $c \in \mathbf{R} \setminus \left\{\frac{1}{4}\right\}$ також задовольняє умову задачі.
26.2. Ні.
26.4. Якщо $\deg f = n$, то слід розглянути множину, що містить $n+1$ різних раціональних чисел і застосувати інтерполяційну формулу Лагранжа.

26.6. а) $f(x) = 2x^2 - x + 1$; б) $f(x) = \frac{x^2 - 4x + 6}{3}$; в) $f(x) = 2x$.

26.7. а) $f(x) = 2x^2 - x + 1$;

б) $f(x) = \frac{1}{24}x(x-1)(x-2)(x-3) + x + 1$;

в) $f(x) = 1 + 2x + \frac{2^2x(x-1)}{2!} + \ldots + \frac{2^nx(x-1)\ldots(x-n+1)}{n!}$.

26.8. а) $f(x) = 3x^2 - 1$;
б) $f(x) = -x + 5$;
в) $f(x) = i(x^2-1)(x-i) - (x-1)(x-i) - x + 1 - i$, $f(2i) = 8$, $f(0) = 0$;
г) $f(x) = 1 + \frac{1}{3}(x-1) - \frac{1}{48}(x-1)(x-4) + \frac{1}{720}(x-1)(x-4)(x-9)$,
$f(\bar{3}) = 1\frac{87}{120} = 1{,}725$, $(\sqrt{3} = 1{,}732\ldots)$, $f(2) = 1\frac{142}{360} = 1{,}39(4)$, $(\sqrt{2} = 1{,}4142\ldots)$.

26.9. $f(x) = \bar{3}(x+\bar{3})^2x(x+\bar{1})$.
26.10. $f_1(x) = x$, $f_2(x) = \bar{2}x$, $f_3(x) = \bar{2}x + \bar{1}$, $f_4(x) = x + \bar{1}$, $f_5(x) = \bar{2}x + \bar{2}$, $f_6(x) = x + \bar{2}$.

26.12. а) $\frac{x-1}{x-2}$; б) $\frac{3x+2}{(x^2+x+1)(x^3+1)}$;
в) $(x^3 - x + 1)(x^4 - x^2 + 1)$; г) заданий дріб нескоротний.
26.13. а) Так; б) ні; в) так; г) так; д) ні; е) ні.
26.14. а) $\frac{-5}{(2x-1)} + \frac{3}{x}$;
б) заданий дріб неправильний;
в) $\frac{1}{x+1} - \frac{3}{(x+1)^2} + \frac{3}{(x+1)^3}$;
г) $\frac{1}{x-1} - \frac{x-1}{x^2+1}$; д) $\frac{1}{x^2+x+2} - \frac{x-2}{(x^2+x+2)^2}$;
е) $\frac{x+1}{x^2+1} - \frac{x+2}{x^2+x+1}$; є) $\frac{6}{x^3} - \frac{4}{x^2} + \frac{1}{x+3} + \frac{3}{(x+3)^2}$;
ж) $\frac{x}{8(x^2+2x+2)} - \frac{x-4}{8(x^2-2x+2)}$;
з) $\frac{\sqrt{2}}{8(x-\sqrt{2})} - \frac{\sqrt{2}}{8(x+\sqrt{2})} + \frac{1}{2(x^2+2)}$.

26.15. а) $\frac{1}{3(x-i)} - \frac{1}{3(x+2i)}$;

б) $\frac{1}{x-1} - \frac{1+i}{2(x-i)} + \frac{i-1}{2(x+i)}$;
в) $\frac{1}{4(x-1+i)} - \frac{1}{4(x-1-i)} + \frac{i}{2(x-1+i)^2}$;
г) $\frac{\sqrt{2}}{8(x-\sqrt{2})} - \frac{\sqrt{2}}{8(x+\sqrt{2})} + \frac{\sqrt{2}}{8(x-\sqrt{2}i)} - \frac{\sqrt{2}}{8(x+\sqrt{2}i)}$.
26.16. а) $-\frac{1}{2x} + \frac{x^2}{2(x^3-2)}$; б) $\frac{1}{2(x^2-2)} + \frac{1}{2(x^2+2)}$;
в) $\frac{1}{x} - \frac{x}{x^2+1}$.
26.17. а) $\frac{1}{x} + \frac{2}{x+2} + \frac{2}{x+3}$;
б) $\frac{1}{4x} + \frac{1}{4(x+\bar{1})} + \frac{1}{4(x+\bar{2})} + \frac{1}{4(x+\bar{3})} + \frac{1}{4(x+\bar{4})}$;
в) $\frac{2}{x+2} + \frac{1}{x+3} + \frac{4}{x+4} + \frac{3}{(x+4)^2}$.

26.18. $\sum_{a=\bar{0}}^{\overline{p-1}} \frac{\bar{1}}{(x-\bar{a})(x+\bar{a})}$.

Розділ V

§ 27

27.1. а) $f(x, y) = x^5 + x^4y - 2x^3y^2 - xy^4 + 2y^5 + x^2 - 1$;
б) $f(x, y, z) = x^3y^2z + y^3z^2x + zx^2y - xy^2z^3 - yz^2x^3 - zx^2y^3$.
27.3. а) Від одного до трьох членів; б) від одного до шести членів; в) від одного до чотирьох членів; г) від одного до 10 членів.
27.6. а) 63; б) 728.
27.7. Однорідний многочлен другого степеня від трьох змінних у загальному вигляді містить 6 членів. Кожен з шести коефіцієнтів цих членів може набувати одне із значень $\bar{0}, \bar{1}, \bar{2}\ldots, \overline{p-1}$, і всі можливі варіанти повністю вичерпуються елементами множини Z_p^6. Множина Z_p^6 містить p^6 елементів. Якщо всі коефіцієнти дорівнюють 0, то матимемо нуль-многочлен. Отже, число всіх однорідних многочленів другого степеня від трьох змінних дорівнює $p^6 - 1$.
27.9. а) Вищий член $-3y^2x^4$; б) вищий член $\bar{2}x^2z$; в) вищий член xz.
27.10. а) наприклад, $f_1(x, y) = x + y + \bar{1}$ і $f_2(x, y) = x^2 + y^2 + \bar{1}$;
б) $f_1(x, y) = x^2 + x + y + \bar{1}$ і $f_2(x, y) = x^2 + y^2 + x + \bar{1}$.
27.16. Зробити заміну $x = ty$.
27.17. а) $f(x, y) = (3x^2 - 7xy - 4y^2)(3x^2 + 3xy + 4y^2)$;
б) $f(x, y) = (2x^2 - xy + 3y^2)^2$;
в) $f(x, y) = (x-y)^2$;
г) $f(x, y) = (x-y)(x+\bar{2}y)(x+\bar{3}y)$;
д) $f(x, y) = (x^2 - xy + y^2)(x^2 - 3xy + y^2)$.
27.18. а) $f(x, y, z) = 3(x+y)(x+z)(y+z)$;
б) $f(a, b, c) = -(a-b)(b-c)(c-a)$;
в) $f(a, b, c) = 3(a-b)(b-c)(c-a)$;
г) $f(x, y, z) = (x-y)(y-z)(z-x)$;
д) $f(x, y, z) = 12xyz(x+y+z)$;
е) $f(a, b, c) = 2(a-b)(b-c)(a-c)(a+b+c)$;
є) $f(x, y, z) = (x-y)(y-z)(x-z)(xy+yz+xz)$.
ж) $f(a, b, c) = -(a-b)(b-c)(c-a)(a^2+b^2+c^2+ab+ac+bc)$;
з) $f(x, y, z) = 5(x+y)(x+z)(y+z)(x^2+y^2+z^2+xy+xz+yz)$;
і) $f(x, y, z) = 5(x-y)(y-z)(z-x)(x^2+y^2+z^2-xy-xz-yz)$.
27.19. Використати розклад многочлена $g(x, y, z) = (x+y+z)^3 - x^3 - y^3 - z^3$ на незвідні множники (див. задачу 27.18, а).

§ 28

28.1. а) Ні; б) так; в) так;г) ні; д) так.

28.2. а) Додати x_2^2 і $2x_1$; б) додати x_2^3, x_3^3 і $2x_1x_3$; в) додати x_3^2 і $2x_2x_3$.

28.3. а) $5x_1^4x_2^2x_3$; б) $-3x_1^2x_2^2x_3^2$.

28.4. а) $f(x, y) = \sigma_1^2\sigma_2 + 2\sigma_1^2 - 2\sigma_2^2 - 4\sigma_2$;

б) $f(x, y) = 2\sigma_1^2\sigma_2 - 6\sigma_1\sigma_2^2 - 5\sigma_1\sigma_2$.

28.9. а) $f(x_1, x_2, x_3) = \sigma_1^3 - 3\sigma_1\sigma_2 + 3\sigma_3 - \sigma_1$;

б) $f(x_1, x_2, x_3) = \sigma_1^4\sigma_3 - 4\sigma_1^2\sigma_2\sigma_3 + 2\sigma_2^2\sigma_3 + 4\sigma_1\sigma_3^2 + 2\sigma_3$;

в) $f(x_1, x_2, x_3) = \sigma_1^2\sigma_2 + \frac{28}{3}\sigma_1^3\sigma_3 - \sigma_2^3 + \frac{10}{3}\sigma_1\sigma_2\sigma_3$;

б) $f(x_1, x_2, x_3) = 2\sigma_1^2 - 6\sigma_2$.

д) $f(x_1, x_2, x_3) = -5\sigma_1^3 + 36\sigma_1\sigma_2 + 132\sigma_3$;

е) $f(x_1, x_2, x_3) = \sigma_1^3\sigma_3 - \sigma_2^3$.

28.10. а) 0; б) $\frac{1}{2}$; в) $-\frac{5}{3}$.

28.11. а) $o(x_1, x_2, x_3) = \sigma_1^2\sigma_2 - \frac{7}{3}\sigma_2^2$.

б) $o(x_1, x_2, x_3, x_4) = \sigma_2$;

в) $o(x_1, x_2, \ldots, x_n) = \sigma_1^3 - 3\sigma_1\sigma_2 + 3\sigma_3$.

§ 29

29.1. а) $(x, y) \in \{(2, 3), (3, 2)\}$; б) $(x, y) \in \{(1, 2), (2, 1)\}$;
в) $(x, y) \in \{(5, 3), (3, 5), (-3, -5), (-5, -3)\}$; г) $(x, y) \in \{(3, -2); (-2, 3)\}$;
д) $(x, y) \in \{(1, 2), (2, 1)\}$; е) $(x, y, z) \in \{(1, 2, -2), (1, -2, 2), (2, 1, -2), (2, -2, 1), (-2, 2, 1), (-2, 1, 2)\}$;
є) $(x, y, z) \in \{(1, -2, 3), (1, -3, 2), (2, -1, 3), (2, -3, 1), (3, -1, 2), (3, -2, 1)\}$.

29.2. а) $(x, y) \in \{(1, 64), (64, 1)\}$;
б) $(x, y) \in \{(16, 81), (81, 16), (-16, -81), (-81, -16)\}$.

29.3. а) $\{1, 4\}$; б) $\{3, 4, 6 \pm \sqrt{29}\}$; в) $\{2, 11\}$;
г) $\{-8, -73\}$; д) $x = 0$.

29.4. а) $f(x, y) = (2x + y)(x + 2y)(x - 5y)(5x - y)$;
б) $f(x, y) = (2x^2 + 3xy + 2y^2)(x - 3y)(3x - y)$;
в) $f(x, y) = (x^2 - xy + y^2)(2x^2 + xy + 2y^2)$;
г) $f(x, y) = (x - 3y)(3x - y)(2x + 3y)(3x + 2y)$.

29.5. а) $f(x, y, z) = \sigma_1\sigma_2 = (x + y + z)(xy + xz + yz)$;
б) $f(x, y, z) = (xy + xz + yz)(x^2 + y^2 + z^2)$;
в) $f(x, y, z) = 2((x + y + z)^2 - 3xy - 3xz - 3yz)^2$;
г) $f(x, y, z) = (xy + xz + yz)^2$.

29.6. $\frac{f(x, y, z)}{g(x, y, z)} = \frac{1}{x + y + z}$.

29.7. $x^2 - 12x + 27 = 0$.

29.8. Застосувавши рекурентну формулу задачі 28.5 і метод математичної індукції, довести, що $x^n + y^n$ є цілим числом. Далі, показати, що $s_n = -s_{n-3} + 5(7s_{n-2} - s_{n-3})$ для всіх $n > 3$. Подільність на 5 числа s_n приведе до подільності на 5 одного з чисел s_1, s_2 або s_3, що неможливо.

29.9. $t^3 - 2t^2 - 47t - 144 = 0$.

§ 30

30.1. а) 162; б) —128; в) 0; г) —3564; д) 1768; е) 41; є) 10; ж) 651; з) 44; к) —7; л) 136; м) 59.

30.3. а) $\lambda = 1$; б) $\lambda = 2$; г) $\lambda = 2$; д) $\lambda = -1$.

30.4. а) —108; б) 0; в) —27036; г) 144; д) 0; е) 725; є) 50000;
ж) $(-1)^{\frac{n(n-1)}{2}} n^n a^{n-1}$.

30.8. а) $\lambda = 3$; б) $\lambda \in \{0, \pm 2\}$; в) $\lambda = 2 + 4i$.

30.9. а) $(x, y) \in \left\{(3, 2), (-3, -2), \left(2\sqrt{2}, -\frac{3\sqrt{2}}{2}\right), \left(-2\sqrt{2}, \frac{3\sqrt{2}}{2}\right)\right\}$;

б) $(x, y) \in \{(\sqrt{3}, 0), (-\sqrt{3}, 0), (2, -1)\}$;

в) $(x, y) \in \left\{(1, 0), (2, 1), \left(\frac{-19 - \sqrt{177}}{2}, \frac{9 + \sqrt{177}}{2}\right)\right\}$;

г) $(x, y) = (-1, 3)$;
д) $(x, y) \in \{(0, 0), (2, -1), (1, 2), (1, 68), (2, 52)\}$;
е) $(x, y) = (1, 2)$.

Розділ VI

§ 31

31.3. Ні.

31.4. $Q(\sqrt{5})$.

31.5. $Q[x]/\langle x^2 + 1\rangle$.

31.6. Можна, наприклад, встановити ізоморфізм між полем $R[x]/\langle x^2 + 1\rangle$ і полем комплексних чисел C.

31.7. Ні (наприклад, рівняння $x^3 + 2 = 0$ не має коренів у цьому полі).

31.8. а) $m = 9$; б) $m = 13$; в) $m = 4$; г) $m = 1 + \sqrt{13}$.

31.9. а) Ні; б) так.

31.10. а) $f(x) = 5\left(x + \frac{1 - 7i}{5}\right)\left(x + \frac{1 + 7i}{5}\right)$;

б) $f(x) = (x - 1)(x - i)$;

в) $f(x) = \left(x - \frac{3 - \sqrt{5}}{2}\right)^2\left(x - \frac{3 + \sqrt{5}}{2}\right)^2$;

г) $f(x) = (x - 3 + 2i)(x + 3 - 2i)(x - 3 - 2i)(x + 3 + 2i)$;

д) $f(x) = (x - 1)(x + 1)(x - i)(x + i)\left(x - \frac{\sqrt{2}}{2} - \frac{\sqrt{2}}{2}i\right)\left(x - \frac{\sqrt{2}}{2} + \frac{\sqrt{2}}{2}i\right)\left(x + \frac{\sqrt{2}}{2} - \frac{\sqrt{2}}{2}i\right)\left(x + \frac{\sqrt{2}}{2} + \frac{\sqrt{2}}{2}i\right)$;

е) $f(x) = (x - i)(x + i)\left(x + \frac{4 + \sqrt{17}}{2}\right)\left(x + \frac{4 - \sqrt{17}}{2}\right)$.

31.11. а) $f(x) = x^3 - (1 + i)x^2 + (1 + 2i)x + 1 - i$;
б) $f(x) = x^5 - (10 + 2i)x^4 + (14 + 20i)x^3 - (64 + 28i)x^2 + (40 + 128i)x - 80i$;
в) $f(x) = x^4 + (3 + 6i)x^3 + (-12 + 18i)x^2 - (36 + 8i)x - 24i$.

31.12. 23.

31.13. 7.

31.15. а) $y^3 + 2y^2 + 25 = 0$; б) $y^3 - 6y^2 - \frac{2}{9}y - \frac{2}{3} = 0$.

31.16. Знайти суму квадратів коренів многочлена.

31.17. а) $f(x) = x^3 + 6x^2 + 5x - 6$ і $x_1 = -2$, $x_{2,3} = -2 \pm \sqrt{7}$;

б) $f(x) = x^3 - 18x^2 + 68x + 24$ і $x_1 = 6$, $x_{2,3} = 6 \pm 2\sqrt{10}$.

31.18. Якщо $r = 8$, то $x_1 = 1$, $x_2 = 2$, $x_3 = 4$; якщо $r = 20$, то $x_1 = -2$, $x_2 = -1$, $x_3 = 10$; якщо $r = 28 - 12\sqrt{2}$, то $x_1 = \sqrt{2}$, $x_2 = 2\sqrt{2}$, $x_3 = 7 - 3\sqrt{2}$; якщо $r = 28 + 12\sqrt{2}$, то $x_1 = -2\sqrt{2}$, $x_2 = -\sqrt{2}$, $x_3 = 7 + 3\sqrt{2}$.

31.19. $f(x) = x^5 - \frac{5}{4}(3 + i)x^4 + \frac{10}{3}(1 + 5i)x^3 - 10(1 + 3i)x^2 - 40(1 - i)x - \frac{605}{12} + \frac{305}{12}i$.

31.21. $x_1 = \sqrt{3} - \sqrt{2}$, $x_2 = \sqrt{3}$, $x_3 = \sqrt{3} + \sqrt{2}$.

31.22. $x_1 = -\frac{5}{2}$, $x_2 = \frac{1}{2}$, $x_3 = \frac{3}{2}$.

31.23. $x_1 = 1$, $x_2 = 2$, $x_3 = 3$, та $p = 11$ і $q = -6$.

§ 32

32.1. а) $x_{1,2} = -1 \pm i\sqrt{3}$, $x_{3,4} = \frac{1 \pm \sqrt{13}}{2}$; б) $x_{1,2} = -1 \pm i$, $x_{3,4} = \frac{3 \pm \sqrt{11}i}{2}$;

в) $x_{1,2} = 2 \pm i$, $x_3 = -4$, $x_4 = 1$; г) $x_{1,2} = 2 \pm i$, $x_{3,4} = 3 \pm \sqrt{2}i$.

32.2. $a = -20$, $b = -50$, $x_2 = -3 - i$, $x_3 = 5$.

32.5. а) Так; б) ні; в) так; г) ні.

32.6. $a = -243$, $x_{1,2} = \pm 9i$, $x_3 = -1$, $x_4 = 3$.

32.10. а) $f(x) = (x^2 - 2x + 5)(x + 1)(x + 5)$;

б) $f(x) = \left(x^2 + x + \frac{3 + \sqrt{5}}{2}\right)\left(x^2 + x + \frac{3 - \sqrt{5}}{2}\right)$;

в) $f(x) = \frac{1}{4}(2x^2 + (1 + \sqrt{5})x + 2)(2x^2 + (1 - \sqrt{5})x + 2)$;

г) $f(x) = (x^2 - 3x + 3)(x^2 + x + 1)$;

д) $f(x) = (x^2 + 1)(x + 1)^2(x^2 - x + 1)$.

32.11. а) Ні; б) так.

32.12. Ні.

§ 33

33.1. а) 31; б) $-\frac{229}{108}$; в) $\frac{i}{27}$; г) $-\frac{175}{2916}$; д) 0; е) $4 + i$.

33.2. а) $x_1 = -2$, $x_{2,3} = 1$;

б) $x_1 = i$, $x_2 = \frac{3 - \sqrt{3}}{2}i$, $x_3 = \frac{-3 - \sqrt{3}}{2}i$;

в) $x_1 = \sqrt[3]{28 + \sqrt{272}} + \sqrt[3]{28 - \sqrt{272}}$,

$x_{2,3} = -\frac{x_1}{2} \pm \frac{\sqrt[3]{28 + \sqrt{272}} - \sqrt[3]{28 - \sqrt{272}}}{2}\sqrt{3}i$;

г) $x_1 = -\frac{1}{2}$, $x_{2,3} = 1$;

д) $x_1 = \sqrt[3]{\frac{9}{2} + \sqrt{\frac{139}{108}}} + \sqrt[3]{\frac{9}{2} - \sqrt{\frac{139}{108}}} + 2$, $x_{2,3} = -\frac{x_1 + 2}{2} \pm \frac{\sqrt{3}}{2}i \times$

$\times\left(\sqrt[3]{\frac{9}{2} + \sqrt{\frac{139}{108}}} - \sqrt[3]{\frac{9}{2} - \sqrt{\frac{139}{108}}}\right)$;

е) $x_1 = \sqrt[3]{\frac{79}{54} + \frac{\sqrt{77}}{3}} + \sqrt[3]{\frac{79}{54} - \frac{\sqrt{77}}{3}}$;

$x_{2,3} = -\frac{3x_1 - 2}{6} \pm \frac{\sqrt{3}}{2}i\left(\sqrt[3]{\frac{79}{54} + \frac{\sqrt{77}}{3}} - \sqrt[3]{\frac{79}{54} - \frac{\sqrt{77}}{3}}\right) + \frac{2}{3}$;

е) $x_{1,2,3} = 2\sqrt[3]{-2 - 2i}$;

ж) $x_1 = (1 + \sqrt{6})i$, $x_{2,3} = -\frac{1 + \sqrt{6}}{2}i \pm \frac{1 - \sqrt{6}}{2} \cdot \frac{\sqrt{3}}{2}i$.

33.3. $a \in]-\infty; 0[\cup]1; +\infty[$.

33.4. Якщо $a = 1$, то $x = 0$. Якщо $a = \frac{4}{31}$, то $x = -\frac{3}{2}$.

33.5. $D = -\frac{3}{4}a^6$.

33.6. Якщо $a \in]-\infty; -1[\cup]-1; 0[\cup]3; +\infty[$, то рівняння має один дійсний і два комплексних корені; якщо $a \in \{-1, 0, 3\}$, то рівняння має три дійсних корені, два з яких дорівнюють один одному; якщо $a \in]0;3[$, то рівняння має три різних дійсних корені.

33.9. Зробити заміну. Прирівнявши коефіцієнти при відповідних степенях змінної в здобутому і шуканому рівняннях, матимемо $n = \frac{9a_0 - a_2a_1}{2(a_2^2 - 3a_1)}$; $m = \sqrt{-\frac{3n^2 + 2a_2n + a_1}{3}}$, $a = m^3$ і $b = n^3 + a_2n^2 + a_1n + a_0$.

33.10. а) $n = -3$, $m = 1$ і $y^3 - 3y^2 - 3y + 1 = 0$;

б) $n = \frac{1}{2}$, $m = \frac{5}{6}\sqrt{3}$, $\frac{125}{72}\sqrt{3}y^3 + \frac{27}{4}y^2 - \frac{125}{24}\sqrt{3}y - \frac{9}{4} = 0$.

в) $n = -2$, $m = 1$, $y^3 - 2y^2 - 3y + \frac{2}{3} = 0$.

33.12. а) $\varphi = \frac{\pi}{4}$; $y_1 = \operatorname{tg}\frac{\pi}{12}$, $y_2 = -1$, $y_3 = \operatorname{tg}\frac{5}{12}\pi$; б) $\varphi = \frac{\pi}{6}$; $y_1 = \operatorname{tg}\frac{\pi}{18}$, $y_2 = \operatorname{tg}\frac{13}{18}\pi$, $y_3 = \operatorname{tg}\frac{7}{18}\pi$; в) $\varphi = \frac{3}{4}\pi$; $y_1 = 1$, $y_2 = \operatorname{tg}\frac{11}{12}\pi$, $y_3 = \operatorname{tg}\frac{7}{12}\pi$; г) $\varphi = \arcsin\frac{1}{\sqrt{5}}$;

$y_1 = \operatorname{tg}\frac{\varphi}{3}$, $y_2 = \operatorname{tg}\frac{\varphi + 2\pi}{3}$, $y_3 = \operatorname{tg}\frac{\varphi + 4\pi}{3}$.

33.13. а) $x_1 = -\frac{b}{a}$, $x_{2,3} = \pm\sqrt{-\frac{c}{a}}$.

33.17. а) $x = -\frac{3}{4}$; б) $x = \frac{1}{2}$; в) $x_1 = -2$, $x_2 = 1$; г) $x = -3$; д) $x_1 \approx -2,6$, $x_2 \approx -0,4$, $x_3 = \frac{1}{2}$.

33.18. а) $x_{1,2} = \frac{1 \pm \sqrt{11}i}{2}$, $x_{3,4} = \frac{-1 \pm \sqrt{3}i}{2}$;

б) $x_{1,2} = \sqrt{2}i$, $x_{3,4} = \frac{-1 \pm \sqrt{15}i}{2}$;

в) $x_{1,2} = \frac{+1 \pm \sqrt{29}}{2}$, $x_{3,4} = \frac{5 \pm i\sqrt{7}}{3}$;

г) $x_{1,2} = \frac{-1 \pm i\sqrt{11}}{6}$, $x_{3,4} = \frac{-3 \pm \sqrt{21}}{6}$;

д) $x_{1,2} = \frac{1 + \sqrt{3} \pm \sqrt{12 + 2\sqrt{3}}}{4}$, $x_{3,4} = \frac{1 - \sqrt{3} \pm \sqrt{12 - 2\sqrt{3}}}{4}$.

33.20. а) $x_{1,2} = -1 \pm 2i$, $x_{3,4} = -1 \pm i$; б) $x_{1,2} = \frac{1 \pm \sqrt{3}i}{2}$, $x_3 = -1$, $x_4 = 2$.

33.22. а) $x_{1,2} = \frac{\sqrt{2} - 1 \pm i\sqrt{5 + 2\sqrt{2}}}{2}$, $x_{3,4} = \frac{\sqrt{2} + 1 \pm i\sqrt{5 - 2\sqrt{2}}}{2}$;

б) $x_{1,2} = \frac{-5 \pm \sqrt{17}}{2}$, $x_{3,4} = \frac{-1 \pm \sqrt{7}i}{2}$.

§ 34

34.1. а) $\frac{1}{8} < |x| < 8$; б) $\frac{7}{8} < |x| < 8$; в) $2 < |x| < 7$; г) $\frac{1}{55} < |x| < 28$.

34.2. а) $\frac{3}{2}$; б) 2; в) 2; г) 4, розглянути многочлен $\varphi(x) = -f(x)$.

34.3. а) 1; б) 1; в) $\frac{1}{2}$.

34.4. а) 6; б) 2; в) 3; г) 100.

34.5. а) Додатних коренів два або жодного, від'ємних — два або жодного; б) додатних коренів три або один, від'ємних — немає; в) додатних коренів два або жодного, від'ємних — п'ять або один; г) додатний корінь один, від'ємних — п'ять, три або один; д) додатний корінь один; від'ємних — два або жодного.

34.6. а) $]-2;\ -1[,\ ]1;\ 3[$; б) $\left]-\frac{9}{2};\ -1\right[,\ \left]\frac{9}{2};\ 1\right[$; в) $]-5;\ -\frac{1}{4}[,\ ]\frac{1}{4};\ 5[$; г) $\left]-\frac{5}{2};\ -\frac{1}{4}\right[,\ \left]\frac{1}{4};\ \frac{5}{2}\right[$; д) $]-4;\ -\frac{1}{4}[,\ ]\frac{1}{4};\ 4[$.

34.8. а) $x_1 \in]-2;\ -1[$, $x_2 \in]-1;\ 0[$, $x_3 \in]1;\ 2[$;
б) $x_1 \in]-2;\ -1[$, $x_2 \in]0;\ 1[$, $x_3 \in]1;\ 2[$;
в) один дійсний корінь: $x \in]0;\ 1[$;
г) два дійсних корені: $x_1 \in]0;\ 1[$, $x_2 \in]5;\ 6[$;
д) три дійсних корені: $x_1 \in]-3;\ -2[$, $x_2 \in]-1;\ 0[$; $x_3 = 1$;
е) два дійсних корені: $x_1 \in]0;\ 1[$, $x_2 \in]1;\ 2[$;
є) дійсних коренів многочлен не має.

Розділ VII

§ 35

35.1. а) $x_1 = -3$, $x_2 = 2$, $x_{3,4} = \frac{5 \pm \sqrt{17}}{2}$; б) $x_1 = -2$, $x_{2,3} = 2 \pm i$; в) $x_1 = -2$, $x_2 = 3$, $x_{3,4} = \pm 4$; г) $x_1 = \frac{1}{2}$, $x_{2,3} = 1 \pm i$; д) $x_1 = \frac{1}{3}$, $x_{2,3} = \frac{-1 \pm i\sqrt{15}}{8}$; е) $x_1 = -\frac{1}{2}$, $x_{2,3} = \frac{2 \pm i}{5}$; є) $x_1 = \frac{1}{2}$, $x_{2,3} = -1 \pm \sqrt{3}\,i$; ж) $x_{1,2} = 1$, $x_{3,4} = -3$; з) $x_1 = a$, $x_2 = b$, $x_3 = c$; к) $x_1 = 2a$, $x_2 = a$, $x_3 = -1$; л) $x_1 = 1$, $x_2 = a$, $x_3 = 1 - a$; м) $x_1 = 1$, $x_2 = b - a$, $x_3 = b + a$.

35.2. а) $x_1 = -1$, $x_2 = 2$; б) рівняння раціональних коренів не має; в) $x_1 = -3$, $x_2 = -1$, $x_3 = 1$; г) $x = -3$; д) $x_{1,2} = 1$.

35.3. а) $f(x) = (x^2 + x + 1)(x + 1)(x - 1)$; б) $f(x) = (x - 1)(x^3 - 6x + 2)$; в) $f(x) = (x^2 + 1)(6x^2 - 13x + 6)$; г) $f(x) = (3x^2 - x + 4)(3x^2 - 4x + 4)$; д) $f(x) = 2(x^2 + 8x + 23)(x + 3)(x + 5)$; е) $f(x) = (x^3 + 3x^2 + 3x - 4)(x^3 + 3x^2 + 3x - 3)$.

35.4. а) Многочлен не має цілих коренів; б) застосувати критерій Ейзенштейна; в) зробити заміну $x = y + 1$ і застосувати критерій Ейзенштейна; г) многочлен не має цілих коренів і не розкладається у добуток двох квадратних тричленів з з кільця $Q[x]$; е) зробити заміну $x = y + 1$ і застосувати критерій Ейзенштейна.

35.5. а) $f(x) = (x^2 + 4x + 1)(x^2 - 3x + 1)$; б) незвідний; в) незвідний; г) зробити заміну $x = y - 1$ і довести, що $f(x)$ є незвідним.

35.7. а) Довести, що $f(x)$ не ділиться на многочлени $\varphi_1(x) = x$, $\varphi_2(x) = x + 1$ і $\varphi_3(x) = x^2 + x + 1$ у кільці $Z_2[x]$ і застосувати задачу 35.6; г) многочлен не має раціональних коренів.

§ 36

36.1. а) $f(x) = x^4 - 4x^2 - 1$; б) $f(x) = x^4 - 4x^3 + 8x - 1$; в) $f(x) = x^4 - 56x^2 + 4$; г) $f(x) = x^3 + 3x^2 + 3x + 3$; д) $f(x) = x^6 - 15x^4 + 6x^3 + 75x^2 + 90x - 116$; е) $f(x) = x^6 - 4x^3 - 3$; є) $f(x) = x^6 - 6x^5 + 12x^4 - 8x^3 - 6$; ж) $f(x) = x^2 - 2x + 4$.

36.2. а) $Q(\sqrt{2} + \sqrt{5})$; б) $Q(\sqrt{3})$; в) $Q(\sqrt{5} + \sqrt{7})$; г) $Q(\sqrt{p} + \sqrt{q})$; д) $Q(\sqrt{2} + \sqrt{3})$; е) $Q(\sqrt{2} + \sqrt{3} + \sqrt{5})$.

36.3. а) $1,\ \sqrt[3]{3},\ \sqrt[3]{9}$; б) $1,\ \sqrt{3}$; в) $1,\ \sqrt{3},\ \sqrt{5},\ \sqrt{15}$; г) $1,\ \sqrt{5},\ \sqrt{7},\ \sqrt{35}$; д) $1,\ \sqrt{2},\ \sqrt{3},\ \sqrt{5},\ \sqrt{10},\ \sqrt{6},\ \sqrt{15},\ \sqrt{30}$.

§ 37

37.1. а) $-1 - \omega$; б) $\frac{1}{2}\omega(\omega^2 - \omega - 1)$; в) $\frac{1}{255}\omega(\omega^2 - 1)(64\omega^3 - 16\omega^2 + 4\omega - 257)$; г) $-\frac{1}{1509}\omega(64\omega^2 - 24\omega - 503)$; д) $\frac{1}{20}(\omega^2 + \omega)(\omega^2 + 5)$.

37.2. а) $-\sqrt[4]{8} - \sqrt[4]{4} + 3\sqrt[4]{2} + 1$; б) $\frac{1}{6}\left(\sqrt[3]{4} - 2\sqrt[3]{2} + 4\right)$; в) $\frac{1}{93}\left(-2\sqrt[3]{4} + 17\sqrt[3]{2} - 5\right)$; г) $\frac{1}{33}\left(-\sqrt[3]{49} + 5\sqrt[3]{7} + 8\right)$; д) $-\frac{1}{567}\left(81\sqrt[4]{27} + 345\sqrt[4]{9} + 821\sqrt[4]{3} + 81\right)$.

37.3. а) $\sqrt[3]{36} + \sqrt[3]{30} + \sqrt[3]{25}$; б) $\sqrt[5]{81} + \sqrt[5]{54} + \sqrt[5]{36} + \sqrt[5]{24} + \sqrt[5]{16}$; в) $\left(\sqrt[3]{3} + \sqrt[8]{2}\right)\left(\sqrt[3]{3} + \sqrt[4]{2}\right)\left(\sqrt{3} + \sqrt{2}\right)$; г) $\frac{1}{8}\left(\sqrt[9]{5^8} - 9\sqrt[9]{5^7} \cdot 3 + \sqrt[9]{5^6} \cdot 3^2 - \ldots + \sqrt[9]{3^8}\right)$

37.4. $\frac{(\sqrt{a} + \sqrt{b} + \sqrt{c})(\sqrt{ab} + \sqrt{ac} + \sqrt{bc}) - (a\sqrt{a} + b\sqrt{b} + c\sqrt{c}) - 5\sqrt{abc}}{2(ab + ac + bc) - (a^2 + b^2 + c^2)}$;

в) $\frac{\left(\sqrt[3]{a^2} + \sqrt[3]{b^2} + \sqrt[3]{c^2} - \sqrt[3]{ab} - \sqrt[3]{ac} - \sqrt[3]{bc}\right)\left((a+b+c)^2 + 3(a+b+c)\sqrt[3]{abc} + 9\sqrt[3]{(abc)^2}\right)}{(a + b + c)^3 - 27abc}$.

37.5. а) $a + a^2 + b^3 - 3ab = 0$; б) $a^2p^3 + aq^3 + r^3 - 3apqr = 0$; в) $ab = 0$.

Додаток 1

Таблиця простих чисел від 2 до 4057 та їхніх первісних коренів

p	g	p	g	p	g	p	g	p	g	p	g	p	g
2	1	179	2	419	2	661	2	947	2	1229	2	1523	2
3	2	181	2	421	2	673	5	953	3	1231	3	1531	2
5	2	191	19	431	7	677	2	967	5	1237	2	1543	5
7	3	193	5	433	5	683	5	971	6	1249	7	1549	2
11	2	197	2	439	15	691	3	977	3	1259	2	1553	3
13	2	199	3	443	2	701	2	983	5	1277	2	1559	19
17	3	211	2	449	3	709	2	991	6	1279	3	1567	3
19	2	223	3	457	13	719	11	997	7	1283	2	1571	2
23	5	227	2	461	2	727	5	1009	11	1289	6	1579	3
29	2	229	6	463	3	733	6	1013	3	1291	2	1583	5
31	3	233	3	467	2	739	3	1019	2	1297	10	1597	11
37	2	239	7	479	13	743	5	1021	10	1301	2	1601	3
41	6	241	7	487	3	751	3	1031	14	1303	6	1607	5
43	3	251	6	491	2	757	2	1033	5	1307	2	1609	7
47	5	257	3	499	7	761	6	1039	3	1319	13	1613	3
53	2	263	5	503	5	769	11	1049	3	1321	13	1619	2
59	2	269	2	509	2	773	2	1051	7	1327	3	1621	2
61	2	271	6	521	3	787	2	1061	2	1361	3	1627	3
67	2	277	5	523	2	797	2	1063	3	1367	5	1637	2
71	7	281	3	541	2	809	3	1069	6	1373	2	1657	11
73	5	283	3	547	2	811	3	1087	3	1381	2	1663	3
79	3	293	2	557	2	821	2	1091	2	1399	13	1667	2
83	2	307	5	563	2	823	3	1093	5	1409	3	1669	2
89	3	311	17	569	3	827	2	1097	3	1423	3	1693	2
97	5	313	10	571	3	829	2	1103	5	1427	2	1697	3
101	2	317	2	577	5	839	11	1109	2	1429	6	1699	3
103	5	331	3	587	2	853	2	1117	2	1433	3	1709	3
107	2	337	10	593	3	857	3	1123	2	1439	7	1721	3
109	6	347	2	599	7	859	2	1129	11	1447	3	1723	3
113	3	349	2	601	7	863	5	1151	17	1451	2	1733	2
127	3	353	3	607	3	877	2	1153	5	1453	2	1741	2
131	2	359	7	613	2	881	3	1163	5	1459	5	1747	2
137	3	367	6	617	3	883	2	1171	2	1471	6	1753	7
139	2	373	2	619	2	887	5	1181	7	1481	3	1759	6
149	2	379	2	631	2	907	2	1187	2	1483	2	1777	5
151	6	383	5	641	3	911	17	1193	3	1487	5	1783	10
157	5	389	2	643	11	919	7	1201	11	1489	14	1787	2
163	2	397	5	647	5	929	3	1213	2	1493	2	1789	6
167	5	401	3	653	2	937	5	1217	3	1499	2	1801	11
173	2	409	21	659	2	941	2	1223	5	1511	11	1811	6

p	g	p	g	p	g	p	g	p	g	p	g	p	g
1823	5	2131	2	2437	2	2749	6	3083	2	3433	5	3733	2
1831	3	2137	10	2441	6	2753	3	3089	3	3449	3	3739	7
1847	5	2141	2	2447	5	2767	3	3109	6	3457	7	3761	3
1861	2	2143	3	2459	2	2777	3	3119	7	3461	2	3767	5
1867	2	2153	3	2467	2	2789	2	3121	7	3463	3	3769	7
1871	14	2161	23	2473	5	2791	6	3137	3	3467	2	3779	2
1873	10	2179	7	2477	2	2797	2	3163	3	3469	2	3793	5
1877	2	2203	5	2503	3	2801	3	3167	5	3491	2	3797	2
1879	6	2207	5	2521	17	2803	2	3169	7	3499	2	3803	2
1889	3	2213	2	2531	2	2819	2	3181	7	3511	7	3821	3
1901	2	2221	2	2539	2	2833	5	3187	2	3517	2	3823	3
1907	2	2237	2	2543	5	2837	2	3191	11	3527	5	3833	3
1913	3	2239	3	2549	2	2843	2	3203	2	3529	17	3847	5
1931	2	2243	2	2551	6	2851	2	3209	3	3533	2	3851	2
1933	5	2251	7	2557	2	2857	11	3217	5	3539	2	3853	2
1949	2	2267	2	2579	2	2861	2	3221	10	3541	7	3863	5
1951	3	2269	2	2591	7	2879	7	3229	6	3547	2	3877	2
1973	2	2273	3	2593	7	2887	5	3251	6	3557	2	3881	13
1979	2	2281	7	2609	3	2897	3	3253	2	3559	3	3889	11
1987	2	2287	19	2617	5	2903	5	3257	3	3571	2	3907	2
1993	5	2293	2	2621	2	2909	2	3259	3	3581	2	3911	13
1997	2	2297	5	2633	3	2917	5	3271	3	3583	3	3917	2
1999	3	2309	2	2647	3	2927	5	3299	2	3593	3	3919	3
2003	5	2311	3	2657	3	2939	2	3301	6	3607	5	3923	2
2011	3	2333	2	2659	2	2953	13	3307	2	3613	2	3929	3
2017	5	2339	2	2663	5	2957	2	3313	10	3617	3	3931	2
2027	2	2341	7	2671	7	2963	2	3319	6	3623	5	3943	3
2029	2	2347	3	2677	2	2969	3	3323	2	3631	15	3947	2
2039	7	2351	13	2683	2	2971	10	3329	3	3637	2	3967	6
2053	2	2357	2	2687	5	2999	17	3331	3	3643	2	3989	2
2063	5	2371	2	2689	19	3001	14	3343	5	3659	2	4001	3
2069	2	2377	5	2693	2	3011	2	3347	2	3671	13	4003	2
2081	3	2381	3	2699	2	3019	2	3359	11	3673	5	4007	5
2083	2	2383	5	2707	2	3023	5	3361	22	3677	2	4013	2
2087	5	2389	2	2711	7	3037	2	3371	2	3691	2	4019	2
2089	7	2393	3	2713	5	3041	3	3373	5	3697	5	4021	2
2099	2	2399	11	2719	3	3049	11	3389	3	3701	2	4027	3
2111	7	2411	6	2729	3	3061	6	3391	3	3709	2	4049	3
2113	5	2417	3	2731	3	3067	2	3407	5	3719	7	4051	6
2129	3	2423	5	2741	2	3079	6	3413	2	3727	3	4057	5

Додаток 2

ТАБЛИЦІ ПЕРВІСНИХ КОРЕНІВ ТА ІНДЕКСІВ

Просте число 3

Первісні корені: 2

N	0	1	2	3	4	5	6	7	8	9
0		0	1							

I	0	1	2	3	4	5	6	7	8	9
0	1	2								

Просте число 5

Первісні корені: 2, 3

N	0	1	2	3	4	5	6	7	8	9
0		0	1	3	2					

I	0	1	2	3	4	5	6	7	8	9
0	1	2	4	3						

Просте число 7

Первісні корені: 3, 5

N	0	1	2	3	4	5	6	7	8	9
0		0	2	1	4	5	3			

I	0	1	2	3	4	5	6	7	8	9
0	1	3	2	6	4	5				

Просте число 11

Первісні корені: 2, 6, 7, 8

N	0	1	2	3	4	5	6	7	8	9
0		0	1	8	2	4	9	7	3	6
1	5									

I	0	1	2	3	4	5	6	7	8	9
0	1	2	4	8	5	10	9	7	3	6

Просте число 13

Первісні корені: 2, 6, 7, 11

N	0	1	2	3	4	5	6	7	8	9
0		0	1	4	2	9	5	11	3	8
1	10	7	6							

I	0	1	2	3	4	5	6	7	8	9
0	1	2	4	8	3	6	12	11	9	5
1	10	7								

Просте число 17

Первісні корені: 3, 5, 6, 7, 11, 12, 14.

N	0	1	2	3	4	5	6	7	8	9
0		0	14	1	12	5	15	11	10	2
1	3	7	13	4	9	6	8			

I	0	1	2	3	4	5	6	7	8	9
0	1	3	9	10	13	5	15	11	16	14
1	8	7	4	12	2	6				

[1] Скрізь за основу таблиці індексів береться найменший первісний корінь.

Просте число 19

Первісні корені: 2, 3, 10, 14, 15

N	0	1	2	3	4	5	6	7	8	9
0		0	1	13	2	16	14	6	3	8
1	17	12	15	5	7	11	4	10	9	

I	0	1	2	3	4	5	6	7	8	9
0	1	2	4	8	16	13	7	14	9	18
1	17	15	11	3	6	12	5	10		

Просте число 23

Первісні корені: 5, 7, 10 11, 14, 15, 17, 19, 20, 21

N	0	1	2	3	4	5	6	7	8	9
0		0	2	16	4	1	18	19	6	10
1	3	9	20	14	21	17	8	7	12	15
2	5	13	11							

I	0	1	2	3	4	5	6	7	8	9
0	1	5	2	10	4	20	8	17	16	11
1	9	22	18	21	13	19	3	15	6	7
2	12	14								

Просте число 29

Первісні корені: 2, 3, 8, 10, 11, 14, 15, 18, 19, 21, 26, 27

N	0	1	2	3	4	5	6	7	8	9
0		0	1	5	2	22	6	12	3	10
1	23	25	7	18	13	27	4	21	11	9
2	24	17	26	20	8	16	19	15	14	

I	0	1	2	3	4	5	6	7	8	9
0	1	2	4	8	16	3	6	12	24	19
1	9	18	7	14	28	27	25	21	13	26
2	23	17	5	10	20	11	22	15		

Просте число 31

Первісні корені: 3, 11, 12, 13, 17, 21, 22, 24

N	0	1	2	3	4	5	6	7	8	9
0		0	24	1	18	20	25	28	12	2
1	14	23	19	11	22	21	6	7	26	4
2	8	29	17	27	13	10	5	3	16	9
3	15									

I	0	1	2	3	4	5	6	7	8	9
0	1	3	9	27	19	26	16	17	20	29
1	25	13	8	24	10	30	28	22	4	12
2	5	15	14	11	2	6	18	23	7	21

Просте число 37

Первісні корені: 2, 5, 13, 15, 17, 18, 19, 20, 22, 24, 32, 35

N	0	1	2	3	4	5	6	7	8	9
0		0	1	26	2	23	27	32	3	16
1	24	30	28	11	33	13	4	7	17	35
2	25	22	31	15	29	10	12	6	34	21
3	14	9	5	20	8	19	18			

I	0	1	2	3	4	5	6	7	8	9
0	1	2	4	8	16	32	27	17	34	31
1	25	13	26	15	30	23	9	18	36	35
2	33	29	21	5	10	20	3	6	12	24
3	11	22	7	14	28	19				

Просте число 41

Первісні корені: 6, 7, 11, 12, 13, 15, 17, 19, 22, 24, 26, 28, 29, 30, 34, 35

N	0	1	2	3	4	5	6	7	8	9
0		0	26	15	12	22	1	39	38	30
1	8	3	27	31	25	37	24	33	16	9
2	34	14	29	36	13	4	17	5	11	7
3	23	28	10	18	19	21	2	32	35	6
4	20									

I	0	1	2	3	4	5	6	7	8	9
0	1	6	36	11	25	27	39	29	10	19
1	32	28	4	24	21	3	18	26	33	34
2	40	35	5	30	16	14	2	12	31	22
3	9	13	37	17	20	38	23	15	8	7

Просте число 43

Первісні корені: 3, 5, 12, 18, 19, 20, 26, 28, 29, 30, 33, 34

N	0	1	2	3	4	5	6	7	8	9
0		0	27	1	12	25	28	35	39	2
1	10	30	13	32	20	26	24	38	29	19
2	37	36	15	16	40	8	17	3	5	41
3	11	34	9	31	23	18	14	7	4	33
4	22	6	21							

I	0	1	2	3	4	5	6	7	8	9
0	1	3	9	27	38	28	41	37	25	32
1	10	30	4	12	36	22	23	26	35	19
2	14	42	40	34	16	5	15	2	6	18
3	11	33	13	39	31	7	21	20	17	8
4	24	29								

Просте число 47

Первісні корені: 5, 10, 11, 13, 15, 19, 20, 22, 23, 26, 29, 30, 31, 33, 35, 39, 40, 41, 43, 44, 45

N	0	1	2	3	4	5	6	7	8	9
0		0	18	20	36	1	38	32	8	40
1	19	7	10	11	4	21	26	16	12	45
2	37	6	25	5	28	2	29	14	22	35
3	39	3	44	27	34	33	30	42	17	31
4	9	15	24	13	43	41	23			

I	0	1	2	3	4	5	6	7	8	9
0	1	5	25	31	14	23	21	11	8	40
1	12	13	18	43	27	41	17	38	2	10
2	3	15	28	46	42	22	16	33	24	26
3	36	39	7	35	34	29	4	20	6	30
4	9	45	37	44	32	19				

Просте число 53

Первісні корені: 2, 3, 5, 8, 12, 14, 18, 19, 20, 21, 22, 26, 27, 31, 32, 33, 34, 35, 39, 41, 45, 48, 50, 51

N	0	1	2	3	4	5	6	7	8	9
0		0	1	17	2	47	18	14	3	34
1	48	6	19	24	15	12	4	10	35	37
2	49	31	7	39	20	42	25	51	16	46
3	13	33	5	23	11	9	36	30	38	41
4	50	45	32	22	8	29	40	44	21	28
5	43	27	26							

I	0	1	2	3	4	5	6	7	8	9
0	1	2	4	8	16	32	11	22	44	35
1	17	34	15	30	7	14	28	3	6	12
2	24	48	43	33	13	26	52	51	49	45
3	37	21	42	31	9	18	36	19	38	23
4	46	39	25	50	47	41	29	5	10	20
5	40	27								

Просте число 59

Первісні корені: 2, 6, 8, 10, 11, 13, 14, 18, 23, 24, 30, 31, 32, 33, 34, 37, 38, 39, 40, 42, 43, 44, 47, 50, 52, 54, 55, 56

N	0	1	2	3	4	5	6	7	8	9
0		0	1	50	2	6	51	18	3	42
1	7	25	52	45	19	56	4	40	43	38
2	8	10	26	15	53	12	46	34	20	28
3	57	49	5	17	41	24	44	55	39	37
4	9	14	11	33	27	48	16	23	54	36
5	13	32	47	22	35	31	21	30	29	

I	0	1	2	3	4	5	6	7	8	9
0	1	2	4	8	16	32	5	10	20	40
1	21	42	25	50	41	23	46	33	7	14
2	28	56	53	47	35	11	22	44	29	58
3	57	55	51	43	27	54	49	39	19	38
4	17	34	9	18	36	13	26	52	45	31
5	3	6	12	24	48	37	15	30		

Просте число 61

Первісні корені: 2, 6, 7, 10, 17, 18, 26, 30, 31, 35, 43, 44, 51, 54, 55, 59

N	0	1	2	3	4	5	6	7	8	9
0		0	1	6	2	22	7	49	3	12
1	23	15	8	40	50	28	4	47	13	26
2	24	55	16	57	9	44	41	18	51	35
3	29	59	5	21	48	11	14	39	27	46
4	25	54	56	43	17	34	58	20	10	38
5	45	53	42	33	19	37	52	32	36	31
6	30									

I	0	1	2	3	4	5	6	7	8	9
0	1	2	4	8	16	32	3	6	12	24
1	48	35	9	18	36	11	22	44	27	54
2	47	33	5	10	20	40	19	38	15	30
3	60	59	57	53	45	29	58	55	49	37
4	13	26	52	43	25	50	39	17	34	7
5	14	28	56	51	41	21	42	23	46	31

Просте число 67

Первісні корені: 2, 7, 11, 12, 13, 18, 20, 28, 31, 32, 34, 41, 44, 46, 48, 50, 51, 57, 61, 63

N	0	1	2	3	4	5	6	7	8	9
0		0	1	39	2	15	40	23	3	12
1	16	59	41	19	24	54	4	64	13	10
2	17	62	60	28	42	30	20	51	25	44
3	55	47	5	32	65	38	14	22	11	58
4	18	53	63	9	61	27	29	50	43	46
5	31	37	21	57	52	8	26	49	45	36
6	56	7	48	35	6	34	33			

I	0	1	2	3	4	5	6	7	8	9
0	1	2	4	8	16	32	64	61	55	43
1	19	38	9	18	36	5	10	20	40	13
2	26	52	37	7	14	28	56	45	23	46
3	25	50	33	66	65	63	59	51	35	3
4	6	12	24	48	29	58	49	31	62	57
5	47	27	54	41	15	30	60	53	39	11
6	22	44	21	42	17	34				

Просте число 71

Первісні корені: 7, 11, 13, 21, 22, 28, 31, 33, 35, 42, 44, 47, 52, 53, 55, 56, 59, 61, 62, 63, 65, 67, 68, 69

N	0	1	2	3	4	5	6	7	8	9
0		0	6	26	12	28	32	1	18	52
1	34	31	38	39	7	54	24	49	58	16
2	40	27	37	15	44	56	45	8	13	68
3	60	11	30	57	55	29	64	20	22	65
4	46	25	33	48	43	10	21	9	50	2
5	62	5	51	23	14	59	19	42	4	3
6	66	69	17	53	36	67	63	47	61	41
7	35									

I	0	1	2	3	4	5	6	7	8	9
0	1	7	49	59	58	51	2	14	27	47
1	45	31	4	28	54	23	19	62	8	56
2	37	46	38	53	16	41	3	21	5	35
3	32	11	6	42	10	70	64	22	12	13
4	20	69	57	44	24	26	40	67	43	17
5	48	52	9	63	15	34	25	33	18	55
6	30	68	50	66	36	39	60	65	29	61

Просте число 73

Первісні корені: 5, 11, 13, 14, 15, 20, 26, 28, 29, 31, 33, 34, 39, 40, 42, 44, 45, 47, 53, 58, 59, 60, 62, 68

N	0	1	2	3	4	5	6	7	8	9
0		0	8	6	16	1	14	33	24	12
1	9	55	22	59	41	7	32	21	20	62
2	17	39	63	46	30	2	67	18	49	35
3	15	11	40	61	29	34	28	64	70	65
4	25	4	47	51	71	13	54	31	38	66
5	10	27	3	53	26	56	57	68	43	5
6	23	58	19	45	48	60	69	50	37	52
7	42	44	36							

I	0	1	2	3	4	5	6	7	8	9
0	1	5	25	52	41	59	3	15	2	10
1	50	31	9	45	6	30	4	20	27	62
2	18	17	12	60	8	40	54	51	36	34
3	24	47	16	7	35	29	72	68	48	21
4	32	14	70	58	71	63	23	42	64	28
5	67	43	69	53	46	11	55	56	61	13
6	65	33	19	22	37	39	49	26	57	66
7	38	44								

Просте число 79

Первісні корені: 3, 6, 7, 28, 29, 30, 34, 35, 37, 39, 43, 47, 48, 53, 54, 59, 60, 63, 66, 68, 70, 74, 75, 77

N	0	1	2	3	4	5	6	7	8	9
0		0	4	1	8	62	5	53	12	2
1	66	68	9	34	57	63	16	21	6	32
2	70	54	72	26	13	46	38	3	61	11
3	67	56	20	69	25	37	10	19	36	35
4	74	75	58	49	76	64	30	59	17	28
5	50	22	42	77	7	52	65	33	15	31
6	71	45	60	55	24	18	73	48	29	27
7	41	51	14	44	23	47	40	43	39	

I	0	1	2	3	4	5	6	7	8	9
0	1	3	9	27	2	6	18	54	4	12
1	36	29	8	24	72	58	16	48	65	37
2	32	17	51	74	64	34	23	69	49	68
3	46	59	19	57	13	39	38	35	26	78
4	76	70	52	77	73	61	25	75	67	43
5	50	71	55	7	21	63	31	14	42	47
6	62	28	5	15	45	56	10	30	11	33
7	20	60	22	66	40	41	44	53		

Просте число 83

Первісні корені: 2, 5, 6, 8, 13, 14, 15, 18, 19, 20, 22, 24, 32, 34, 35, 39, 42, 43, 45, 46, 47, 50, 52, 53, 54, 55, 56, 57, 58, 60, 62, 66, 67, 71, 72, 73, 74, 76, 79, 80

N	0	1	2	3	4	5	6	7	8	9
0		0	1	72	2	27	73	8	3	62
1	28	24	74	77	9	17	4	56	63	47
2	29	80	25	60	75	54	78	52	10	12
3	18	38	5	14	57	35	64	20	48	67
4	30	40	81	71	26	7	61	23	76	16
5	58	46	79	59	53	51	11	37	13	34
6	19	66	39	70	6	22	15	45	58	50
7	36	33	65	69	21	44	49	32	68	43
8	31	42	41							

I	0	1	2	3	4	5	6	7	8	9
0	1	2	4	8	16	32	64	45	7	14
1	28	56	29	58	33	66	49	15	30	60
2	37	74	65	47	11	22	44	5	10	20
3	40	80	77	71	59	35	70	57	31	62
4	41	82	81	79	75	67	51	19	38	76
5	69	55	27	54	25	50	17	34	68	53
6	23	46	9	18	36	72	61	39	78	73
7	63	43	3	6	12	24	48	13	26	52
8	21	42								

Просте число 89

Первісні корені: 3, 6, 7, 13, 14, 15, 19, 23, 24, 26, 27, 28, 29, 30, 31, 33, 35, 38, 41, 43, 46, 48, 51, 54, 56, 58, 59, 60, 61, 62, 63, 65, 66, 70, 74, 75, 76, 82, 83, 86

N	0	1	2	3	4	5	6	7	8	9
0		0	16	1	32	70	17	81	48	2
1	86	84	33	23	9	71	64	6	18	35
2	14	82	12	57	49	52	39	3	25	59
3	87	31	80	85	22	63	34	11	51	24
4	30	21	10	29	28	72	73	54	65	74
5	68	7	55	78	19	66	41	36	75	43
6	15	69	47	83	8	5	13	56	38	58
7	79	62	60	20	27	53	67	77	40	42
8	46	4	37	61	26	76	45	60	44	

I	0	1	2	3	4	5	6	7	8	9
0	1	3	9	27	81	65	17	51	64	14
1	42	37	22	66	20	60	2	6	18	54
2	73	41	34	13	39	28	84	74	44	43
3	40	31	4	12	36	19	57	82	68	26
4	78	56	79	59	88	86	80	62	8	24
5	72	38	25	75	47	52	67	23	69	29
6	87	83	71	35	16	48	55	76	50	61
7	5	15	45	46	49	58	85	77	53	70
8	32	7	21	63	11	33	10	30		

Просте число 97

Первісні корені: 5, 7, 10, 13, 14, 15, 17, 21, 23, 26, 29, 37, 38, 39, 40, 41, 56, 57, 58, 59, 60, 68, 71, 74, 76, 80; 82, 83, 84, 87, 90, 92

N	0	1	2	3	4	5	6	7	8	9
0		0	34	70	68	1	8	31	6	44
1	35	86	42	25	65	71	40	89	78	81
2	69	5	24	77	76	2	59	18	3	13
3	9	46	74	60	27	32	16	91	19	95
4	7	85	39	4	58	45	15	84	14	62
5	36	63	93	10	52	87	37	55	47	67
6	43	64	80	75	12	26	94	57	61	51
7	66	11	50	28	29	72	53	21	33	30
8	41	88	23	17	73	90	38	83	92	54
9	79	56	49	20	22	82	48			

I	0	1	2	3	4	5	6	7	8	9
0	1	5	25	28	43	21	8	40	6	30
1	53	71	64	29	48	46	36	83	27	38
2	93	77	94	82	22	13	65	34	73	74
3	79	7	35	78	2	10	50	56	86	42
4	16	80	12	60	9	45	31	58	96	92
5	72	69	54	76	89	57	91	67	44	26
6	33	68	49	51	61	14	70	59	4	20
7	3	15	75	84	32	63	24	23	18	90
8	62	19	95	87	47	41	11	55	81	17
9	85	37	88	52	66	39				

Додаток 3

Таблиця квадратів натуральних чисел від 1 до 99

	0	1	2	3	4	5	6	7	8	9
0	0	1	4	9	16	25	36	49	64	81
1	100	121	144	169	196	225	256	289	324	361
2	400	441	484	529	576	625	676	729	784	841
3	900	961	1024	1089	1156	1225	1296	1369	1444	1521
4	1600	1681	1764	1849	1936	2025	2116	2209	2304	2401
5	2500	2601	2704	2809	2916	3025	3136	3249	3364	3481
6	3600	3721	3844	3969	4096	4225	4356	4489	4624	4761
7	4900	5041	5184	5329	5476	5625	5776	5929	6084	6241
8	6400	6561	6724	6889	7056	7225	7396	7569	7744	7921
9	8100	8281	8464	8649	8836	9025	9216	9409	9604	9801

СПИСОК ЛІТЕРАТУРИ

1. Завало С. Т. та ін. Алгебра і теорія чисел.— К.: Вища шк. Головне вид-во, 1976.— Ч. 2.— 384 с.
2. Завало С. Т. и др. Алгебра и теория чисел.— К.: Вища шк. Головное изд-во, 1980.— Ч. 2.— 402 с.
3. Куликов Л. Я. Алгебра и теория чисел.— М.: Высш. шк., 1979.— 559 с.
4. Ляпин Е. С., Евсеев А. Е. Алгебра и теория чисел.— М.: Просвещение, 1974.— Ч. 1.— 383 с.
5. Ляпин Е. С., Евсеев А. Е. Алгебра и теория чисел.— М.: Просвещение, 1978.— Ч. 2.— 448 с.
6. Курош А. Г. Курс высшей алгебры.— М.: Наука, 1971.— 432 с.
7. Окунев Л. Я. Высшая алгебра.— М.: Просвещение, 1966.— 336 с.
8. Кострикин А. И. Введение в алгебру.— М.: Наука, 1977.— 496 с.
9. Проскуряков И. В. Числа и многочлены.— М.: Просвещение, 1965.— 284 с.
10. Виноградов И. М. Основы теории чисел.— М.: Наука, 1981.— 176 с.
11. Бухштаб А. А. Теория чисел.— М.: Просвещение, 1966.— 384 с.
12. Михелович Ш. Х. Теория чисел.— М.: Высш. шк., 1967.— 336 с.
13. Грибанов В. У., Титов П. И. Сборник упражнений по теории чисел.— М.: Просвещение, 1964.— 143 с.
14. Бородін О. І. Теорія чисел.— К.: Вища шк. Головне вид-во, 1970.—274 с.
15. Фаддеев Д. К., Соминский И. С. Сборник задач по высшей алгебре.— М.: Наука, 1977.— 288 с.
16. Кудреватов Г. А. Сборник задач по теории чисел.— М.: Просвещение, 1970.— 128 с.
17. Оре О. Приглашение в теорию чисел.— М.: Наука, 1980.— 128 с.
18. Фаддеев Д. К. Лекции по алгебре.— М.: Наука, 1984.— 416 с.
19. Алгебра и теория чисел / Н. А. Казачек, Г. Н. Перлатов, Н. Я. Виленкин, А. И. Бородин — М.: Просвещение, 1974.— 200 с.
20. Яковкин М. В. Вычислительные действия над многочленами.— М.: Учпедгиз, 1961.— 80 с.
21. Давыдов А. К. Сборник задач по алгебре и элементарным функциям.— М.: Учпедгиз, 1959.— 150 с.
22. Ляпин С. Е. и др. Сборник задач по элементарной алгебре.— М.: Просвещение, 1973.— 351 с.
23. Окунев Л. Я. Сборник задач по высшей алгебре.— М.: Просвещение, 1964.— 185 с.
24. Алгебра і теорія чисел: Практикум: В 2-х ч. / С. Т. Завало, С. С. Левіщенко, В. В. Пилаев, І. О. Рокицький — К.: Вища шк. Головне вид-во, 1983.— Ч. 1.— 232 с.
25. Проскуряков И. В. Сборник задач по линейной алгебре.— М.: Наука, 1974.— 384 с.
26. Боревич З. И., Шафаревич И. Р. Теория чисел.— М.: Наука, 1972.— 495 с.
27. Калужнин Л. А. Введение в общую алгебру.— М.: Наука, 1973.— 448 с.
28. Ван-дер-Варден Б. Л. Алгебра.— М.: Мир, 1977.— 623 с.
29. Постников М. М. Теория Галуа.— М.: Физматгиз, 1963.— 220 с.
30. Постников М. М. Введение в теорию алгебраических чисел.— М.: Наука, 1982.— 239 с.
31. Эдвардс Г. Последняя теорема Ферма.— М.: Мир, 1980.— 484 с.
32. Хинчин А. Я. Цепные дроби.— М.: Наука, 1978.— 112 с.
33. Кантор И. Л., Солодовников А. С. Гиперкомплексные числа.— М.: Наука, 1973.— 144 с.
34. Скорняков Л. А. Элементы алгебры.— М.: Наука, 1980.— 240 с.
35. Хассе Г. Лекции по теории чисел.— М.: Изд-во иностр. лит., 1953.— 528 с.

36. Дэвенпорт Г. Высшая арифметика.— М.: Наука. 1965.— 175 с.
37. Джекобсон Н. Теория колец.— М.: Изд-во иностр. лит., 1947.— 288 с.
38. Ленг С. Алгебра.— М.: Мир, 1968.— 564 с.
39. Садовничий В. А., Подколозин А. С. Задачи студенческих олимпиад по математике.— М.: Наука, 1978.— 207 с.
40. Венгерские математические олимпиады.— М.: Мир, 1976.— 543 с.
41. Зубалевич Г. И. Сборник задач московских математических олимпиад.— М.: Просвещение, 1967.— 232 с.
42. Шклярский Д. О. и др. Избранные задачи и теоремы элементарной математики: Арифметика и алгебра.— М.: Наука, 1976.— 378 с.
43. Глухов М. М., Солодовников А. С. Задачник-практикум по курсу высшей алгебры.— М.: Просвещение, 1965.— 207 с.
44. Болтянский В. Г., Виленкин Н. Я. Симметрия в алгебре.— М.: Наука, 1967.— 283 с.

ОСНОВНІ ПОЗНАЧЕННЯ

$\pi(x)$ — число простих чисел, які не перевищують x, 7
(a, b) — найбільший спільний дільник цілих чисел a і b, 11
$[a, b]$ — найменше спільне кратне цілих чисел a і b, 12
$\tau(n)$ — число всіх натуральних дільників n, 17
$\sigma(n)$ — сума всіх натуральних дільників n, 17
$\varphi(n)$ — функція Ейлера, 17
$[x]$ — ціла частина дійсного числа x, 17
$\{x\}$ — дробова частина дійсного числа x, 18
$[q_0; q_1, q_2, \ldots, q_n, \ldots]$ — ланцюговий дріб, 25
$[(q_0; q_1, q_2, \ldots, q_n)]$ — чистий періодичний ланцюговий дріб, 25
$[q_0; q_1, \ldots, q_m, (p_0, \ldots, p_n)]$ — мішаний періодичний ланцюговий дріб, 25
m_g — запис числа m в g-ковій системі числення, 37
$\sim$ — знак асоційованості, 45
$<x>$ — головний ідеал, породжений елементом x, 51
K/I — фактор-кільце кільця K за ідеалом I, 51
Z_m — фактор-кільце $Z/<m>$ кільця Z цілих чисел за головним ідеалом $<m>$, 51
$\bar{a}$ — клас лишків з представником a, 51
$\equiv$ — знак конгруентності, 51
$\simeq$ — знак гомоморфізму, 57
$\cong$ — знак ізоморфізму, 57
$\mathrm{Ker}\varphi$ — ядро гомоморфізму φ, 58
$\mathrm{Nr}(Z)$ — норма елемента Z, 64
$K_a^{(m)}$ — клас лишків з представником a за модулем m, 77
$\left(\frac{a}{p}\right)$ — символ Лежандра, 104
$P_m(a) = \delta_m(a)$ — показник числа a за модулем m, 111
$\mathrm{ind}_g a \pmod m$ — індекс числа a за модулем m при основі g, 115
$P[x]$ — кільце многочленів від однієї змінної x над кільцем P, 126
$\deg f$ — степінь многочлена f, 127
(f, g) — найбільший спільний дільник многочленів f і g, 142
$[f, g]$ — найменше спільне кратне многочленів f і g, 142
$R[x_1, x_2, \ldots, x_n]$ — кільце многочленів від n змінних $x_1, x_2, \ldots, x_n$ над областю цілісності R, 165
$\sigma_1, \sigma_2, \ldots, \sigma_n$ — елементарні симетричні многочлени, 170
$R(f, g)$ — результант многочленів f і g, 178
$D(f)$ — дискримінант многочлена $f(x)$, 179
$P(a)$ — просте розширення поля P, 202

ПРЕДМЕТНЫЙ ПОКАЖЧИК

ЗМІСТ

Сергей Трофимович Завало
Сергей Сергеевич Левищенко
Владимир Владимирович Пылаев
Иван Александрович Рокицкий

АЛГЕБРА И ТЕОРИЯ ЧИСЕЛ

ПРАКТИКУМ
Часть 2

Допущено Министерством просвещения УССР в качестве учебного пособия для студентов физико-математических факультетов педагогических институтов

(На украинском языке)

Киев,
Головное издательство
издательского объединения «Выща школа»

Редактор Г. П. Трофімчук
Художній редактор С. В. Анненков
Технічний редактор І. І. Каткова
Коректор Н. В. Волкова

Здано до набору 19.03.85. Підп. до друку 07.03.86. Формат 60×90/16. Папір друк. № 2. Літ. гарн. Вис. друк. Друк. арк. 16,5. Фарб.-відб. 16,14. Обл.-вид. арк. 20,18. Тираж 3460 пр. Вид. № 7082. Зам. № 5-271. Ціна 85 к.

Головне видавництво видавничого об'єднання «Вища школа», 252054, Київ-54, вул. Гоголівська, 7

Харківська книжкова фабрика «Комуніст», 310012, Харків, вул. Енгельса, 11.