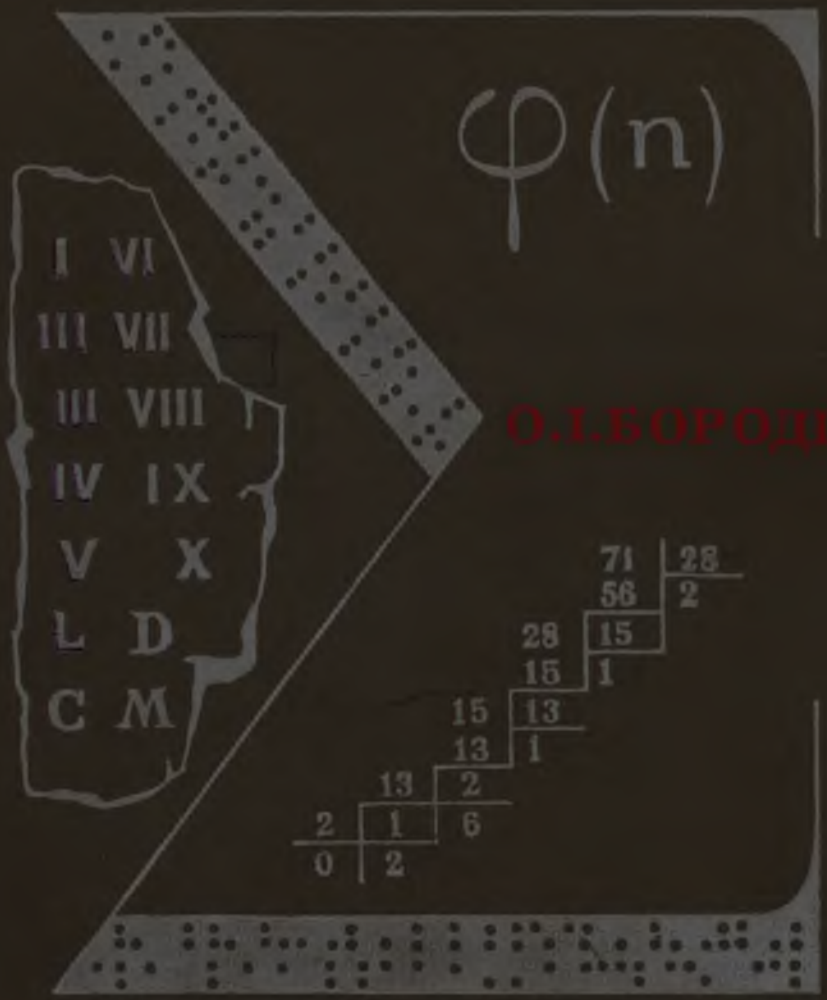
ТЕОРІЯ



О.І.БОРОДІН

ЧИСЕЛ

О. І. БОРОДІН

ТЕОРІЯ ЧИСЕЛ

ВИДАННЯ ТРЕТЄ, ПЕРЕРОБЛЕНЕ І ДОПОВНЕНЕ

Допущено Міністерством освіти УРСР
як підручник для фізико-математичних факультетів
педагогічних інститутів УРСР

ВИДАВНИЦТВО „ВИЩА ШКОЛА"
КИЇВ — 1970

УДК 511.2(075.8)

Теория чисел. Бородин А. И. «Вища школа», 1970, 275 стр. (на украинском языке).

Изложенный в книге материал соответствует действующей программе по теории чисел для педагогических институтов. Кроме теоретического материала, в ней рассмотрены примеры, которые иллюстрируют теорию, облегчают изучение и усвоение соответствующих вопросов программы. В конце каждого раздела помещены примеры и задачи, предназначенные для практических занятий и составления вариантов контрольных работ для студентов, а в конце каждого параграфа даны контрольные вопросы для самопроверки.
Учебник предназначен для студентов физико-математических факультетов педагогических институтов

Табл. 35. Библ. 84.

ПЕРЕДМОВА ДО 1-ГО ВИДАННЯ

Цей підручник з теорії чисел складено на основі лекцій, які автор читає з 1947 р. в Донецькому педагогічному інституті (на стаціонарі і на заочному відділі). Підручник відповідає діючій програмі з теорії чисел для фізико-математичних факультетів педагогічних інститутів. Крім теоретичного матеріалу, у ньому подано практичні застосування теорії чисел і її методів, зокрема арифметичні застосування теорії конгруенцій.

У тексті докладно розглянуто ряд прикладів, які ілюструють теорію й полегшують вивчення та засвоєння відповідного матеріалу. В кінці кожного розділу вміщено приклади й задачі як обчислювального, так і теоретичного характеру, призначені для практичних занять і складання варіантів контрольних робіт для студентів-заочників. Деякі задачі, а також вказівки до їх розв'язування взято з різних посібників з теорії чисел. Це стосується здебільшого задач теоретичного характеру.

Висловлюю щиру подяку доцентам Галетову І. П. і Сукалло А. А. за ряд цінних зауважень, які були враховані при остаточній редакції підручника.

ПЕРЕДМОВА ДО 2-ГО ВИДАННЯ

Це видання відрізняється від попереднього тим, що в ньому багато положень уточнено, замінено доведення деяких теорем (на нашу думку) більш доступними, виправлено помічені помилки. Деякі параграфи значно перероблено; особливо це стосується § 48, 49 і 50. Перероблено також § 4, 8, 11, 12, 13, 19, 21, 32, 33 і 38; § 11 і 12 об'єднані. Дещо розширено історичний матеріал.

ПЕРЕДМОВА ДО 3-ГО ВИДАННЯ

Це видання відрізняється від попереднього насамперед тим, що в ньому після кожного параграфа подано контрольні запитання для самоперевірки, додано матеріал про ірраціональні числа (§ 42) відповідно до нової програми з теорії чисел, додано розв'язування двочленних показникових конгруенцій (§ 32), значно скорочено вступ, вилучено історичні відомості з тексту

і виносок, історичні коментарі, що містять короткий огляд розвитку розглянутих понять, подано після кожного розділу. Крім цього, значно перероблено § 13, 34, 38, виправлено помічені помилки і неточності в окремих означеннях, формулюваннях і доведеннях теорем, додано деякі задачі теоретичного характеру і вказівки до них тощо.

Це видання підручника не лише відповідає новій діючій програмі з теорії чисел для педагогічних інститутів, а й цілком охоплює весь програмний матеріал для студентів університетів, тому вони також можуть користуватися ним.

Автор

ВСТУП

Предмет теорії чисел. Основні розділи теорії чисел

Теорія чисел належить до найбільш стародавніх розділів математики. У класичному розумінні — це вивчення властивостей натуральних (цілих додатних) чисел.

Теорію чисел іноді називають *вищою арифметикою*, бо вона виникла із задач арифметики, пов'язаних з множенням і діленням цілих чисел.

Теорія чисел має давню історію, і в цій галузі математики, починаючи з середини XVIII століття і до цього часу, досягнуто видатних успіхів. Але багато основних питань, які виникли в процесі розвитку теорії чисел, незважаючи на елементарність їх постановки, не були розв'язані протягом ряду століть не тільки засобами самої теорії чисел, а й залученням найдосконаліших засобів інших розділів математики.

Розвиток теорії чисел має величезне значення для багатьох розділів математики. Важко назвати такий розділ математики, який не був би пов'язаний з поняттям натурального числа, що є одним з основних понять усієї математики. Теорія чисел в сучасному розумінні вивчає не тільки властивості цілих раціональних чисел, а й властивості інших класів чисел. Використовуючи при розв'язуванні своїх задач результати і методи різних математичних дисциплін, теорія чисел, у свою чергу, відіграє велику роль у розвитку і вдосконаленні цих дисциплін.

Років 80 тому німецький математик Кронекер говорив, що теорія чисел тим добра, що вона не має застосувань. Тепер ця абстрактна галузь математики широко використовується у найрізноманітніших галузях науки. Результати, здобуті в геометрії чисел, використовують для наближеного обчислення складних інтегралів. Теорія чисел допомагає розв'язувати проблеми теорії інформації і значно зменшує затрати машинного часу при розв'язуванні спеціальних задач. Нарешті, слід зазначити, що теорія чисел тісно пов'язана з деякими питаннями природознавства, її застосовують у кристалографії при дослідженні решіток кристалів. Усе це робить теорію чисел однією з найважливіших дисциплін математики.

Теорія чисел у сучасному розумінні вивчає властивості двох класів чисел: чисел алгебраїчних і чисел трансцендентних (див. розд. VIII).

Питання теорії чисел, пов'язані з властивостями алгебраїчних чисел, називаються *теорією алгебраїчних чисел*; відповідно питання теорії чисел, пов'язані з властивостями трансцендентних чисел, називаються *теорією трансцендентних чисел*. До теорії чисел входять проблеми розв'язування невизначених алгебраїчних рівнянь з цілими коефіцієнтами різних степенів у цілих (або, більш загально, алгебраїчних) числах, до яких безпосередньо належать задачі про наближення чисел тих чи інших класів за допомогою раціональних або алгебраїчних чисел. Ці розділи теорії чисел називаються відповідно: *теорією діофантових рівнянь* і *теорією діофантових наближень*.

Серед методів дослідження теорії чисел слід виділити такі:

1. Елементарні методи теорії чисел. Ці методи використовують відомості з елементарної математики і елементи аналізу нескінченно малих. Слід мати на увазі, що елементарність методу не свідчить ще про його простоту.

2. Аналітична теорія чисел. До неї належать ті розділи теорії чисел, для вивчення яких доводиться застосовувати методи математичного аналізу в широкому розумінні цього слова, а саме: теорію функцій дійсної і комплексної змінних, теорію рядів, теорію ймовірностей тощо.

3. Алгебраїчна теорія чисел. Цей напрям містить питання, пов'язані з вивченням різних класів алгебраїчних чисел, які для свого розв'язання потребують залучення тих або інших розділів сучасної алгебри, наприклад, теорії груп, теорії Галуа, теорії кілець і полів тощо.

4. Геометрична теорія чисел. Сюди відносяться ті розділи теорії чисел, для розгляду яких доводиться застосовувати геометричні поняття, зокрема, так звані «просторові решітки», тобто системи точок, координати яких в заданій прямокутній системі координат є цілі числа.

Для розв'язання тієї або іншої проблеми теорії чисел можуть одночасно застосовувати кілька або навіть усі з перелічених нами методів. Так, наприклад, методи аналітичної теорії чисел застосовують у алгебраїчній і геометричній теорії чисел.

Курс теорії чисел у педагогічному інституті можна поділити на такі три розділи: 1) теорія конгруенцій та її застосування; 2) неперервні дроби і арифметичне дослідження ірраціональних чисел; 3) числові функції.

Ряд важливих проблем теорії чисел безпосередньо або посередньо пов'язаний з поняттям подільності цілих чисел, тому встановлення основних властивостей подільності можна розглядати як перший розділ теорії чисел. Теорія конгруенцій — природне продовження теорії подільності — є одним з найважливіших допоміжних апаратів теорії чисел і займає значну частину нашого курсу.

Вивчення курсу теорії чисел має велике значення для вчителя математики. У ньому докладно викладаються і обгрунтовуються

питання подільності цілих чисел, теорія періодичних десяткових дробів, теорія неперервних або ланцюгових дробів (зокрема скінченних), розв'язування невизначених рівнянь першого степеня в цілих числах тощо, тобто питання, з якими повинен бути обізнаний кожен учитель математики. Деякі питання теорії чисел з успіхом можна розглядати на заняттях шкільного математичного гуртка.

Слід зауважити, що крім деяких питань аналітичної теорії чисел, для засвоєння курсу теорії чисел досить відомостей тільки з елементарного курсу математики. Але через те що методи доведень, які подаються в курсі теорії чисел, дуже різноманітні і часто штучні, вивчення теорії чисел становить певні труднощі.

Коротка історія розвитку теорії чисел

Протягом більш як двадцяти п'яти століть теорія чисел була улюбленою галуззю дослідження видатних математиків і багатьох аматорів. Ще в Стародавній Греції, в так званій Піфагорейській школі (IV ст. до н. е.) вивчалась подільність цілих чисел, були виділені окремі підкласи цілих чисел, як, наприклад, прості числа, складені числа тощо.

Праця видатного математика древності Архімеда (близько 287—212 р. до н. е.) під назвою «Псамміт», або «Числення піщинок», відіграла вирішальну роль у створенні самого поняття про нескінченний ряд натуральних чисел. Інший видатний математик Стародавньої Греції — Евклід (III ст. до н. е.) у своїх знаменитих «Початках» дав систематичну побудову теорії подільності на основі так званого *алгоритму Евкліда* для знаходження найбільшого спільного дільника двох цілих чисел, довів нескінченність простих чисел тощо.

Велике, навіть вирішальне значення для розвитку теорії чисел мали праці знаменитого александрійського математика Діофанта (близько III ст. н. е.). Йому належить один з перших творів з теорії чисел, який звичайно називають «Арифметикою», що складається з 13 книг, з яких до нас дійшло тільки 7. У цьому творі викладено основи алгебри і подано багато задач, які зводяться до невизначених рівнянь різних степенів, причому вказано ряд методів знаходження розв'язків таких рівнянь у раціональних числах. Згадані розділи теорії чисел і названо на честь цього вченого: теорія діофантових рівнянь і теорія діофантових наближень.

В Індії у працях Аріабхатти (VI ст.), Брамагупти (VII ст.) і Бхаскари (XII ст.) досліджено ряд задач, які стосуються розв'язування діофантових рівнянь першого і другого степеня в цілих числах.

У трактаті з алгебри знаменитого узбецького вченого аль-Хорезмі (IX ст.), від імені якого «Аль-джебр і вал мукабала» походить саме слово алгебра, не тільки значно вдосконалено алгебраїчний апарат, а й продовжено дослідження Діофанта. Ця і

пізніші праці середньоазіатських учених Омара Хайяма (1048—1123), Джемшида Гіяседдіна Каші (?— бл. 1436) та інших відіграли також важливу роль у передачі європейським математикам знань, набутих грецькими, індійськими і арабськими математиками.

Середньовічна математика не внесла в теорію чисел нічого істотно нового.

Розквіт теорії чисел в Європі почався з праць славетного французького математика П. Ферма (1601—1665). Юрист за освітою і професією, Ферма займався найрізноманітнішими математичними питаннями, не дбаючи про опублікування добутих ним чудових результатів, більшість яких відома з листування Ферма з видатними французькими математиками — Паскалем (1623—1662), Декартом (1596—1650), англійцем Валлісом (1616—1703) та іншими видатними математиками того часу. Частина теоретико-числових співвідношень, які відкрив Ферма, дійшла до нас лише у формі записів на полях екземпляра «Арифметики» Діофанта, який належав Ферма.

Ферма справедливо вважають батьком теорії чисел; відкриття Ферма викликали загальний інтерес до теорії чисел, і багато досягнень цієї науки пов'язано з спробами розв'язати ряд задач, які він поставив. Незважаючи на це, аж до Л. Ейлера майже нічого істотного в напрямі обгрунтування теорії чисел як науки не було зроблено.

Теорія чисел як наука починає своє існування власне з Л. Ейлера (1707—1783). Видатний петербурзький академік значно розширив область теорії чисел, поставивши ряд нових проблем і створивши нові методи дослідження. Ейлер написав близько 150 праць з теорії чисел. Слід зауважити, що в листуванні Ейлера з петербурзьким академіком Х. Гольдбахом (1690—1764) було висловлено три знамениті проблеми: 1) всяке непарне число $n > 7$ є сума трьох простих чисел; 2) всяке парне число $n \geqslant 4$ є сума двох простих чисел; 3) всяке непарне число, починаючи з 5, можна подати у вигляді $p + 2k^2$, де k — ціле, а p — просте число.

Перші дві проблеми ще раніше висловив англійський математик Варінг (1734—1798). Дві останні проблеми досі остаточно не розв'язані.

Ідеї Ейлера мали великий вплив на розвиток теорії конгруенцій, аналітичної теорії чисел, діофантових рівнянь і теорії форм.

Отже можна зробити висновок, що хоч теорія чисел належить до найстародавніших розділів математики, але тільки в XVII—XVIII ст. вона формується як наука в працях Ферма і, головним чином, у працях Ейлера.

Дальший розвиток теорії чисел до Гаусса в основному пов'язаний з працями англійського математика Е. Варінга і видатних французьких математиків А. Лежандра (1752—1833) і Ж. Лагранжа (1736—1813); майже всі видатні математики в цей період займаються теорією чисел.

Зазначимо лише, що згодом славі Варінга особливо сприяла висловлена ним у 1770 р. теорема, відома як проблема Варінга, про те, що всяке натуральне число можна подати у вигляді суми однакових степенів цілих додатних чисел, число яких нижче від деякої границі, яка цілком визначається показником степеня і не залежить від числа, що розкладається.

Видатному німецькому математикові К. Гауссу (1777—1855) належить заслуга у створенні основних методів і систематичній побудові теорії конгруенцій. Якщо до Гаусса теорія чисел була просто збіркою окремих результатів та ідей, які пізніше оформились у загальні методи, то після праць Гаусса вона почала розвиватись у різних напрямах як стрункa теорія. Значення Гаусса в історії розвитку теорії чисел величезне і, не перебільшуючи, можна сказати, що праці Гаусса в значній мірі визначили її розвиток у XIX ст.

Дальший розвиток теорії чисел в Європі в основному пов'язаний з іменами німецьких математиків: Діріхле (1805—1859), Рімана (1826—1866), Куммера (1810—1893), Дедекінда (1831—1916), Кронекера (1823—1891), Мінковського (1864—1909), Якобі (1804—1851), французьких математиків: Коші (1789—1857), Ліувілля (1809—1882), Ерміта (1822—1901) і особливо з науковою діяльністю математиків так званої Петербурзької школи теорії чисел.

Провідна роль російської математики в розвитку теорії чисел. Петербурзька школа

Видатних результатів у галузі теорії чисел було досягнуто ще в дореволюційній Росії. Можна сказати, що теорія чисел вперше оформилась як наука в працях Ейлера в нашій країні; саме тут було покладено початок і окремих галузей теорії чисел — аналітичній (Л. Ейлер), алгебраїчній (Є. І. Золотарьов) і геометричній (Г. Ф. Вороний, незалежно від німецького математика Г. Мінковського). В СРСР теорія чисел розвинулась далі; виникла і нова її галузь — теорія трансцендентних чисел (О. О. Гельфонд)[1].

Але найвизначніших результатів з теорії чисел було досягнуто в працях великого російського математика і механіка Пафнутія Львовича Чебишова (1821—1894), який створив теоретико-числову школу, так звану Петербурзьку школу теорії чисел — єдину за своїм значенням у всьому світі. У дальшому розвитку теорії чисел російські вчені займали провідну роль. Петербурзька школа теорії

[1] Теорію трансцендентних чисел можна віднести до області діофантових наближень, бо трансцендентність числа встановлюється за характером наближень його раціональними або алгебраїчними числами

чисел уславилась такими іменами, як П. Л. Чебишов, О. М. Коркін, Є. І. Золотарьов, А. А. Марков, Г. Ф. Вороний, заслуги яких у розвитку теорії чисел важко переоцінити.

У працях П. Л. Чебишова, які характеризувались винятковою аналітичною проникливістю і надовго визначали як тематику, так і методи дослідження найвидатніших російських математиків, висвітлювались найрізноманітніші питання чистої й прикладної математики.

П. Л. Чебишов займався дослідженням розподілу простих чисел, що не розроблялося з часів Евкліда. Ці дослідження привели Чебишова до квадратичних форм з додатним дискримінантом. Пізніше теорію квадратичних форм досліджували його учні — О. М. Коркін, Є. І. Золотарьов, А. А. Марков, Г. Ф. Вороний. Праця П. Л. Чебишова про наближення різних класів чисел раціональними числами відіграла важливу роль у розвитку теорії діофантових наближень. П. Л. Чебишову належить також перше доведення постулату Бертрана[1] та багато іншого.

Коркін Олександр Миколайович (1837—1908), професор Петербурзького університету, разом з П. Л. Чебишовим відіграв велику роль у створенні Петербурзької математичної школи. Його праці з теорії чисел привернули до цієї галузі математики увагу ряду талановитих учених: Є. І. Золотарьова, А. А. Маркова, Г. Ф. Вороного, Д. О. Граве (1863—1939). О. М. Коркін розробив метод розв'язання двочленних конгруенцій, який дає дуже добрі результати. О. М. Коркін і Є. І. Золотарьов своїми спільними працями про мінімуми додатних форм здобули велику славу.

Золотарьов Єгор Іванович (1847—1878) — учень О. М. Коркіна, видатний математик — прожив тільки 31 рік[2], але й за таке коротке життя встиг написати ряд надзвичайно важливих праць. Крім згаданих досліджень, що стосуються теорії квадратичних форм і невизначених рівнянь третього степеня, він перший побудував загальну теорію алгебраїчних чисел, випередивши Дедекінда на чотири роки. Тому творцем теорії ідеалів і, отже, теорії подільності цілих алгебраїчних чисел слід вважати Є. І. Золотарьова, його методи стали пізніше одними з основних у теорії алгебраїчних чисел. Заслуги Золотарьова в цій галузі довгий час ігнорували на Заході, де створення теорії подільності цілих алгебраїчних чисел приписували Дедекінду.

Пізніше професор Петербурзького університету І. І. Іванов (1862—1939) встановив еквівалентність алгебраїчних теорій Золотарьова та Дедекінда.

---

[1] Див. § 49, стор. 226.

[2] Життя і блискуча наукова діяльність Золотарьова обірвались через нещасний випадок — на залізничній станції Олександрівська він потрапив під поїзд.

Академік Марков Андрій Андрійович (1856—1922) є автором визначних праць з багатьох галузей математики: теорії алгебраїчних неперервних дробів, теорії скінченних різниць, теорії функцій, що найменш відхиляються від нуля, і особливо теорії ймовірностей. У теорії чисел дуже важливе значення мають праці А. А. Маркова про верхню границю мінімумів невизначених квадратичних форм; вони стали основою для роботи багатьох математиків в СРСР і за кордоном.

Вороний Георгій Федосійович (1868—1908), за національністю українець, професор Варшавського університету, член-кореспондент Російської академії наук, працював майже виключно в галузі теорії чисел. Г. Ф. Вороний поділяє з Мінковським пріоритет щодо створення геометричної теорії чисел. Одна з його праць тісно пов'язана з геометричними дослідженнями славетного російського кристалографа Є. С. Федорова; вона стосується і теорії квадратичних форм, і геометрії. Праця Г. Ф. Вороного «Про одну задачу з теорії асимптотичних функцій» (1903) стимулювала розвиток сучасної аналітичної теорії чисел. Праці Вороного з аналітичної теорії чисел стосуються також загальних питань про методи підсумовування функцій; один з цих методів дістав назву методу Вороного. Теорія чисел, розроблена в працях Вороного, була розвинута в працях радянських математиків: І. М. Виноградова, Б. М. Делоне, Б. О. Вєнкова та ін.

Слід зазначити, що багато результатів, здобутих математиками Петербурзької школи, лише через деякий час досягли вчені в Західній Європі і в Америці.

Радянська школа теорії чисел як провідний напрям сучасної теорії чисел

За останні десятиліття найвизначніших результатів у теорії чисел, безперечно, досягли радянські математики на чолі з академіком І. М. Виноградовим.

Виноградов Іван Матвійович (нар. в 1891 р.), один з найвидатніших сучасних математиків, присвятив свою діяльність аналітичній теорії чисел. Основи цієї теорії були викладені ще Ейлером; видатні результати в розвитку аналітичної теорії чисел, як уже говорилося, належать математикам Петербурзької школи теорії чисел.

І. М. Виноградов є творцем нового методу в аналітичній теорії чисел, який дав йому змогу зробити в цій галузі математики ряд відкриттів, що належать до найвидатніших досягнень теорії чисел за весь час її існування. Досить тільки вказати, що за допомогою створеного ним оригінального методу оцінки тригонометричних

сум І. М. Виноградов не тільки розв'язав (1934) [1] проблему Варінга, а й знизив оцінку для числа доданків, близьку до остаточної.

Цей самий глибокий метод дав можливість Виноградову (опубл. 1937 р.) розв'язати відому проблему Гольдбаха для всіх непарних чисел, більших від деякої сталої [2]. За цю працю І. М. Виноградов був удостоєний Державної премії І-го ступеня (1940 р.). Метод Виноградова є найдосконалішим в аналітичній теорії чисел. Він виклав цей метод у своїй книзі «Новий метод аналітичної теорії чисел». У 1945 р. І. М. Виноградову присвоєно високе звання Героя Соціалістичної Праці.

Методи, створені І. М. Виноградовим, розвинені й успішно застосовуються багатьма радянськими математиками до розв'язання ряду центральних проблем теорії чисел.

Академік Юрій Володимирович Лінник (н. 1915 р.) показав, що метод Виноградова можна застосувати до розв'язання найважчих проблем теорії ймовірностей.

Він навів ряд оцінок тригонометричних сум методом Виноградова, дав елементарне доведення проблеми Варінга. Крім того, Лінник довів, що будь-яке досить велике число є сума семи кубів (замість восьми, як це вважалось раніше). В 1947 р. Ліннику було присуджено Державну премію, а в 1969 р. йому було присвоєно звання Героя Соціалістичної Праці.

Відмінний від методу Виноградова метод в аналітичній теорії чисел належить видатному радянському математику чл.-кор. АН УРСР Льву Генріховичу Шнірельману (1905—1938).

Праці Шнірельмана належать до числа кращих досягнень радянської математики (див. § 51). Його дослідження продовжили багато вітчизняних і зарубіжних математиків.

Праці Виноградова і Шнірельмана внесли в науку багато принципіально нового, що зовсім не випливало з методів, встановлених раніше.

У галузі діофантових рівнянь і діофантових наближень численні і важливі результати належать членам-кореспондентам АН СРСР Делоне Борису Миколайовичу (н. 1890 р.) і Хінчину Олександру Яковичу (1894—1959).

Визначні праці Делоне охоплюють ряд питань, спільних для алгебри, геометрії і теорії чисел. Теорія бінарних кубічних рівнянь з від'ємним дискримінантом набула в працях Делоне повного завершення; він також показав, що за допомогою цілком своєрідного алгоритму, який він назвав «алгоритмом підвищення», можна прак-

[1] Проблему Варінга вперше розв'язав німецький математик Гільберт у 1909 р., але його метод давав дуже велике значення для числа доданків і мав частковий характер. У 1920—1925 рр. англійські математики Харді і Літлвуд застосували новий метод до розв'язання проблеми Варінга, але й він давав дуже велике значення числа доданків.

[2] Докладніше див. § 51.

Висновок. *Ціле число a тоді і тільки тоді кратне $b \neq 0$, коли остача від ділення a на b дорівнює нулю.*

Справді, якщо $r = 0$, то рівність $a = bq + r$ перетворюється в $a = bq$, звідки випливає, що a ділиться на b. Навпаки, якщо a ділиться на b, то матимемо рівність $a = b \cdot c$, де c — ціле. Звідси внаслідок єдиності частки і остачі виходить, що $c = q$, а остача r дорівнює нулю.

Властивість 4 цілих чисел дає змогу в питаннях подільності обмежуватись тільки додатними числами. Взагалі, в питаннях подільності числа a і $-a$ рівноправні; такі числа, що відрізняються тільки знаком або множником -1, називаються *асоційовними*. Далі розглядатимемо лише додатні дільники.

Ряд властивостей подільності цілих чисел тісно пов'язаний з поняттям найбільшого спільного дільника.

Контрольні запитання

1. Дайте означення числового кільця.
2. Поясніть зміст твердження: a ділиться на b.
3. Користуючись лише означенням подільності цілих чисел, доведіть наслідки 1 і 3 з теореми 2.
4. Сформулюйте теорему про ділення з остачею.
5. Яка умова є необхідною і достатньою для подільності a на $b \neq 0$?
6. Яка буде частка і остача від ділення 5 на 7, 120 на 13, 529 на 23.

§ 2. Найбільший спільний дільник двох чисел

Якщо цілі числа a і b діляться на деяке натуральне число δ, то δ називається їх *спільним дільником*. Найбільший із спільних дільників чисел a і b називається *найбільшим спільним дільником* (скорочено н. с. д.) і позначається символом (a, b).

Якщо обидва числа a і b дорівнюють нулю одночасно, то поняття їх спільного дільника, а також і найбільшого спільного дільника втрачає смисл (бо нуль має нескінченну множину дільників); тому далі, говорячи про спільні дільники заданих чисел, ми завжди припускаємо, що принаймні одне з них відмінне від нуля.

Через те, що будь-яке ціле число має скінченне число дільників, то скінченним буде й число спільних дільників двох даних чисел a і b, отже, найбільший спільний дільник цих чисел завжди існує і дорівнює деякому натуральному числу.

Якщо найбільший спільний дільник двох заданих чисел дорівнює 1, то ці числа називаються *взаємно простими*.

З наведених вище означень випливають такі два твердження:

Теорема 1. *Якщо a ділиться на b, то сукупність спільних дільників a і b збігається з сукупністю дільників одного b, зокрема, $(a, b) = b$.*

Справді, всякий спільний дільник чисел a і b є дільником і одного b. Навпаки, оскільки a ділиться на b, то будь-який дільник числа b є також дільником числа a, тобто він буде спільним дільником чисел a і b. Отже, сукупність спільних дільників чисел a і b збігається з сукупністю дільників одного b. І через те що найбільший дільник числа b є саме b, то $(a, b) = b$.

Теорема 2. *Якщо a, b, c, d — цілі числа, пов'язані співвідношенням $a = bd + c$, то сукупність спільних дільників чисел a і b збігається з сукупністю спільних дільників чисел b і c; зокрема $(a, b) = (b, c)$.*

Справді, всякий спільний дільник чисел a і b (на підставі теореми 2, § 1) буде дільником також і числа c. Навпаки, всякий спільний дільник чисел b і c буде дільником числа a і, отже, є спільним дільником чисел a і b. Отже, спільні дільники чисел a і b збігаються із спільними дільниками чисел b і c, зокрема $(a, b) = (b, c)$.

Контрольні запитання

1. Яке число називається найбільшим спільним дільником двох чисел?
2. Користуючись означенням, знайдіть найбільший спільний дільник чисел 15 і 0.
3. Які числа називаються взаємно простими?
4. Перевірте, чи виконується теорема 2 для чисел: $a = 650$, $b = 52$, $d = 12$, $c = 26$.

§ 3. Алгоритм Евкліда і властивості найбільшого спільного дільника двох чисел

Для знаходження найбільшого спільного дільника двох чисел є дуже простий спосіб, відомий під назвою алгоритму Евкліда [1], або способу послідовного ділення. Він полягає ось у чому: припустимо, що a і b цілі числа, причому $a > b$, $b > 0$. Поділимо a на b і частку позначимо через q_0, а остачу через r_1; $0 \leqslant r_1 < b$. Далі, поділимо b на r_1, добуту частку позначимо через q_1 і остачу через r_2; $0 \leqslant r_2 < r_1$ і т. д.

Процес вважається закінченим, коли дістаємо остачу, що дорівнює нулю. Легко переконатися, що описаний процес є скінченним. Справді, внаслідок означення остачі маємо ряд спадних цілих додатних чисел: $b > r_1 > r_2 > \dots$. Але такий ряд не може мати

[1] Слово *алгоритм*, або *алгорифм*, походить від перекрученого латинським перекладачем імені видатного узбецького математика аль-Хорезмі, автора відомого трактату з алгебри. Спочатку це слово означало «майстерність лічби», а тепер вживається для позначення певної послідовності операцій. Зокрема в машинній обчислювальній математиці роль алгоритму є фундаментальною.

більш як b членів. Запишемо тепер цей процес за допомогою такої системи рівностей:

$$\begin{aligned}
a &= bq_0 + r_1, && 0 < r_1 < b;\\
b &= r_1q_1 + r_2, && 0 < r_2 < r_1;\\
r_1 &= r_2q_2 + r_3, && 0 < r_3 < r_2;\\
&\dots\dots\dots\dots\dots\dots\dots\dots\dots\\
r_{n-2} &= r_{n-1}q_{n-1} + r_n, && 0 < r_n < r_{n-1};\\
r_{n-1} &= r_nq_n,
\end{aligned} \qquad (1)$$

причому $r_{n+1} = 0$.

На підставі теореми 2, § 2 з рівностей (1), розглядаючи їх зверху вниз, переконуємось, що спільні дільники чисел a і b збігаються з спільними дільниками чисел b і r_1; останні збігаються з спільними дільниками чисел r_1 і r_2 і т. д. Отже, спільні дільники чисел a і b збігаються з спільними дільниками чисел r_{n-1} і r_n і, нарешті, вони збігатимуться з дільниками одного числа r_n (на підставі теореми 1, § 2).

Зокрема, маємо:

$$(a, b) = (br_1) = (r_1, r_2) = \dots = (r_{n-1}, r_n) = r_n.$$

Цим ми довели такі дві теореми:

Теорема 1. *Сукупність спільних дільників чисел a і b збігається з дільниками їх найбільшого спільного дільника.*

Теорема 2. *Найбільший спільний дільник двох чисел a і b дорівнює останній остачі алгоритму Евкліда, що не дорівнює нулю.*

Оскільки при знаходженні найбільшого спільного дільника за допомогою алгоритму Евкліда кожна остача при діленні є дільником при наступному діленні, то відповідні обчислення зручно проводити за схемою, яку ми продемонструємо на такому прикладі.

Приклад. Знайти найбільший спільний дільник чисел 816 і 323. Обчислення найраціональніше розмістити так:

	816	323 | 2
	646	
323	170	| 1
170		
170	153	| 1
153		
153	17	| 9
153		
0		

Тут остання, відмінна від нуля, остача дорівнює 17, отже, $(816, 323) = 17$.

Теорема 3. *Якщо два числа a і b помножити на натуральне число m, то їх н. с. д. збільшиться у m раз, тобто*

$$(am,\ bm) = m\,(a,\ b).$$

Справді, помножаючи рівності (1) на m, дістанемо нові рівності де замість a, b, r_1, ..., r_n стоятимуть am, bm, r_1m, ..., r_nm тобто алгоритм Евкліда застосовано до чисел am і bm; оскільки остання остача, що не дорівнює нулю, буде r_nm, то дістанемо:

$$(am,\ bm) = r_nm = m\,(a,\ b).$$

Теорема 4. *Якщо два числа a і b поділити на їхній спільний дільник δ, то на δ поділиться і їхній найбільший спільний дільник, тобто* $\left(\frac{a}{\delta}, \frac{b}{\delta}\right) = \frac{(a,\ b)}{\delta}$.

Справді, на підставі теореми 3 знаходимо:

$$(a,\ b) = \left(\frac{a}{\delta}\cdot\delta,\ \frac{b}{\delta}\cdot\delta\right) = \left(\frac{a}{\delta},\ \frac{b}{\delta}\right)\delta, \text{ звідки } \left(\frac{a}{\delta},\ \frac{b}{\delta}\right) = \frac{(a,\ b)}{\delta}.$$

Теорема 5. *Для того, щоб дільник d був найбільшим спільним дільником двох чисел a і b, необхідно і достатньо, щоб частки* $\frac{a}{d}$ *і* $\frac{b}{d}$ *були взаємно прості, тобто* $\left(\frac{a}{d},\ \frac{b}{d}\right) = 1$.

Справді, якщо $(a,\ b) = d$, то, за теоремою 4, маємо:

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

Навпаки, якщо $\left(\frac{a}{d},\ \frac{b}{d}\right) = 1$, то, помноживши обидві частини цієї рівності на d, згідно з теоремою 3 дістанемо: $(a,\ b) = d$.

Контрольні запитання

1. Як визначити найбільший спільний дільник двох чисел? Які його основні властивості?
2. Чому процес послідовного ділення в алгоритмі Евкліда скінченний?
3. На підставі якої теореми написано рівності (1)?
4. Що можна сказати про порівняльну величину остач r_1, r_2, ..., r_n?
5. Перевірте на числових прикладах справедливість теорем 3, 4, 5.

§ 4. Основні теореми про подільність

Як наслідок з алгоритму Евкліда дістанемо теорему, за допомогою якої легко буде довести властивості взаємно простих чисел, які є основними для всієї теорії подільності.

Теорема 1. *Якщо d — найбільший спільний дільник двох чисел a і b, то завжди можна знайти такі цілі числа x і y, що буде справедлива рівність: $ax + by = d$.* Інакше кажучи, *найбільший спільний дільник двох чисел завжди можна подати у вигляді лінійної комбінації цих чисел.*

Справді, з рівностей (1), § 3 матимемо:

$$r_1 = a - bq_0 = 1\cdot a + (-q_0)\,b = ax_1 + by_1,$$

де $x_1 = 1$, $y_1 = -q_0$; з наступної рівності, записаної у вигляді $r_2 = b - r_1q_1$, випливає, що r_2 також можна подати у вигляді лінійної комбінації чисел a і b:

$$r_2 = b - (ax_1 + by_1)\,q_1 = a\,(-q_1x_1) + b\,(1 - q_1y_1) = ax_2 + by_2,$$

де $x_2 = -q_1x_1$, $y_2 = 1 - q_1y_1$ — цілі числа. Так, переходячи від рівності до рівності зверху вниз, ми дістанемо, що $r_n = ax_n + by_n$, де x_n, y_n — цілі числа. Оскільки $r_n = d$, то, позначаючи $x_n = x$, $y_n = y$, дістанемо рівність $ax + by = d$, що й треба було довести.

Висновок. *Якщо a і b взаємно прості числа, то завжди можна знайти такі цілі числа x і y, що буде справедлива рівність*

$$ax + by = 1. \qquad (1)$$

Теорема 2. *Якщо добуток ab ділиться на c і $(b,\ c) = 1$, то a ділиться на c.*

Справді, оскільки $(b,\ c) = 1$, то за теоремою 1 : $bx + cy = 1$. Помноживши цю рівність на a, дістанемо: $abx + acy = a$. Але ліва частина цієї рівності при будь-яких цілих x і y ділиться на c, отже, і права частина цієї рівності, тобто a, ділиться на c.

Теорема 3. *Якщо a ділиться на b і на c і $(b,\ c) = 1$, то a ділиться і на bc.*

Справді, з $a \vdots b$ випливає, що $a = b\cdot a_1$, де a_1 — ціле; далі, $a \vdots c$, тобто $ba_1 \vdots c$, але $(b,\ c) = 1$, тоді за теоремою 2 $a_1 \vdots c$ і, отже, $a_1 = ca_2$. Таким чином, $a = ba_1 = bca_2$. Ця рівність і показує, що $a \vdots bc$.

Теорема 4. *Якщо два числа a і b взаємно прості з третім числом c, то й добуток ab взаємно простий з c.*

Справді, з умови $(a,\ c) = 1$ маємо: $ax + cy = 1$. Помноживши цю рівність на b, дістаємо $abx + bcy = b$. Припустимо тепер супротивне, тобто нехай $(ab,\ c) = d > 1$; тоді ліва частина рівності $abx + bcy = b$ ділитиметься на d і, отже, $b \vdots d$. Але із зробленого припущення випливає, що й $c \vdots d$; отже, $(b,\ c) = d > 1$, що суперечить умові, згідно з якою $(b,\ c) = 1$. Що й треба було довести.

Цю теорему можна узагальнити так: *якщо кожне з чисел a_1, a_2, ..., a_m взаємно просте з кожним з чисел b_1, b_2, ..., b_n,* то й добуток $a_1a_2 \ldots a_m$ *взаємно простий з добутком $b_1b_2 \ldots b_n$.*

Справді, маємо $(a_i,\ b_k) = 1$, де $i = 1, 2, \ldots, m$, $k = 1, 2, \ldots, n$. Тоді, внаслідок доведеної теореми, $(a_1a_2, b_k) = 1$, а отже, $(a_1a_2a_3, b_k) = 1$, і т. д. Нарешті, дістанемо $(a_1a_2 \ldots a_m,\ b_k) = 1$, а це означає, що добуток $a_1a_2 \ldots a_m = A$ взаємно простий з b_k $(k = 1, 2, \ldots, n)$.

Так само матимемо:

$$(A, b_1) = (A, b_1b_2) = \cdots = (A, b_1, b_2 \ldots b_n) = 1,$$

тобто добуток $a_1a_2 \ldots a_m$ взаємно простий з добутком $b_1b_2 \ldots b_n$.

Висновок. *Якщо числа a і b взаємно прості, то будь-які їхні натуральні степені — взаємно прості числа.*

Справді, поклавши

$$a_1 = a_2 = \cdots = a_m = a \text{ і } b_1 = b_2 = \cdots = b_n = b,$$

дістанемо $(a^m, b^n) = 1$.

На підставі цього висновку можна твердити, що *жодний натуральний степінь нескоротного дробу не може бути скоротним дробом і, зокрема, натуральним числом.* Останнє означає, що *корінь n-го степеня з натурального числа не може дорівнювати нескоротному дробу.*

Контрольні запитання

1. Як розуміти, що найбільший спільний дільник двох чисел є їхньою лінійною комбінацією?
2. При якій умові числа a і b взаємно прості?
3. Перелічіть властивості взаємно простих чисел.
4. Доведіть, що $\sqrt[3]{5}$ — ірраціональне число.

§ 5. Найбільший спільний дільник кількох чисел

Якщо цілі числа $a_1, a_2, \ldots, a_k$ всі діляться на деяке натуральне число δ, то δ називають їхнім спільним дільником. Найбільший із спільних дільників називається їхнім *найбільшим спільним дільником* і позначається символом $(a_1, a_2, \ldots, a_k)$.

Якщо найбільший спільний дільник чисел $a_1, a_2, \ldots, a_k$ дорівнює 1, то ці числа називаються *взаємно простими.* Якщо кожне з чисел $a_1, a_2, \ldots, a_n$ взаємно просте з кожним іншим з них, то ці числа називаються *попарно взаємно простими* (або *попарно простими*).

З цих означень виходить, що *коли числа $a_1, a_2, \ldots, a_k$ попарно взаємно прості, то вони будуть і взаємно простими.* Справді, якби при цьому $(a_1, a_2, \ldots, a_k) = d > 1$ і, наприклад a_1 ділилося б на d і a_2 ділилося б на d, то a_1 і a_2 не були б взаємно прості, а це суперечить тому, що ці числа попарно взаємно прості.

Обернене твердження взагалі несправедливе, що видно хоч би з такого прикладу: $(35, 21, 16) = 1$, але $(35, 21) = 7$.

Очевидно, що для двох чисел поняття «попарно взаємно прості» і «взаємно прості» збігаються.

Щоб знайти найбільший спільний дільник більш як двох чисел, можна скористатись таким твердженням:

$$(a_1, a_2, \ldots, a_{k-1}, a_k) = ((a_1, a_2, \ldots, a_{k-1}), a_k).$$

Справді, введемо позначення

$$(a_1, a_2) = d_2, (d_2, a_3) = d_3, \ldots, (d_{k-2}, a_{k-1}) = d_{k-1}, (d_{k-1}, a_k) = d_k, \quad (1)$$

і покажемо, що

$$(a_1, a_2, \ldots, a_{k-1}, a_k) = (d_{k-1}, a_k) = d_k.$$

Для $k = 2$, тобто для двох чисел a_1 і a_2 твердження справедливе і за теоремою 1, § 3 матимемо, що спільні дільники чисел a_1 і a_2 збігаються з дільниками d_2. Припустимо, що твердження справедливе для $k - 1$ $(k \geqslant 3)$ чисел $a_1, a_2, \ldots, a_{k-1}$ і покажемо, що воно справедливе для k чисел. З останньої рівності (1), за теоремою 1, § 3 матимемо, що спільні дільники чисел d_{k-1} і a_k збігаються з дільниками d_k; але за припущенням спільні дільники чисел $a_1, a_2, \ldots, a_{k-1}$ збігаються з дільниками d_{k-1}, і, отже, спільні дільники чисел $a_1, a_2, \ldots, a_{k-1}, a_k$ збігатимуться з дільниками числа d_k. Оскільки найбільший дільник числа d_k є саме d_k, то й дістанемо, що $(a_1, a_2, \ldots, a_{k-1}, a_k) = d_k = (d_{k-1}, a_k)$. Зокрема $(a_1, a_2, \ldots, a_{k-1}) = d_{k-1}$, а тому $(a_1, a_2, \ldots, a_{k-1}, a_k) = ((a_1, a_2, \ldots, a_{k-1}), a_k)$, що й треба було довести.

З доведення випливає, що задача відшукання найбільшого спільного дільника більш як двох чисел зводиться до такої самої задачі для двох чисел, тобто до відшукання чисел $d_2, d_3, \ldots, d_k$.

Переглядаючи подане вище доведення, легко переконатися, що теорема 1, § 3 справедлива більш як для двох чисел. Так само будуть справедливі більш як для двох чисел і теореми 3, 4, 5, § 3, бо від множення на натуральне число m або від ділення на спільний дільник δ усіх чисел $a_1, a_2, \ldots, a_k$ відповідно помножаться на m або поділяться на δ всі $d_2, d_3, \ldots, d_k$.

Контрольні запитання

1. Яка різниця між поняттями «взаємно прості числа» і «попарно взаємно прості числа»?
2. Яке з понять «взаємно прості» і «попарно взаємно прості» є наслідком другого? Коли ці два поняття збігаються?
3. Покажіть справедливість теорем 1, 3, 4, 5, § 3 для кількох чисел.

§ 6. Найменше спільне кратне

Нехай дано два натуральних числа a і b. Існує нескінченна множина цілих чисел, які діляться одночасно на a і b, тобто є *спільними кратними* цих чисел. Це, наприклад, числа ab, $2ab$, ..., тому особливого значення набуває поняття найменшого спільного кратного цих чисел.

Найменшим спільним кратним (скорочено н. с. к.) натуральних чисел a і b називається їх спільне кратне m, яке є найменшим серед усіх натуральних спільних кратних цих чисел, тобто найменше

натуральне число, що ділиться на a і b. Будемо його позначати символом $[a, b]$.

Нехай M — будь-яке довільне спільне кратне чисел a і b. Через те що воно ділиться на a, то $M = ak$, де k — ціле. Але M ділиться також на b, тому цілим має бути й

$$\frac{ak}{b} = \frac{a \cdot \frac{bt}{d}}{\frac{b}{d}} = \frac{\frac{abt}{d}}{\frac{b}{d}} = \frac{abt}{b} \quad (1)$$

Поклавши $(a, b) = d$, маємо $a = a_1 d$, $b = b_1 d$, і вираз (1) можна подати так: $\frac{a_1 k}{b_1}$, де $(a_1, b_1) = 1$. Через те що $\frac{a_1 k}{b_1}$ є ціле і $(a_1, b_1) = 1$, то, за теоремою 2, § 4, k має ділитись на b_1, тобто $k = b_1 t = \frac{bt}{d}$, де t — ціле число. Звідси маємо:

$$M = \frac{ab}{d} t. \quad (2)$$

Навпаки, очевидно, що всяке M такого виду кратне як a, так і b. Отже, формула (2) дає загальний вигляд усіх спільних кратних чисел a і b.

Найменше спільне кратне дістанемо при $t = 1$. Отже, маємо

$$[a, b] = m = \frac{ab}{d} = \frac{ab}{(a, b)}. \quad (3)$$

Формулу (2), виведену для M, можна тепер переписати так:

$$M = \frac{ab}{(a, b)} \cdot t = mt. \quad (2')$$

З рівностей (2′) і (3) випливають такі теореми:

Теорема 1. *Спільні кратні двох чисел a і b збігаються з кратними їхнього найменшого спільного кратного* (або, що те саме: *всяке спільне кратне M чисел a і b ділиться на їхнє найменше спільне кратне m).*

Теорема 2. *Найменше спільне кратне двох чисел дорівнює їхньому добутку, поділеному на їхній найбільший спільний дільник.*

Теорема 3. *Найменше спільне кратне двох чисел a і b тоді і тільки тоді дорівнює їх добутку, коли a і b взаємно прості.*

Справді, якщо $(a, b) = 1$, то $[a, b] = \frac{ab}{(a, b)} = ab$. Навпаки, якщо $[a, b] = ab$, то, враховуючи, що $[a, b] = \frac{ab}{(a, b)}$, робимо висновок, що $(a, b) = 1$.

Поширимо тепер поняття найменшого спільного кратного більш як на два числа.

Задано натуральні числа $a_1, a_2, \ldots, a_k$ $(k \geqslant 2)$. Ціле число, яке ділиться на кожне з цих чисел, називається *спільним кратним* цих чисел. Існує, очевидно, нескінченна множина спільних кратних цих

чисел. Найменше натуральне з них називається *найменшим спільним кратним даних чисел.* Позначатимемо його символом $[a_1, a_2, \ldots, a_k]$.

Щоб знайти найменше спільне кратне більш як двох чисел, можна скористатися таким твердженням:

$$[a_1, a_2, \ldots, a_{k-1}, a_k] = [[a_1, a_2, \ldots, a_{k-1}], a_k].$$

Справді, введемо позначення:

$$[a_1, a_2] = m_2, [m_2, a_3] = m_3, \ldots, [m_{k-2}, a_{k-1}] = m_{k-1}, [m_{k-1}, a_k] = m_k \quad (1)$$

і покажемо, що

$$[a_1, a_2, \ldots, a_{k-1}, a_k] = [m_{k-1}, a_k] = m_k.$$

Для $k = 2$, тобто для двох чисел a_1 і a_2 твердження справедливе і за теоремою 1, § 6 матимемо, що спільні кратні чисел a_1 і a_2 збігаються з кратними числа m_2. Нехай твердження справедливе для $k - 1$ $(k \geqslant 3)$ чисел $a_1, a_2, \ldots, a_{k-1}$, покажемо тоді, що воно буде справедливе і для k чисел. З останньої рівності (1) за теоремою 1, § 6 матимемо, що спільні кратні чисел m_{k-1} і a_k збігаються з кратними числа m_k; але за припущенням спільні кратні чисел $a_1, a_2, \ldots, a_{k-1}$ збігаються з кратними числа m_{k-1} і отже, спільні кратні чисел $a_1, a_2, \ldots, a_{k-1}, a_k$, збігатимуться з кратними числа m_k. Оскільки найменше натуральне число кратне числа m_k є саме m_k, то й дістанемо, що $[a_1, a_2, \ldots, a_{k-1}, a_k] = m_k = [m_{k-1}, a_k]$. Зокрема, $[a_1, a_2, \ldots, a_{k-1}] = m_{k-1}$, а тому

$$[a_1, a_2, \ldots, a_{k-1}, a_k] = [[a_1, a_2, \ldots, a_{k-1}], a_k],$$

що й треба було довести.

З доведення випливає, що задача відшукання найменшого спільного кратного більш як двох чисел зводиться до такої самої задачі для двох чисел, тобто до відшукання чисел $m_2, m_3, \ldots m_k$.

З доведення випливає справедливість теореми 1 більш як для двох чисел.

Легко також узагальнити теорему 3, § 6 більш як для двох чисел.

Теорема 4. *Найменше спільне кратне кількох чисел дорівнює їхньому добутку тоді і тільки тоді, коли ці числа попарно взаємно прості.*

Справді, припустимо, що ці числа попарно взаємно прості, тоді маємо:

$$[a_1, a_2] = m_2 = a_1 a_2, (m_2, a_3) = 1;$$
$$[m_2, a_3] = m_3 = m_2 a_3 = a_1 a_2 a_3, (m_3, a_4) = 1$$

і т. д. Маємо:

$$[a_1, a_2, \ldots, a_k] = a_1 a_2 \ldots a_k.$$

Навпаки, якщо $[a_1, a_2, \ldots, a_k] = a_1 a_2 \ldots a_k$, то числа a_1, a_2, $\ldots$, a_k попарно взаємно прості.

Справді, припустимо, що серед чисел $a_1, a_2, \ldots, a_k$ є хоч одна пара не взаємно простих, наприклад: $(a_1, a_2) = \delta > 1$. Позначимо $a_1 = u\delta$, $a_2 = v\delta$.

Число

$$M = uv\delta a_3 a_4 \ldots a_k < a_1 a_2 a_3 \ldots a_k,$$

бо $uv\delta = \frac{a_1 a_2}{\delta} < a_1 a_2$.

Тим часом M ділиться на числа: $a_1 = u\delta$, $a_2 = v\delta$, $a_3, \ldots, a_k$; отже, M є спільне кратне, яке є меншим від н. с. к., що неможливо. Отже, кожні два з даних чисел взаємно прості.

Приклад. Знайти [343, 147, 231].

Знаходимо спочатку [343, 147].

Для цього за допомогою алгоритму Евкліда визначаємо (343, 147) = 49, а тому

$$[343, 147] = \frac{343 \cdot 147}{49} = 1029.$$

Тепер знайдемо [343, 147, 231] = [1029, 231]. Для цього обчислюємо (1029, 231) = 21, а тому

$$[1029, 231] = \frac{1029 \cdot 231}{21} = 11\,319.$$

Отже, маємо

$$[343, 147, 231] = 11\,319.$$

Контрольні запитання

1. Яке число називається спільним кратним даних чисел?
2. Яке число називається найменшим спільним кратним двох чисел? Кількох чисел?
3. Чому дорівнює найменше спільне кратне двох чисел?
4. Чи справедлива теорема 2, § 6 для кількох чисел. Чому?
5. Узагальніть теорему 3, § 6 для кількох чисел.
6. При якій умові найменше спільне кратне кількох чисел дорівнює їхньому добутку?

§ 7. Зв'язок алгоритму Евкліда з неперервними дробами

Алгоритм Евкліда використовується також і для знаходження найбільшої спільної міри двох відрізків a і b. Як у цьому випадку, так і в розглянутій задачі знаходження найбільшого спільного дільника двох чисел a і b за допомогою цього алгоритму, відбувається розкладанням дробу $\frac{a}{b}$ в так званий неперервний, або ланцюговий, дріб.

Припустимо, що a і b є задані натуральні числа. Застосуємо до них алгоритм Евкліда

$$a = bq_0 + r_1;\ \frac{a}{b} = q_0 + \frac{r_1}{b} = q_0 + \frac{1}{\frac{b}{r_1}},$$

$$b = r_1 q_1 + r_2;\ \frac{b}{r_1} = q_1 + \frac{r_2}{r_1} = q_1 + \frac{1}{\frac{r_1}{r_2}},$$

$$r_1 = r_2 q_2 + r_3;\ \frac{r_1}{r_2} = q_2 + \frac{r_3}{r_2} = q_2 + \frac{1}{\frac{r_2}{r_3}},$$

$$\ldots\ldots\ldots\ldots\ldots\ldots\ldots$$

$$r_{n-2} = r_{n-1} q_{n-1} + r_n;\ \frac{r_{n-2}}{r_{n-1}} = q_{n-1} + \frac{r_n}{r_{n-1}} = q_{n-1} + \frac{1}{\frac{r_{n-1}}{r_n}},$$

$$r_{n-1} = r_n q_n;\ \frac{r_{n-1}}{r_n} = q_n,$$

звідки

$$\frac{a}{b} = q_0 + \frac{1}{q_1 + \frac{1}{\frac{r_1}{r_2}}} = q_0 + \frac{1}{q_1 + \frac{1}{q_2 + \frac{1}{\frac{r_2}{r_3}}}} = \cdots = q_0 + \frac{1}{q_1 + \frac{1}{q_2 + \ddots + \frac{1}{q_n}}}.$$

Вираз у правій частині має назву *скінченного неперервного, або ланцюгового, дробу* (він ніби складається з окремих ланок q_0, $\frac{1}{q_1}, \ldots, \frac{1}{q_n}$). Його часто позначають символом $[q_0; q_1, q_2, \ldots, q_n]$.

Отже,

$$\frac{a}{b} = [q_0; q_1, q_2, \ldots, q_n] = q_0 + \frac{1}{q_1 + \ddots + \frac{1}{q_n}}, \qquad (1)$$

де n називається *довжиною неперервного дробу*, а числа q_0, q_1, q_2, $\ldots$, q_{n-1} — *неповними частками*.

Якщо $\frac{a}{b}$ — правильний дріб, то $q_0 = 0$ і матимемо такий розклад:

$$\frac{a}{b} = 0 + \frac{1}{q_1 + \ddots + \frac{1}{q_n}} = [0; q_1, q_2, \ldots, q_n].$$

Якщо ж дано від'ємний дріб $\frac{a}{b}$, то його завжди можна подати так: $-k + \frac{a_1}{b}$, де k — ціле додатне, а $\frac{a_1}{b}$ — правильний додатний дріб.

Отже:

$$-k + \frac{a_1}{b} = [-k;\ q_1, q_2,\ \ldots,\ q_n],$$

де всі q_i, крім $q_0 = -k$, додатні.

Зауважимо, що всяке число можна розглядати як неперервний дріб, який має тільки одну ланку: наприклад, $5 = [5]$. Дріб виду $\frac{1}{a}$ можна розглядати як неперервний дріб з двома ланками: $\frac{1}{a} = [0;\ a]$. За означенням довжини неперервного дробу ціле число матиме довжину, що дорівнює нулю. Отже, доведено таку теорему.

Теорема. *Будь-яке раціональне число можна розкласти в скінченний неперервний дріб виду (1), де q_0 — будь-яке ціле число а q_1, q_2, ... — натуральні числа.*

Дроби

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

$$\frac{P_k}{Q_k} = q_0 + \cfrac{1}{q_1 + \ddots + \cfrac{1}{q_k}} \quad (k \leqslant n) \qquad (2)$$

називаються *підхідними дробами*. Очевидно, що останній підхідний дріб у розкладі раціонального числа $r = \frac{a}{b}$ дорівнює цьому числу, тобто $\frac{P_n}{Q_n} = \frac{a}{b}$. Дріб $\frac{P_k}{Q_k} = [q_0;\ q_1,\ \ldots,\ q_k]$ називається *підхідним дробом порядку k* відносно даного неперервного дробу, причому під P_k і Q_k розумітимемо чисельник і знаменник дробу $\frac{P_k}{Q_k}$, який дістаємо формальним згортанням правої частини $[q_0;\ q_1,\ \ldots,\ q_k]$ без будь-яких скорочень (якщо навіть вони й можливі).

Зауваження. Якщо поставити вимогу, щоб останній знаменник був більший від одиниці, то розклад раціонального числа в неперервний дріб буде єдиним. Якщо ж не вимагати, щоб $q_n > 1$, то можна дане раціональне число розкласти в неперервний дріб двома способами: якщо один з них дає розклад $[q_0;\ q_1,\ \ldots,\ q_{n-1},\ q_n]$ і $q_n > 1$, то другий $[q_0;\ q_1,\ \ldots,\ q_n - 1,\ 1]$. Тут число ланок збільшується на одиницю, останній знаменник $q_{n+1} = 1$. Якщо маємо розклад $[q_0;\ q_1,\ \ldots,\ q_{n-1},\ 1]$, то його можна подати так: $[q_0;\ q_1,\ \ldots,\ q_{n-1} + 1]$. Тут число ланок зменшується на одиницю, і останній знаменник $q_{n-1} + 1 > 1$. Це зауваження дає можливість вибирати номер останнього підхідного дробу (при розкладанні в неперервний дріб) парним або непарним.

Контрольні запитання

1. Як пов'язаний алгоритм Евкліда з неперервними дробами?
2. Яке число називається довжиною скінченного неперервного дробу (1)?
3. Якими числами є q_0, q_1, q_2, ..., q_n? Як вони називаються?
4. Які дроби називаються підхідними до неперервного дробу (1)?
5. Коли розклад раціонального числа в скінченний, неперервний дріб є єдиним?

§ 8. Основні властивості підхідних дробів

Теорема 1. *Чисельники і знаменники трьох послідовних підхідних дробів пов'язані залежностями*

$$P_{k+1} = q_{k+1}P_k + P_{k-1};\quad Q_{k+1} = q_{k+1}Q_k + Q_{k-1}.\ (k \geqslant 1) \qquad (1)$$

Зауважимо спочатку, що P_k і Q_k залежать лише від q_0, q_1, q_2, ..., q_k.

Цю теорему доведено методом математичної індукції. У справедливості рекурентних формул (1) для $k = 1$ переконуємося безпосередньо:

$$\frac{P_0}{Q_0} = \frac{q_0}{1},\ P_0 = q_0,\ Q_0 = 1;$$

$$\frac{P_1}{Q_1} = q_0 + \frac{1}{q_1} = \frac{q_0q_1 + 1}{q_1},\ P_1 = q_0q_1 + 1,\ Q_1 = q_1;$$

$$\frac{P_2}{Q_2} = q_0 + \frac{1}{q_1 + \frac{1}{q_2}} = q_0 + \frac{q_2}{q_1q_2 + 1} = \frac{(q_0q_1 + 1)\,q_2 + q_0}{q_1q_2 + 1} = \frac{q_2P_1 + P_0}{q_2Q_1 + Q_0}.$$

Припустимо тепер, що ці формули справедливі для підхідного дробу порядку k $(k > 1)$ і доведемо, що тоді вони будуть такими самими і для підхідного дробу порядку $k + 1$.

За припущенням маємо:

$$\frac{P_k}{Q_k} = \frac{q_kP_{k-1} + P_{k-2}}{q_kQ_{k-1} + Q_{k-2}}.$$

Але підхідний дріб порядку $k + 1$ утворюється з підхідного дробу порядку k додаванням до нього однієї ланки, тобто заміною q_k на $q_k + \frac{1}{q_{k+1}}$. Отже,

$$\frac{P_{k+1}}{Q_{k+1}} = \frac{\left(q_k + \frac{1}{q_{k+1}}\right)P_{k-1} + P_{k-2}}{\left(q_k + \frac{1}{q_{k+1}}\right)Q_{k-1} + Q_{k-2}} = \frac{q_{k+1}(q_kP_{k+1} + P_{k-2}) + P_{k-1}}{q_{k+1}(q_kQ_{k+1} + Q_{k-2}) + Q_{k-1}} =$$

$$= \frac{q_{k+1}P_k + P_{k-1}}{q_{k+1}Q_k + Q_{k-1}}.$$

що й доводить таке твердження. Рекурентні формули (1) не тільки дають зручний спосіб обчислення підхідних дробів, але є також формальною основою всієї теорії неперервних дробів. Чисельники і знаменники підхідних дробів доцільно обчислювати за такою схемою:

k		0	1	2		$k-2$	$k-1$	k		$n-1$	n
q_k		q_0	q_1	q_2		q_{k-2}	q_{k-2}	q_k		q_{n-1}	q_n
p_k	1	$P_0=q_0$	P_1	P_2		P_{k-2}	P_{k-1}	P_k		P_{n-1}	$P_n=a$
Q_k	0	$Q_0=1$	Q_1	Q_2		Q_{k-2}	Q_{k-1}	Q_k	...	Q_{n-1}	$Q_n=b$

Приклад. Розкласти в неперервний дріб число $-\frac{99}{170}$ і обчислити всі підхідні дроби.

Маємо: $-\frac{99}{170}=-1+\frac{71}{170}$;

$$\begin{array}{r|l} 170 & 71 \\ 142 & 2 \\ \hline 71 & 28 \\ 56 & 2 \\ \hline 28 & 15 \\ 15 & 1 \\ \hline 15 & 13 \\ 13 & 1 \\ \hline 13 & 2 \\ 2 & 1 \\ \hline 0 & 2 \end{array} \quad 6.$$

Отже, шуканий розклад буде

$$-\frac{99}{170}[-1;\ 2,\ 2,\ 1,\ 1,\ 6,\ 2]=-1+\cfrac{1}{2+\cfrac{1}{2+\cfrac{1}{1+\cfrac{1}{1+\cfrac{1}{6+\frac{1}{2}}}}}}$$

Тут матимемо:

k		0	1	2	3	4	5	6
q_k		-1	2	2	1	1	6	2
P_k	1	-1	-3	-7	-10	-17	-119	-337
Q_k	0	1	2	5	7	12	79	170

Отже: $\frac{P_0}{Q_0}=-1$; $\frac{P_1}{Q_1}=-\frac{1}{2}$; $\frac{P_2}{Q_2}=-\frac{3}{5}$; $\frac{P_3}{Q_3}=-\frac{4}{7}$; $\frac{P_4}{Q_4}=-\frac{7}{12}$; $\frac{P_5}{Q_5}=-\frac{46}{79}$; $\frac{P_6}{Q_6}=-\frac{99}{170}$;

Теорема 2. *Між чисельниками і знаменниками двох послідовних підхідних дробів має місце залежність:*

$$P_{k+1}Q_k-P_kQ_{k+1}=(-1)^k \quad (k\geqslant 0). \tag{2}$$

Справді, знайдемо різницю:

$$\frac{P_{k+1}}{Q_{k+1}}-\frac{P_k}{Q_k}=\frac{h_{k+1}}{Q_kQ_{k+1}},$$

де

$$h_{k+1}=P_{k+1}Q_k-P_kQ_{k+1};$$

підставляючи замість P_{k+1} і Q_{k+1} їхні вирази з формул (1), матимемо:

$$h_{k+1}=(q_{k+1}P_k+P_{k-1})Q_k-P_k(q_{k+1}Q_k+Q_{k-1})=P_{k-1}Q_k-P_kQ_{k-1}=-h_k,$$

звідки $h_{k+1}=-h_k$.

Але з цього співвідношення в поєднанні з тим, що $h_1=P_1Q_0-P_0Q_1=(q_0q_1+1)\cdot 1-q_0q_1=1$, а отже, $h_2=-1$ і т. д., маємо $h_{k+1}=(-1)^k$, тобто $P_{k+1}Q_k-P_kQ_{k+1}=(-1)^k$. Цим теорему повністю доведено.

Зокрема, в попередньому прикладі маємо:

$$P_5Q_4-P_4Q_5=-46\cdot 12-(-7)\cdot 79=(-1)^4=1.$$

Висновок 1. *Різницю між двома суміжними підхідними дробами можна подати у вигляді*

$$\frac{P_{k+1}}{Q_{k+1}}-\frac{P_k}{Q_k}=\frac{(-1)^k}{Q_kQ_{k+1}}. \tag{3}$$

Висновок 2. *Кожний підхідний дріб є нескоротним.*

Справді, припустимо, що $(P_k, Q_k) = d > 1$, тоді ліва частина рівності (2) має ділитись на d, а отже, і права частина цієї рівності $(-1)^k$ також має ділитись на d, що неможливо.

Зауваження. Якщо раціональне число $\frac{a}{b}$ розкласти в неперервний дріб, то останній підхідний дріб $\frac{P_n}{Q_n}$ у цьому розкладі нескоротний і дорівнює $\frac{a}{b}$. Отже, розкладання в неперервний дріб дає змогу скорочувати дроби.

Приклад. За допомогою розкладання в неперервний дріб скоротити дріб $\frac{1180}{1829}$.

Маємо: $\frac{1180}{1829} = [0; 1, 1, 1, 4, 2]$. Знайдемо тепер останній підхідний дріб у цьому розкладі.

q_k		0	1	1	1	4	2
P_k	1	0	1	1	2	9	20
Q_k	0	1	1	2	3	14	31

Звідси $\frac{P_n}{Q_n} = \frac{P_5}{Q_5} = \frac{20}{31}$ і, отже, $\frac{1180}{1829} = \frac{20}{31}$.

Теорема 3. *Підхідні дроби парного порядку із зростанням номера дробу утворюють зростаючу послідовність, а підхідні дроби непарного порядку — спадну послідовність, отже, будь-який підхідний дріб непарного порядку більший за будь-який підхідний дріб парного порядку.*

Доведемо спочатку, що для всіх $k \geqslant 2$

$$\frac{P_{k-2}}{Q_{k-2}} - \frac{P_k}{Q_k} = \frac{(-1)^{k-1} q_k}{Q_k Q_{k-2}}.$$

Справді, користуючись теоремами 1 і 2, маємо:

$$\frac{P_{k-2}}{Q_{k-2}} - \frac{P_k}{Q_k} = \frac{P_{k-2}Q_k - P_k Q_{k-2}}{Q_k Q_{k-2}} =$$

$$= \frac{(q_k Q_{k-1} + Q_{k-2}) P_{k-2} - (q_k P_{k-1} + P_{k-2}) Q_{k-2}}{Q_k Q_{k-2}} = \frac{(-1)^{k-1} q_k}{Q_k Q_{k-2}}.$$

Зауважимо, що знаменники підхідних дробів зростають із збільшенням номера дробу $(Q_k = q_k Q_{k-1} + Q_{k-2} \geqslant Q_{k-1} + Q_{k-2} > Q_{k-1}$. Тому з доведеної рівності можна зробити висновок, що підхідні

дроби парних порядків утворюють зростаючу послідовність, а підхідні дроби непарних порядків — спадну послідовність. Далі, внаслідок теореми 2, кожний підхідний дріб непарного порядку більший від дробу беспосередньо наступного парного порядку; але, очевидно, що

$$\frac{P_0}{Q_0} < \frac{P_1}{Q_1} \text{ і } \frac{P_1}{Q_1} > \frac{P_k}{Q_k}$$

при довільному k, отже, всі підхідні дроби парного порядку менші від усіх підхідних дробів непарного порядку.

Знаючи, що дріб $\frac{a}{b}$ дорівнює $\frac{P_n}{Q_n}$ (останньому підхідному дробу), можна записати:

$$\frac{P_0}{Q_0} < \frac{P_2}{Q_2} < \frac{P_4}{Q_4} < \cdots < \frac{a}{b} < \cdots < \frac{P_5}{Q_5} < \frac{P_3}{Q_3} < \frac{P_1}{Q_1}.^1 \qquad (4)$$

Нерівності (4) і доводять нашу теорему.

Крім цього, нерівності (4) показують, що розкладуваний дріб $\alpha = \frac{a}{b}$ завжди міститься між двома будь-якими суміжними[2] підхідними дробами, інтервал між якими із зростанням порядку зменшується. Цим і пояснюється назва «підхідні дроби». Нерівності (4) показують навіть більше, а саме, що $\frac{a}{b}$ лежить між будь-яким парним і будь-яким непарним підхідними дробами.

Теорема 4. *Парні підхідні дроби дають наближення до* $\alpha = \frac{a}{b}$ *з недостачею, а непарні — з надвишком, причому, оцінка похибки визначається нерівностями:*

$$\left|\alpha - \frac{P_k}{Q_k}\right| < \frac{1}{Q_k Q_{k+1}} < \frac{1}{Q_k (Q_k + Q_{k-1})} < \frac{1}{Q_k^2}. \qquad (5)$$

Справді, перше твердження беспосередньо випливає з нерівностей (4). Далі, на підставі теореми 3, можна записати, що

$$\left|\alpha - \frac{P_k}{Q_k}\right| < \left|\frac{P_{k+1}}{Q_{k+1}} - \frac{P_k}{Q_k}\right| = \frac{1}{Q_k Q_{k+1}}$$

(див. теорему 2), і через те що $Q_{k+1} \geqslant Q_k + Q_{k-1}$, то

$$\left|\alpha - \frac{P_k}{Q_k}\right| < \frac{1}{Q_k Q_{k+1}} < \frac{1}{Q_k (Q_k + Q_{k-1})} < \frac{1}{Q_k^2}.$$

---

[1] У нерівностях (4) два знаки $< 1 >$ одночасно рівностями бути не можуть.

[2] Будь-які підхідні дроби, що стоять поряд у ряді $\frac{P_0}{Q_0}, \frac{P_1}{Q_1}, \ldots, \frac{P_k}{Q_k}$, називають суміжними.

Зауваження. Хоч оцінки похибки

$$\frac{1}{Q_k(Q_k+Q_{k-1})},\ \frac{1}{Q_k^2}$$

і гірші, ніж оцінка $\frac{1}{Q_kQ_{k+1}}$, але вони значно зручніші, бо при оцінці $\frac{1}{Q_k(Q_k+Q_{k-1})}$ не потрібно знати знаменник Q_{k+1} наступного підхідного дробу, а тільки попереднього, а при оцінці похибки $\frac{1}{Q_k^2}$ взагалі не потрібно знати знаменник ні попереднього, ні наступного підхідного дробу.

Контрольні запитання

1. Як пов'язані між собою чисельники і знаменники трьох послідовних підхідних дробів?
2. Перевірте формулу (1) для трьох послідовних підхідних дробів у розкладі числа $-\frac{99}{170}$ в неперервний дріб.
3. З якою метою в таблиці для знаходження підхідних дробів у стовпці перед P_0 і Q_0 ставлять числа 1 і 0?
4. Який зв'язок між чисельниками і знаменниками двох послідовних підхідних дробів?
5. Чому будь-який підхідний дріб парного порядку менший від будь-якого підхідного дробу непарного порядку?
6. Чому дорівнює похибка, яку допускають при заміні раціонального числа $\frac{a}{b}$ підхідним дробом $\frac{P_k}{Q_k}$?

§ 9. Застосування неперервних дробів до розв'язування невизначених рівнянь першого степеня з двома невідомими

Розв'язування невизначеного рівняння першого степеня з двома невідомими, тобто рівняння

$$ax+by=c, \qquad (1)$$

в загальному випадку не становить інтересу, бо, надаючи одному з невідомих довільного значення, зразу ж дістаємо значення другого невідомого.

Набагато цікавішою і складнішою буде така задача: знайти цілі розв'язки рівняння (1) при цілих a, b і c. Вона тісно зв'язана з питаннями подільності; так, наприклад, при довільному цілому значенні y різниця $c-by$ буде цілою, але відповідне $x=\frac{c-by}{a}$, взагалі кажучи, при цих значеннях y не буде цілим; все залежатиме від подільності $c-by$ на a.

Доведемо такі два твердження.

Теорема 1. *Якщо права частина рівняння* (1) *не ділиться на найбільший спільний дільник* $d=(a, b)$ *коефіцієнтів лівої частини, то це рівняння не має розв'язків у цілих числах.*

Справді, при довільних цілих x і y ліва частина рівняння (1) ділиться на d, а права — не ділиться на d, що суперечить теоремі 2, § 1.

Надалі можна буде обмежитись рівнянням (1), в якому $(a, b)=1$, бо якщо $(a, b)=d>1$ і c ділиться на d, то, скоротивши обидві частини рівняння (1) на d, матимемо, що в новому рівнянні $(a, b)=1$. Можна вважати також, що a і b не дорівнюють нулю. Коли б хоч один коефіцієнт дорівнював нулю, то ми мали б фактично одне рівняння з одним невідомим.

Теорема 2. *Якщо* x_1 *і* y_1 *є яка-небудь пара цілих значень* x *і* y, *що задовольняють рівняння* (1), *де* $(a, b)=1$, *то загальний розв'язок цього рівняння в цілих числах можна подати у вигляді:*

$$x=x_1+bt, \qquad y=y_1-at,$$

де t *— довільне ціле число.*

Справді, за умовою теореми, маємо: $ax_1+by_1=c$.

Віднімаючи цю рівність почленно від рівняння (1), знайдемо:

$$a(x-x_1)+b(y-y_1)=0,$$

звідки $\frac{y-y_1}{x-x_1}=-\frac{a}{b}$.

Оскільки $(a, b)=1$ за умовою, то

$$y-y_1=-at, \quad x-x_1=bt,$$

де t — довільне ціле число, і остаточно маємо:

$$x=x_1+bt, \qquad y=y_1-at.$$

Отже, розв'язування рівняння (1) в цілих числах зводиться до знаходження якого-небудь окремого розв'язку цього рівняння.

Розкладемо $\frac{a}{b}$ в неперервний дріб[1]; нехай $\frac{P_n}{Q_n}$ буде останнім підхідним дробом у цьому розкладі, тоді $\frac{a}{b}=\frac{P_n}{Q_n}$. За умовою $(a, b)=1$, і тому що всякий підхідний дріб нескоротний, то $(P_n, Q_n)=1$, отже, $P_n=a$ і $Q_n=b$.

---

[1] Зауважимо, що a і b, тобто коефіцієнти рівняння $ax+by=c$, завжди можна вважати натуральними числами. Для цього досить, в разі потреби, відповідно змінити знаки перед x і y. Наприклад, рівняння $12x-19y=7$ записуємо так: $12x+19(-y)=7$, або $12x+19Y=7$, де $x=x$, $Y=-y$.

Скориставшись теоремою 2, § 8, матимемо:

$$P_nQ_{n-1} - P_{n-1}Q_n = (-1)^{n-1}, \text{ або } aQ_{n-1} - bP_{n-1} = (-1)^{n-1}.$$

Помноживши останню рівність на $(-1)^{n-1} \cdot c$, дістаємо:

$$a[(-1)^{n-1}cQ_{n-1}] + b[(-1)^n cP_{n-1}] = c.$$

Порівнюючи знайдену рівність з рівнянням $ax + by = c$, переконуємось, що

$$x_1 = (-1)^{n-1}cQ_{n-1} \text{ і } y_1 = (-1)^n cP_{n-1}$$

є частинним розв'язком заданого рівняння. Цим, беручи до уваги теорему 2, доведено таке твердження:

Теорема 3. *Загальний розв'язок у цілих числах невизначеного рівняння* $ax + by = c$, *де* $(a, b) = 1$, *можна подати у вигляді*

$$x = (-1)^{n-1}cQ_{n-1} + bt, \quad y = (-1)^n cP_{n-1} - at, \qquad (2)$$

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

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

Насамперед перепишемо задане рівняння так: $117(-x) + 343y = 119$. Тоді стоятиме завдання визначити невідомі $-x$ та y.

Розкладаючи $\frac{a}{b} = \frac{117}{343}$ в неперервний дріб, дістанемо:

$$\frac{117}{343} = [0;\ 2,\ 1,\ 13,\ 1,\ 1,\ 1,\ 2].$$

У даному випадку $n = 7$, $P_{n-1} = P_6 = 44$, $Q_{n-1} = Q_6 = 129$, і одним з частинних розв'язків рівняння буде:

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

Загальний розв'язок, за формою (2), запишеться так:

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

або

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

Тут ми дістали порівняно великі за абсолютною величиною частинні значення x_0, y_0, але з загального розв'язку легко дістати інші окремі значення для x і y, які будуть найменші за абсолютною величиною. Якщо покладемо $t = -45$, дістанемо $x_1 = 84$, $y_1 = 29$, і загальний розв'язок рівняння буде:

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

Тут t замінено на $-t$.

Зауважимо, що можна було б у цій задачі зразу визначити x і y. Справді, розкладаючи $-\frac{117}{343}$ в неперервний дріб, дістанемо

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

маємо $n = 8$, $a = -117$, $b = 343$, $c = 119$, $P_{n-1} = P_7 = -44$, $Q_{n-1} = Q_7 = 129$; тому

$$x_0 = (-1)^7 \cdot 119 \cdot 129 = -15\,351,$$
$$y_0 = (-1)^8 \cdot 119 \cdot (-44) = -44 \cdot 119 = -5236.$$

Отже,

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

При $t = 45$ дістаємо той самий результат:

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

На закінчення цього параграфа спинимось на одному елементарному способі розв'язування невизначених рівнянь першого степеня, який, по суті, збігається з поданим вище, але не потребує знання теорії неперервних дробів; цей спосіб раніше часто викладали в курсах елементарної алгебри.

Для визначеності покладемо $|a| > |b| \neq 0$; тоді з рівняння $ax + by = c$ дістанемо $y = \frac{c - ax}{b}$; покладемо $c = bq_1 + r_1$ і $a = bs + a_1$, де $|a_1| < |b|$, $|r_1| < |b|$; тоді, відокремлюючи цілу частину, дістанемо:

$$y = q_1 - sx + \frac{r_1 - a_1x}{b}.$$

Вимога, щоб y було цілим при цілому x, еквівалентна вимозі, щоб $\frac{r_1 - a_1x}{b} = t_1$ було цілим числом. Отже, можна записати нове рівняння з двома невідомими x і t_1, але вже з коефіцієнтами, істотно меншими [1]:

$$bt_1 + a_1x = r_1.$$

Аналогічно перетворюючи останнє рівняння, прийдемо до нового рівняння з коефіцієнтами, істотно меншими від попереднього. Цей процес продовжуємо доти, поки не дістанемо рівняння, в якому один з коефіцієнтів при невідомому дорівнюватиме 1 і яке безпосередньо розв'язується в цілих числах. Підставляючи знайдені значення невідомих в оберненому порядку, знайдемо розв'язок даного рівняння $ax + by = c$, причому відразу в загальному вигляді. Те, що в результаті дістанемо рівняння з коефіцієнтом 1 при

[1] Найбільший коефіцієнт у цьому рівнянні за абсолютною величиною не більший від найменшого коефіцієнта даного рівняння.

одному з невідомих, випливає з того, що вказаний процес відокремлення цілої частини, по суті, збігається з алгоритмом Евкліда для знаходження н. с. д. чисел a і b, але за умовою $(a, b) = 1$.

Проілюструємо це на прикладі. Розв'яжемо те саме рівняння:

$$-117x + 343y = 119.$$

Маємо:

$$x = \frac{343y - 119}{117} = 3y - 1 + \frac{-8y - 2}{117} = 3y - 1 - 2 \cdot \frac{4y + 1}{117} = 3y - 1 - 2t_1,$$

де $\frac{4y+1}{117} = t_1$ — ціле число. З добутого рівняння знаходимо:

$$y = \frac{117t_1 - 1}{4} = 29t_1 + \frac{t_1 - 1}{4} = 29t_1 + t,$$

де $\frac{t_1 - 1}{4} = t$ — ціле число. Останнє рівняння розв'язується вже беспосередньо, а саме: $t_1 = 1 + 4t$. Підставляючи знайдене значення t_1 у вираз для y, матимемо:

$$y = 29 + 117t$$

і далі

$$x = 3(29 + 117t) - 1 - 2(1 + 4t) = 84 + 343t.$$

Для скорочення викладок при діленні 343 на 117 беремо від'ємну остачу — 8 замість додатної 109 і потім з дробової частини виносимо спільний множник — 2.

Коли за змістом задачі треба невизначене рівняння розв'язати в цілих додатних числах, то слід спочатку це рівняння розв'язати в цілих числах, а потім розв'язати систему нерівностей

$$\begin{aligned} x &> 0, \\ y &> 0 \end{aligned}$$

відносно t.

З того, що дане невизначене рівняння має розв'язок в цілих числах (розв'язків у цілих числах або немає, або їх нескінченна множина) ще не випливає, що воно матиме розв'язки в цілих додатних числах. Взагалі, невизначене рівняння може не мати розв'язків у цілих додатних числах і може мати скінченну або нескінченну множину таких розв'язків.

Щоб пояснити це, розв'яжемо таку задачу: нехай на 1 крб. треба купити 20 поштових марок — вартістю по 6 коп., 4 коп. і 3 коп. Скільки буде марок кожної вартості, коли вважати, що купуватимуть всі три види марок?

Позначимо через x число марок вартістю 6 коп., через y — число марок вартістю 4 коп. і через z — число трикопієчних марок. Дістанемо систему двох рівнянь з трьома невідомими:

$$\begin{cases} 6x + 4y + 3z = 100, \\ x + y + z = 20. \end{cases}$$

Справді, очевидно, що всяке d виду (4) ділить a. Навпаки, нехай d ділить a, тоді $a = dq$, де q — ціле $\geqslant 1$, і, отже, всі прості дільники числа d входять до канонічного розкладу числа a з показниками β_i де $0 \leqslant \beta_i \leqslant \alpha_i$. Тому всі дільники d числа a матимуть вигляд (4).

Припустимо, що дано два натуральних числа a і b. Їхні канонічні розклади завжди можна записати в такому вигляді:

$$a = p_1^{\alpha_1} p_2^{\alpha_2} \dots p_s^{\alpha_s} \text{ і } b = p_1^{\gamma_1} p_2^{\gamma_2} \dots p_s^{\gamma_s},$$

причому припускаємо, що α_i і γ_i можуть набувати й нульових значень. Внаслідок цього можна для зручності в обох розкладах писати одні й ті самі співмножники $p_1, p_2, \dots, p_s$, пронумерувавши всі прості числа, які входять до розкладу хоч би одного з чисел a і b. Тоді будуть справедливі такі висновки.

Висновок 2. *Найбільший спільний дільник чисел a і b матиме вигляд*:

$$(a, b) = p_1^{\lambda_1} p_2^{\lambda_2} \dots p_s^{\lambda_s}, \text{ де } \lambda_i = \min(\alpha_i, \gamma_i).$$

Висновок 3. *Найменше спільне кратне чисел a і b матиме вигляд:*

$$[a, b] = p_1^{\mu_1} p_2^{\mu_2} \dots p_s^{\mu_s}, \text{ де } \mu_i = \max(\alpha_i, \gamma_i).$$

Ці твердження очевидні. З них безпосередньо випливає тотожність:

$$(ab)[a, b] = ab,$$

і їх без змін можна поширити на випадок більш, як двох чисел.

Контрольні запитання

1. Яке число називається простим?
2. Перелічить основні властивості простих чисел.
3. Сформулюйте основну теорему арифметики цілих чисел.
4. У чому полягає факторизація заданого числа?
5. Чому при складанні таблиці простих чисел «решетом Ератосфена» не треба знати ознак подільності на прості числа?
6. Коли за допомогою «решета Ератосфена» можна вважати закінченим складання таблиці простих чисел, які не перевищують натурального числа N?
7. Який вигляд мають дільники числа $a = p_1^{\alpha_1} p_2^{\alpha_2} \dots p_s^{\alpha_s}$?
8. Чому дорівнюють найбільший спільний дільник і найменше спільне кратне двох чисел, якщо відомі канонічні розклади цих чисел?

Вправи

1. Довести, що одне з трьох послідовних чисел ділиться на 3.
2. Довести, що $n(n + 1)(n + 2)$ ділиться на 6 при будь-якому натуральному n.
3. Довести, що $8 \cdot 23^{23} - 71 \cdot 32^{32}$ ділиться на 10.

4. Знайти остачу від ділення числа

$$88^{33} + 33^{88} \text{ на } 7.$$

Відповідь. 3.

5. Довести, що коли $(mn + pq) \vdots (m - p)$, то $(mq + np) \vdots (m - p)$.

6. Дано цілі числа a, b, c, d, n, які задовольняють умови $(b, n) = 1$, $(ad - bc) \vdots n$, $(a - b) \vdots n$. Довести, що $(c - d) \vdots n$.

7. За допомогою алгоритму Евкліда знайти найбільший спільний дільник кожної з таких груп чисел: а) 42 628 і 33 124; б) 299, 391, 667; в) 1955, 2431, 3111, 4862.

Відповідь. а) $(42\,628, 33\,124) = 4$; б) $(299, 391, 667) = 23$; в) $(1955, 2431, 3111, 4862) = 17$.

8. Довести, що коли $a = cq + r$ і $b = cq_1 + r_1$, де a, b, q, q_1, r, r_1 — цілі невід'ємні числа і c — ціле додатне число, то $(a, b, c) = (r, r_1, c)$. Сформулювати правило, яке звідси випливає, для знаходження найбільшого спільного дільника (a, b, c) послідовним подвійним діленням. Узагальнити це правило на випадок n чисел.

9. Користуючись виведеним у попередній задачі правилом послідовного подвійного ділення, знайти найбільший спільний дільник чисел 2337, 4389 і 5909.

Відповідь. $(2337, 4389, 5909) = 19$.

10. Знайти найменше спільне кратне чисел: а) 120 і 96; б) 232, 460 і 280.

Відповідь. а) $[120, 96] = 480$; б) $[232, 460, 280] = 186\,760$.

11. Розкласти в неперервні дроби: а) $\frac{37}{81}$; б) $\frac{1811}{691}$; в) $\frac{1723}{1447}$; г) $\frac{3203}{1289}$; д) $\frac{4513}{18355}$; е) 2,98976; є) 2,71828; ж) 3,14159.

Відповідь. а) [0; 2, 5, 3, 2]; б) [2; 1, 1, 1, 1, 1, 3, 7, 1, 2]; в) [1; 5, 4, 8, 2, 1, 2]; г) [2; 2, 16, 39]; д) [0; 4, 14, 1, 8, 2, 7, 2]; е) [2; 1, 96, 1, 1, 1, 10]; є) [2; 1, 2, 1, 1, 4, 1, 1, 6, 10, 1, 1, 2]; ж) [3; 7, 15, 1, 25, 1, 7, 4].

12. Розкласти в неперервні дроби: а) $\frac{343}{226}$ і $\frac{226}{343}$; б) $\frac{117}{343}$ і $\frac{343}{117}$. Порівняйте підхідні дроби в цих розкладах.

Відповідь. а) $\frac{343}{226} = [1; 1; 1, 13, 1, 1, 1, 2]$ і $\frac{226}{343} = [0; 1, 1, 1, 13, 1, 1, 1, 2]$; підхідні дроби відповідно дорівнюватимуть: $\frac{1}{1}, \frac{2}{1}, \frac{3}{2}, \frac{41}{27}, \frac{44}{29}, \frac{85}{56}, \frac{129}{85}, \frac{343}{226}$ і $\frac{0}{1}, \frac{1}{1}, \frac{1}{2}, \frac{2}{3}, \frac{27}{41}, \frac{29}{44}, \frac{56}{85}, \frac{86}{129}, \frac{226}{343}$; б) $-\frac{117}{343} = [-1; 1, 1, 1, 13, 1, 1, 1, 2]$ і $\frac{343}{117} = -3; 14, 1, 1, 1, 2$; підхідні дроби відповідно дорівнюватимуть: $-1, 0, -\frac{1}{3}, -\frac{14}{41}, -\frac{15}{44}, -\frac{29}{85}, -\frac{44}{129}, -\frac{117}{343}$ і $-\frac{3}{1}, -\frac{41}{14}, -\frac{44}{15}, -\frac{85}{29}, -\frac{129}{44}, -\frac{343}{117}$.

13. Розв'язати в цілих числах невизначені рівняння: а) $49x + 9y = 400$; б) $12x + 31y = 170$; в) $3827x + 3293y = 1869$.

Відповідь. а) $x = 1 - 9t$, $y = 39 + 49t$; б) $x = 9 + 31t$; $y = 2 - 12t$; в) $x = -15 + 37t$, $y = 18 - 43t$.

14. Розв'язати в цілих додатних числах невизначені рівняння: а) $8x + 13y = 15$; б) $23x - 42y = 72$; в) $15x + 28y = 185$.

Відповідь. а) Рівняння в цілих додатних числах розв'язків не має; б) $x = 4 + 42t$, $y = 23t$, де t — довільне ціле додатне число; в) $x = 3$, $y = 5$.

15. Розкласти число 100 на суму таких двох цілих додатних чисел, щоб одне з них ділилось на 7, а друге на 11.

Відповідь. 56 і 44.

16. Для настилання підлоги завширшки 3 *м* є дошки завширшки 11 *см* і 13 *см*. Скільки треба взяти дощок того й другого розміру, коли вважати, що довжина кімнати і довжина дощок однакові і дошки кладуться вздовж кімнати?

Відповідь. 19 дощок завширшки 11 *см* і 7 дощок завширшки 13 *см*, або 6 дощок завширшки 11 *см* і 18 дощок завширшки 13 *см*.

17. 26 осіб витратили разом 88 монет, причому кожен чоловік витратив 6, жінка 4, а дівчина 2 монети. Скільки було чоловіків, жінок і дівчат?

Відповідь. Задача має 10 розв'язків: (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).

18. Хтось купив 30 птахів за 30 монет; з числа цих птахів за кожних 3 горобців було заплачено 1 монету, за кожні дві горлиці також 1 монету і, нарешті, за кожного голуба — по 2 монети. Скільки куплено птахів кожного виду?

Відповідь. Горобців 9, горлиць 10, голубів 11.

19. Відомо (теорема 1, § 4), що найбільший спільний дільник двох чисел a і b лінійно виражається через ці числа з цілими коефіцієнтами, тобто, існують такі два цілі числа x і y, що

$$d = (a, b) = ax + by.$$

Узагальнити це твердження для кількох чисел.

20. Довести, що два додатних нескоротних дроби рівні тоді і тільки тоді, коли рівні їхні чисельники і знаменники.

21. Довести, що сума

$$\frac{1}{2} + \frac{1}{3} + \ldots + \frac{1}{n} \quad (n > 1)$$

не може бути цілим числом.

22. Довести, що сума

$$\frac{1}{3} + \frac{1}{5} + \ldots + \frac{1}{2n+1} \quad (n > 0)$$

не може бути цілим числом.

Довести, що коли $2^n + 1$ — просте число, де n — ціле додатне, то $n = 2^k$, де k — ціле невід'ємне.

24. Довести, що коли $2^n - 1$ — просте число, то і n — просте число.

25. Довести, що існує нескінченна множина простих чисел виду $6m - 1$.

26. Довести існування нескінченної множини простих чисел виду $4m - 1$.

27. За допомогою «решета Ератосфена» скласти таблицю простих чисел, які менші за 200.

28. Знайти канонічний розклад чисел: а) 82 798 848; б) 4 497 552 259 200; в) 67 463 283 888 000.

Відповідь: а) $2^8 \cdot 3^5 \cdot 11^3$; б) $2^7 \cdot 3^3 \cdot 5^2 \cdot 7^2 \cdot 11 \cdot 13 \cdot 17 \cdot 19 \cdot 23$; в) $2^6 \cdot 3^4 \cdot 5^2 \cdot 7^2 \cdot 11 \cdot 13 \cdot 17 \cdot 19 \cdot 23$.

29. Скільки є способів розкладання числа на добуток двох взаємно простих множників?

Відповідь. 2^{k-1}, де k — число різних простих множників даного числа.

30. Нехай $n = p_1^{\alpha_1} p_2^{\alpha_2} \ldots p_k^{\alpha_k}$ — канонічний розклад натурального числа n. Довести, що $\sqrt[m]{n}$ тоді і тільки тоді є цілим числом, коли показники $\alpha_1, \alpha_2, \ldots, \alpha_k$ канонічного розкладу діляться на m.

31. Довести, що алгебраїчна сума нескоротних дробів, у яких знаменники попарно взаємно прості, не може бути цілим числом.

32. Довести, що цілі додатні розв'язки рівняння $x^2 + y^2 = z^2$, що задовольняють умову $(x, y, z) = 1$, можна дістати за формулами:

$$x = uv, \quad y = \frac{u^2 + v^2}{2}, \quad z = \frac{u^2 + v^2}{2}$$

при цьому $u > v > 0$, $(u, v) = 1$; u, v — непарні.

ІСТОРИЧНІ КОМЕНТАРІ

1. Так званий алгоритм Евкліда був запропонований спочатку в геометричній формі для знаходження найбільшої міри двох відрізків або, взагалі, двох геометричних величин. У цій формі він є в «Початках» Евкліда. Про алгоритм Евкліда для знаходження найбільшого спільного дільника двох чисел при скороченні дробів йдеться у відомій пам'ятці стародавньої китайської математики — «Математика в дев'яти книгах».

2. Підхідними неперервними дробами користувався в свій час ще арабський математик аль-Каласаді (пом. 1486); він застосовував їх при діленні з остачею і позначав ними дробове число.

Схему для обчислення підхідних дробів, подібну розглянутій нами в § 8, склав німецький математик Швентер (1585—1636).

3. Розв'язуванням невизначених рівнянь першого степеня в цілих числах, крім Діофанта, займались китайські (з II ст.) і індійські (VI ст.) вчені, а також учені народів Середньої Азії (з IX ст.). Метод розв'язування невизначених рівнянь першого степеня в цілих числах знову був знайдений у XVII ст. французьким математиком Баше де Мезеріаком (1581—1638). Розв'язання цієї задачі зумовило побудову дуже важливої для теорії чисел теорії неперервних дробів. У другому виданні книги «Приємні і цікаві задачі» (1624) Баше де Мезеріак розв'язує рівняння $ax - by = 1$. Він фактично застосовує процес, який зводиться до послідовного обчислення підхідних дробів. Цей популярний твір Баше де Мезеріака дуже вплинув на розвиток теорії чисел, сприяючи виникненню інтересу до цієї області математики. Велике значення для розвитку теорії чисел мало й те, що в 1621 р. Баше де Мезеріак здійснив видання творів Діофанта грецькою і латинською мовами з доповненнями і примітками. Після Баше де Мезеріака в XVII і XVIII ст. різні способи розв'язання невизначного рівняння першого степеня з двома невідомими в цілих числах пропонували французький математик Роль (1652—1719), англійський математик Саундерсон (1632—1739), Ейлер та інші.

У явному вигляді неперервні дроби до розв'язання таких рівнянь застосував Лагранж.

4. Задачі, які зводяться до систем невизначених рівнянь, зустрічаються в італійського математика Леонардо Пізанського (Фібоначчі) (бл. 1170 — після 1228) і в Баше де Мезеріака. Фібоначчі був першим з математиків, хто показав, що для знаходження дільників натурального числа a досить випробувати його подільність на числа, які не перевищують $\sqrt{a}$ (див. властивість 5 простих чисел).

5. Третю і шосту властивості простих чисел вперше довів Евклід (в своїх «Початках») Теорема Евквліда про нескінченно велике число простих чисел є першою задачею з теорії розподілу простих чисел у натуральному ряді.

6. Повне доведення теореми про єдиноможливість подання натурального числа $a > 1$ у вигляді добутку простих чисел вперше дав Гаусс; до нього це твердження необгрунтовано вважали очевидним. Евклід користувався цим твердженням для побудови теорії подільності.

7. Так зване «решето Ератосфена» належить старогрецькому вченому Ератосфену (276—196 до н. е.). Він вивчав також многокутні числа, збудував приклад для розв'язування задачі про подвоєння куба (мезолябій) і заклав основи математичної географії.

8. Перші таблиці факторизації (таблиці простих чисел) були опубліковані ще в XVII ст. Одна з них, складена в 1668 р. англійським математиком Пеллем (1610—1685), дає змогу робити факторизацію чисел у межах 100 000. Факторизацію чисел у межах 10 000 000 натуральних чисел було здійснено і опубліковано в першій половині XIX ст. Таблиця, опублікована в 1909 р. американським математиком Лемером (1867—1938), дає для кожного натурального числа, яке лежить у межах перших 10 000 000, найменший простий дільник. Чеський математик Кулик (1793—1863) склав таблицю для факторизації чисел у межах до 100 000 000, але ці таблиці досі не надруковані. Радянський учитель математики В. А. Голубєв (н. 1891) виконав величезну роботу по складанню таблиць простих чисел від 11 000 000 до 15 000 000.

Таблицю простих чисел, які лежать у межах перших 11 мільйонів, видано. Таблицю перших 6 мільйонів простих чисел, найбільше з яких дорівнює 104 395 301, записано в 1959 р. на мікроплівку.

9. Задача № 17 називається на честь німецького математика задачею Адама Різе (1492—1559) — автора популярних у свій час підручників з арифметики і алгебри.

10. Рівняння $x^2 + y^2 = z^2$, яке зустрічається в задачі № 32, називається рівнянням Піфагора; його розв'язання в цілих числах пов'язане з задачею відшукання всіх прямокутних трикутників, сторони яких визначаються цілими раціональними додатними числами. Розв'язання цього рівняння було відоме ще стародавнім грекам і народам Індії.

Розділ II

НАЙВАЖЛИВІШІ ЧИСЛОВІ ФУНКЦІЇ, ЩО ЗУСТРІЧАЮТЬСЯ В ТЕОРІЇ ЧИСЕЛ

Числовими функціями називають такі функції, які набувають цілих значень або визначені для цілих значень аргументу.

§ 11. Числова функція $[x]$ і її застосування

Важливу роль у теорії чисел відіграє функція $[x]$[1]; вона визначається для всіх дійсних x і є найбільшим цілим числом, що не перевищує x: $x - 1 < [x] \leqslant x$. Ця функція називається *цілою частиною* від x (або антьє від x). Зокрема $[0] = 0$, $[2] = 2$, $[3{,}7] = 3$, $[-1{,}2] = -2$, $[\sqrt{3}] = 1$, $[-\pi] = -4$ і т. д. Отже, ця функція набуває тільки цілих значень при довільних дійсних значеннях аргументу x.

Очевидно маємо:

$$[x] \leqslant x < [x] + 1,$$

або

$$x = [x] + \theta,$$

де $0 \leqslant \theta < 1$.

Число θ, визначене останньою формулою, називається *дробовою частиною* x і позначається символом $\{x\}$, так що $\{x\} = x - [x]$; зокрема $\{2\} = 0$, $\{1{,}7\} = 0{,}7$, $\{-4{,}15\} = 0{,}85$, $\{\sqrt{2}\} = \sqrt{2} - 1$ і т. д.

За означенням $\{x\}$ є завжди невід'ємним числом, меншим від одиниці, тобто $0 \leqslant \{x\} < 1$.

З означення функції $[x]$ випливають такі її основні властивості:

[1] $[x]$ — позначення Гаусса; Лежандр позначав цю функцію символом Ex.

Властивість 1. *Якщо* $x = n + \theta$, *де* n *— ціле і* $0 \leqslant \theta < 1$, то $n = [x]$.

Ця властивість випливає з нерівностей:

$$0 \leqslant x - n < 1, \text{ або } x - 1 < n \leqslant x.$$

Властивість 2. $[a + b] \geqslant [a] + [b]$.

Справді, маємо:

$$a + b = [a] + [b] + \{a\} + \{b\}.$$

Тут можливі два випадки: по-перше, $0 \leqslant \{a\} + \{b\} < 1$; тоді очевидно, що $[a + b] = [a] + [b]$; по-друге, $1 \leqslant \{a\} + \{b\} < 2$; у цьому разі матимемо $[a + b] = [a] + [b] + 1$, тобто $[a + b] > [a] + [b]$. Отже, в будь-якому випадку

$$[a + b] \geqslant [a] + [b].$$

Приклади.

а) $\left[3\frac{1}{2} + 5\frac{1}{4}\right] = \left[8\frac{3}{4}\right] = 8$; $\left[3\frac{1}{2}\right] = 3$, $\left[5\frac{1}{4}\right] = 5$ і $\left[3\frac{1}{2} + 5\frac{1}{4}\right] = \left[3\frac{1}{2}\right] + \left[5\frac{1}{4}\right]$;

б) $\left[1\frac{4}{5} + 5\frac{5}{6}\right] = \left[7\frac{19}{30}\right] = 7$, $\left[1\frac{4}{5}\right] = 1$, $\left[5\frac{5}{6}\right] = 5$ і $\left[1\frac{4}{5} + 5\frac{5}{6}\right] > \left[1\frac{4}{5}\right] + \left[5\frac{5}{6}\right]$.

Властивість 3. *Якщо* α *— дійсне, додатне число і* b *— натуральне число, то натуральних чисел, які не перевищують* α *і діляться на* b, *буде точно* $\left[\frac{\alpha}{b}\right]$.

Справді, нехай числами, кратними b, і такими, що не перевищують α, будуть k чисел: b, $2b$, $3b \ldots$, kb. Тоді буде справедлива нерівність: $kb \leqslant \alpha < (k + 1)b$, звідки $k \leqslant \frac{\alpha}{b} < k + 1$, тобто, $k = \left[\frac{\alpha}{b}\right]$.

Властивість 4. *Якщо* $\alpha > 0$ *— будь-яке дійсне число і* b *— натуральне число*, то

$$\left[\frac{[\alpha]}{b}\right] = \left[\frac{\alpha}{b}\right].$$

Справді, між $[\alpha]$ і α немає натуральних чисел і тому кількість чисел, кратних b, і таких, що не перевищують $[\alpha]$ і відповідно α, буде однаковою. За властивістю 3 в першому випадку їх буде, $\left[\frac{[\alpha]}{b}\right]$, а в другому — $\left[\frac{\alpha}{b}\right]$. Отже,

$$\left[\frac{[\alpha]}{b}\right] = \left[\frac{\alpha}{b}\right].$$

Щоб показати важливість запровадженої функції, розглянемо приклади її застосувань.

Теорема 1. *Показник, з яким дане просте число* p *входить до добутку* $n!$, *дорівнює:*

$$\left[\frac{n}{p}\right] + \left[\frac{n}{p^2}\right] + \cdots + \left[\frac{n}{p^k}\right], \text{ де } p^k \leqslant n,$$

але вже $p^{k+1} > n$. (Якщо вже $p > n$, то $n!$ зовсім не ділиться на p).

Справді, на підставі властивості 3, число співмножників добутку $n! = 1 \cdot 2 \cdot 3 \cdots n$, кратних p, дорівнюватиме $\left[\frac{n}{p}\right]$; ці співмножники будуть: p, $2p$, $\ldots$ $\left[\frac{n}{p}\right]p$. Інші числа цього добутку на p не діляться. Отже, поява числа p в канонічному розкладі $n!$ визначається добутком

$$M = p \cdot 2p \cdot 3p \cdots \left[\frac{n}{p}\right]p = p^{\left[\frac{n}{p}\right]} \cdot 1 \cdot 2 \cdot 3 \cdots \left[\frac{n}{p}\right].$$

Позначимо $\left[\frac{n}{p}\right] = n_1$, тоді $M = 1 \cdot 2 \cdot 3 \cdots n_1 \cdot p^{n_1}$. Серед множників 1, 2 $\ldots$ n_1 можуть бути числа, які діляться на p: p, $2p$, $3p$, $\ldots$, $\left[\frac{n_1}{p}\right]p$. Їх добуток дорівнює

$$1 \cdot 2 \cdot 3 \cdots \left[\frac{n_1}{p}\right] \cdot p^{\left[\frac{n_1}{p}\right]}$$

або, позначаючи через $n_2 = \left[\frac{n_1}{p}\right] = \left[\frac{n}{p} : p\right] = \left[\frac{n}{p^2}\right]$ (див. властивість 4), дістанемо:

$$M = M_1 \cdot 1 \cdot 2 \cdot 3 \cdots n_2 \cdot p^{n_1 + n_2},$$

де M_1 — добуток множників, що не діляться на p. Якщо $n_2 < p$, то процес закінчено; якщо $n_2 \geqslant p$, продовжуємо його далі.

Міркуючи аналогічно, дістанемо:

$$M = M_2 \cdot 1 \cdot 2 \cdot 3 \cdots n_3 \cdot p^{n_1 + n_2 + n_3},$$

де

$$n_3 = \left[\frac{n_2}{p}\right] = \left[\frac{n}{p^3}\right]$$

і т. д.

Очевидно, що цей процес скінченний, бо $n > n_1 > n_2 > \ldots$, і при досить великому k виявиться, що $n_k < p$ і

$$\left[\frac{n_k}{p}\right] = \left[\frac{n}{p^{k+1}}\right] = 0.$$

Отже,

$$M = M_{k-1} \cdot 1 \cdot 2 \cdot 3 \cdots n_k \cdot p^{n_1 + n_2 + n_3 + \cdots + n_k}.$$

Серед множників 1, 2, ... , n_k немає таких, що діляться на p, бо $n_k < p$; M_{k-1} також не містить множників, кратних p, отже, до канонічного розкладу $n!$ просте число p ввійде з показником, який дорівнює:

$$n_1 + n_2 + \cdots + n_k = \left[\frac{n}{p}\right] + \left[\frac{n}{p^2}\right] + \cdots + \left[\frac{n}{p^k}\right] = \sum_{s=1}^{k}\left[\frac{n}{p^s}\right]^1,$$

що й треба було довести.

На практиці обчислення краще проводити за формулою:

$$n_s = \left[\frac{n_{s-1}}{p}\right], \text{ тобто } \left[\frac{n}{p^s}\right] = \left[\left[\frac{n}{p^{s-1}}\right] : p\right].$$

Приклад. Знайти показник степеня, з яким число 3 входить до добутку 701!

Обчислення проводимо, згідно із зробленим зауваженням, за такою схемою:

$$\begin{array}{r|l} 701 & 3 \\ \hline 233 & 3 \\ \hline 77 & 3 \\ \hline 25 & 3 \\ \hline 8 & 3 \\ \hline 2 & \end{array}$$

Додаючи частки, знайдемо, що шуканий показник дорівнює $233 + 77 + 25 + 8 + 2 = 345$.

Зауваження. Ця теорема, очевидно, дає можливість знаходити канонічний розклад числа $n!$.

Приклад. Знайти канонічний розклад числа $30! = 1 \cdot 2 \cdot 3 \cdots 30$.

Очевидно, що до канонічного розкладу 30! входять тільки прості числа, менші за 30. Знайдемо, з якими показниками вони входитимуть до цього розкладу:

$$\begin{array}{r|l} 30 & 2 \\ \hline 15 & 2 \\ \hline 7 & 2 \\ \hline 3 & 2 \\ \hline 1 & \end{array} \qquad \begin{array}{r|l} 30 & 3 \\ \hline 10 & 3 \\ \hline 3 & 3 \\ \hline 1 & \end{array} \qquad \begin{array}{r|l} 30 & 5 \\ \hline 6 & 5 \\ \hline 1 & \end{array} \qquad \begin{array}{r|l} 30 & 7 \\ \hline 4 & \end{array} \qquad \begin{array}{r|l} 30 & 11 \\ \hline 2 & \end{array} \qquad \text{і т. д.}$$

Маємо: $30! = 2^{26} \cdot 3^{14} \cdot 5^7 \cdot 7^4 \cdot 11^2 \cdot 13^2 \cdot 17 \cdot 19 \cdot 23 \cdot 29$.

---

[1] Зауважимо, що $\left[\frac{n}{p^s}\right] = 0$, якщо $s > k$. Отже, замість скінченної суми $\sum_{s=1}^{k}\left[\frac{n}{p^s}\right]$ ми могли б написати нескінченну суму $\sum_{s=1}^{\infty}\left[\frac{n}{p^s}\right]$ і тоді про число k можна було б і не згадувати.

Теорема 2. *Якщо a, b, ... , l, n — натуральні числа і $n \geqslant a + b + \cdots + l$, то $\frac{n!}{a!b!\cdots l!}$ — натуральне число.*

Доведення. Візьмемо довільне просте число $p \leqslant n$. До канонічного розкладу чисел a, b, ... , l воно ввійде з показниками степенів, що відповідно дорівнюють:

$$\alpha = \left[\frac{a}{p}\right] + \left[\frac{a}{p^2}\right] + \cdots,$$
$$\beta = \left[\frac{b}{p}\right] + \left[\frac{b}{p^2}\right] + \cdots,$$
$$\cdots\cdots\cdots\cdots$$
$$\lambda = \left[\frac{l}{p}\right] + \left[\frac{l}{p^2}\right] + \cdots.$$

Отже, до канонічного розкладу знаменника число p ввійде з показником степеня

$$\mu = \alpha + \beta + \cdots + \lambda = \left[\frac{a}{p}\right] + \left[\frac{b}{p}\right] + \cdots + \left[\frac{l}{p}\right] + \left[\frac{a}{p^2}\right] + \left[\frac{b}{p^2}\right] + \cdots + \left[\frac{l}{p^2}\right] + \cdots.$$

До канонічного розкладу чисельника число p ввійде з показником степеня

$$\nu = \left[\frac{n}{p}\right] + \left[\frac{n}{p^2}\right] + \cdots.$$

Оскільки $n \geqslant a + b + \cdots + l$, то

$$\frac{n}{p} \geqslant \frac{a}{p} + \frac{b}{p} + \cdots + \frac{l}{p},$$
$$\frac{n}{p^2} \geqslant \frac{a}{p^2} + \frac{b}{p^2} + \cdots + \frac{l}{p^2},$$
$$\cdots\cdots\cdots\cdots$$

З останніх нерівностей дістанемо (властивість 2):

$$\left[\frac{n}{p}\right] \geqslant \left[\frac{a}{p} + \frac{b}{p} + \cdots + \frac{l}{p}\right] \geqslant \left[\frac{a}{p}\right] + \left[\frac{b}{p}\right] + \cdots + \left[\frac{l}{p}\right];$$
$$\left[\frac{n}{p^2}\right] \geqslant \left[\frac{a}{p^2} + \frac{b}{p^2} + \cdots + \frac{l}{p^2}\right] \geqslant \left[\frac{a}{p^2}\right] + \left[\frac{b}{p^2}\right] + \cdots + \left[\frac{l}{p^2}\right];$$
$$\cdots\cdots\cdots\cdots \qquad \cdots\cdots\cdots\cdots$$

Додаючи останні нерівності, бачимо, що $\nu \geqslant \mu$. Отже, після скорочення дробу $\frac{n!}{a!b!\cdots l!}$ на p^μ канонічний розклад знаменника не міститиме p^μ. Але p — довільне просте число, що не перевищує n, тому канонічний розклад знаменника не міститиме простих

чисел і знаменник дорівнюватиме 1; отже, розглядуваний дріб є натуральне число, що й треба було довести.

Приклад. Якщо $m < n$, то

$$\frac{n(n-1)\cdot\cdot(n-m+1)}{1\ 2\ 3\cdots m} = C_n^m$$

є натуральне число.

Справді, помножуючи чисельник і знаменник на $(n-m)!$, дістанемо $C_n^m = \frac{n!}{m!(n-m)!}$; оскільки $n = m + (n-m)$, то внаслідок доведеної теореми C_n^m є натуральним числом. Цим ми довели, не вдаючись до теорії сполук, що біноміальні коефіцієнти є натуральними числами.

Контрольні запитання

1. Дайте означення функції $[x]$.
2. Що називається дробовою частиною x? Яких значень може набувати дробова частина?
3. Побудуйте графіки функції $[x]$ і $\{x\}$.
4. Сформулюйте основні властивості функції $[x]$.
5. Перевірте на числових прикладах властивості 2, 3, 4 функції $[x]$.
6. З яким показником просте число p входить у добуток $n!$

§ 12. Формули для числа дільників і суми дільників даного числа

Особливо важливу роль у теорії чисел відіграють так звані мультиплікативні функції.

Функція $\theta(n)$ називається *мультиплікативною*, якщо: а) вона визначена для всіх натуральних n і не перетворюється в нуль хоч при одному такому значенні n; б) для довільних натуральних взаємно простих n_1 і n_2 справедлива рівність:

$$\theta(n_1 \cdot n_2) = \theta(n_1) \cdot \theta(n_2)\ ^1.$$

Приклад. Функція $\theta(n) = n^s$, де s — будь-яке дійсне або комплексне число, є мультиплікативною. Справді, навіть при довільних n_1 і n_2 маємо:

$$\theta(n_1 \cdot n_2) = (n_1 n_2)^s = n_1^s n_2^s = \theta(n_1) \cdot \theta(n_2).$$

З означення мультиплікативної функції, зокрема, випливають такі її властивості:

[1] Якщо ця рівність виконується для довільних натуральних n_1 і n_2, то кажуть також, що функція $\theta(n)$ цілком мультиплікативна або мультиплікативна в широкому розумінні; ясно, що функція, мультиплікативна в широкому розумінні, тим більше буде мультиплікативною за нашим означенням (або, як іноді говорять, мультиплікативною у вузькому розумінні).

Властивість 1. $\theta(1) = 1$.

Справді, якщо $\theta(n_0) \neq 0$, тоді

$$\theta(n_0) = \theta(n_0 \cdot 1) = \theta(n_0)\theta(1).$$

Отже, $\theta(1) = 1$.

Властивість 2. *Якщо* $\theta_1(n)$ і $\theta_2(n)$ — *мультиплікативні функції, то і їх добуток також буде мультиплікативною функцією.*

Справді, позначаючи $\theta_0(n) = \theta_1(n) \cdot \theta_2(n)$, знаходимо:

$$\theta_0(1) = \theta_1(1) \cdot \theta_2(1) = 1;$$

далі, при $(n_1, n_2) = 1$ знаходимо:

$$\theta_0(n_1 n_2) = \theta_1(n_1 n_2) \cdot \theta_2(n_1 n_2) = \theta_1(n_1)\theta_1(n_2)\theta_2(n_1)\theta_2(n_2) =$$
$$= [\theta_1(n_1)\theta_2(n_1)]\,[\theta_1(n_2)\theta_2(n_2)] = \theta_0(n_1) \cdot \theta_0(n_2),$$

що й доводить наше твердження.

Властивість 3. *Якщо* $\theta(n)$ — *мультиплікативна функція, а* $n_1, n_2, \ldots, n_s$ — попарно взаємно прості числа, то

$$\theta(n_1, n_2 \ldots n_s) = \theta(n_1)\theta(n_2) \ldots \theta(n_s).$$

Справді, для $s = 1, 2$ твердження справедливе; припустимо що воно справедливе для $s-1$ і доведемо його справедливість для s. Оскільки $(n_i, n_j) = 1$ при всіх $i \neq j$ за умовою, то $(n_1 n_2 \ldots n_{s-1}, n_s) = 1$. За означенням мультиплікативної функції дістанемо: $\theta(n_1 n_2 \ldots n_{s-1}, n_s) = \theta(n_1 n_2 \ldots n_{s-1})\theta(n_s)$; але за припущенням $\theta(n_1 n_2 \ldots n_{s-1}) = \theta(n_1)\theta(n_2) \ldots \theta(n_{s-1})$, і справедливість цієї властивості стає очевидною.

Властивість 4. Нехай $\theta(n)$ — мультиплікативна функція і $n = p_1^{\alpha_1} p_2^{\alpha_2} \ldots p_k^{\alpha_k}$ — канонічний розклад числа n. Позначимо символом $\sum_{d/n}$ суму, поширену на всі натуральні дільники d числа n (включаючи 1 і саме n). При цих позначеннях справедлива така важлива тотожність, яка виражає *основну властивість мультиплікативних функцій:*

$$\sum_{d/n} \theta(d) = [1 + \theta(p_1) + \cdots + \theta(p_1^{\alpha_1})] \cdots [1 + \theta(p_k) + \cdots + \theta(p_k^{\alpha_k})] \qquad (1)$$

(у випадку $n = 1$ вважаємо, що права частина дорівнює 1).

Для доведення цієї тотожності розкриємо дужки в її правій частині. Дістанемо суму доданків виду $\theta(p^{\beta_1}) \cdot \theta(p_2^{\beta_2}) \cdots \theta(p_k^{\beta_k})$, де $0 \leqslant \beta_i \leqslant \alpha_i$ $(i = 1, 2, \ldots, k)$, або, внаслідок мультиплікативності цієї функції, $\theta(p_1^{\beta_1} p_2^{\beta_2} \cdots p_k^{\beta_k}) = \theta(d)$, бо $p_1^{\beta_1} p_2^{\beta_2} \cdots p_k^{\beta_k}$ є не що інше, як дільники d числа n (див. висновок 1, § 10). З правила множення многочлена на многочлен випливає, що жоден та-

кий доданок не буде пропущений і не повториться більше, ніж один раз. Тобто, матимемо вираз, що стоїть в лівій частині тотожності (1).

При $\theta(n) = n^s$ тотожність (1) набере вигляду:

$$\sum_{d/n} d^s = (1 + p_1^s + p_1^{2s} + \cdots + p_1^{\alpha_1 s}) \cdots (1 + p_k^s + p_k^{2s} + \cdots + p_k^{\alpha_k s})^1. \quad (2)$$

Зокрема, при $s = 1$ ліва частина тотожності (2) дасть *суму всіх натуральних дільників числа* n; позначаючи її через $S(n)$, матимемо:

$$S(n) = \sum_{d/n} d = (1 + p_1 + p_1^2 + \cdots + p_1^{\alpha_1}) \cdots (1 + p_k + p_k^2 + \cdots + p_k^{\alpha_k}). \quad (2')$$

Спрощуючи праву частину, дістанемо:

$$S(n) = \frac{p_1^{\alpha_1+1} - 1}{p_1 - 1} \cdot \frac{p_2^{\alpha_2+1} - 1}{p_2 - 1} \cdots \frac{p_k^{\alpha_k+1} - 1}{p_k - 1}. \quad (3)$$

Вважаючи в тотожності (2) $s = 0$, бачимо, що її ліва частина при цьому визначає *число всіх натуральних дільників даного* n: позначаючи його через $\tau(n)$, дістанемо:

$$\tau(n) = (\alpha_1 + 1)(\alpha_2 + 1) \cdots (\alpha_k + 1). \quad (4)$$

Зауважимо, що, розкривши дужки в правій частині тотожності (2'), ми матимемо всі дільники числа n.

Приклад. Знайти суму дільників, число дільників і самі дільники числа $680 = 2^3 \cdot 5 \cdot 17$.

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

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

Самі дільники числа 680 знайдемо, розкриваючи дужки у виразі

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

Матимемо:

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

Функції $\tau(n)$ і $S(n)$ — мультиплікативні.

[1] Ця тотожність, між іншим, виражає суму s-х степенів усіх натуральних дільників числа n.

Справді, якщо $(a, b) = 1$ і $a = p_1^{\alpha_1} p_2^{\alpha_2} \cdots p_s^{\alpha_s}$, і $b = q_1^{\beta_1}, q_2^{\beta_2} \cdots q_t^{\beta_t}$ — канонічні розклади чисел a і b, то $p_1^{\alpha_1} p_2^{\alpha_2} \cdots p_s^{\alpha_s} q_1^{\beta_1} q_2^{\beta_2} \cdots q_t^{\beta_t}$ — канонічний розклад числа ab і тоді дістанемо:

$$S(ab) = \frac{p_1^{\alpha_1+1} - 1}{p_1 - 1} \cdots \frac{p_s^{\alpha_s} - 1}{p_s - 1} \cdot \frac{q_1^{\beta_1+1} - 1}{q_1 - 1} \cdots \frac{q_t^{\beta_t+1} - 1}{q_t - 1} = S(a) S(b);$$

$$\tau(ab) = (\alpha_1 + 1) \cdots (\alpha_s + 1)(\beta_1 + 1) \cdots (\beta_t + 1) = \tau(a) \tau(b).$$

Функції $S(n)$ і $\tau(n)$ є найпростішими прикладами мультиплікативних числових функцій; у них і аргумент, і значення функцій набувають тільки цілих додатних значень.

Контрольні запитання

1. Яка числова функція називається мультиплікативною?
2. Чи є функція $[x]$ мультиплікативною?
3. Напишіть основну числову тотожність для мультиплікативних функцій.
4. За якими формулами обчислюють кількість дільників і суму дільників даного числа?

§ 13. Функція Ейлера і її основні властивості

Функція Ейлера[1] $\varphi(n)$ визначається для всіх натуральних n і *являє собою кількість натуральних чисел, менших від* n *і взаємно простих з* n; при цьому припускається, що $\varphi(1) = 1$.

Для невеликих значень n значення функції $\varphi(n)$ можна знайти простим підрахунком кількості чисел, менших від n і взаємно простих з n, наприклад, $\varphi(2) = 1$, $\varphi(3) = 2$, $\varphi(4) = 2$, $\varphi(5) = 4$, $\varphi(6) = 2$, $\varphi(7) = 6$, $\varphi(8) = 4$, $\varphi(9) = 6$ і т. д.

Визначимо значення $\varphi(n)$ для будь-якого натурального n.

Спочатку доведемо такі твердження.

Теорема 1. *Функція Ейлера мультиплікативна, тобто* $\varphi(m \cdot n) = \varphi(m) \cdot \varphi(n)$, якщо $(m, n) = 1$. Щоб довести цю теорему, розмістимо числа від 1 до mn у вигляді такої таблиці:

$$\begin{array}{llll} 1, & 2, \ldots, & r, \ldots, & m; \\ m+1, & m+2, \ldots, & m+r, \ldots, & 2m; \\ 2m+1, & 2m+2, \ldots, & 2m+r, \ldots, & 3m; \\ \ldots & \ldots & \ldots & \ldots \\ (n-1)m+1, & (n-1)m+2, & (n-1)m+r & (n-1)m+m = mn. \end{array} \quad (1)$$

Визначимо тепер з таблиці (1) кількість чисел, взаємно простих з mn. Взаємно простими з добутком mn будуть ті і тільки ті числа, які взаємно прості як з m, так і з n. Тому відберемо

[1] В алгебрі функція Ейлера $\varphi(n)$ виражає число первісних коренів n-го степеня з одиниці.

з таблиці (1) спочатку всі числа, взаємно прості з m, а з них ті, які взаємно прості з n.

Числа одного стовпця або одночасно взаємно прості з m, або ні, бо $(r, m) = (m, km + r)$ (за теоремою 2, § 2). Отже, можна говорити про «стовпці, взаємно простих з m» і визначати їх число за кількістю чисел, взаємно простих з m одного рядка, наприклад першого; тому кількість таких стовпців за означенням дорівнює $\varphi(m)$.

Розглянемо тепер будь-який стовпець таблиці (1), наприклад:

$$r,\ m + r,\ 2m + r,\ \ldots,\ (n-1)m + r. \tag{2}$$

Усього в цьому стовпці n чисел; покажемо що всі вони при діленні на n даватимуть різні остачі. Справді, припустимо супротивне, тобто:

$$k_1 m + r = nq_1 + s \text{ і } k_2 m + r = nq_2 + s,$$

де k_1, k_2 і s — цілі невід'ємні, менші від n. Тоді, віднімаючи від першої рівності другу, дістанемо: $(k_1 - k_2)m = n(q_1 - q_2)$. Остання рівність показує, що $(k_1 - k_2)m \vdots n$, але $(m, n) = 1$ за умовою, отже $(k_1 - k_2) \vdots n$, але це неможливо, бо k_1 і k_2 різні і $|k_1 - k_2| < n$. Маємо, що від ділення чисел ряду (2) на n діставатимемо остачі $s = 0, 1, 2, 3, \ldots, n-1$; позначаючи через $y = km + r = nq + s$ на підставі теореми 2, § 2 дістанемо, що спільні дільники чисел y і n збігаються з спільними дільниками чисел n і s і, зокрема, $(y, n) = (s, n)$. Отже, в ряді чисел (2) буде стільки взаємно простих з n, скільки їх буде в ряді $0, 1, 2, \ldots, n-1$, тобто $\varphi(n)$. Отже, в таблиці (1) є $\varphi(m) \cdot \varphi(n)$ чисел, взаємно простих як з m, так і з n, а, отже, і з mn. З другого боку, таблиця (1) має всі числа від 1 до mn, і, отже, в ній $\varphi(m \cdot n)$ чисел, взаємно простих з mn, і ми дістанемо, що $\varphi(m \cdot n) = \varphi(m) \times \varphi(n)$ і теорему доведено.

Теорема 2. *Нехай p — просте число і $\alpha \geqslant 1$ — будь-яке натуральне число, тоді*

$$\varphi(p^\alpha) = p^{\alpha-1}(p-1) = p^\alpha\left(1 - \frac{1}{p}\right). \tag{3}$$

Справді, розглянемо ряд чисел від 1 до p^α. Запишемо його в такому вигляді:

$$1, 2, \ldots, p, \ldots, 2p, \ldots, 3p, \ldots, p \cdot p = p^2, \ldots p^{\alpha-1}p = p^\alpha.$$

Зрозуміло що цей ряд має $p^{\alpha-1}$ чисел, які діляться на p і, отже, не є взаємно простими з p^α; інші числа цього ряду не діляться на p, отже, вони будуть взаємно прості як з p, так і з p^α. Отже,

$$\varphi(p^\alpha) = p^\alpha - p^{\alpha-1} = p^{\alpha-1}(p-1) = p^\alpha\left(1 - \frac{1}{p}\right).$$

Зокрема,

$$\varphi(p) = p - 1 \tag{4}$$

Теорема 3. *Якщо $n > 1$ і $n = p_1^{\alpha_1} p_2^{\alpha_2} \cdots p_k^{\alpha_k}$ — канонічний розклад числа n,* то

$$\varphi(n) = n\left(1 - \frac{1}{p_1}\right)\left(1 - \frac{1}{p_2}\right)\cdots\left(1 - \frac{1}{p_k}\right). \tag{5}$$

Справді, внаслідок мультиплікативності, матимемо:

$$\varphi(n) = \varphi(p_1^{\alpha_1} p_2^{\alpha_2} \cdots p_k^{\alpha_k}) = \varphi(p_1^{\alpha_1})\varphi(p_2^{\alpha_2}) \cdots \varphi(p_k^{\alpha_k}) =$$
$$= p_1^{\alpha_1}\left(1 - \frac{1}{p_1}\right) p_2^{\alpha_2}\left(1 - \frac{1}{p_2}\right) \cdots p_k^{\alpha_k}\left(1 - \frac{1}{p_k}\right) =$$
$$= n\left(1 - \frac{1}{p_1}\right)\left(1 - \frac{1}{p_2}\right)\cdots\left(1 - \frac{1}{p_k}\right).$$

Формулу (4) можна переписати так:

$$\varphi(n) = p_1^{\alpha_1 - 1}(p_1 - 1) p_2^{\alpha_2 - 1}(p_2 - 1) \cdots p_k^{\alpha_k - 1}(p_k - 1). \tag{6}$$

На практиці зручніше користуватися формулою (5).

Приклад. Знайти кількість чисел, менших за 1620 і взаємно простих з цим числом, тобто знайти $\varphi(1620)$. Маємо:

$$1620 = 2^2 \cdot 3^4 \cdot 5;\ \varphi(1620) = 1620\left(1 - \frac{1}{2}\right)\left(1 - \frac{1}{3}\right)\left(1 - \frac{1}{5}\right) =$$
$$= 432.$$

Теорема 4. *Сума значень $\varphi(d)$, яка поширюється на всі натуральні дільники d числа n, дорівнює самому числу n, тобто*

$$\sum_{d/n} \varphi(d) = n. \tag{7}$$

Справді, припустимо, що $n = p_1^{\alpha_1} p_2^{\alpha_2} \cdots p_k^{\alpha_k}$ — канонічний розклад числа n. Через те що функція Ейлера є мультиплікативною, то на підставі тотожності (1), § 12 і формул (3) і (4) матимемо:

$$\sum_{d/n} \varphi(d) = [1 + \varphi(p_1) + \varphi(p_1^2) + \cdots + \varphi(p_1^{\alpha_1})] \cdots [1 + \varphi(p_k) +$$
$$+ \varphi(p_k^2) + \cdots + \varphi(p_k^{\alpha_k})] = [1 + (p_1 - 1) + p_1(p_1 - 1) +$$
$$+ \cdots + p_1^{\alpha_1 - 1}(p_1 - 1)] \cdots [1 + (p_k - 1) + p_k(p_k - 1) +$$
$$+ \cdots + p_k^{\alpha_k - 1}(p_k - 1)] = p_1^{\alpha_1} p_2^{\alpha_2} \cdots p_k^{\alpha_k} = n.$$

Приклад. Перевірити тотожність (7) для $n = 30$.
Дільники d числа 30 будуть: 1, 2, 3, 5, 6, 10, 15, 30;

$$\sum_{d/30} \varphi(d) = \varphi(1) + \varphi(2) + \varphi(3) + \varphi(5) + \varphi(6) + \varphi(10) +$$
$$+ \varphi(15) + \varphi(30) = 1 + 1 + 2 + 4 + 2 + 4 + 8 + 8 = 30.$$

Контрольні запитання

1. Що означає функція Ейлера $\varphi(n)$?
2. Чому $\varphi(1) = 1$?
3. За якою формулою обчислюють функцію Ейлера?
4. Користуючись теоремою 3, знайти: $\varphi(35)$, $\varphi(77)$, $\varphi(88)$?
5. Чому дорівнює сума значень функції Ейлера по всіх дільниках даного числа?

§ 14. Функція Мебіуса

Функцією Мебіуса називається така числова функція $\mu(n)$, яка визначена для всіх натуральних n і характеризується такими умовами: 1) $\mu(1) = 1$, 2) $\mu(n) = 0$, якщо n ділиться на квадрат простого числа; 3) $\mu(n) = (-1)^k$, якщо n не ділиться на квадрат числа, відмінного від одиниці; при цьому k позначає число простих дільників n. Наприклад,

$$\mu(2) = -1,\ \mu(3) = -1,\ \mu(4) = 0,\ \mu(5) = -1,\ \mu(6) = 1,$$
$$\mu(63) = 0 \text{ і т. д.}$$

Отже, функція $\mu(n)$ набуває лише значення 0,1 і -1. Неважко переконатися, що функція Мебіуса є також мультиплікативною функцією, тобто для будь-яких натуральних взаємно простих n_1 і n_2 маємо:

$$\mu(n_1 n_2) = \mu(n_1)\,\mu(n_2).$$

Справді, якщо хоч би одне з чисел n_1 або n_2 ділиться на квадрат простого числа, то очевидно $\mu(n_1 n_2) = 0$; $\mu(n_1)\,\mu(n_2) = 0$, тобто

$$\mu(n_1 n_2) = \mu(n_1)\,\mu(n_2);$$

припустимо тепер, що

$$n_1 = p_1 p_2 \cdots p_s,\ n_2 = q_1 q_2 \cdots q_t,$$

де $p_1, p_2, \ldots, p_s$; $q_1, q_2, \ldots, q_t$ — різні прості числа, тоді

$$\mu(n_1) = (-1)^s,\ \mu(n_2) = (-1)^t$$

$$\mu(n_1 n_2) = (-1)^{s+t} = \mu(n_1)\,\mu(n_2).$$

Теорема 1. *Якщо* $\theta(n)$ *мультиплікативна функція і* $n = p_1^{\alpha_1} p_2^{\alpha_2} \cdots p_k^{\alpha_k}$ *— канонічний розклад числа* n, *то справедлива рівність:*

$$\sum_{d/n} \mu(d) \cdot \theta(d) = [1 - \theta(p_1)]\,[1 - \theta(p_2)] \cdots [1 - \theta(p_k)] \qquad (1)$$

(для випадку $n = 1$ вважаємо, що права частина дорівнює 1).

Справді, якщо $\mu(n)$ — мультиплікативна функція, то й $\theta(n) = \mu(n) \cdot \theta(n)$ буде мультиплікативною (див. властивість 2, § 12). Застосовуючи до функції $\theta_1(n)$ тотожність (1), § 12 і маючи на увазі, що $\theta_1(p_i) = \theta(p_i)$ і $\theta_1(p_i^s) = 0$ при $s > 1$ (бо $\mu(p_i) = -1$ і $\mu(p_i^s) = 0$ за означенням), переконаємося в справедливості теореми.

Висновок 1.

$$\sum_{d/n} \mu(d) = \begin{cases} 0, & \text{якщо } n > 1; \\ 1, & \text{якщо } n = 1. \end{cases} \qquad (2)$$

Твердження одразу випливає з рівності (1) при $\theta(n) = 1$.

Висновок 2.

$$\sum_{d/n} \frac{\mu(d)}{d} = \begin{cases} \left(1 - \frac{1}{p_1}\right)\left(1 - \frac{1}{p_2}\right) \cdots \left(1 - \frac{1}{p_n}\right), & \text{якщо } n > 1; \\ 1, & \text{якщо } n = 1 \end{cases} \qquad (3)$$

Це твердження також безпосередньо випливає з рівності (1) при $\theta(d) = \frac{1}{d}$ (бо $\theta(d) = d^s$ при будь-якому S і, зокрема, при $s = -1$ є мультиплікативною функцією).

Теорема 2. (Принцип обернення Дедекінда-Ліувілля). *Якщо* $\Phi(n)$ *— однозначна функція, визначена для всіх натуральних* n *і*

$$F(n) = \sum \Phi(d), \qquad (4)$$

то

$$\Phi(n) = \sum_{d/n} \mu(d) \cdot F\left(\frac{n}{d}\right). \qquad (5)$$

Доведення. Припустимо, що d — будь-який дільник числа n; напишемо формулу (4) для числа $\frac{n}{d}$:

$$F\left(\frac{n}{d}\right) = \sum_{\delta / \frac{n}{d}} \Phi(\delta).$$

Помножимо обидві частини цієї рівності на $\mu(d)$ і підсумуємо за всіма дільниками d числа n; тоді дістанемо:

$$\sum_{d/n} \mu(d) F\left(\frac{n}{d}\right) = \sum_{d/n} \sum_{\delta \left/ \frac{n}{d}\right.} \mu(d) \Phi(\delta).$$

Тут d і δ такі дільники числа n, що $\frac{n}{d\delta}$ — ціле число, тобто d можна вважати дільником числа $\frac{n}{\delta}$. Змінюючи порядок підсумовування в правій частині останньої рівності, матимемо:

$$\sum_{\delta \left/ \frac{n}{d}\right.} \sum_{d/n} \mu(d) \Phi(\delta) = \sum_{\delta \left/ \frac{n}{d}\right.} [\Phi(\delta) \sum_{d/n} \mu(d)].$$

Але, згідно з висновком 1, $\sum \mu(d) = 0$, крім випадку, коли $d = \frac{n}{\delta} = 1$, тобто коли $\delta = n$. Тоді $\sum \mu(d) = 1$. Отже, в правій частині останньої рівності тільки один доданок зовнішньої суми не дорівнює нулю, а саме, коли $\delta = n$ він дорівнюватиме $\Phi(n)$. Звідси

$$\sum_{d/n} \mu(d) F\left(\frac{n}{d}\right) = \Phi(n).$$

Формулу (5) називають «*формулою оберненця*» *Дедекінда-Ліувілля*. Її записують так: $F(n) = \int \Phi(n)$, $\Phi(n) = \int F(n)$ і $F(n)$ називають *числовим інтегралом* від $\Phi(n)$, взятим по дільниках, а $\Phi(n)$ називають *числовою похідною від* $F(n)$.

Приклад 1. Якщо $\Phi(n) = n$, то $F(n) = S(n)$. Це безпосередньо випливає з означення функції $S(n)$ і з рівності (4); аналогічно, якщо $\Phi(n) = 1$, то $F(n) = \tau(n)$.

Приклад 2. Якщо $F(n) = n = p_1^{\alpha_1} \dots p_n^{\alpha_n} > 1$, то за формулою (5) дістаємо, що

$$\Phi(n) = \sum_{d/n} \mu(d) \frac{n}{d} = n \sum_{d/n} \frac{\mu(d)}{d}.$$

Але $\sum_{d/n} \varphi(d) = n$ за теоремою 4, § 14 отже, $\varphi(n) = \Phi(n)$, бо

$$F(n) = n = \sum_{d/n} \Phi(d).$$

Використавши формулу (3) висновку 2, знайдемо, що

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

Отже, ми іншим способом знайшли значення функції Ейлера.

Важливе значення в теорії чисел має числова функція $\pi(x)$, яка позначає число простих чисел, що не перевищують дійсного числа x, наприклад, $\pi(1) = 0$, $\pi(2) = 1$, $\pi(3) = 2$, $\pi(\sqrt{7}) = 1$, $\pi\left(12\frac{1}{2}\right) = 5$ і т. д. Тут аргумент набуває довільних невід'ємних дійсних значень, а функція — лише цілих невід'ємних (див. § 47).

Контрольні запитання

1. Дайте означення функції Мебіуса.
2. Чи є функція Мебіуса мультиплікативною?
3. Як пов'язані між собою функція Мебіуса $\mu(d)$ і довільна мультиплікативна функція $Q(d)$; де d — дільник деякого натурального числа n?
4. Чому дорівнюють значення $\sum_{d/n} \mu(d)$ і $\sum_{d/n} \frac{\mu(d)}{d}$?
5. Сформулюйте принцип обернення Дедекінда-Ліувілля.
6. Застосуйте принцип обернення Дедекінда-Ліувілля до знаходження значень $S(n)$, $\tau(n)$ і $\varphi(n)$.

Вправи

1. Розв'язати рівняння $[2ax] = m$, де $a \neq 0$ і x — дійсні числа.

Відповідь. $x = \frac{m + \theta}{2a}$, де θ — дійсне число, що задовольняє умову $0 \leqslant \theta < 1$.

2. Знайти, при якому цілому додатному m справджуються співвідношення: а) $[32{,}6\ m] = 97$; б) $[27{,}4\ m] = 140$.

Відповідь. а) $m = 3$; б) такого m немає.

3. Довести, що $[x] + \left[x + \frac{1}{2}\right] = [2x]$ для будь-якого дійсного x.

4. Довести, що

$$[x] + \left[x + \frac{1}{n}\right] + \dots + \left[x + \frac{n-1}{n}\right] = [nx]$$

для будь-якого дійсного x і цілого $n \geqslant 2$.

5. Знайти показник, з яким просте число 7 входить до добутку 81 561!.

Відповідь. Шуканий показник дорівнює 13 589.

6. Знайти канонічний розклад чисел: а) 40!; б) 50!; в) 60!; г) 75!.

Відповідь. а) $40! = 2^{38} \cdot 3^{18} \cdot 5^9 \cdot 7^5 \cdot 11^3 \cdot 13^3 \cdot 17^2 \cdot 19^2 \cdot 23 \cdot 29 \cdot 31 \cdot 37$;

б) $50! = 2^{47} \cdot 3^{22} \cdot 5^{12} \cdot 7^8 \cdot 11^4 \cdot 13^3 \cdot 17^2 \cdot 19^2 \cdot 23^2 \cdot 29 \cdot 31 \cdot 37 \cdot 41 \cdot 43 \cdot 47$;

в) $60! = 2^{56} \cdot 3^{28} \cdot 5^{14} \cdot 7^9 \cdot 11^5 \cdot 13^4 \cdot 17^3 \cdot 19^3 \cdot 23^2 \cdot 29^2 \cdot 31 \cdot 37 \cdot 41 \cdot 43 \times$
$\times 47 \cdot 53 \cdot 59$;

г) $75! = 2^{71} \cdot 3^{35} \cdot 5^{18} \cdot 7^{11} \cdot 11^6 \cdot 13^5 \cdot 17^4 \cdot 19^3 \cdot 23^3 \cdot 29^2 \cdot 31^2 \cdot 37^2 \cdot 41 \times$
$\times 43 \cdot 47 \cdot 53 \cdot 59 \cdot 61 \cdot 67 \cdot 71 \cdot 73$.

7. Знайти число дільників числа n, якщо: а) $n = 4520$; б) $n = 27\,504$; в) $n = 116\,424$; г) $n = 1\,002\,001$; д) $n = 1\,294\,700$.

Відповідь: а) 16; б) 30; в) 96; г) 27; д) 54.

8. Знайти суму дільників для чисел попередньої задачі.

Відповідь: а) 10 260; б) 77 376; в) 410 400; г) 1 387 323; д) 3 116 988.

9. Знайти всі натуральні дільники числа 4520.

Відповідь. 1, 2, 4, 5, 8, 10, 20, 40, 113, 226, 452, 565, 904, 1130, 2260, 4520.

10. Знайти найменше натуральне число, що має 15 дільників.

Відповідь. 144.

11. Усі натуральні дільники цілого числа $n > 1$, крім самого n, називаються *правильними*, або *властивими*, *дільниками*. Очевидно, що сума всіх правильних дільників числа n визначиться різницею: $\sigma(n) = S(n) - n$. Це число $n > 1$ називають *досконалим*, якщо сума його правильних дільників дорівнює n, тобто якщо $\sigma(n) = n$. Звідси випливає, що для досконалого числа n $S(n) = 2n$.

Якщо $S(n) < 2n$, то число n називають *недостатнім*, а якщо $S(n) > 2n$, то *надлишковим*.

Довести такі твердження; а) якщо n має вигляд $n = 2^k(2^{k+1} - 1) = 2^k p$, де $p = 2^{k+1} - 1$ — просте, то n — досконале число; б) числа n, що мають зазначений у попередній задачі вигляд, є єдиними досконалими числами;

в) число $p = 2^{k+1} - 1$ може бути простим тоді і тільки тоді, коли показник $(k+1)$ — число просте.

12. Нехай x деяке дійсне додатне число, $p_1, p_2, \ldots p_k$ — різні прості числа. Позначимо через $B(x, p_1, p_2, \ldots p_k)$ — кількість цілих додатних чисел, які не перевищують x і не діляться на жодне з простих чисел $p_1, p_2, \ldots p_k$. Довести, що справджується така формула:

$$B(x; p_1, p_2, \ldots p_k) = [x] - \left[\frac{x}{p_1}\right] - \cdots - \left[\frac{x}{p_k}\right] + \left[\frac{x}{p_1 p_2}\right] + \cdots + \left[\frac{x}{p_{k-1} p_k}\right] - \left[\frac{x}{p_1 p_2 p_3}\right] - \cdots - \left[\frac{x}{p_{k-2} p_{k-1} p_k}\right] + \cdots + (-1)^k \left[\frac{x}{p_1 p_2 \ldots p_k}\right]. \quad (1)$$

У третьому рядку правої частини рівності (1) фігурують найрізноманітніші комбінації по два з k чисел $p_1, p_2 \ldots p_k$; у четвертому рядку цієї рівності — найрізноманітніші комбінації по три з тих самих k чисел і т. д.

13. Користуючись формулою (1) попередньої задачі, знайти вираз функції Ейлера $\varphi(n)$, де $n = p_1^{\alpha_1} p_2^{\alpha_2} \ldots p_k^{\alpha_k}$ — канонічний розклад числа n.

14. Знайти число натуральних чисел, які не перевищують 1327 і не діляться на жодне з простих чисел 5, 7, 13.

Відповідь. 840.

15. Знайти число натуральних чисел, які не перевищують 2429 і взаємно прості з 568.

Відповідь. 1198.

16. Довести, що коли $x \geqslant 2$ і $p_1, p_2, \ldots p_k$ є k послідовних простих чисел, які не перевищують $\sqrt{x}$, то

$$\pi(x) = B(x; p_1, p_2 \ldots p_k) + k - 1,$$

де $\pi(x)$ — число простих чисел, які не перевищують x.

17. Користуючись результатом попередньої задачі, знайти $\pi(200)$.

Відповідь. $\pi(200) = 46$.

18. Припустимо, що $x > 0$ — дійсне число і $a_1, a_2, \ldots, a_k$ — попарно взаємно прості натуральні числа. Позначимо через $B(x; a_1, a_2, \ldots a_k)$ число натуральних чисел, які не перевищують x і не діляться на жодне з чисел $a_1, a_2 \ldots, a_k$. Довести, що для $B(x; a_1, \ldots, a_k)$ справедлива формула, аналогічна формулі (1) задачі 12.

19. Довести, що коли x — натуральне число, яке ділиться на $a_1, a_2, \ldots, a_k$, де $a_1, a_2, \ldots, a_k$ — натуральні попарно взаємно прості числа, то

$$B(x; a_1, a_2, \ldots, a_k) = x\left(1 - \frac{1}{a_1}\right)\left(1 - \frac{1}{a_2}\right)\left(1 - \frac{1}{a_3}\right) \ldots \left(1 - \frac{1}{a_k}\right).$$

20. Користуючись результатом попередньої задачі, знайти число натуральних чисел, які не перевищують 82 798 848 і взаємно прості з 3168.

Відповідь. 25 090 560.

21. В ряді натуральних чисел 1, 2, ..., 2700, починаючи з 1, викреслюється кожне четверте, кожне п'яте і кожне дев'яте число (включаючи й викреслені). Скільки чисел залишиться?

Відповідь. $B(2700; 4; 5, 9) = 1440$.

22. Знайти число натуральних чисел, менших від n і взаємно простих з n, якщо: а) $n = 3560$; б) $n = 4520$; в) $n = 116\,424$; г) $n = 1\,002\,001$; д) $n = 1\,294\,700$.

Відповідь. а) 1 408; б) 1792; в) 30 240; г) 720 720; д) 466 400.

23. Довести, що коли а) $n = mp$, де $(m, p) = p$ і p — просте число, то $\varphi(n) = \varphi(mp) = \varphi(m)\, p$; б) $n = mq$, де $(m, q) = 1$ і q — просте число, то $\varphi(n) = \varphi(mq) = \varphi(m)(q - 1)$.

24. Користуючись результатами попередньої задачі, вивести рекурентну формулу:

$$\varphi(mp^k) = \varphi(m)\, p^{k-1}(p - 1); \quad (m, p) = 1.$$

25. На підставі формули, виведеної в задачі 21, знайти вираз для функції Ейлера:

$$\varphi(n) = n \cdot \prod_p \left(1 - \frac{1}{p}\right),$$

де p набуває всіх значень простих дільників числа n.

26. Довести, що $\varphi(4n) = 2\varphi(2n)$ і $\varphi(4n + 2) = \varphi(2n + 1)$.

27. Дано, що $\varphi(11^n) = 13\,310$. Знайти n.

Відповідь. $n = 4$.

28. Дано, що $\varphi(n) = 1792$ і $n = 2^\alpha \cdot 5^\beta \cdot 113^\gamma$. Знайти n.

Відповідь. $n = 2^3 \cdot 5 \cdot 113 = 4520$.

29. Визначити n при умові, що $\varphi(n) = 80$.

Відповідь. $n = 200$.

30. Знайти натуральне число x з умови:

а) $\varphi(2x) = \varphi(3x)$; б) $\varphi(5x) = \varphi(7x)$.

Відповідь а) $x = 2^\alpha \cdot y$, де $\alpha > 0$ і y — натуральне число, що не ділиться на 2 і на 3; б) такого x немає.

31. При якому натуральному n справедлива рівність $\varphi(n) = \frac{1}{3} n$?

Відповідь. При $n = 2^\alpha \cdot 3^\beta$; $\alpha > 0$; $\beta > 0$.

32. Довести, що для натурального числа n рівність $\varphi(n) = \frac{1}{4} n$ неможлива.

33. Тотожність $\sum_{d|n} \varphi(d) = n$ перевірити на прикладі $n = 100$.

34. Довести, що кількість чисел ряду 1, 2, ..., n, які мають з n один і той самий найбільший спільний дільник δ, дорівнює $\varphi\left(\frac{n}{\delta}\right)$.

35. Користуючись результатом попередньої задачі, довести, що $\sum_{d|n} \varphi(d) = n$.

36. Скласти таблицю значень функції $\varphi(n)$ для всіх $n = 1, 2, \ldots, 50$, користуючись тільки формулою $\varphi(p^\alpha) = p^{\alpha-1}(p - 1)$ і тим, що $\varphi(n)$ — мультиплікативна функція.

37. Скількома нулями закінчується число 100!?

Відповідь. 24 нулями.

38. Чи ділиться C_{1000}^{500} на 7?

Відповідь. Ні.

39. Тотожність $\sum_{d|n} \mu(d) = 0$ перевірити на прикладі $n = 420$.

40. Скласти таблицю значень функції $\mu(n)$ для всіх $n = 1, 2, \ldots, 100$.

ІСТОРИЧНІ КОМЕНТАРІ

1. Теорема 1, § 11 вперше зустрічається у другому виданні «Теорії чисел» (1808) Лежандра.

2. Доведення твердження задачі 11 дав ще Евклід у IX книзі його «Початків». Твердження задачі 11 вперше довів Ейлер. Цікаво, що досі невідомо жодного непарного досконалого числа і не доведено, що їх нема. Зауважимо, що твердження задачі 11, будучи необхідним, не є достатнім; так наприклад, при простому $k + 1 = 11$ маємо: $2^{11} - 1 = 2047 = 23 \cdot 89$. Зазначимо тут, що поряд з досконалими числами ще в Стародавній Греції вивчали так звані дружні числа. Два натуральні числа називаються *дружніми*, якщо сума всіх правильних дільників першого з них дорівнює другому, а сума всіх правильних дільників другого дорівнює першому, тобто якщо $\sigma(n_1) = n_2$, $\sigma(n_2) = n_1$ або $S(n_1) - n_1 = n_2$, $S(n_2) - n_2 = n_1$. Перша пара дружніх чисел є пара: $n_1 = 284$, $n_2 = 220$. Ейлер дав таблицю 60 пар дружніх чисел. Тепер відомо кілька сотень пар дружніх чисел, однак, серед них немає жодної пари, в якій одне число було б парним, а друге непарним, і невідомо, чи є взагалі такі пари.

3. Функцію $\varphi(n)$ ввів Ейлер у 1760 році.

Слід мати на увазі, що функція Ейлера $\varphi(m)$ не завжди є найменшим натуральним значенням k, таким, коли $a^k \equiv 1 \pmod m$. Щоб знайти значення k, менші, ніж $\varphi(m)$, які задовольняють цю конгруенцію, в розгляд вводять *узагальнену функцію Ейлера* $L(m)$. Її означають для всіх значень m так:

$$L(1) = 1, \text{ а при } m > 1,\ L(m) = [p_1^{\alpha_1 - 1}(p_1 - 1),\ p_2^{\alpha_2 - 1}(p_2 - 1), \ldots, p_k^{\alpha_k - 1}(p_k - 1)].$$

При $m = p^\alpha$ функції $\varphi(m)$ і $L(m)$ очевидно збігаються.

Приклад. $L(680) = L(2^3 \cdot 5 \cdot 17) = [4, 4, 16] = 16$.

4. Формулу (5) § 13, яка дає загальний вираз функції Ейлера, називають іноді формулою Гаусса.

5. Формула додавання для функції Ейлера $\sum_{d|n} \varphi(d) = n$ є тотожністю, вона зустрічається вперше у Гаусса і тому називається його ім'ям.

6. Формулу (1) задачі № 12 вперше навів Лежандр; і її називають формулою Лежандра.

7. Мебіус (1790—1898) — німецький математик і астроном; основні його праці стосуються геометрії. Фактично в неявному вигляді функцію Мебіуса розглядав ще Ейлер.

Розділ III

КЛАСИ ЗА ДАНИМ МОДУЛЕМ. КОНГРУЕНЦІЇ І КЛАСИ

§ 15. Конгруенції і їхні основні властивості

Припустимо, що m є натуральне число; розглядатимемо цілі числа у зв'язку з остачами від ділення їх на це натуральне m, яке називають модулем. Згідно з теоремою про ділення з остачею кожному числу a відповідатиме певна остача r від ділення a на m:

$$a = mq + r, \quad 0 \leqslant r < m.$$

Якщо двом цілим числам a і b відповідає одна й та сама остача r від ділення їх на m, то вони називаються *конгруентними* (або *порівнянними*) *за модулем* m. Це позначається символом:

$$a \equiv b \pmod m \tag{1}$$

читається: a конгруентне з b за модулем m.

Деякі автори позначають це коротше:

$$a \equiv b\ (m). \tag{1'}$$

Співвідношення (1) [або (1')] між числами називають конгруенцією, або порівнянням.

Приклади. $48 \equiv 84 \pmod{18}$; $131 \equiv 1 \pmod{13}$; $10 \equiv 1 \pmod{11}$.

Знаком $\not\equiv$ позначають неконгруентність чисел за даним модулем. Так, наприклад, $7 \not\equiv 3 \pmod{11}$, $13 \not\equiv 6 \pmod{16}$.

Теорема 1. *Конгруентність чисел a і b за модулем m рівносильна:*

а) *можливості подати a у формі $a = b + mt$, де t — ціле;*

б) *подільності $a - b$ на m.*

Справді, нехай дано конгруенцію $a \equiv b \pmod m$. Тоді за означенням конгруенції матимемо:

$$a = mq + r,\ b = mq_1 + r, \text{ де } 0 \leqslant r < m,$$

звідки

$$a - b = m(q - q_1),\ a = b + mt,$$

де $t = q - q_1$ — ціле число.

Навпаки, нехай маємо рівність $a = b + mt$, де t — ціле; подаючи b у формі

$$b = mq_1 + r,\ 0 \leqslant r < m,$$

знаходимо, що

$$a = m(q_1 + t) + r = mq + r,$$

де $q = q_1 + t$ — ціле, тобто

$$a \equiv b \pmod m.$$

Отже, твердження а) доведено.

З твердження а) безпосередньо випливає твердження б).

Справді, якщо $a \equiv b + mt$, де t — ціле, то це співвідношення можна переписати так:

$$a - b = m \cdot t,$$

а це означає, що $a - b$ ділиться на m. Отже, з твердження $a \equiv b \pmod m$ випливає, що $a - b$ ділиться на m і, навпаки, з подільності $a - b$ на m відразу ж дістанемо конгруенцію $a \equiv b \pmod m$.

Конгруенції мають багато властивостей, подібних до властивостей рівностей.

Властивість 1. *Для конгруенції справджуються закони: рефлективності, симетричності і транзитивності*, тобто відповідно: а) $a \equiv a \pmod m$; б) з конгруенції $a \equiv b \pmod m$ випливає, що $b \equiv a \pmod m$ і в) якщо $a \equiv b \pmod m$ і $b \equiv c \pmod m$, то $a \equiv c \pmod m$.

Доведення а) $a - a$ завжди ділиться на m, отже, $a \equiv a \pmod m$;

б) якщо $a - b$ ділиться на m, то і $b - a$ ділитиметься на m, тобто з $a \equiv b \pmod m$; випливає, що $b \equiv a \pmod m$;

в) за умовою, $a - b$ і $b - c$ діляться на m; тоді

$$(a - b) + (b - c) = a - c$$

також ділитиметься на m, отже, $a \equiv c \pmod m$.

Властивість 2. *Конгруенції за одним і тим самим модулем можна почленно додавати (або віднімати).*

Справді, нехай дано конгруенції

$$\begin{aligned} a_1 &\equiv b_1 \pmod m, \\ a_2 &\equiv b_2 \pmod m, \\ &\dots\dots\dots \\ a_k &\equiv b_k \pmod m. \end{aligned} \tag{2}$$

Тоді, згідно з теоремою 1, можемо написати ряд рівностей:

$$a_1 = b_1 + mt_1,\ a_2 = b_2 + mt_2,\ \dots,\ a_k = b_k + mt_k, \tag{3}$$

де $t_1, t_2, \dots, t_k$ — цілі числа.

Додаючи почленно ці рівності, дістанемо:

$$a_1 + a_2 + \dots + a_k = b_1 + b_2 + \dots + b_k + m(t_1 + t_2 + \dots + t_k) = b_1 + b_2 + \dots + b_k + mT,$$

де T — ціле, тобто

$$a_1 + a_2 + \dots + a_k \equiv b_1 + b_2 + \dots + b_k \pmod m.$$

Висновок 1. *Доданок, що стоїть у якій-небудь частині конгруенції, можна переносити в іншу частину, змінивши знак на протилежний.*

Справді, додаючи конгруенцію $a + b \equiv c \pmod m$ до очевидної конгруенції $-b \equiv -b \pmod m$, дістанемо:

$$a \equiv c - b \pmod m.$$

Висновок 2. *Можна додати до обох частин або відняти від обох частин конгруенції одне й те саме число.*

Справді, додаючи (або віднімаючи) конгруенції $a \equiv b \pmod m$ і $c \equiv c \pmod m$ маємо:

$$a \pm c \equiv b \pm c \pmod m.$$

Висновок 3. *До кожної частини конгруенції можна додати (або відняти від неї) довільне число, кратне модулю.*

Справді, додаючи до конгруенції $a \equiv b \pmod m$ конгруенцію $\pm mk \equiv 0 \pmod m$, дістанемо:

$$a \pm mk \equiv b \pmod m.$$

Властивість 3. *Конгруенції за одним і тим самим модулем можна почленно перемножати.*

Справді, розглянемо знову конгруенції (2) і рівності (3), які з них випливають. Перемножуючи почленно рівності (3), дістанемо:

$$a_1 \cdot a_2 \dots a_k = b_1 \cdot b_2 \dots b_k + mT,$$

де T — ціле число. Отже, за теоремою 1 маємо:

$$a_1 \cdot a_2 \dots a_k \equiv b_1 \cdot b_2 \dots b_k \pmod m.$$

Висновок 1. *Обидві частини конгруенції можна помножити на одне й те саме ціле число.*

Справді, перемножуючи конгруенцію $a \equiv b \pmod m$ з конгруенцією $k \equiv k \pmod m$, дістанемо $ak \equiv bk \pmod m$.

Висновок 2. *Обидві частини конгруенції можна підносити до одного й того самого цілого невід'ємного степеня, тобто якщо* $a \equiv b \pmod m$, то $a^n \equiv b^n \pmod m$, де n — ціле $\geqslant 0$.

Властивості 2 і 3 можна узагальнити такою теоремою:

Теорема 2. Якщо

$$f(x_1, x_2, \dots, x_n) = \sum a x_1^{k_1} x_2^{k_2} \dots x_n^{k_n}$$

— многочлен з цілими коефіцієнтами і

$$a \equiv b \pmod m,\ \alpha_1 \equiv \beta_1 \pmod m,\ \alpha_2 \equiv \beta_2 \pmod m,\ \dots,\ \alpha_n \equiv \beta_n \pmod m,$$

то

$$\sum a\alpha_1^{k_1}\alpha_2^{k_2} \dots \alpha_n^{k_n} \equiv \sum b\beta_1^{k_1}\beta_2^{k_2} \dots \beta_n^{k_n} \pmod m. \tag{4}$$

Справді, на підставі властивості 3 (наслідок 2) знаходимо:

$$\alpha_1^{k_1} \equiv \beta_1^{k_1} \pmod m,\ \alpha_2^{k_2} \equiv \beta_2^{k_2} \pmod m,\ \dots,\ \alpha_n^{k_n} \equiv \beta_n^{k_n} \pmod m.$$

Перемножаючи почленно всі ці конгруенції і конгруенцію $a \equiv b \pmod m$, а потім підсумовуючи знайдені добутки (властивість 2), ми й прийдемо до конгруенції (4).

Зокрема, якщо

$$f(x) = a_0x^n + a_1x^{n-1} + \dots + a_{n-1}x + a_n$$

многочлен від одного аргументу x з цілими коефіцієнтами і $x \equiv x' \pmod m$, *то*

$$f(x) \equiv f(x') \pmod m,$$

Останнє твердження (як побачимо далі) є теоретичним обгрунтуванням для виведення ознак подільності. Теорема 2 дає можливість замінити в конгруенції всі відомі сталі коефіцієнти числами, меншими від модуля m. Зокрема, всі числа, що діляться на модуль, можна замінити нулями; можна, за бажанням, всі коефіцієнти в конгруенції зробити додатними.

Властивість 4. *Обидві частини конгруенції можна поділити на їхній спільний дільник, якщо він взаємно простий з модулем.*

Нехай

$$a \equiv b \pmod m,\ a = a_1 d,\ b = b_1 d \text{ і } (m, d) = 1,$$

тоді

$$a - b = d(a_1 - b_1)$$

ділиться на m і, оскільки $(m, d) = 1$, то $a_1 - b_1$, ділитиметься на m (теорема 2, § 4), а це означає, що

$$a_1 \equiv b_1 \pmod m.$$

У цій властивості дуже істотне застереження, що спільний дільник має бути взаємно простий з модулем (тоді як обидві частини рівності можна ділити на будь-який їхній спільний дільник); наприклад, $30 \equiv 18 \pmod{12}$, але $5 \not\equiv 3 \pmod{12}$.

Досі ми розглядали властивості конгруенції за одним і тим самим модулем; вони багато в чому були подібні до відповідних властивостей рівностей. Тепер розглянемо інші властивості конгруенції, в яких особливу роль відіграє модуль.

Властивість 5. *Обидві частини конгруенції і модуль можна помножити на одне й те саме натуральне число.*

Справді, з конгруенції $a \equiv b \pmod m$ випливає рівність $a = b + mt$, де t — ціле; помножаючи її на ціле $k > 0$, дістанемо $ak = bk + mk \cdot t$, звідки випливає конгруенція

$$ak \equiv bk \pmod{mk}.$$

Властивість 6. *Обидві частини конгруенції і модуль можна поділити на будь-який їхній спільний дільник.*

Справді, припустимо, що $a \equiv b \pmod m$ і

$$a = a_1 d,\ b = b_1 d,\ m = m_1 d,$$

тоді маємо

$$a = b + mt,$$

або $a_1 d = b_1 d + m_1 dt$. Звідси, скорочуючи обидві частини останньої рівності на d, дістанемо:

$$a_1 = b_1 + m_1 t;$$

отже, $a_1 \equiv b_1 \pmod{m_1}$.

Властивість 7. *Якщо конгруенція має місце за кількома модулями, то вона матиме місце і за модулем, що дорівнює їхньому найменшому спільному кратному.*

Справді, нехай дано:

$$a \equiv b \pmod{m_1},$$
$$a \equiv b \pmod{m_2},$$
$$\dots\dots\dots$$
$$a \equiv b \pmod{m_k};$$

це означає, що $a - b$ ділиться на всі модулі $m_1, m_2, \dots, m_k$, отже, $a - b$ має ділитись і на їхнє найменше спільне кратне $m = [m_1, m_2, \dots, m_k]$. (Це випливає з правила знаходження н. с. к. кількох чисел, викладеного в § 6), а це означає, що

$$a \equiv b \pmod m.$$

Властивість 8. *Якщо конгруенція має місце за модулем m, то вона матиме місце і за будь-яким дільником d цього модуля.*

Справді, з конгруенції $a \equiv b \pmod m$ випливає, що $a - b$ ділиться на m; тому $a - b$ ділитиметься і на будь-який дільник d числа m, тобто $a \equiv b \pmod d$.

Властивість 9. *Якщо одна частина конгруенції і модуль діляться на яке-небудь ціле число, то і друга частина конгруенції ділиться на це число.*

Справді, з конгруенції $a \equiv b \pmod m$ випливає рівність $a = b + mt$; якщо a і m діляться на d, то (згідно з теоремою 2, § 1) і b має ділитись на d, що й стверджувалось.

Властивість 10. *Числа a і b, конгруентні між собою за модулем m, мають з ним один і той самий найбільший спільний дільник.*

Справді, припустимо, що $a \equiv b \pmod m$, звідки $a = b + mt$. Згідно з теоремою 2, § 2, сукупність спільних дільників a і m збігається з спільними дільниками чисел b і m, зокрема $(a, m) = (b, m)$.

Контрольні запитання

1. Які числа називаються конгруентними? Якій рівності еквівалентна конгруенція?
2. Сформулюйте властивості конгруенцій, аналогічні властивостям рівностей.
3. Сформулюйте властивості конгруенцій, відмінні від властивостей рівностей.
4. Сформулюйте правило скорочення конгруенції.

§ 16. Класи за даним модулем. Кільце класів.

Класом чисел за даним модулем m називається множина всіх цілих чисел, конгруентних з деяким певним числом a. Оскільки при діленні цілих чисел на деяке натуральне число m можна дістати тільки m різних невід'ємних остач (а саме: 0, 1, 2, ..., $m - 1$), то множина всіх цілих чисел розіб'ється на m класів чисел за модулем m, що не мають спільних елементів.

Із сказаного випливає, що всім числам даного класу відповідає одна й та сама остача r від ділення їх на число m; отже, дістанемо всі числа цього класу, якщо у формі $mq + r$, де r — стале, q набуватиме значень усіх цілих чисел.

Отже, числа цього класу модуля m на числовій прямій утворюють двосторонню послідовність цілих точок, які лежать від одної на однаковій відстані m, тобто кожний клас є двосторонньою арифметичною прогресією з різницею, що дорівнює модулю m. Цікавою ілюстрацією класів лишків за модулем m є клавіатура (необмежена в обидва боки); класи лишків відповідають при цьому тонам однакової назви, які відрізняються один від одного лише на цілі октави. Як приклад класів за модулем 7 є дні календаря (до одного класу належать ті дні, які припадають на той самий день тижня).

З означення конгруентності двох чисел a і b за модулем m безпосередньо сказаного відразу ж випливає таке твердження.

Два цілих числа a і b тоді і тільки тоді належать до одного класу за модулем m, коли вони конгруентні за цим модулем.

Будь-яке число даного класу називається *лишком*, або *представником* цього класу. Отже, якщо число a є представником деякого класу за модулем m, то будь-яке інше число b цього класу задовольняє умову: $b \equiv a \pmod m$, або $b = a + mt$, де t — деяке ціле число, тобто, інакше кажучи, $b = a + mt$ є загальний вигляд цілих чисел, які належать до того самого класу, що й a.

Символом C_a позначатимемо той клас чисел, одним з лишків якого є число a. Звідси попереднє твердження означає, що $C_a = C_b$ *тоді і тільки тоді, коли* $a \equiv b \pmod m$.

Отже, запровадження класів дає змогу замінювати конгруенцію чисел рівністю відповідних класів і, навпаки, рівність класів — відповідною конгруенцією. Водночас це твердження показує рівноправність усіх чисел цього класу.

Означимо алгебраїчні операції «додавання» і «множення» класів.

Припустимо, що C_a і C_b є два будь-які класи чисел за модулем m і припустимо, що a — будь-який лишок класу C_a, b — будь-який лишок класу C_b. Тоді під *сумою* $C_a + C_b$ класів C_a і C_b розумітимемо клас C_{a+b}, одним з лишків якого є $a + b$.

Покажемо, що означена таким способом сума класів не залежить від вибору лишків a і b. Справді, нехай a' і b' — які-небудь інші лишки класів C_a і C_b; тоді

$$a' \equiv a \pmod m, \qquad (1)$$
$$b' \equiv b \pmod m. \qquad (2)$$

Додаючи почленно ці конгруенції, дістанемо:

$$a' + b' \equiv a + b \pmod m,$$

тобто $a' + b'$ міститься в тому самому класі C_{a+b}, що й $a + b$.

Звідси випливає, що означена нами *операція додавання класів однозначна і завжди здійсненна.*

Аналогічно означається множення класів, а саме: під *добутком* $C_a \cdot C_b$ класів C_a і C_b розуміють клас C_{ab}, одним з лишків якого є ab.

Означений таким способом добуток класів також не залежить від вибору лишків. Справді, при попередніх позначеннях перемножимо почленно конгруенції (1) і (2). Дістанемо:

$$a'b' \equiv ab \pmod m.$$

Це показує, що $a'b'$ міститься в тому самому класі C_{ab}, що й ab. Означена таким способом *операція множення класів однозначна і завжди здійсненна.*

Означені нами *операції над класами задовольняють комутативний і асоціативний закони додавання і множення класів, а також дистрибутивний закон*, що зв'язує ці операції. Для прикладу доведемо справедливість комутативного закону множення. За означенням маємо:

$$C_a \cdot C_b = C_{ab}, \quad C_b \cdot C_a = C_{ba}.$$

Але $ba = ab$, бо арифметичне множення чисел підлягає комутативному закону, тому $C_{ba} = C_{ab}$ і $C_a \cdot C_b = C_b \cdot C_a$, що й треба було довести. Аналогічно можна довести й інші арифметичні закони.

Роль нуля при додаванні класів відіграє клас C_0, бо $C_a + C_0 = C_{a+0} = C_a$. Тепер неважко пересвідчитись, що рівняння $C_a + x = C_b$ завжди розв'язується однозначно, його розв'язком буде клас C_{b-a}. Це означає, що операція віднімання класів однозначна і завжди здійсненна.

Нагадаємо, що непорожня множина R разом з означеними в ній алгебраїчними операціями «додавання» і «множення» називається *кільцем*, якщо справджуються такі вимоги: 1) додавання підлягає комутативному й асоціативному законам; 2) виконувана операція обернена до операції додавання; 3) для множення справедливий асоціативний закон; 4) справджується дистрибутивний закон, тобто для будь-яких трьох елементів a, b і c з R справедливі рівності:

$$c(a + b) = ca + cb \text{ і } (a + b)c = ac + bc.$$

Зокрема, кільце називається *комутативним*, якщо не тільки додавання, а й множення комутативне.

З попереднього випливає, що сукупність усіх класів чисел за модулем m разом з означеними в ній операціями додавання і множення класів задовольняє всі вимоги загального означення комутативного кільця. Тому ми приходимо до такого твердження:

Теорема 1. *Сукупність всіх класів чисел за модулем m утворює комутативне кільце відносно операцій додавання і множення класів.*

Як відомо, в усякому кільці справедливе твердження: якщо в добутку двох або кількох елементів кільця хоча б один із співмножників є нуль, то й добуток дорівнює нулю. Обернене твердж-

ження виконується не завжди. Може трапитись, що $ab = 0$, але ні $a \neq 0$, ні $b \neq 0$; у цьому разі a і b називають *дільниками нуля*, а саме кільце — *кільцем з дільниками нуля*.

Розглянемо тепер окремо випадки простого і складеного модуля.

1) $m = p$ — просте число. Елементами, або лишками, класів можна вважати числа $0, 1, \ldots, p-1$. Припустимо, що a і b — будь-які числа з системи $1, 2, \ldots, p-1$, тобто $a \not\equiv 0 \pmod p$ і $C_a \neq C_0$, $b \not\equiv 0 \pmod p$ і $C_b \neq C_0$; тоді

$$C_a \cdot C_b = C_{ab} \neq C_0,$$

оскільки

$$ab \not\equiv 0 \pmod p, \text{ бо } (a, p) = 1 \text{ і } (b, p) = 1.$$

Далі, якщо $C_a \cdot C_b = C_0$, то це означатиме, що $ab \equiv 0 \pmod p$, тобто ab ділиться на p, але це буде можливо тільки тоді, коли або $a = 0$, або $b = 0$ і p є число просте і $a < p$, $b < p$.

Отже, дістанемо, що у випадку простого модуля p, якщо добуток класів є нульовий клас C_0, то принаймні один із співмножників є нульовий клас. І приходимо до такого висновку:

Сукупність усіх класів чисел за простим модулем утворює комутативне кільце без дільників нуля.

2) Припустимо тепер, що m — складене число, нехай $m = ab$, де a і b менші за m і більші від 1; тоді

$$ab \equiv 0 \pmod m.$$

За умовою $C_a \neq C_0$, $C_b \neq C_0$, але

$$C_a \cdot C_b = C_{ab} = C_0,$$

тобто C_a і C_b будуть дільниками нуля, і ми дістанемо таке твердження:

Сукупність усіх класів чисел за складеним модулем m утворює комутативне кільце з дільниками нуля.

Приклад. Нехай $m = 6$. За цим модулем маємо шість класів:

$$C_0, C_1, C_2, C_3, C_4, C_5;$$

розглянемо добуток

$$C_2 \cdot C_3 = C_6 = C_0,$$

або

$$C_3 \cdot C_4 = C_{12} = C_6 = C_0.$$

Отже, наприклад, C_2 і C_3, C_3 і C_4 є дільниками нуля в кільці класів за модулем 6.

Контрольні запитання

1. Напишіть по кілька чисел, що належать до кожного класу за модулем 6.
2. Яка умова є необхідною і достатньою для того, щоб два числа належали до того самого класу за модулем m?
3. Яке означення операцій «додавання» і «множення» класів?
4. Що розуміють під словами: множина містить дільники нуля?
5. Наведіть приклад кільця класів чисел з дільниками нуля.

§ 17. Повна система лишків

Як ми вже говорили, будь-яке число класу називається лишком за модулем m відносно всіх чисел того самого класу.

Під *найменшим невід'ємним лишком* класу розуміють найменше число серед невід'ємних чисел цього класу; він є не що інше, як невід'ємна остача r, що утворюється при діленні довільного числа певного класу на модуль m.

Лишок ρ, найменший за абсолютною величиною, називається *абсолютно найменшим лишком*; його легко знайти за таким правилом: $\rho = r$, якщо $r < \frac{m}{2}$; $\rho = r - m$, якщо $r > \frac{m}{2}$; нарешті, якщо m парне і $r = \frac{m}{2}$, то за ρ можна взяти будь-яке з двох чисел $\frac{m}{2}$, або $\frac{m}{2} - m = -\frac{m}{2}$.

Беручи від кожного класу по одному лишку, дістанемо так звану *повну систему лишків* за модулем m.

Найчастіше за повну систему лишків за модулем m беруть *найменші невід'ємні лишки* $0, 1, 2, \ldots, m-1$ або *абсолютно найменші лишки*.

Приклад. Написати повну систему найменших невід'ємних лишків і повну систему абсолютно найменших лишків за модулем $m = 10$.

Повна система найменших невід'ємних лишків за модулем 10 буде:

$$0, 1, 2, 3, 4, 5, 6, 7, 8, 9.$$

Повну систему абсолютно найменших лишків за модулем 10 можна записати у вигляді:

$$0, 1, 2, 3, 4, 5, -4, -3, -2, -1$$

або у вигляді

$$0, 1, 2, 3, 4, -5, -4, -3, -2, -1.$$

Повна система лишків за модулем m має такі основні властивості.

Властивість 1. *Будь-які m чисел, які попарно не конгруентні між собою за модулем m, утворюють повну систему лишків за цим модулем.*

Справді, через те що ці числа попарно неконгруентні за модулем m, вони є лишками різних класів за цим модулем, а оскільки всіх класів m, тобто стільки, скільки й чисел даної системи, то до кожного класу напевно попадає по одному числу (лишку), а це й означає, що дані m чисел утворюють повну систему лишків за модулем m.

Властивість 2. *Якщо $(a, m) = 1$ і x пробігає повну систему лишків за модулем m, то вираз $ax + b$,* де *b,— довільне ціле число, також пробігатиме повну систему лишків за цим модулем.*

Справді, чисел $ax + b$ буде стільки ж, скільки чисел x, тобто m. Згідно з властивістю 1 залишається показати, що будь-які два числа $ax_1 + b$ і $ax_2 + b$, які відповідають неконгруентним x_1 і x_2, самі будуть неконгруентні між собою за модулем m.

Припустимо супротивне, тобто

$$ax_1 + b \equiv ax_2 + b \pmod m,$$

тоді дістанемо:

$$ax_1 \equiv ax_2 \pmod m.$$

За умовою $(a, m) = 1$. Ділячи обидві частини останньої конгруенції на a, дістанемо $x_1 \equiv x_2 \pmod m$, що неможливо, бо x_1 і x_2 належать до різних класів лишків за модулем m, а тому $x_1 \not\equiv x_2 \pmod m$.

Приклад. Нехай x пробігає повну систему найменших невід'ємних лишків за модулем 8. Знайти відповідні невід'ємні лишки виразу $3x + 2$. Маємо:

$$x = 0,\ 1,\ 2,\ 3,\ 4,\ 5,\ 6,\ 7;$$

відповідно:

$$3x + 2 \equiv 2,\ 5,\ 0,\ 3,\ 6,\ 1,\ 4,\ 7 \pmod 8.$$

Контрольні запитання

1. Як дістати повну систему лишків за модулем m?
2. Напишіть повну систему абсолютно найменших лишків, найменших невід'ємних лишків і довільних лишків за модулем 8.
3. Сформулюйте основні властивості повної системи лишків.
4. З якою метою при доведенні властивості 2 використовується умова $(a, b) = 1$?
5. Перевірте справедливість властивості 2 на числовому прикладі.

§ 18. Зведена система лишків. Група класів, взаємно простих з модулем

Згідно з властивістю 10, § 15, числа одного й того самого класу за модулем m мають з модулем один і той самий найбільший спільний дільник. Особливо важливі класи, що містять числа, взаємно прості з модулем. Через те що кожен клас за модулем m цілком характеризується будь-яким своїм лишком, то, взявши за повну систему лишків найменші невід'ємні лишки $0, 1, 2, \ldots, m - 1$, легко побачити, що *класів чисел, взаємно простих з модулем m, буде стільки, скільки буде чисел, менших від m і взаємно простих з m, тобто $\varphi(m)$.*

Беручи від кожного такого класу чисел по одному лишку, дістанемо так звану *зведену систему лишків* за модулем m. Її можна скласти з числа повної системи лишків, взаємно простих з модулем. Звичайно зведену систему лишків виділяють з повної системи найменших невід'ємних лишків: $0, 1, 2, \ldots, m - 1$.

Приклад. Зведена система лишків за модулем 20 містить

$$\varphi(20) = \varphi(4) \cdot \varphi(5) = 8$$

лишків, взаємно простих з 20:

$$1,\ 3,\ 7,\ 9,\ 11,\ 13,\ 17,\ 19.$$

Зведена система лишків має такі основні властивості:

Властивість 1. *Будь-які $\varphi(m)$ чисел, що попарно неконгруентні за модулем m і взаємно прості з модулем, утворюють зведену систему лишків за модулем m.*

Справді, оскільки ці числа попарно неконгруентні між собою за модулем m і взаємно прості з m, то вони є лишками різних класів чисел за модулем m, взаємно простих з m. Усіх таких класів є $\varphi(m)$, тобто стільки, скільки даних чисел, тому до кожного класу напевно попаде по одному числу (лишку), а це й означає, що певні $\varphi(m)$ чисел утворюють зведену систему лишків за модулем m.

Властивість 2. *Якщо $(a, m) = 1$ і x пробігає зведену систему лишків за модулем m, то вираз ax теж пробігатиме зведену систему лишків за цим модулем.*

Справді, чисел виду ax буде стільки ж, скільки чисел x, тобто $\varphi(m)$. Згідно з властивістю 1, залишається показати, що вони попарно неконгруентні за модулем m і взаємно прості з m. За умовою $(a, m) = 1$ і $(x, m) = 1$ (оскільки x пробігає зведену систему лишків за модулем m), отже, $(ax, m) = 1$ (див. теорему 4, § 4). Коли б тепер

$$ax_1 \equiv ax_2 \pmod m,$$

то, скорочуючи на a, ми дістали б $x_1 \equiv x_2 \pmod m$, що неможливо (бо x_1 і x_2 належать до різних класів чисел за модулем m). Цим наше твердження доведено.

Нагадаємо, що непорожня множина G разом з означеною в ній алгебраїчною операцією (множенням) називається *групою*, якщо ця операція асоціативна і якщо необмежено й однозначно здійсненна обернена операція, тобто якщо розв'язними є рівняння $ax = b$, $ya = b$ для будь-яких a і b з G. Якщо, крім того, групова операція комутативна, то група називається *комутативною*, або *абельовою*. Вимога розв'язності рівнянь $ax = b$, $ya = b$ еквівалентна тому, щоб у групі існував єдиний одиничний елемент і для всякого a — єдиний обернений елемент a^{-1}, тобто такий, що $aa^{-1} = a^{-1}a = 1$.

Тепер неважко довести таке твердження:

Теорема. *Сукупність усіх класів чисел, взаємно простих з модулем m, утворює скінченну абельову групу порядку $\varphi(n)$ відносно множення класів.*

Справді, нехай $(a, m) = 1$, $(b, m) = 1$, тоді $(ab, m) = 1$. Звідси випливає, що $C_a \cdot C_b = C_{ab}$, де C_a, C_b, C_{ab} — класи, взаємно прості з модулем m; це означає, що в розглядуваній множині $\varphi(m)$ класів, взаємно простих з модулем m, означена алгебраїчна операція «множення» класів. Ця операція, як раніш було показано, є асоціативною і комутативною. Роль одиниці виконуватиме, очевидно, клас C_1, бо $C_a \cdot C_1 = C_a$. Покажемо тепер, що для всякого класу C_a, де $(a, m) = 1$, обернений, тобто такий клас C_x, де $(x, m) = 1$, отже,

$$C_a \cdot C_x = C_{ax} = C_1.$$

Для цього досить показати, що існує таке x, взаємно просте з m, що має місце конгруенція $ax \equiv 1 \pmod m$. Нехай x пробігає зведену систему лишків за модулем m, тоді за доведеним ax також пробігатиме зведену систему лишків за цим модулем. Але 1 є один із зведених лишків за довільним модулем, отже, при деякому єдиному $x = x_1$ дістанемо $ax_1 \equiv 1 \pmod m$. Відповідний клас чисел, що містить x_1, і буде оберненим до класу C_a. А це означає, що всі вимоги абельової групи виконані, і теорему доведено.

Контрольні запитання

1. Що називається зведеною системою лишків за модулем m?
2. Сформулюйте основні властивості зведеної системи лишків.
3. Напишіть зведену систему найменших невід'ємних лишків і довільну зведену систему лишків за модулем 12.
4. Чи пробігає вираз $ax + b$, де $(a, m) = 1$, зведену систему лишків за модулем m при умові, що x пробігає зведену систему лишків?
5. Перевірте справедливість властивості 2 на числовому прикладі.
6. Як розуміти, що для кожного класу чисел, взаємно простих з модулем, існує обернений клас?
7. Чи утворює сукупність усіх класів чисел за модулем групу відносно множення класів? Те саме відносно додавання класів?

ред чисел 0, 1, 2, 3, 4. Безпосередньою перевіркою встановлюємо, що тільки $x = 1$ задовольняє задану конгруенцію, тому розв'язком цієї конгруенції буде клас чисел $x \equiv 1 \pmod 5$, тобто $x = 1 + 5t$, де t — будь-яке ціле число. Отже, задана конгруенція четвертого степеня за модулем 5 має лише один розв'язок.

За властивостями конгруенцій до обох частин конгруенції можна додавати і від обох частин віднімати числа, кратні модулю. Тому в даній конгруенції завжди можна коефіцієнти замінити їхніми найменшими невід'ємними або абсолютно найменшими лишками за модулем, що дорівнює модулю конгруенції. Інакше кажучи, коефіцієнти конгруенції завжди можна зробити за абсолютною величиною меншими від модуля m, а, за бажанням, можна зробити їх тільки додатними, меншими від m.

Приклад. Конгруенція

$$8x^5 - 12x^3 - 13x^2 - 15x + 6 \equiv 0 \pmod 5$$

еквівалентна конгруенції

$$3x^5 - 2x^3 - 3x^2 + 1 \equiv 0 \pmod 5,$$

або конгруенції

$$3x^5 + 3x^3 + 2x^2 + 1 \equiv 0 \pmod 5.$$

Щоб знайти розв'язки останньої конгруенції, випробуємо, наприклад, абсолютно найменші лишки за модулем 5: 0, 1, 2, —2, —1. Безпосередньо видно, що 0, 1, —1 задану конгруенцію не задовольняють. При дальшому випробуванні можна скористатись схемою Горнера з тією тільки відмінністю, що для полегшення кожного разу можна відкидати числа, кратні модулю

	3	0	3	2	0	1
2	3	$6 \equiv 1$	$5 \equiv 0$	2	4	$9 \equiv 4$
—2	3	$6 \equiv -1$	$5 \equiv 0$	2	—4	$9 \equiv 4$

Отже, конгруенція $3x^5 + 3x^3 + 2x^2 + 1 \equiv 0 \pmod 5$ не має розв'язків, а тому не має розв'язків і конгруенція

$$8x^5 - 12x^3 - 13x^2 - 15x + 6 \equiv 0 \pmod 5.$$

При розв'язуванні конгруенції з невідомою величиною іноді доводиться помножати обидві частини конгруенції на ціле число. Для тотожних конгруенцій ця операція, як раніш було показано, завжди законна. Для конгруенцій з невідомою величиною таке перетворення не завжди законне, тобто, інакше кажучи, при такому перетворенні конгруенції може порушитись еквівалентність даної і добутої конгруенцій.

то, скорочуючи на a, ми дістали б $x_1 \equiv x_2 \pmod m$, що неможливо (бо x_1 і x_2 належать до різних класів чисел за модулем m). Цим наше твердження доведено.

Нагадаємо, що непорожня множина G разом з означеною в ній алгебраїчною операцією (множенням) називається *групою*, якщо ця операція асоціативна і якщо необмежено й однозначно здійсненна обернена операція, тобто якщо розв'язними є рівняння $ax = b$, $ya = b$ для будь-яких a і b з G. Якщо, крім того, групова операція комутативна, то група називається *комутативною*, або *абельовою*. Вимога розв'язності рівнянь $ax = b$, $ya = b$ еквівалентна тому, щоб у групі існував єдиний одиничний елемент і для всякого a — єдиний обернений елемент a^{-1}, тобто такий, що $aa^{-1} = a^{-1}a = 1$.

Тепер неважко довести таке твердження:

Теорема. *Сукупність усіх класів чисел, взаємно простих з модулем m, утворює скінченну абельову групу порядку $\varphi(n)$ відносно множення класів.*

Справді, нехай $(a, m) = 1$, $(b, m) = 1$, тоді $(ab, m) = 1$. Звідси випливає, що $C_a \cdot C_b = C_{ab}$, де C_a, C_b, C_{ab} — класи, взаємно прості з модулем m; це означає, що в розглядуваній множині $\varphi(m)$ класів, взаємно простих з модулем m, означена алгебраїчна операція «множення» класів. Ця операція, як раніш було показано, є асоціативною і комутативною. Роль одиниці виконуватиме, очевидно, клас C_1, бо $C_a \cdot C_1 = C_a$. Покажемо тепер, що для всякого класу C_a, де $(a, m) = 1$, обернений, тобто такий клас C_x, де $(x, m) = 1$, отже,

$$C_a \cdot C_x = C_{ax} = C_1.$$

Для цього досить показати, що існує таке x, взаємно просте з m, що має місце конгруенція $ax \equiv 1 \pmod m$. Нехай x пробігає зведену систему лишків за модулем m, тоді за доведеним ax також пробігатиме зведену систему лишків за цим модулем. Але 1 є один із зведених лишків за довільним модулем, отже, при деякому єдиному $x = x_1$ дістанемо $ax_1 \equiv 1 \pmod m$. Відповідний клас чисел, що містить x_1, і буде оберненим до класу C_a. А це означає, що всі вимоги абельової групи виконані, і теорему доведено.

Контрольні запитання

1. Що називається зведеною системою лишків за модулем m?
2. Сформулюйте основні властивості зведеної системи лишків.
3. Напишіть зведену систему найменших невід'ємних лишків і довільну зведену систему лишків за модулем 12.
4. Чи пробігає вираз $ax + b$, де $(a, m) = 1$, зведену систему лишків за модулем m при умові, що x пробігає зведену систему лишків?
5. Перевірте справедливість властивості 2 на числовому прикладі.
6. Як розуміти, що для кожного класу чисел, взаємно простих з модулем, існує обернений клас?
7. Чи утворює сукупність усіх класів чисел за модулем групу відносно множення класів? Те саме відносно додавання класів?

§ 19. Теореми Ейлера і Ферма

Як застосування властивостей зведеної системи лишків, доведемо теореми Ейлера і Ферма, що відіграють фундаментальну роль у теорії конгруенцій і широко застосовуються як у теоретичних дослідженнях, так і в арифметиці.

Теорема Ейлера. *Якщо m — натуральне число, a — будь-яке ціле число і $(a, m) = 1$, то має місце конгруенція*

$$a^{\varphi(m)} \equiv 1 \pmod m,$$

де $\varphi(m)$ — функція Ейлера.

Справді, припустимо, що x пробігає зведену систему найменших невід'ємних лишків за модулем m:

$$x = r_1, r_2, \ldots, r_{\varphi(m)}.$$

Тоді, за властивістю 2 зведеної системи лишків, ax також пробігатиме зведену систему лишків за цим модулем. Отже, можна написати таку систему конгруенцій:

$$\begin{aligned} ar_1 &\equiv \rho_1 \pmod m, \\ ar_2 &\equiv \rho_2 \pmod m, \\ &\ldots\ldots\ldots \\ ar_{\varphi(m)} &\equiv \rho_{\varphi(m)} \pmod m, \end{aligned}$$

де $\rho_1, \rho_2, \ldots, \rho_{\varphi(m)}$ є також найменші невід'ємні лишки, взаємно прості з модулем m, тобто ті самі числа, що й $r_1, r_2, \ldots, r_{\varphi(m)}$, але розміщені в іншому порядку. Перемножуючи почленно ці конгруенції, матимемо:

$$a^{\varphi(m)} r_1 r_2 \ldots r_{\varphi(m)} \equiv \rho_1 \rho_2 \ldots \rho_{\varphi(m)} \pmod m.$$

Скорочуючи обидві частини цієї конгруенції на число $r_1 r_2 \ldots r_{\varphi(m)} = \rho_1 \rho_2 \ldots \rho_{\varphi(m)}$, взаємно просте з m (бо всі r_i і ρ_i взаємно прості з m за умовою), дістанемо:

$$a^{\varphi(m)} \equiv 1 \pmod m.$$

Теорема Ферма. *При простому p і a, що не ділиться на p, має місце конгруенція:*

$$a^{p-1} \equiv 1 \pmod p.$$

Ця теорема безпосередньо випливає з теореми Ейлера при простому $m = p$, бо $\varphi(p) = p - 1$.

Часто теорему Ферма формулюють трохи інакше:

При будь-якому цілому a має місце конгруенція

$$a^p \equiv a \pmod p,$$

де p — просте число.

Справді, помножаючи конгруенцію $a^{p-1} \equiv 1 \pmod p$ на a, дістанемо конгруенцію $a^p \equiv a \pmod p$, яка справедлива вже для всіх цілих a, бо вона справедлива і для a, кратного p.

Так, наприклад, при $a = 4$ і $p = 7$ дістанемо:

$$4^7 = (4^2)^3 \cdot 4 \equiv 2^3 \cdot 4 \equiv 4 \pmod 7.$$

Контрольні запитання

1. Сформулюйте теореми Ейлера і Ферма.
2. З якою метою використовується при доведенні теореми Ейлера умова $(a, m) = 1$?
3. Перевірте справедливість теореми Ейлера на числовому прикладі $a = 9$, $m = 16$.
4. Покажіть, що $a^{22} \equiv a^2 \pmod{25}$. (При розв'язуванні розгляньте два випадки: $a \vdots 5$ і a не $\vdots 5$).

Вправи

1. Знайти найменші невід'ємні і абсолютно найменші лишки за модулем 13 для чисел 3, 8, 16, —43, 132, 278, —423, 1327. Які з цих чисел належать до одного і того самого класу за модулем 13?

Відповідь. Найменшими невід'ємними лишками будуть відповідно числа: 3, 8, 3, 9, 2, 5, 6, 1; абсолютно найменшими лишками будуть відповідно числа: 3, —5, 3, —4, 2, 5, 6, 1; числа 3 і 16 належать до одного й того самого класу за модулем 13, тобто $3 \equiv 16 \pmod{13}$.

2. Знайти зведену систему найменших невід'ємних лишків за модулем 40.

Відповідь. 1, 3, 7, 9, 11, 13, 17, 19, 21, 23, 27, 29, 31, 33, 37, 39.

3. Чи утворюють степені 2^0, 2^1, 2^2, 2^3, 2^4, 2^5, 2^6, 2^7, 2^8, 2^9 разом з числом 0 повну систему лишків за модулем 11?

Відповідь. Утворюють.

4. Перевірити формули $5^{\varphi(26)} \equiv 1 \pmod{26}$, $2^{\varphi(45)} \equiv 1 \pmod{45}$, $3^{\varphi(40)} \equiv 1 \pmod{40}$.

5. Припустимо, що x пробігає повну систему найменших невід'ємних лишків за модулем 8; знайти відповідні найменші невід'ємні лишки для виразу $7x + 4$.

Відповідь. Якщо $x = 0, 1, 2, 3, 4, 5, 6, 7$, то відповідно $7x + 4 \equiv 4, 3, 2, 1, 0, 7, 6, 5 \pmod 8$.

6. Знайти найменший невід'ємний лишок чисел $8^{80} + 13^{90}$ за модулем 17.

Відповідь. 0.

7. Довести, що квадрат всякого непарного числа конгруентний з одиницею за модулем 8.

8. Довести, що непарне число виду $4k + 3$ не можна подати як суму двох квадратів цілих чисел.

9. Довести, що коли $(n, 8) = 1$, то $n^2 \equiv 1 \pmod 8$.

10. Користуючись малою теоремою Ферма, довести, що, p і $8p^2 + 1$ можуть бути одночасно простими тільки при $p = 3$.

11. Виходячи з розкладу бінома Ньютона для $(a + b)^p$, довести, що $(a + b)^p \equiv a^p + b^p \pmod p$. Узагальнюючи цей результат для випадку трьох і більше чисел, вивести малу теорему Ферма.

12. Якщо p — просте і $a \equiv b \pmod{p^n}$, то $a^{p^m} \equiv b^{p^m} \pmod{p^{n+m}}$; тут m і n — цілі невід'ємні числа. Вивести звідси теорему Ейлера, вважаючи відомою малу теорему Ферма.

13. Довести, що натуральне число p тоді і тільки тоді є простим, коли

$$C^k_{p-1} \equiv (-1)^k \pmod p,$$

де C^k_{p-1} — всі можливі біноміальні коефіцієнти в розкладі $(a + b)^{p-1}$ ($k = 0, 1, 2, \ldots, p - 1$).

14. Підставляючи у вираз $z = 5y + 3x$ значення $x = 0, 1, 2, 3, 4$; $y = 0, 1, 2$, перевірити, що ми дістанемо для z повну систему лишків за модулем 15.

15. Нехай m — натуральне число, a b — цілі числа і $(a, m) = 1$. Довести, що коли x пробігає повну систему лишків за модулем m, то

$$\sum_x \left\{\frac{ax + b}{m}\right\} \equiv \frac{1}{2}(m - 1) \pmod m.$$

16. Нехай $m_1, m_2, \ldots, m_k$ — натуральні, попарно взаємно прості числа. Довести, що ми дістанемо повну систему лишків за модулем $m_1 m_2 \ldots m_k$, якщо у формі

$$x_1 + m_1 x_2 + m_1 m_2 x_3 + \cdots + m_1 m_2 \ldots m_{k-1} x_k$$

числа $x_1, x_2, \ldots, x_k$ пробігатимуть повні системи лишків відповідно за модулями $m_1, m_2, \ldots m_k$.

17. Припустимо, що $m_1, m_2, \ldots, m_k$ — натуральні, попарно взаємно прості числа і $m_1 m_2 \ldots m_k = m_1 M_1 = m_2 M_2 = \cdots = m_k M_k$.

а) довести, що дістанемо повну систему лишків за модулем $m_1 m_2 \ldots m_k$, якщо у формі

$$M_1 x_1 + M_2 x_2 + \cdots + M_k x_k$$

числа $x_1, x_2, \ldots, x_k$ пробігатимуть повні системи лишків відповідно за модулями $m_1, m_2, \ldots, m_k$.

б) довести, що ми дістанемо зведену систему лишків за модулем $m_1 m_2 \ldots m_k$, якщо у формі

$$M_1 x_1 + M_2 x_2 + \cdots + M_k x_k$$

числа $x_1, x_2, \ldots, x_k$ пробігатимуть зведені системи лишків за модулями $m_1, m_2, \ldots, m_k$.

18. Довести, що коли $(a, b) = 1$ і x пробігає повну систему лишків за модулем a, а y пробігає повну систему лишків за модулем b, то $z = ay + bx$ пробігатиме повну систему лишків за модулем ab; z тоді і тільки тоді буде взаємно простим з ab, коли x взаємно просте з a і y взаємно просте з b. Інакше кажучи, якщо x пробігає зведену систему лишків за модулем a, а y — зведену систему лишків за модулем b, то z пробігатиме зведену систему лишків за модулем ab.

19. Користуючись результатом задачі 18, довести мультиплікативність функції Ейлера.

ІСТОРИЧНІ КОМЕНТАРІ

Теорему, доведену в § 19, на відміну від так званої великої теореми Ферма (див. історичні коментарі до розд. VIII), називають малою теоремою Ферма. Перше з відомих доведень цієї теореми належить видатному німецькому математику і філософу Лейбніцу (1646 — 1716). Завдяки цій теоремі за допомогою електронно-лічильних машин було вивчено подільність чисел $2^{p-1} - 1$ на p^2 при $p < 50\,000$. З'ясувалось, що $2^{p-1} - 1$ — ділиться на p^2 лише для $p = 1093$ і 3511. Ейлер дав кілька різних доведень теореми Ферма, з яких перше було дано до 1736 р. У 1760 р. Ейлер узагальнив теорему Ферма. Цю узагальнену теорему і називають теоремою Ейлера.

Доведено, що для будь-якого натурального числа a існує безліч складених чисел m, таких, що $a^{m-1} = 1 \pmod m$.

Невідомо, чи є нескінченною множина складених чисел m, таких, що $a^{m-1} \equiv 1 \pmod m$ для всіх a, взаємно простих з m, якщо їх задовольняють ті самі значення невідомого x.

Розділ IV

КОНГРУЕНЦІЇ З НЕВІДОМОЮ ВЕЛИЧИНОЮ[1]

§ 20. Класи розв'язків конгруенції довільного степеня

Нехай m — натуральне число. Конгруенція виду

$$f(x) \equiv 0 \pmod m, \qquad (1)$$

де $f(x) = a_0x^n + a_1x^{n-1} + \cdots + a_{n-1}x + a_n$ є многочлен степеня n з цілими коефіцієнтами і $a_0 \not\equiv 0 \pmod m$, називається *алгебраїчною конгруенцією n-го степеня з одним невідомим x.*

Розв'язати конгруенцію — це означає знайти всі значення невідомого x, які її задовольняють.

Дві конгруенції з одним невідомим називаються *рівносильними*, або *еквівалентними*, якщо їх задовольняють ті самі значення невідомого x.

Теорема 1. *Якщо $x = x_1$ задовольняє конгруенцію* (1), *то всяке число, яке належить до того самого класу лишків за модулем m, що й число x_1, також задовольняє цю конгруенцію*, тобто *розв'язком буде весь клас чисел $x \equiv x_1 \pmod m$.*

Це твердження безпосередньо випливає з властивостей конгруенцій. Справді, нехай x_2 — будь-яке число, яке належить до того самого класу лишків за модулем m, що й x_1; тоді $x_2 \equiv x_1 \pmod m$. За умовою x_1 є розв'язок конгруенції (1), тобто має місце тотожна конгруенція $f(x_1) \equiv 0 \pmod m$, але тоді матиме місце й конгруенція $f(x_2) \equiv 0 \pmod m$ (див. висновок з теореми 2, § 15), тобто x_2 також буде розв'язком конгруенції. Оскільки x_2 — будь-яке число класу $x \equiv x_1 \pmod m$, то весь цей клас задовольнятиме дану конгруенцію.

Розв'язки конгруенції (1), що належать до одного класу чисел за модулем m вважають за один розв'язок цієї конгруенції. При цьому конгруенція (1) має стільки розв'язків, скільки класів чисел її задовольняють. Через те що за модулем m всього m класів чисел, то за допомогою скінченного числа випробувань можна знайти всі розв'язки конгруенції (1), але при великому модулі це досить важко.

Приклад. Розглянемо конгруенцію

$$x^4 + x^3 + x^2 + x + 1 \equiv 0 \pmod 5.$$

Розв'язки цієї конгруенції за модулем 5 містяться тільки серед чисел повної системи лишків за модулем 5, тобто, наприклад, серед чисел 0, 1, 2, 3, 4. Безпосередньою перевіркою встановлюємо, що тільки $x = 1$ задовольняє задану конгруенцію, тому розв'язком цієї конгруенції буде клас чисел $x \equiv 1 \pmod 5$, тобто $x = 1 + 5t$, де t — будь-яке ціле число. Отже, задана конгруенція четвертого степеня за модулем 5 має лише один розв'язок.

[1] Подібно до того, як рівності поділяють на тотожності і рівняння, серед конгруенцій також можна розрізняти тотожні (такі, що зовсім не містять букв, або справджуються при довільних означеннях букв, які входять до них) і такі, що містять невідомі (тобто такі величини, які лише за певних значень їх задовольняють конгруенцію).

За властивостями конгруенцій до обох частин конгруенції можна додавати і від обох частин віднімати числа, кратні модулю. Тому в даній конгруенції завжди можна коефіцієнти замінити їхніми найменшими невід'ємними або абсолютно найменшими лишками за модулем, що дорівнює модулю конгруенції. Інакше кажучи, коефіцієнти конгруенції завжди можна зробити за абсолютною величиною меншими від модуля m, а, за бажанням, можна зробити їх тільки додатними, меншими від m.

Приклад. Конгруенція

$$8x^5 - 12x^3 - 13x^2 - 15x + 6 \equiv 0 \pmod 5$$

еквівалентна конгруенції

$$3x^5 - 2x^3 - 3x^2 + 1 \equiv 0 \pmod 5,$$

або конгруенції

$$3x^5 + 3x^3 + 2x^2 + 1 \equiv 0 \pmod 5.$$

Щоб знайти розв'язки останної конгруенції, випробуємо, наприклад, абсолютно найменші лишки за модулем 5: 0, 1, 2, —2, —1. Безпосередньо видно, що 0, 1, —1 задану конгруенцію не задовольняють. При дальшому випробуванні можна скористатись схемою Горнера з тією тільки відмінністю, що для полегшення кожного разу можна відкидати числа, кратні модулю

	3	0	3	2	0	1
2	3	$6 \equiv 1$	$5 \equiv 0$	2	4	$9 \equiv 4$
—2	3	$6 \equiv -1$	$5 \equiv 0$	2	—4	$9 \equiv 4$

Отже, конгруенція $3x^5 + 3x^3 + 2x^2 + 1 \equiv 0 \pmod 5$ не має розв'язків, а тому не має розв'язків і конгруенція

$$8x^5 - 12x^3 - 13x^2 - 15x + 6 \equiv 0 \pmod 5.$$

При розв'язуванні конгруенції з невідомою величиною іноді доводиться помножати обидві частини конгруенції на ціле число. Для тотожних конгруенцій ця операція, як раніш було показано, завжди законна. Для конгруенцій з невідомою величиною таке перетворення не завжди законне, тобто, інакше кажучи, при такому перетворенні конгруенції може порушитись еквівалентність даної і добутої конгруенцій.

Приклад. Конгруенція

$$x^4 + x^3 + x^2 + x + 1 \equiv 0 \pmod 5,$$

як ми бачили, має один розв'язок: $x \equiv 1 \pmod 5$. Але, якщо обидві частини цієї конгруенції помножити на 5, то дістанемо конгруенцію:

$$5x^4 + 5x^3 + 5x^2 + 5x + 5 \equiv 0 \pmod 5,$$

розв'язком якої буде вже будь-яке ціле число. Вона, по суті, перетворюється в тотожну конгруенцію $0 \cdot x \equiv 0 \pmod 5$.

Отже, виникає питання, коли множення обох частин конгруенції з невідомою величиною на ціле число є законним? Відповідь на це дає теорема 2.

Теорема 2. *Якщо обидві частини конгруенції* (1) *помножити на ціле число k, взаємно просте з модулем m, то дістанемо конгруенцію, еквівалентну даній.*

Справді, припустимо, що $x = \alpha$ задовольняє конгруенцію (1), тоді

$$f(\alpha) \equiv 0 \pmod m.$$

Помножаючи обидві частини цієї тотожної конгруенції на k, дістанемо:

$$k \cdot f(\alpha) \equiv 0 \pmod m. \qquad (2)$$

Отже, α завдовольняє конгруенцію

$$k \cdot f(x) \equiv 0 \pmod m. \qquad (3)$$

Навпаки, якщо $x = \alpha$ задовольняє конгруенцію (3), тобто $k \cdot f(\alpha) \equiv 0 \pmod m$, тоді обидві частини конгруенції (2) можна скоротити на k, не змінюючи модуля, бо $(k, m) = 1$ (див. властивість 4, § 15), отже,

$$f(\alpha) \equiv 0 \pmod m,$$

тобто α задовольняє конгруенцію (1), що й доводить наше твердження.

Зауважимо, що при розв'язуванні конгруенцій з невідомою величиною можна, *не змінюючи модуля*, скорочувати обидві частини конгруенції тільки на такий їх спільний дільник, який взаємно простий з модулем (див. властивість 4, § 15).

Далі в цьому розділі ми докладніше розглянемо конгруенції з одним невідомим і покажемо, зокрема, що теорія конгруенцій з одним невідомим багато в чому нагадує теорію алгебраїчних рівнянь з одним невідомим.

Контрольні запитання:

1. Дайте означення алгебраїчної конгруенції n-го степеня з одним невідомим.
2. Яке число називається розв'язком конгруенції?

3. Які конгруенції називаються еквівалентними?
4. Які розв'язки конгруенцій не вважаються різними?
5. Чи завжди при множенні обох частин конгруенції на ціле число дістаємо еквівалентну конгруенцію?
6. Чи дістанемо еквівалентні конгруенції при множенні обох частин конгруенції і модуля на ціле число?

§ 21. Конгруенції першого степеня. Поле класів за простим модулем

Конгруенцію першого степеня після перенесення вільних членів у праву частину, а членів, що містять невідоме x,— у ліву частину, завжди можна подати в такому вигляді:

$$ax \equiv b \pmod m, \quad a \not\equiv 0 \pmod m. \qquad (1)$$

Визначимо спочатку, при яких умовах ця конгруенція має розв'язки і якщо має, то скільки.

Випадок 1. Припустимо, що в конгруенції (1) $(a, m) = 1$; тоді на підставі властивостей повної системи лишків (властивість 2, § 17) можемо твердити, що коли x пробігає повну систему лишків за модулем m, то ax так само пробігатиме повну систему лишків за цим модулем. Отже, зокрема, при одному і тільки одному значенні $x = x_0$ з повної системи лишків матимемо тотожну конгруенцію $ax_0 \equiv b \pmod m$. Цим ми довели таку теорему.

Теорема 1. *Якщо $(a, m) = 1$, то конгруенція* (1) *має єдиний розв'язок.*

Випадок 2. Припустимо, що $(a, m) = d > 1$, тоді $a = a_1 d$, $m = m_1 d$ і $(a_1, m_1) = 1$. Через те що в конгруенції (1) a і m діляться на d, то для того щоб конгруенція мала місце при деяких цілих x, і b повинно ділитись на d (див. властивість 9, § 15). Отже, ми можемо записати, що $b = b_1 d$.

Якщо b не ділиться на d, то конгруенція не має розв'язків. Скорочуючи обидві частини конгруенції (1) і модуль на d, дістанемо *нову конгруенцію:*

$$a_1 x \equiv b_1 \pmod{m_1}, \qquad (2)$$

де $(a_1, m_1) = 1$, *рівносильну даній.*

Справді, нехай $x = \alpha$ задовольняє конгруенцію (1), тоді маємо тотожну конгруенцію: $a\alpha \equiv b \pmod m$. Скорочуючи тепер обидві частини і модуль цієї конгруенції на d, дістанемо нову тотожну конгруенцію

$$a_1 \alpha \equiv b_1 \pmod{m_1}, \text{ де } (a_1, m_1) = 1,$$

яка й показує, що α задовольняє конгруенцію (2). Навпаки, нехай β задовольняє конгруенцію (2), тобто $a_1\beta \equiv b_1 \pmod{m_1}$. Помножаючи цю тотожну конгруенцію і модуль на d, дістанемо: $a\beta \equiv b \pmod m$. Остання тотожна конгруенція показує, що β задовольняє конгруенцію (1).

Далі, конгруенція (2), за доведеним, має єдиний розв'язок за модулем m_1; нехай цим розв'язком буде клас чисел $x \equiv x_0 \pmod{m_1}$, де x_0 — найменший невід'ємний лишок цього класу. Внаслідок еквівалентності конгруенцій (1) і (2), цей клас буде також і розв'язком конгруенції (1) за модулем m, але за модулем $m = m_1 d$ він розпадеться на кілька класів, а саме на стільки, скільки в ньому буде додатних чисел, менших за m; цими числами, очевидно, будуть такі d чисел:

$$x_0,\ x_0 + m_1,\ x_0 + 2m_1,\ \ldots,\ x_0 + (d-1)\,m_1, \qquad (3)$$

бо $0 \leqslant x_0 < m_1$.

Оскільки d чисел виду (3) менші за m і різні, то вони не конгруентні між собою за модулем m. Тому один клас за модулем m_1 розпадеться на d класів за модулем $m = m_1 d$. Отже, конгруенція (1) матиме d розв'язків

$$x \equiv x_0,\ x_0 + m_1,\ x_0 + 2m_1,\ \ldots,\ x_0 + (d-1)\,m_1 \pmod{m}. \qquad (3')$$

Зауважимо, що ці d класів за модулем m і клас $x \equiv x_0 \pmod{m_1}$ складаються з одних і тих самих цілих чисел.

Цим ми довели таке твердження:

Теорема 2. *Якщо $(a, m) = d > 1$ і b ділиться на d, то конгруенція (1) має d розв'язків виду (3'); якщо ж у цьому випадку b не ділиться на d, то конгруенція (1) розв'язків не має.*

Отже, для знаходження розв'язків конгруенції

$$ax \equiv b \pmod{m} \qquad (1)$$

досить, очевидно, вміти знаходити розв'язок цієї конгруенції, коли $(a, m) = 1$.

При невеликому m розв'язок конгруенції можна знайти випробуванням чисел повної системи лишків за модулем m; найзручніше за повну систему лишків брати або найменші невід'ємні лишки, або абсолютно найменші лишки. Але цей спосіб при великому m стає дуже громіздким. Вкажемо два інших, практично зручніших способи.

Спосіб 1 грунтується на теоремі Ейлера. Нехай треба розв'язати конгруенцію (1), якщо $(a, m) = 1$. Помножаючи цю конгруенцію на $a^{\varphi(m)-1}$, дістанемо еквівалентну конгруенцію:

$$a^{\varphi(m)} \cdot x \equiv b a^{\varphi(m)-1} \pmod{m} \qquad (4)$$

(див. теорему 2, § 20). Але, за теоремою Ейлера, при $(a, m) = 1$ $a^{\varphi(m)} \equiv 1 \pmod{m}$, отже, з конгруенції (4) матимемо:

$$x \equiv b a^{\varphi(m)-1} \pmod{m}. \qquad (4')$$

Цей розв'язок конгруенції (4) і буде єдиним розв'язком еквівалентної їй конгруенції (1).

Приклад. Розв'язати конгруенцію

$$37x \equiv 28 \pmod{24}.$$

Спочатку замінимо коефіцієнти їх найменшими невід'ємними лишками за модулем 24 (див. висновок 3 з властивості 2, § 15):

$$13x \equiv 4 \pmod{24}.$$

Через те що $(13,24) = 1$, ця конгруенція має єдиний розв'язок. Знайдемо його за формулою (4'):

$$x \equiv 4 \cdot 13^{\varphi(24)-1} = 4 \cdot 13^{8-1} = 4 \cdot 13\,(13^2)^3 \equiv 4 \cdot 1^3 \equiv 4 \pmod{24}.$$

Отже, $x \equiv 4 \pmod{24}$ є шуканим розв'язком цієї конгруенції, у чому легко переконатись звичайною підстановкою:

$$13 \cdot 4 \equiv 4 \pmod{24}.$$

Недоліком цього способу є те, що при великому $\varphi(m)$ знаходження найменшого невід'ємного лишку того класу чисел за модулем m, в якому є число $ba^{\varphi(m)-1}$, стає громіздким.

Спосіб 2 розв'язування конгруенції (1) при $(a, m) = 1$ грунтується на теорії неперервних дробів.

Розкладемо $\frac{m}{a}$ в неперервний дріб (при цьому зауважимо, що a завжди можна вважати додатним і меншим за m). Позначимо через $\frac{P_{n-1}}{Q_{n-1}}$ передостанній, а через $\frac{P_n}{Q_n}$ — останній підхідний дріб у цьому розкладі, так що $\frac{P_n}{Q_n} = \frac{m}{a}$. Через те що будь-який неперервний дріб є нескоротний і, за умовою, $(a, m) = 1$, то матимемо, що $m = P_n$, $a = Q_n$. Згідно з відомою властивістю підхідних дробів (див. теорему 2, § 9):

$$P_n Q_{n-1} - P_{n-1} Q_n = (-1)^{n-1}.$$

Замінюючи P_n і Q_n відповідно через m і a дістанемо:

$$mQ_{n-1} - aP_{n-1} = (-1)^{n-1}.$$

Ця рівність еквівалентна конгруенції (див. теорему 1, § 16).

$$aP_{n-1} \equiv (-1)^n \pmod{m}.$$

Помножаючи обидві частини останньої конгруенції на $(-1)^n \cdot b$, дістаємо:

$$a\,[(-1)^n P_{n-1} b] \equiv b \pmod{m}.$$

Порівнюючи цю тотожну конгруенцію з заданою конгруенцією (1), бачимо, що

$$x \equiv (-1)^n P_{n-1} b \pmod{m} \qquad (5)$$

є розв'язком конгруенції (1); тут P_{n-1} — чисельник передостаннього підхідного дробу в розкладі $\frac{m}{a}$ у неперервний дріб.

Зауваження. Конгруенція (1) еквівалентна рівнянню першого степеня з двома невідомими: $ax = b + my$, або $ax - my = b$. Тому розв'язання конгруенції (1) можна звести до розв'язання в цілих числах рівняння $ax - my = b$ і навпаки. Ми бачили, що це рівняння має розв'язки, якщо $(a, m) = 1$, або якщо b ділиться на (a, m) (див. § 9). Невизначені рівняння першого степеня почали записувати і розв'язувати у формі конгруенцій, починаючи з Гаусса.

Приклад. Розв'язати конгруенцію $105x = 75 \pmod{125}$.

Маємо $(105, 125) = 5$ і 75 ділиться на 5, тому дана конгруенція має 5 розв'язків. Скорочуючи обидві частини конгруенції і модуль на 5, дістанемо конгруенцію:

$$21x \equiv 15 \pmod{25}. \qquad (6)$$

Розкладаючи $\frac{25}{21}$ у неперервний дріб, дістанемо: $\frac{25}{21} = [1, 5, 4]$. Знаходимо:

k		0	1	2
q_k		1	5	4
P_k	1	1	6	25

Звідси $n = 2$; $P_{n-1} = P_1 = 6$; за формулою (5) дістаємо розв'язок конгруенції (6):

$$x \equiv 6 \cdot 15 \equiv 15 \pmod{25}.$$

Звідси задана конгруенція $105x = 75 \pmod{125}$ матиме п'ять таких розв'язків: $x \equiv 15, 40, 65, 90, 115 \pmod{125}$. Тут кожний розв'язок, згідно з доведенням теореми 2, виходить з попереднього додаванням $m_1 = \frac{m}{d} = 25$.

Далі доведемо таке твердження.

Теорема 3. *Сукупність усіх класів чисел за простим модулем p утворює скінченне поле щодо встановлених раніше операцій додавання і множення класів.*

Нагадаємо, що *полем* називається таке комутативне кільце P, в якому існує принаймні один елемент, відмінний від нуля, і в якому розв'язується рівняння $ax = b$ при будь-яких елементах $a \neq 0$ і b з P. У § 16 було показано, що сукупність усіх класів чисел за простим модулем утворює комутативне кільце без дільників нуля. Лишається показати, що в цьому кільці рівняння

$$C_a \cdot C_x = C_b$$

розв'язне для будь-яких класів

$$C_a \neq C_0 \text{ і } C_b.$$

Через те що $C_a \neq C_0$, то $a \not\equiv 0 \pmod{p}$ і конгруенція

$$ax \equiv b \pmod{p},$$

за теоремою 1, матиме єдиний розв'язок $x \equiv x_0 \pmod{p}$.

Цей розв'язок і утворює клас чисел C_{x_0} з лишком x_0, що задовольняє рівняння:

$$C_a \cdot C_x = C_{ax} = C_b,$$

бо $ax_0 \equiv b \pmod{p}$ і, отже, лишки ax_0 і b належать до одного й того самого класу $C_{ax_0} = C_b$. Цим теорему доведено.

Зауваження. Якщо модуль — число складене, то сукупність класів чисел поля вже не утворює, бо однією з найхарактерніших властивостей поля є відсутність у ньому дільників нуля [1], а в § 16 ми довели, що сукупність усіх класів чисел за складеним модулем утворює комутативне кільце з дільниками нуля.

Контрольні запитання

1. При якій умові розв'язується конгруенція першого степеня з одним невідомим?
2. Скільки розв'язків має конгруенція $ax \equiv b \pmod{m}$, якщо вона розв'язна?
3. Як знайти усі розв'язки конгруенції $ax \equiv b \pmod{m}$ при умові $(a, m) = d > 1$, коли відомо один розв'язок цієї конгруенції?
4. Написати формулу для знаходження розв'язків конгруенції першого степеня, яка грунтується на застосуванні неперервних дробів, і пояснити зміст букв, що входять до неї.
5. Чи утворює поле сукупність усіх класів чисел за складеним модулем? Чому?
6. Яким конгруенціям еквівалентне рівняння $ax + by = c$?

§ 22. Система конгруенцій першого степеня

Обмежимося системою конгруенцій:

$$\begin{cases} a_1x \equiv b_1 \pmod{m_1}; & (a_1, m_1) = 1, \\ a_2x \equiv b_2 \pmod{m_2}; & (a_2, m_2) = 1, \\ \dots\dots\dots\dots\dots\dots \\ a_kx \equiv b_k \pmod{m_k}; & (a_k, m_k) = 1 \end{cases}$$

з одним невідомим, але різними модулями [2].

Розв'язати систему конгруенцій з одним невідомим — означає знайти такі цілі значення невідомого x, які задовольняли б усі конгруенції цієї системи.

[1] Справді, нехай $ab = 0$; і $a \neq 0$; у полі є обернений елемент a^{-1} до елемента a, тобто такий, що $a^{-1}a = a \cdot a^{-1} = 1$. Помножаючи тепер рівність $ab = 0$ на a^{-1}, дістанемо, що $b = 0$. Це й означає, що будь-яке поле не має дільників нуля.

[2] Цей випадок не має аналогії в теорії алгебраїчних рівнянь.

Дві системи конгруенцій з невідомим x називають *рівнозначними* (або *еквівалентними*), якщо їх задовольняють ті самі значення невідомого x. Якщо $x \equiv \alpha$ за деяким модулем задовольняють систему (1), то весь цей клас чисел вважатимемо за один розв'язок цієї системи. Якщо ця система має хоча б один розв'язок, то вона називається сумісною.

Насамперед зауважимо, що, розв'язуючи окремо кожну з конгруенцій (1), матимемо систему, еквівалентну заданій:

$$\begin{cases} x \equiv c_1 \pmod{m_1}, \\ x \equiv c_2 \pmod{m_2}, \\ \dots\dots\dots \\ x \equiv c_k \pmod{m_k}. \end{cases} \qquad (2)$$

Отже, досить уміти розв'язувати систему конгруенцій (2).

Неважко показати, що *коли система* (2) *сумісна, то вона має єдиний розв'язок за модулем* M, *що дорівнює найменшому спільному кратному чисел* $m_1, m_2, \dots, m_k$.

Справді, припустимо, що α і β — будь-які два розв'язки системи (2), тоді:

$$\alpha \equiv c_i \pmod{m_i} \text{ і } \beta \equiv c_i \pmod{m_i} \quad (i = 1, 2, \dots, k).$$

Звідси $\alpha \equiv \beta \pmod{m_i}$, тобто різниця $\alpha - \beta$ ділитиметься на числа $m_1, m_2, \dots, m_k$, отже, вона ділитиметься і на їхнє найменше спільне кратне $M = [m_1, m_2, \dots, m_k]$.

Таким чином, $\alpha \equiv \beta \pmod{M}$, а такі розв'язки не вважаються різними.

Розглянемо спочатку окремий випадок, коли модулі $m_1, m_2, \dots, m_k$ системи (2) попарно взаємно прості.

Теорема 1. *Якщо модулі* $m_1, m_2, \dots, m_k$ *попарно взаємно прості, то система конгруенцій (2) має єдиний розв'язок:*

$$x \equiv x_0 \pmod{m_1, m_2 \dots m_k}, \qquad (3)$$

де

$$x_0 = M_1 y_1 c_1 + M_2 y_2 c_2 + \dots + M_k y_k c_k,$$

причому числа M_i і y_i *визначаються з умов:*

$$M_i = \frac{m_1 m_2 \dots m_k}{m_i} = \frac{M}{m_i}, \quad M_i y_i \equiv 1 \pmod{m_i} \quad (i = 1, 2, \dots, k). \qquad (4)$$

Справді, підставляючи значення x_0 в конгруенцію системи (2) $x \equiv c_i \pmod{m_i}$ $(i = 1, 2, \dots, k)$ і беручи до уваги, що всі $M_i \neq M_i$, згідно з (4), діляться на m_i, і конгруенція $M_i y_i \equiv 1 \pmod{m_i}$ має єдиний розв'язок щодо y_i, бо $(M_i, m_i) = 1$, дістанемо:

$$x_0 \equiv M_i y_i c_i \equiv c_i \pmod{m_i},$$

тобто x_0, визначене вказаним способом, задовольняє будь-яку конгруенцію системи (2), а тому і всю цю систему. Тим самим показано,

що x_0 є єдиним розв'язком системи (2) за модулем $M = m_1 m_2 \dots m_k$, бо найменше спільне кратне попарно взаємно простих чисел дорівнює їхньому добутку.

Приклад. Знайти число, яке при діленні на 17, 13 і 10 дає відповідно остачі 15, 11 і 3.

Позначимо шукане число через x, тоді задача зведеться до розв'язання такої системи конгруенцій:

$$\begin{cases} x \equiv 15 \pmod{17}, \\ x \equiv 11 \pmod{13}, \\ x \equiv 3 \pmod{10}. \end{cases}$$

Маємо

$$M = 17 \cdot 13 \cdot 10 = 2210,$$

$$M_1 = \frac{2210}{17} = 130, \quad M_2 = \frac{2210}{13} = 170, \quad M_3 = \frac{2210}{10} = 221.$$

Розв'язуючи допоміжні конгруенції

$$130 y_1 \equiv 1 \pmod{17}, \quad 170 y_2 \equiv 1 \pmod{13} \text{ і } 221 y_3 \equiv 1 \pmod{10},$$

дістанемо:

$$y_1 = 14, \quad y_2 = 1, \quad y_3 = 1.$$

Отже, за теоремою 1,

$$x \equiv x_0 = 130 \cdot 14 \cdot 15 + 170 \cdot 1 \cdot 11 + 211 \cdot 1 \cdot 3 = 29\,833 = 1103 \pmod{2210}$$

буде розв'язком заданої системи конгруенцій. Звідси випливає, що найменшим натуральним числом, яке задовольняє умову задачі, буде $x = 1103$.

У загальному випадку, коли модулі $m_1, m_2 \dots, m_k$ *можуть і не бути попарно взаємно простими*, систему (2) можна розв'язати так.

З першої конгруенції системи (2) випливає, що всі значення x, які його задовольняють, матимуть форму $x = c_1 + m_1 t_1$, де t_1 пробігає всі цілі числа. Щоб вибрати з них значення x, які б задовольняли й другу конгруенцію, визначимо t_1 з умови, що

$$c_1 + m_1 t_1 \equiv c_2 \pmod{m_2},$$

або

$$m_1 t_1 \equiv c_2 - c_1 \pmod{m_2}.$$

Ця конгруенція першого степеня щодо t_1 матиме розв'язки, якщо $c_2 - c_1$ ділиться на (m_1, m_2); інакше ця остання конгруенція не має розв'язків, а значить система (2) несумісна. Нехай $c_2 - c_1$ ділиться на (m_1, m_2). Розв'язуючи цю конгруенцію, дістанемо:

$$t_1 \equiv t_1' \left(\mathrm{mod} \frac{m_2}{(m_1, m_2)} \right).$$

Тоді сукупність усіх значень t_1, що задовольняють другу конгруенцію, буде:

$$t_1 = t_1' + \frac{m_2}{(m_1, m_2)} t_2,$$

де t_2 пробігає всі цілі числа. Звідси дістанемо:

$$x = c_1 + m_1 t_1' + \frac{m_1 m_2}{(m_1, m_2)} t_2 = y_2 + [m_1, m_2] t_2, \qquad (5)$$

де $y_2 = c_1 + m_1 t_1$ задовольнятимуть перші дві конгруенції. Тепер з чисел (5), аналогічно, виберемо ті, які задовольнятимуть третю конгруенцію. Так знову, або прийдемо до конгруенції відносно t_2, яка не має розв'язків, а значить система (2) несумісна, або знайдемо, що значення

$$x = y_3 + [m_1, m_2, m_3] t_3,$$

де t_3 — ціле, або

$$x \equiv y_3 \pmod{[m_1, m_2, m_3]}$$

задовольнятимуть перші три конгруенції і т. д. Якщо така система (2) сумісна, то, зрештою, за доведеним на початку цього параграфа, прийдемо до єдиного розв'язку цієї системи за модулем

$$[m_1, m_2, \ldots, m_k].$$

Приклад. Розв'язати систему конгруенцій:

$$\begin{cases} x \equiv 2 \pmod{15}, \\ x \equiv 7 \pmod{20}, \\ x \equiv 12 \pmod{35}. \end{cases}$$

З першої конгруенції маємо $x = 2 + 15t_1$, де t_1 — ціле число. Щоб визначити t_1, підставимо значення x у другу конгруенцію; тоді матимемо:

$$15t_1 \equiv 5 \pmod{20}$$

або, скорочуючи на 5, знайдемо:

$$3t_1 \equiv 1 \pmod 4.$$

Звідси $t_1 \equiv 3 \pmod 4$ або $t_1 = 3 + 4t_2$, де t_2 — будь-яке ціле число. Тепер

$$x = 2 + 15t_1 = 47 + 60t_2$$

задовольнятиме дві перші конгруенції. З цих чисел x виберемо такі, які б задовольняли й третю конгруенцію; для цього визначимо t_2 з умови:

$$47 + 60t_2 \equiv 12 \pmod{35},$$

звідси випливає:

$$25t_2 = 0 \pmod{35}, \quad 5t_2 \equiv 0 \pmod 7, \quad t_2 \equiv 0 \pmod 7,$$

або $t_2 = 7t$, де t — будь-яке ціле.

Отже, розв'язком даної системи буде $x = 47 + 420t$ або $x \equiv 47 \pmod{420}$.

Тепер зауважимо, що коли в системі (1) $(a_i, m_i) = d_i > 1$ для деяких $i = 1, 2, \ldots, k$ і b_i ділиться на d_i, тоді i-та конгруенція системи (1) матиме d_i розв'язків, і ми дістанемо кілька систем конгруенцій виду (2); тому система (1) матиме кілька розв'язків. Для складання систем виду (2) треба кожен розв'язок однієї конгруенції системи (1) скомбінувати з кожним розв'язком решти конгруенцій цієї системи[1].

Приклад. Розв'язати систему конгруенцій:

$$\begin{cases} 14x \equiv 12 \pmod{18}; \\ x \equiv 5 \pmod{25}. \end{cases}$$

Перша конгруенція має два розв'язки:

$$\begin{cases} x \equiv 6 \pmod{18}; \\ x \equiv 15 \pmod{18}. \end{cases}$$

Отже, розв'язування цієї системи конгруенцій зводиться до розв'язання таких двох систем:

$$\begin{cases} x \equiv 6 \pmod{18}, \\ x \equiv 5 \pmod{25}; \end{cases} \qquad \begin{cases} x \equiv 15 \pmod{18}, \\ x \equiv 5 \pmod{25}; \end{cases}$$

Розв'яжемо першу систему; дістанемо:

$$x \equiv 6 \pmod{18},$$

звідси

$$x = 6 + 18t_1; \quad 6 + 18t_1 \equiv 5 \pmod{25};$$

отже,

$$t_1 \equiv 18 \pmod{25},$$

або

$$t_1 = 18 + 25t; \quad x = 6 + 18(18 + 25t) = 330 + 450t,$$

тобто

$$x \equiv 330 \pmod{450}.$$

Розв'язуючи аналогічно другу систему, дістанемо:

$$x \equiv 105 \pmod{450}.$$

Отже, ця система конгруенцій має два розв'язки:

$$x = 105, 330 \pmod{450}.$$

---

[1] Якщо позначимо через $S_1, S_2, \ldots, S_k$ число розв'язків, які відповідають конгруенціям системи (1), а через S — число розв'язків цієї системи, то

$$S = S_1 S_2 \ldots S_k.$$

Контрольні запитання

1. Дайте означення розв'язку системи конгруенції 1-го степеня з одним невідомим?
2. Які системи конгруенцій називаються еквівалентними?
3. За яким модулем визначають розв'язок системи конгруенцій (2)?
4. Напишіть формулу для розв'язання системи конгруенцій (2), якщо модулі попарно взаємно прості. Поясніть зміст букв, які входять до формули.
5. Чи застосовний другий спосіб для розв'язання системи конгруенцій, якщо модулі попарно взаємно прості?
6. Як з розв'язків першої конгруенції системи (2) знайти числа, які задовольняють другу систему?
7. Чи може система конгруенцій першого степеня з одним невідомим не мати розв'язків або мати більш як один розв'язок? У якому випадку?

§ 23. Зведення конгруенцій за складеним модулем до системи конгруенцій за простими модулями

Теорема 1. *Якщо* $m_1, m_2, \ldots, m_k$ *— попарно взаємно прості числа, то конгруенція*

$$f(x) = a_0x^n + a_1x^{n-1} + \ldots + a_{n-1}x + a_n \equiv 0 \pmod{m_1m_2 \ldots m_k} \quad (1)$$

еквівалентна системі конгруенцій:

$$\begin{cases} f(x) \equiv 0 \pmod{m_1}, \\ f(x) \equiv 0 \pmod{m_2}, \\ \ldots\ldots\ldots \\ f(x) \equiv 0 \pmod{m_k}. \end{cases} \quad (2)$$

При цьому, позначаючи через

$$S_1, S_2, \ldots, S_k$$

числа розв'язків окремих конгруенцій (2) за відповідними модулями і через S *— число розв'язків конгруенції* (1), матимемо:

$$S = S_1S_2 \ldots S_k.$$

Перша частина твердження безпосередньо випливає з властивостей 8 і 7, § 15. Справді, нехай α задовольняє конгруенцію (1), тобто

$$f(\alpha) \equiv 0 \pmod{m_1m_2 \ldots m_k},$$

а звідси й поготів

$$f(\alpha) \equiv 0 \pmod{m_i},$$

тобто α — задовольняє будь-яку конгруенцію системи (2).

Навпаки, якщо β задовольняє систему конгруенцій (2), то матимуть місце тотожні конгруенції:

$$f(\beta) \equiv 0 \pmod{m_i} \quad (i = 1, 2, \ldots, k).$$

Але тоді (див. властивість 7, § 6) ця конгруенція матиме місце і за модулем, який дорівнює найменшому спільному кратному чисел $m_1, m_2, \ldots, m_k$, тобто, зважаючи на те, що вони попарно взаємно прості, за модулем $m_1m_2 \ldots m_k$:

$$f(\beta) \equiv 0 \pmod{m_1m_2 \ldots m_k};$$

це означає, що β також задовольняє конгруенцію (1).

Друге твердження випливає з таких міркувань: припустимо, що

$$x \equiv \alpha_i \pmod{m_i}$$

є будь-який розв'язок конгруенції

$$f(x) \equiv 0 \pmod{m_i},$$

тоді завжди можна знайти єдине число x_1 (див. теорему 1, § 22), яке є розв'язком системи лінійних конгруенцій:

$$\begin{cases} x \equiv \alpha_1 \pmod{m_1}, \\ x \equiv \alpha_2 \pmod{m_2}, \\ \ldots\ldots\ldots \\ x \equiv \alpha_k \pmod{m_k}. \end{cases} \quad (3)$$

Число x_1 визначається за модулем $m = m_1m_2 \ldots m_k$; воно буде розв'язком системи (2), а, отже, і конгруенції (1). Але, комбінуючи кожен розв'язок однієї конгруенції з системи (2) з кожним розв'язком решти конгруенцій, ми, очевидно, дістанемо $S_1S_2 \ldots S_k = S$ лінійних систем конгруенцій типу (3). Кожна така система має єдиний розв'язок, який є розв'язком як системи (2), так і конгруенції (1), отже, цим і доведено другу частину теореми.

Висновок 1. *Якщо хоч одна з конгруенцій системи* (2) *не має розв'язків, то й задана конгруенція* (1) *також не матиме розв'язків.*

Висновок 2. *Дослідження і розв'язування конгруенції*

$$f(x) \equiv 0 \pmod{m},$$

де $m = p_1^{\alpha_1}p_2^{\alpha_2} \ldots p_k^{\alpha_k}$ *— канонічний розклад модуля* m, *зводиться до дослідження і розв'язування конгруенцій*: $f(x) \equiv 0 \pmod{p_i^{\alpha_i}}$ $(i = 1, 2, \ldots, k)$ [1]. Це випливає з того, що числа $p_1^{\alpha_1}, p_2^{\alpha_2}, \ldots, p_k^{\alpha_k}$ попарно взаємно прості.

Отже, все зводиться до того, що доводиться окремо досліджувати і розв'язувати конгруенції виду

$$f(x) \equiv 0 \pmod{p^\alpha}, \quad (4)$$

---

[1] З цієї причини в теорії конгруенцій звичайно приймають, що модуль конгруенції — просте число або степінь простого числа.

де p — просте число, α — ціле додатне число. Зауважимо, що всякий розв'язок конгруенції (4) буде розв'язком конгруенції

$$f(x) \equiv 0 \pmod{p}. \tag{5}$$

Очевидно, якщо конгруенція (5) не має розв'язків, то й конгруенція (4) розв'язків не матиме. Справді, якщо $f(x)$ не ділиться на p, то $f(x)$ і поготів не ділитиметься на p^α, тобто

$$f(x) \not\equiv 0 \pmod{p^\alpha}$$

ні при якому цілому x.

Теорема 2. *Всякий розв'язок*

$$x \equiv x_1 \pmod{p}$$

конгруенції (5) *при умові, що* $f'(x_1)$ *не ділиться на* p, *дає один єдиний розв'язок конгруенції* (4).

Припустимо, що $x \equiv x_1 \pmod{p}$ є будь-який розв'язок конгруенції (5), тоді $x = x_1 + pt_1$, де t_1 — будь-яке ціле число. З цього класу чисел вибиратимемо ті, які задовольняли б конгруенцію.

$$f(x) \equiv 0 \pmod{p^2}. \tag{6}$$

Для визначення t_1 підставимо в конгруенцію (6) значення $x = x_1 + pt_1$ і розкладемо ліву частину за формулою Тейлора[1]. Враховуючи, що коефіцієнти $\frac{f^k(x_1)}{k!}$ в цьому розкладі будуть цілими, і відкидаючи члени, кратні p^2, дістаємо:

$$f(x_1) + pt_1 f'(x_1) \equiv 0 \pmod{p^2}.$$

Через те що

$$f(x_1) \equiv 0 \pmod{p}$$

за умовою, то, скорочуючи обидві частини утвореної конгруенції і модуль на p, дістанемо конгруенцію першого степеня за простим модулем p відносно t_1:

$$\frac{f(x_1)}{p} + t_1 f'(x_1) \equiv 0 \pmod{p}.$$

Через те що $f'(x_1)$ за умовою не ділиться на p, то ця остання конгруенція має єдиний розв'язок. Нехай розв'язком цієї конгруенції буде $t_1 \equiv t_1' \pmod{p}$; звідси $t_1 = t_1' + pt_2$, де t_2 — будь-яке ціле число.

Вираз для x набере вигляду:

$$x = x_1 + pt_1' + p^2 t_2 = x_2 + p^2 t_2,$$

де $x_2 = x_1 + pt_1'$ — відоме число.

[1] Практично зручно користуватися схемою Горнера розкладу многочлена в ряд Тейлора за степенями $x - x_1 = pt_1$; при цьому, як ми бачимо, досить обмежитись першими двома рядками в такій схемі. Тейлор (1665—1731), Горнер (1786—1837) — англійські математики.

Цей клас чисел вже буде розв'язком конгруенції (6). З цього класу чисел виберемо ті, які задовольняють конгруенцію

$$f(x) \equiv 0 \pmod{p^3}.$$

Для цього підставимо $x = x_2 + p^2 t_2$ в цю конгруенцію і розклавши її ліву частину в ряд Тейлора, дістанемо:

$$f(x_2) + p^2 t_2 f'(x_2) \equiv 0 \pmod{p^3}.$$

Тут $f(x_2)$ ділиться на p^2, бо x_2 є розв'язок конгруенції (6); $f'(x_2)$ не ділиться на p, бо з рівності $x_2 = x_1 + pt_1'$ матимемо, що $x_2 \equiv x_1 \pmod{p}$ і тому

$$f'(x_2) \equiv f'(x_1) \not\equiv 0 \pmod{p}.$$

Скорочуючи тепер обидві частини останньої конгруенції і модуль на p^2, дістанемо конгруенцію першого степеня відносно t_2 за модулем p:

$$\frac{f(x_2)}{p^2} + t_2 f'(x_2) \equiv 0 \pmod{p},$$

яка внаслідок щойно сказаного має один розв'язок: $t_2 \equiv t_2' \pmod{p}$, звідси $t_2 = t_2' + pt_3$ і вираз для x буде:

$$x = x_2 + p^2 t_2' + p^3 t_3 = x_3 + p^3 t_3,$$

де $x_3 = x_2 + p^2 t_2'$ — відоме число, яке є вже розв'язком конгруенції

$$f(x) \equiv 0 \pmod{p^3}.$$

Отже, за цим розв'язком конгруенції (5) знайдемо один розв'язок конгруенції (4) у вигляді:

$$x = x_\alpha + p^\alpha t_\alpha \quad \text{або} \quad x \equiv x_\alpha \pmod{p^\alpha}.$$

Цим не тільки доведено нашу теорему, але й вказано спосіб знаходження розв'язків конгруенції (4), коли відомі розв'язки конгруенції (5).

Зауваження. Якщо $f'(x_1)$ ділиться на p і $f(x_1)$ не ділиться на p^2, то це означає, що яке б не було t_1

$$f(x_1 + pt_1) \not\equiv 0 \pmod{p^2}$$

і конгруенція (6), а, значить, конгруенція (4) не має розв'язків для розглядуваного $x \equiv x_1 \pmod{p}$. Якщо ж $f(x_1)$ ділиться на p^2, тобто $f(x_1) \equiv 0 \pmod{p^2}$, то x_1 буде вже розв'язком конгруенції $f(x) \equiv 0 \pmod{p^2}$[1].

Приклад. Розв'язати конгруенцію

$$f(x) = x^4 + 3x^3 + 2x + 6 \equiv 0 \pmod{45}.$$

[1] Через те що один клас чисел за модулем p розпадається, очевидно, на p класів за модулем p^2, то з одного розв'язку конгруенції (5) дістанемо p розв'язків конгруенції (6).

Маємо: $45 = 3^2 \cdot 5$; тому така конгруенція еквівалентна системі конгруенцій:

$$f(x) \equiv 0 \pmod{3^2}, \quad f(x) \equiv 0 \pmod{5}.$$

Розв'язуємо окремо кожну з конгруенцій. Безпосереднім випробуванням [1] переконуємось, що розв'язком конгруенції

$$f(x) \equiv 0 \pmod{5}$$

буде $x \equiv 2 \pmod{5}$. Тепер розв'язуємо конгруенцію

$$f(x) \equiv 0 \pmod{3^2}.$$

Для цього спочатку треба розв'язати конгруенцію $f(x) \equiv 0 \pmod{3}$, яку можна переписати так:

$$x^4 + 2x \equiv 0 \pmod{3}.$$

Ця конгруенція має, очевидно, розв'язки: $x \equiv 0, 1 \pmod{3}$. З розв'язку $x \equiv 0 \pmod{3}$ дістанемо, що $x = 3t_1$, де t_1 — ціле. Підставляючи це значення x в конгруенцію

$$f(x) \equiv 0 \pmod{9},$$

маємо

$$6 + 3t_1 \cdot 2 \equiv 0 \pmod{9};$$

тут $f(0) = 6$, $f'(0) = 2$; або, скорочуючи обидві частини конгруенції і модуль на 3, дістанемо: $2 + 2t_1 = 0 \pmod{3}$, звідки $t_1 \equiv 2 \pmod{3}$, $t_1 = 2 + 3t$. Отже,

$$x = 3t_1 = 6 + 9t,$$

або

$$x \equiv 6 \pmod{9}$$

буде розв'язком конгруенції $f(x) \equiv 0 \pmod{9}$.

Аналогічно шукатимемо інший розв'язок конгруенції $f(x) \equiv 0 \pmod{9}$. Маємо: $x = 1 + 3t_1'$. Підставляючи в конгруенцію і розкладаючи в ряд Тейлора за степенями $x - 1 = 3t_1'$, дістанемо [2]:

$$12 + 3t_1' \cdot 15 \equiv 0 \pmod{9}.$$

Тут $f'(1) = 15$ ділиться на 3, але $f(1) = 12$ не ділиться на 3^2 і знайдена конгруенція відносно t_1' розв'язків не має, отже, конгруенція $f(x) \equiv 0 \pmod{9}$ не має розв'язків для $x = 1 + 3t_1'$, або для $x = 1 \pmod{3}$.

---

[1] Наприклад, за схемою Горнера.

[2] Див. примітку на стор. 96. Тут матимемо:

	1	3	0	2	6
1	1	4	4	6	$12 = f(1)$
1	1	5	9	$15 = f'(1)$	

Отже, конгруенція $f(x) \equiv 0 \pmod{5}$ має один розв'язок $x \equiv 2 \pmod{5}$ і конгруенція $f(x) \equiv 0 \pmod{9}$ також має один розв'язок $x \equiv 6 \pmod{9}$.

Розв'язуючи тепер спільно конгруенції $x \equiv 2 \pmod{5}$ і $x \equiv 6 \pmod{9}$, дістанемо їхній спільний розв'язок:

$$x \equiv 42 \equiv -3 \pmod{45}.$$

Це й буде єдиним розв'язком цієї конгруенції.

Контрольні запитання

1. Скільки розв'язків має система конгруенцій

$$\begin{cases} 3x \equiv 12 \pmod{15}, \\ 4x \equiv 6 \pmod{14}? \end{cases}$$

2. При якій умові конгруенція $f(x) \equiv 0 \pmod{m_1 \cdot m_2 \dots m_k}$, де $m_1, m_2, \dots, m_k$ — попарно взаємно прості, не має розв'язків?
3. Які конгруенції випливають з розв'язку конгруенції за складеним модулем?
4. З якою метою при доведенні теореми 2 використовують умову, що $f'(x)$ не $\vdots\ p$?
5. Відомо, що конгруенція $f(x) \equiv 0 \pmod{p^2}$ має розв'язок. Чи можна твердити, що конгруенція $f(x) \equiv 0 \pmod{p}$ також має розв'язок? Чи справедливе обернене твердження?

§ 24. Конгруенції n-го степеня за простим модулем. Максимальне число розв'язків

У попередньому параграфі ми бачили, що дослідження й розв'язання конгруенції n-го степеня ($n > 1$) за складеним модулем зводяться зрештою до дослідження і розв'язання відповідних конгруенцій за простими модулями. Тому доведемо тепер деякі загальні теореми, що стосуються конгруенцій n-го степеня за простим модулем p.

Припустимо, що задано конгруенцію [1]:

$$f(x) \triangleq a_0x^n + a_1x^{n-1} + \dots + a_{n-1}x + a_n \equiv 0 \pmod{p}, \quad n > 1, \quad (1)$$

де $a_0 \not\equiv 0 \pmod{p}$ і p — просте число.

Теорема 1. *Конгруенцію* (1) *завжди можна замінити еквівалентною конгруенцією того самого степеня з старшим коефіцієнтом, що дорівнює одиниці.*

Справді, через те що p — просте і a_0 не ділиться на p, то завжди існує єдине число α таке, що $a_0\alpha \equiv 1 \pmod{p}$ (див. теорему 1, § 21). Помножимо тепер конгруенцію (1) на α і замінимо $a_0\alpha$ одиницею,

---

[1] Рівняння

$$a_0x^n + a_1x^{n-1} + \dots + a_{n-1}x + a_n = pt \qquad (*)$$

з цілими коефіцієнтами і $p > 1$ еквівалентне конгруенції (1). Внаслідок такої залежності задачу розв'язання рівняння (*) в цілих числах можна замінити задачею розв'язання конгруенції (1), що й застосовується в теорії чисел.

дістанемо еквівалентну конгруенцію з старшим коефіцієнтом, що дорівнює одиниці:

$$x^n + b_1 x^{n-1} + \ldots + b_{n-1} x + b_n \equiv 0 \pmod{p}; \qquad (1')$$

тут $b_l \equiv a_l \alpha \pmod{p}$.

Теорема 2. *Якщо степінь конгруенції* (1) *не менший від модуля конгруенції, то вона еквівалентна деякій конгруенції степеня не вище* $p-1$ *(за тим самим модулем).*

Справді, поділимо $f(x)$ на $x^p - x$ і частку від ділення позначимо через $q(x)$, а остачу через $r(x)$. Тоді на підставі алгоритму ділення з остачею дістанемо:

$$f(x) = (x^p - x)\, q(x) + r(x),$$

де частка $q(x)$ і остача $r(x)$ будуть многочленами з цілими коефіцієнтами, причому степінь $r(x)$ буде не вище $p-1$. За теоремою Ферма $x^p - x \equiv 0 \pmod{p}$ при будь-якому цілому x, тому дістанемо тотожну конгруенцію:

$$f(x) \equiv r(x) \pmod{p}.$$

Ця тотожна конгруенція показує, що конгруенцію (1) і конгруенцію $r(x) \equiv 0 \pmod{p}$ задовольняють ті самі числа.

Отже, конгруенції

$$f(x) \equiv 0 \pmod{p} \quad \text{і} \quad r(x) \equiv 0 \pmod{p}$$

еквівалентні. Через те що степінь $r(x)$ менший за p, то теорему доведено.

Зокрема, може статись, що $f(x)$ ділиться на $x^p - x$ тобто $r(x) \equiv 0 \pmod{p}$ — тотожна конгруенція за модулем p, тобто остача при зазначеному діленні конгруентна з нулем, і дана конгруенція еквівалентна конгруенції $0 \cdot x \equiv 0 \pmod{p}$ та справедлива при будь-якому цілому x. Далі, нехай остача від ділення $f(x)$ на $x^p - x$ є многочлен нульового степеня, що дорівнює b_{p-1}. Якщо b_{p-1} не ділиться на p, то ця конгруенція не має розв'язків, бо вона зводиться до неправильної конгруенції:

$$b_{p-1} \equiv 0 \pmod{p}$$

Приклад. Якій конгруенції нижче від 5-го степеня еквівалентна конгруенція:

$$f(x) \equiv x^{17} + 2x^{11} + 3x^8 - 4x^7 + 2x - 3 \equiv 0 \pmod{5}.$$

Поділимо $f(x)$ на $x^5 - x$ і замінивши всі коефіцієнти остачі найменшими невід'ємними лишками за модулем 5, дістанемо, що дана конгруенція еквівалентна конгруенції

$$r(x) = 3x^4 + 3x^3 + 3x + 2 \equiv 0 \pmod{5}.$$

Зауваження. Можна вказане ділення на $x^p - x$ фактично і не виконувати, а просто замінити x^n на x^r, де $r > 0$ є остача від

ділення n на $p-1$. Справді, за теоремою Ферма $x^p \equiv x \pmod{p}$, звідси $x^{p+1} \equiv x^2$, $x^{p+2} \equiv x^3 \ldots$ і взагалі:

$$x^n = x^{k(p-1)+r} \equiv x^r \pmod{p}.$$

У нашому прикладі x^{17} можна змінити через x, а $2x^{11}$ через $2x^3$, $3x^8$ через $3x^4$, $-4x^7$ змінити через $-4x^3 \equiv x^3$ тому відразу дістанемо:

$$f(x) \equiv 3x^4 + 3x^3 + 3x + 2 \equiv 0 \pmod{5}.$$

У свою чергу, останню конгруенцію можна спростити так: $x \not\equiv 0 \pmod{5}$, тому $x^{5-1} \equiv 1 \pmod{5}$ і

$$f(x) \equiv 3x^3 + 3x \equiv 0 \pmod{5},$$

або

$$f(x) \equiv x^2 + 1 \equiv 0 \pmod{5}.$$

Очевидні розв'язки останньої конгруенції $x \equiv 2, 3 \pmod{5}$ будуть також і розв'язками даної конгруенції:

$$f(x) \equiv 0 \pmod{5}.$$

Теорема 3. *Якщо* α_1 *— який-небудь розв'язок конгруенції* (1), *то має місце тотожна конгруенція:*

$$f(x) \equiv (x - \alpha_1) f_1(x) \pmod{p}, \qquad (2)$$

де $f_1(x)$ *— многочлен степеня, на одиницю нижчого від степеня многочлена* $f(x)$. *Старший коефіцієнт многочлена* $f_1(x)$ *збігається із старшим коефіцієнтом даного многочлена* $f(x)$ [1].

Справді, поділимо $f(x)$ на $x - \alpha_1$ і частку позначимо через $f_1(x)$, а остачу — через r. За теоремою Безу $r = f(\alpha_1)$, але

$$f(\alpha_1) \equiv 0 \pmod{p}$$

за умовою, тоді конгруенцію

$$f(x) = (x - \alpha_1) f_1(x) + f(\alpha_1) \equiv 0 \pmod{p}$$

можна переписати так:

$$f(x) \equiv (x - \alpha_1) f_1(x) \pmod{p}.$$

При цьому кажуть, що $f(x)$ ділиться на $x - \alpha_1$ за модулем p. Очевидно, й навпаки: з конгруенції (2) випливає: $f(\alpha_1) \equiv 0 \pmod{p}$, тобто, α_1 — корінь конгруенції (1). Отже, маємо такий висновок:

Висновок. *Конгруенція* (1) *має корінь* $x = \alpha_1$ *тоді і тільки тоді, коли ліва її частина* $f(x)$ *ділиться на* $x - \alpha_1$ *за даним модулем* p.

Зауважимо, що теорема 3 і висновок з неї справедливі для складеного модуля m.

---

[1] Ця теорема аналогічна відомому в алгебрі висновку з теореми Безу. Безу (1730—1783) — французький математик.

Теорема 4. *Якщо* $\alpha_1, \alpha_2, \ldots, \alpha_k$ $(k \leqslant n)$[1] *є різні розв'язки конгруенції* (1), *то має місце тотожна конгруенція*:

$$f(x) \equiv (x-\alpha_1)(x-\alpha_2)\ldots(x-\alpha_k) f_k(x) \pmod p, \qquad (3)$$

де степінь $f_k(x)$ *дорівнює* $n-k$ *і старші коефіцієнти* $f(x)$ і $f_k(x)$ *однакові*.

Справді, згідно з теоремою 3 конгруенція (1) еквівалентна конгруенції

$$(x-\alpha_1) f_1(x) \equiv 0 \pmod p. \qquad (2')$$

Через те що α_2 є розв'язок конгруенції (1), то, підставляючи його в еквівалентну конгруенцію (2'), дістанемо тотожну конгруенцію:

$$(\alpha_2-\alpha_1) f_1(\alpha_2) \equiv 0 \pmod p.$$

Але добуток двох чи кількох чисел ділиться на просте число p тоді і тільки тоді, коли на p ділиться принаймні один із співмножників. За умовою α_1 і α_2 різні, тобто

$$\alpha_1 \not\equiv \alpha_2 \pmod p,$$

отже, $\alpha_2-\alpha_1$ не ділиться на p, а тому $f_1(\alpha_2)$ ділиться на p, тобто $f_1(\alpha_2) \equiv 0 \pmod p$: а це означає, що α_2 — розв'язок конгруенції $f_1(x) \equiv 0 \pmod p$. За теоремою 3 дістанемо:

$$f_1(x) \equiv (x-\alpha_2) f_2(x) \pmod p,$$

звідки

$$f(x) \equiv (x-\alpha_1)(x-\alpha_2) f_2(x) \pmod p.$$

Міркуючи аналогічно, зрештою прийдемо до тотожної конгруенції (3). З самого процесу утворення многочленів $f_1(x)$, $f_2(x)$, $\ldots$, $f_k(x)$ видно, що старші коефіцієнти цих многочленів однакові і дорівнюють старшому коефіцієнту a_0 многочлена $f(x)$.

Висновок. *Якщо конгруенція* (1) *n-го степеня за простим модулем* p *(*n *можна вважати не більшим за* $p-1$*) має* n *різних розв'язків* $\alpha_1, \alpha_2, \ldots, \alpha_n$, то справедлива тотожна конгруенція:

$$f(x) \equiv a_0 (x-\alpha_1)(x-\alpha_2)\ldots(x-\alpha_n) \pmod p. \qquad (4)$$

Справді, тут $k=n$, отже, степінь многочлена $f_n(x)$ дорівнюватиме $n-n=0$, тобто $f_n(x)=a_0$.

З конгруенції (4) випливає справедливість такого важливого твердження:

Теорема 5. *Конгруенція n-го степеня за простим модулем не може мати більш як n різних розв'язків.*

[1] Далі степінь конгруенції n завжди вважатимемо меншим від модуля конгруенції p.

Справді, нехай β — який-небудь інший розв'язок конгруенції (1), відмінний від $\alpha_1, \alpha_2, \ldots, \alpha_n$, тобто

$$\beta \not\equiv \alpha_i \pmod p \ (i=1, 2, \ldots, n);$$

покладаючи тепер у тотожній конгруенції (4) $x=\beta$, знайдемо:

$$a_0(\beta-\alpha_1)(\beta-\alpha_2)\ldots(\beta-\alpha_n) \equiv 0 \pmod p, \qquad (4')$$

але різниці $\beta-\alpha_i$ за умовою не діляться на p, тобто взаємно прості з p, а в такому разі й їхній добуток буде взаємно простим з p. Звідси випливає, що коли має місце конгруенція (4'), то a_0 має ділитись на p, а це суперечить умові, за якою $a_0 \not\equiv 0 \pmod p$.

Слід зауважити, по-перше, що ця теорема взагалі не стверджує, що конгруенція n-го степеня за простим модулем p має розв'язки і, по-друге, для складених модулів вона несправедлива; наприклад, конгруенція першого степеня $16x \equiv 32 \pmod{48}$, де $(16, 48)=16$ і 32 ділиться на 16, має шістнадцять розв'язків.

Висновок. *Конгруенція*

$$f(x) = a_0x^n + a_1x^{n-1} + \ldots + a_{n-1}x + a_n \equiv 0 \pmod p$$

має більш як n *розв'язків тоді і тільки тоді, коли вона тотожна, тобто коли всі її коефіцієнти діляться на* p.

Справді, якщо коефіцієнти заданої конгруенції діляться на p, то її задовольняє будь-яке значення x, тобто вона тотожна, і число її розв'язків (яке дорівнює p) буде перевищувати n (бо ми скрізь передбачаємо степінь конгруенції не більший за $p-1$).

Якщо a_0 не ділиться на p, то це конгруенція n-го степеня, і за теоремою 5 вона має не більш як n розв'язків. Якщо ж a_0 ділиться на p, але a_1 не ділиться на p, то степінь цієї конгруенції дорівнюватиме $n-1$ і вона за тією самою теоремою має не більше $n-1$, а тому й не більш як n, розв'язків. Так можна продовжувати далі, і якщо тільки не всі коефіцієнти цієї конгруенції діляться на p, то число її розв'язків, очевидно, не може перевищувати n.

Цей висновок дає змогу легко довести необхідну й достатню ознаку того, що задане число є просте.

Теорема Вільсона. *Ціле число* p *тоді і тільки тоді є простим, коли має місце конгруенція*

$$(p-1)! + 1 \equiv 0 \pmod p. \qquad (5)$$

Справді, припустимо, що p — просте число; якщо $p=2$, то конгруенція (5), очевидно, має місце. Якщо ж $p>2$, то розглянемо конгруенцію:

$$(x-1)(x-2)\cdots[x-(p-1)] - (x^{p-1}-1) \equiv 0 \pmod p.$$

Неважко побачити, що степінь цієї конгруенції не перевищує $p-2$, але вона має $p-1$ розв'язок, а саме безпосередньо видно, що лишки 1, 2, $\ldots$, $p-1$ задовольняють цю конгруенцію, бо, на підставі теореми Ферма, $x^{p-1}-1 \equiv 0 \pmod p$ при будь-якому цілому

$x \not\equiv 0 \pmod p$. Отже, всі її коефіцієнти кратні p, зокрема на p ділиться і вільний член, який дорівнює

$$1 \cdot 2 \cdots (p-1) + 1 = (p-1)! + 1$$

(при $p > 2$ число $p - 1$ — парне), тобто має місце конгруенція (5).

Навпаки, якщо $(p-1)! + 1 \equiv 0 \pmod p$, то p — число просте. Припустимо, що p — число складене, тоді воно ділилося б на деякий простий дільник $q < p$. Тому конгруенція (5) мала б місце і за будь-яким дільником числа p, тобто за модулем q. Через те що $q < p$, то в добутку $1 \cdot 2 \cdot 3 \cdots (p-1)$ один із співмножників дорівнює q, тоді дістанемо з конгруенції (5) за модулем q абсурдну конгруенцію: $1 \equiv 0 \pmod q$, де $1 < q < p$. Ця суперечність і показує, що p має бути просте.

На закінчення цього параграфа зауважимо таке: вважатимемо, що $x \equiv \alpha \pmod p$ є коренем k-ї кратності конгруенції $f(x) \equiv 0 \pmod p$, якщо $f(x)$ ділиться за модулем p на $(x-\alpha)^k$ і не ділиться на $(x-\alpha)^{k+1}$. При такому означенні кратності кореня заданої конгруенції теорема 2 твердить тільки, що конгруенції $f(x) \equiv 0 \pmod p$ і $r(x) \equiv 0 \pmod p$ мають одні й ті самі корені. Може статись, що кратний корінь конгруенції $f(x) \equiv 0 \pmod p$ буде простим для конгруенції $r(x) \equiv 0 \pmod p$, проте може бути і навпаки.

Приклад. Припустимо, що задано конгруенцію:

$$f(x) = x^5 + x^4 + x^3 + 4x^2 + 3 \equiv 0 \pmod 5.$$

Ділячи її на $x^5 - x$, дістанемо еквівалентну конгруенцію

$$r(x) \equiv x^4 + x^3 - x^2 + x - 2 \equiv 0 \pmod 5.$$

Корені заданої конгруенції $x \equiv 1, 2, 3, \pmod 5$; вони задовольняють і конгруенцію $r(x) \equiv 0 \pmod 5$. Але легко перевірити, що

$$f(x) \equiv (x-1)^2 (x-2)^2 (x-3) \pmod 5,$$

тоді як

$$r(x) \equiv (x-1)(x-2)(x-3)^2 \pmod 5,$$

тобто для конгруенції $f(x) \equiv 0 \pmod 5$ корені 1 і 2 — подвійні, а 3 — простий, а для конгруенції $r(x) \equiv 0 \pmod 5$ корені 1 і 2 прості, а 3 — подвійний корінь.

Контрольні запитання

1. Як треба перетворити конгруенцію $f(x) \equiv 0 \pmod p$, щоб старший коефіцієнт дорівнював одиниці? Чи завжди є таке α, що $a_0 \alpha \equiv 1 \pmod p$? Чому?
2. Як застосувати теорему Ферма, щоб перетворити конгруенцію за простим модулем p у еквівалентну конгруенцію з степенем, меншим від p?
3. Яка необхідна і достатня умова того, щоб конгруенція $f(x) \equiv 0 \pmod p$ мала корінь $x = \alpha_1$?
4. Що можна сказати про число розв'язків конгруенції n-го степеня за простим модулем?
5. Чи справедлива теорема 5 для конгруенції за складеним модулем? Навести приклад.
6. Чи можна твердити, що конгруенція виду (5) має понад n розв'язків тоді і тільки тоді, коли всі коефіцієнти діляться на p?
7. Сформулюйте умову, необхідну і достатню для того, щоб натуральне число p було простим.

§ 25. Конгруенції другого степеня; зведення до двочленної конгруенції. Квадратичні лишки і нелишки

Найпростішим випадком конгруенції вищого степеня з одним невідомим є конгруенція другого степеня:

$$ax^2 + bx + c \equiv 0 \pmod m, \quad a \not\equiv 0 \pmod m. \tag{1}$$

Теорія конгруенцій другого степеня пов'язана з розв'язуванням у цілих числах рівнянь другого степеня з двома невідомими. Конгруенція (1) еквівалентна невизначеному рівнянню другого степеня виду

$$ax^2 + bx + c = my.$$

Помножаючи обидві частини конгруенції (1) і модуль на $4a$, дістанемо конгруенцію (див. властивість 5, § 15):

$$4a^2x^2 + 4abx + 4ac \equiv 0 \pmod{4am}. \tag{1'}$$

Останню конгруенцію легко перетворити до двочленного виду, а саме: перенесемо останній член конгруенції в праву частину і до обох частин конгруенції додамо b^2, матимемо:

$$(2ax + b)^2 \equiv b^2 - 4ac \pmod{4am},$$

або, позначаючи $2ax + b = y$, $b^2 - 4ac = D$, дістанемо двочленну конгруенцію виду:

$$y^2 \equiv D \pmod{4am}. \tag{2}$$

Знаючи розв'язок конгруенції (1), завжди знайдемо відповідний розв'язок конгруенції (2):

Навпаки, якщо ми знайшли розв'язок конгруенції (2):

$$y \equiv y_0 \pmod{4am},$$

то з конгруенції

$$2ax + b \equiv y_0 \pmod{4am}$$

знайдемо розв'язок конгруенції (1′) або (1) за модулем m. Взагалі, з рівності $2ax + b = y$ маємо, що $x = \frac{y-b}{2a}$; якщо $y - b$ ділиться на $2a$, то дістанемо розв'язок x конгруенції (1). Отже, серед розв'язків y конгруенції (2) є такі, яким відповідають розв'язки x конгруенції (1). Проте, можуть бути й такі, яким не відповідають розв'язки x; може бути, що кільком різним за модулем $4am$ розв'язкам y відповідатиме один розв'язок x за модулем m.

Але, досліджуючи всі розв'язки y конгруенції (2), ми напевно знайдемо всі розв'язки x конгруенції (1), бо кожному розв'язкові конгруенції (1), за доведеним, неодмінно відповідає розв'язок конгруенції (2). Якщо конгруенція (2) зовсім не має розв'язків, то й конгруенція (1) також їх не має.

Отже, справедливе таке твердження:

Теорема 1. *Конгруенцію 2-го степеня виду* (1) *завжди можна звести до двочленної конгруенції виду* (2).

У деяких окремих випадках зведення конгруенції 2-го степеня (1) до двочленної спрощується.

Випадок 1. $(a, m) = 1$; тоді, визначаючи єдине α з конгруенції $a\alpha \equiv 1 \pmod m$, дістанемо $(\alpha, m) = 1$; помножаючи конгруенцію (1) на α, матимемо:

$$x^2 + b_1 x + c_1 \equiv 0 \pmod m, \qquad (1'')$$

де $b_1 \equiv b\alpha$, $c_1 \equiv c\alpha \pmod m$. Помноживши тепер обидві частини конгруенції (1″) і модуль на 4 і поклавши $2x + b_1 = y$, дістанемо двочленну конгруенцію

$$y^2 \equiv D \pmod{4m}, \qquad (2')$$

де $D = b_1^2 - 4c_1$. Тоді справедливе твердження: кожен розв'язок y конгруенції (2′) неодмінно дає і розв'язок x конгруенції (1″), бо $x = \frac{y - b_1}{2}$ в цьому разі завжди буде ціле, оскільки $y - b_1$ завжди парне, що безпосередньо видно з конгруенції (2′):

$$y^2 - b_1^2 \equiv -4c \pmod{4m}.$$

Але тут також різним розв'язкам за модулем $4m$ можуть відповідати однакові розв'язки за модулем m.

Випадок 2. $b = 2l$ — парне число; тоді, помножаючи обидві частини конгруенції (1) і модуль на a і покладаючи $ax + l = y$, матимемо:

$$y^2 \equiv D \pmod{am}, \qquad (2'')$$

де $D = l^2 - ac$. Цей випадок буває завжди при m непарному, бо коли при цьому b — непарне, то його можна замінити на $b \pm m$ — парне число.

Звичайно, випадки 1 і 2 можуть бути одночасно; в цьому разі конгруенція (1) матиме вигляд:

$$x^2 + 2lx + c \equiv 0 \pmod m.$$

Поклавши $x + l = y$, дістанемо:

$$y^2 \equiv D \pmod m,$$

де $D = l^2 - c$. Цей випадок, наприклад, завжди матиме місце при простому непарному m.

У § 23 ми показали, що дослідження й розв'язання конгруенції вищого степеня за складеним модулем зрештою зводиться до дослідження й розв'язання конгруенцій за простими модулями, тому при дальшому вивченні конгруенцій другого степеня можна обмежитись конгруенцією (1), де $m = p$ — просте число, більше 2. Згідно з останнім зауваженням її завжди можна подати у вигляді:

$$x^2 + 2lx + c \equiv 0 \pmod p.$$

Цю ж конгруенцію, як ми бачили, легко перетворити в еквівалентну двочленну конгруенцію:

$$y^2 \equiv D \pmod p,$$

де $y = x + l$, $D = l^2 - c$.

Приклад 2. Звести конгруенцію другого степеня

$$4x^2 - 11x - 8 \equiv 0 \pmod{13}$$

до двочленної.

Визначимо α так, щоб $4\alpha \equiv 1 \pmod{13}$; матимемо $\alpha \equiv 10 \pmod{13}$. Помножаючи дану конгруенцію на 10 за модулем 13, дістанемо:

$$x^2 - 6x - 2 \equiv 0 \pmod{13};$$

тут $l = -3$, $c = -2$. Отже, $D = 9 + 2 = 11$, і ми дістанемо шукану двочленну конгруенцію

$$y^2 \equiv 11 \pmod{13},$$

де $y = x - 3$.

Розглянемо докладніше двочленні конгруенції другого степеня за простим непарним модулем p:

$$x^2 \equiv a \pmod p, \quad (a, p) = 1. \qquad (3)$$

Випадок, коли $p = 2$, ми не розглядатимемо як тривіальний, бо розв'язком конгруенції (3) за модулем 2 будуть або 0, або 1, залежно від того, чи буде a парним, чи непарним. Якщо $a \equiv 0 \pmod p$, то конгруенція (3), очевидно, матиме тільки один розв'язок $x \equiv 0 \pmod p$. Тому далі p означатиме просте непарне число і a — ціле, яке не ділиться на p. Якщо конгруенція (3) має хоча б один розв'язок, то a називається *квадратичним лишком*, в противному разі a називається *квадратичним нелишком*[1].

Теорема 2. *Якщо a — квадратичний лишок за простим модулем p, то конгруенція (3) має два розв'язки. При цьому, якщо $x \equiv x_0 \pmod p$ є одним розв'язком конгруенції (3), то другим буде $x \equiv -x_0 \pmod p$.*

Справді, якщо a — квадратичний лишок за модулем p, то конгруенція (3) має принаймні один розв'язок; нехай цим розв'язком буде $x \equiv x_0 \pmod p$, тоді матиме місце тотожна конгруенція $x_0^2 \equiv a \pmod p$. Легко побачити, що $x \equiv -x_0 \pmod p$ також буде розв'язком конгруенції (3), оскільки

$$(-x_0^2) = x_0^2 \equiv a \pmod p.$$

Ці розв'язки різні, в противному разі з $x_0 \equiv -x_0 \pmod p$ виходило б, що $2x_0 \equiv 0 \pmod p$, тобто що $2x_0$ ділиться на p, що

[1] Числа $a \equiv 0 \pmod p$, тобто такі, що належать до класу C_0 за модулем p, для яких конгруенція $x^2 \equiv 0 \,(p)$ має один очевидний розв'язок $x \equiv 0 \,(p)$, не зараховують ні до квадратичних лишків, ні до квадратичних нелишків.

неможливо, бо $(2, p) = 1$ і $(x_0, p) = 1$. Останнє виходить з того, що розв'язками конгруенції (3) за простим модулем p можуть бути тільки зведені лишки за цим модулем, тобто числа $1, 2, \ldots, p-1$ які явно взаємно прості з p. Цими двома розв'язками й вичерпуються всі розв'язки конгруенції (3), бо вона є конгруенцією другого степеня за простим модулем і тому, згідно з теоремою 5, § 24, більше, ніж два розв'язки, мати не може.

Теорема 3. *Зведена система лишків за простим модулем p складається з $\frac{p-1}{2}$ квадратичних лишків, конгруентних за модулем p з числами*

$$1^2,\ 2^2,\ \ldots,\ \left(\frac{p-1}{2}\right)^2, \tag{4}$$

і $\frac{p-1}{2}$ квадратичних нелишків.

Справді, всі розв'язки конгруенції (3) слід шукати серед зведеної системи лишків за модулем p. Тому квадратичні лишки за модулем p мають бути конгруентні з квадратами зведених лишків за модулем p, тобто з квадратами чисел (зведена система лишків):

$$-\frac{p-1}{2},\ \ldots,\ -2,\ -1,\ 1,\ 2,\ \ldots,\ \frac{p-1}{2}, \tag{5}$$

інакше кажучи, з числами ряду (4), оскільки числа k і $-k$ дають однакові квадрати. Нарешті, покажемо, що числа ряду (4) неконгруентні між собою за модулем p. Припустимо супротивне, а саме: нехай

$$k^2 \equiv l^2 \pmod p,\ 0 < k < l \leqslant \frac{p-1}{2},$$

але тоді конгруенція другого степеня

$$x^2 \equiv l^2 \pmod p$$

за простим модулем p повинна мати чотири очевидних розв'язки; $\pm k$, $\pm l$. Маємо суперечність з теоремою 5, § 24.

Приклад. Знайти всі квадратичні лишки і нелишки за модулем $p = 11$. Тут $\frac{p-1}{2} = 5$; маємо:

$$1^2 \equiv 1,\ 2^2 \equiv 4,\ 3^2 \equiv 9,\ 4^2 \equiv 5,\ 5^2 \equiv 3 \pmod{11}.$$

Отже, квадратичними лишками за модулем 11 будуть числа: 1, 3, 4, 5, 9; інші зведені лишки будуть квадратичними нелишками: 2, 6, 7, 8, 10. Інакше кажучи, конгруенція $x^2 \equiv a \pmod{11}$ має два розв'язки при $a \equiv 1, 3, 4, 5, 9 \pmod{11}$ і жодного розв'язку при $a \equiv 2, 6, 7, 8, 10 \pmod{11}$.

Теорема 3, по суті, є критерієм розв'язності конгруенції (3). Цей критерій можна замінити іншим, зручнішим.

Критерій Ейлера. *При простому p і a, яке не ділиться на p, a є квадратичним лишком за модулем p тоді і тільки тоді, коли має місце конгруенція:*

$$a^{\frac{p-1}{2}} \equiv 1 \pmod p, \tag{6}$$

і квадратичним нелишком тоді і тільки тоді, коли має місце конгруенція

$$a^{\frac{p-1}{2}} \equiv -1 \pmod p. \tag{7}$$

Справді, за теоремою Ферма $a^{p-1} - 1 \equiv 0 \pmod p$; p — просте непарне, тому $p - 1$ — число парне і, отже, $\frac{p-1}{2}$ — ціле. Розглядаючи ліву частину останньої конгруенції як різницю квадратів, дістанемо:

$$\left(a^{\frac{p-1}{2}} - 1\right)\left(a^{\frac{p-1}{2}} + 1\right) \equiv 0 \pmod p.$$

З цієї конгруенції випливає, що при будь-якому a має місце тільки одна з конгруенцій (6) або (7), в противному разі мали б, $1 \equiv -1 \pmod p$, або $2 \equiv 0 \pmod p$, а це неможливо, бо $p > 2$.

Припустимо, що тепер a є квадратичним лишком за модулем p, тоді, згідно з означенням, він має задовольняти конгруенцію:

$$a \equiv x^2 \pmod p.$$

Підносячи останню до степеня $\frac{p-1}{2}$ і помічаючи, що $x^{p-1} \equiv 1 \pmod p$ (теорема Ферма), дістанемо, що будь-який квадратичний лишок a задовольняє конгруенцію (6). Але всіх квадратичних лишків за модулем p, згідно з теоремою 3, буде $\frac{p-1}{2}$; тому конгруенція (6) має $\frac{p-1}{2}$ розв'язків відносно a, але більш ніж $\frac{p-1}{2}$ розв'язків вона мати не може як конгруенція за простим модулем (див. теорему 5, § 24). Отже, квадратичними лишками a й вичерпуються всі розв'язки конгруенції (6). Це визначає й обернене твердження, тобто, якщо має місце конгруенція (6), то a є квадратичним лишком за модулем p.

Звідси випливає друга частина критерію, бо якщо a — квадратичний нелишок, то

$$a^{\frac{p-1}{2}} \not\equiv 1 \pmod p,$$

отже, задовольняє конгруенцію (7). Навпаки, якщо

$$a^{\frac{p-1}{2}} \equiv -1 \pmod p,$$

то $a^{\frac{p-1}{2}} \not\equiv 1 \pmod p$ і за доведеним не може бути квадратичним лишком, тобто a в цьому разі є квадратичним нелишком за модулем p. Отже, критерій Ейлера доведено повністю.

Приклад. За допомогою критерію Ейлера визначити, чи має розв'язок конгруенція

$$x^2 \equiv 12 \pmod{19}.$$

Послідовно знаходимо:

$$12^{\frac{19-1}{2}} = 12^9 = 12 \cdot (12^2)^4 = 12 \cdot 11^4 = 12 \cdot (11^2)^2 =$$
$$= 12 \cdot 7^2 = 12 \cdot 11 = -1 \pmod{19}.$$

Отже, 12 є квадратичним нелишком за модулем 19, а тому задана конгруенція не має розв'язків. З доведеного критерію випливає справедливість такого твердження:

Теорема Ейлера. *Добуток двох квадратичних лишків або нелишків є квадратичним лишком за даним модулем p; добуток же квадратичного лишку на нелишок є квадратичним нелишком.*

Справді, якщо a і b не діляться на p, то, на підставі критерію Ейлера, матимемо:

$$a^{\frac{p-1}{2}} \equiv \pm 1 \pmod p, \quad b^{\frac{p-1}{2}} \equiv \pm 1 \pmod p.$$

Перемноживши почленно ці конгруенції, знайдемо:

$$(ab)^{\frac{p-1}{2}} \equiv \pm 1 \pmod p.$$

Тут у правій частині буде знак плюс або мінус, інакше кажучи, ab буде квадратичним лишком або нелишком тоді, коли в правих частинах перемножуваних конгруенцій будуть відповідно однакові або різні знаки, тобто якщо a і b будуть одночасно або квадратичними лишками, або нелишками, чи один з них буде лишком, а другий нелишком. Цю теорему легко узагальнити так:

Добуток ряду чисел $a, b, c, \ldots$ дає квадратичний лишок або нелишок залежно від того, чи буде серед співмножників парне число нелишків, чи непарне.

Контрольні запитання

1. Як звести конгруенцію 2-го степеня до двочленної конгруенції? Розглянути окремі випадки.
2. Яке число a називається квадратичним лишком за простим модулем p?
3. Скільки розв'язків може мати квадратична конгруенція за простим модулем?
4. Скільки існує квадратичних лишків за простим модулем p, і з якими числами вони конгруентні?
5. Яка необхідна і достатня умова того, щоб a було квадратичним лишком за простим модулем p?

§ 26. Символ Лежандра. Закон взаємності квадратичних лишків

Критерій Ейлера дає змогу визначити, чи є a квадратичним лишком або нелишком за модулем p, тобто відповідати на запитання: має чи не має розв'язку конгруенція

$$x^2 \equiv a \pmod p.$$

Недоліком цього критерію є його громіздкість, а саме, якщо p — велике, то підносити a до $\frac{p-1}{2}$-го степеня дуже незручно. Щоб полегшити відповідь на поставлене запитання, вводять до розгляду так званий символ Лежандра $\left(\frac{a}{p}\right)$; він значно спрощує запис багатьох результатів і полегшує обчислення. Читається він так: символ a відносно p.

Символ Лежандра $\left(\frac{a}{p}\right)$ визначається для всіх цілих a, які не діляться на p, і дорівнює 1, *якщо a — квадратичний лишок*, і -1, *якщо a — квадратичний нелишок за модулем p*. Число a називається *чисельником*, а p, — *знаменником* символу Лежандра.

Виведемо ряд властивостей символу Лежандра, які дадуть змогу швидко його обчислювати, а отже, визначити, чи є a квадратичним лишком або нелишком за модулем p, тобто вирішувати питання про існування розв'язків конгруенції

$$x^2 \equiv a \pmod p.$$

Насамперед зауважимо, що конгруенції (6) і (7) попереднього параграфа можна буде об'єднати в одну конгруенцію

$$a^{\frac{p-1}{2}} \equiv \left(\frac{a}{p}\right) \pmod p, \qquad (1)$$

що виражає критерій Ейлера.

Основні властивості символу Лежандра.

1. *Якщо* $a \equiv a_1 \pmod p$, то $\left(\frac{a}{p}\right) = \left(\frac{a_1}{p}\right)$.

Ця властивість виходить з того, що числа одного й того самого класу за даним модулем є одночасно або квадратичними лишками, або нелишками. Це також виходить з критерію Ейлера. Припустимо, $a \equiv a_1 \pmod p$, тоді очевидно, що

$$a^{\frac{p-1}{2}} \equiv a_1^{\frac{p-1}{2}} \pmod p,$$

отже, a і a_1 або одночасно є квадратичні лишки, або нелишки за модулем p.

2. $\left(\frac{1}{p}\right) = +1$.

Ця властивість очевидна, бо конгруенція $x^2 \equiv 1 \pmod p$ завжди розв'язна; її розв'язками будуть $x \equiv \pm 1 \pmod p$.

3. $\left(\frac{-1}{p}\right) = (-1)^{\frac{p-1}{2}}$.

Ця властивість безпосередньо випливає з конгруенції (1) при $a = -1$.

Через те що $\frac{p-1}{2}$ буде числом парним, якщо $p = 4k+1$, і непарним, якщо $p = 4k+3$, то цю властивість можна сформулювати так: -1 є *квадратичним лишком простих чисел виду* $4k+1$ *і квадратичним нелишком простих чисел виду* $4k+3$.

Оскільки конгруенцію $x^2 \equiv -1 \pmod p$ можна записати у вигляді $x^2 + 1 \equiv 0 \pmod p$, то цю властивість можна сформулювати і в такій формі:

Цілі значення x, при яких x^2+1 *діляться на просте число* p, *бувають тоді і тільки тоді, коли* p *е число виду* $4k+1$, *тобто коли* $p \equiv 1 \pmod 4$.

4. $\left(\frac{a_1 a_2 \dots a_s}{p}\right) \equiv \left(\frac{a_1}{p}\right)\left(\frac{a_2}{p}\right)\dots\left(\frac{a_s}{p}\right)$[1].

Справді, на підставі критерію Ейлера, маємо:

$$\left(\frac{a_1 a_2 \dots a_s}{p}\right) \equiv (a_1 a_2 \dots a_s)^{\frac{p-1}{2}} = a_1^{\frac{p-1}{2}} a_2^{\frac{p-1}{2}} \dots a_s^{\frac{p-1}{2}} \equiv$$

$$\equiv \left(\frac{a_1}{p}\right)\left(\frac{a_2}{p}\right)\dots\left(\frac{a_s}{p}\right) \pmod p.$$

З останньої конгруенції випливає доводжувана рівність, оскільки числа, які стоять в обох частинах конгруенції, за абсолютною величиною дорівнюють 1. Дві такі величини можуть бути конгруентні за модулем $p > 2$, якщо тільки вони однакові.

Висновок.

$$\left(\frac{ab^2}{p}\right) = \left(\frac{a}{p}\right),$$

тобто *в чисельнику символу Лежандра можна відкидати множники, що є точними квадратами.*

5. $\left(\frac{2}{p}\right) = (-1)^{\frac{p^2-1}{8}}$.

Через те що за модулем 8 всі прості непарні числа будуть числами виду $8k+1$, $8k+3$, $8k+5$, $8k+7$, або $8k \pm 1$ і $8k \pm 3$ і $\frac{p^2-1}{8}$ буде парним при $p = 8k \pm 1$ і непарним при $p = 8k \pm 3$, то цю властивість можна сформулювати так:

[1] Ця властивість по суті є символічним виразом теореми Ейлера (див. § 25)

Число 2 є квадратичним лишком для всіх простих чисел виду $8k \pm 1$ (або $8k+1$, $8k+7$) *і квадратичним нелишком для всіх простих чисел виду* $8k \pm 3$ (або $8k+3$, $8k+5$).

Властивість 5 означає, що простими дільниками чисел виду $x^2 - 2$ можуть бути тільки числа виду $8k \pm 1$.

Приклад. Чи існують цілі x такі, що $x^2 - 2$ ділиться на 97?

Через те, що $97 = 8 \cdot 12 + 1$, то $\left(\frac{2}{97}\right) = +1$, і конгруенція $x^2 - 2 \equiv \pmod{97}$ має розв'язок. Отже, шукані значення x існують і є розв'язками цієї конгруенції.

Цю властивість довести вже набагато складніше; ми її доведемо разом з властивістю 6.

6. Закон взаємності квадратичних лишків. *Якщо* p *і* q *— різні прості непарні числа, то*

$$\left(\frac{q}{p}\right) = (-1)^{\frac{p-1}{2}\cdot\frac{q-1}{2}}\left(\frac{p}{q}\right).$$

Через те що $\frac{p-1}{2}\cdot\frac{q-1}{2}$ буде, очевидно, непарним, якщо p і q є числами виду $4k+3$, і парним, якщо хоч одне з чисел p або q буде числом виду $4k+1$, то властивість 6 можна сформулювати так:

Якщо p і q *є числами виду* $4k+3$, то

$$\left(\frac{q}{p}\right) = -\left(\frac{p}{q}\right);$$

якщо ж хоч одне з чисел p *або* q *є числа виду* $4k+1$, *то*

$$\left(\frac{q}{p}\right) = \left(\frac{p}{q}\right).$$

Перш ніж приступити до доведень властивостей 5 і 6, дамо інше тлумачення символу Лежандра.

Лема Гаусса. *Якщо* a *не ділиться на просте число* $p > 2$, *то*

$$\left(\frac{a}{p}\right) = (-1)^m, \tag{2}$$

де m *— число таких остач від ділення чисел*

$$a,\ 2a,\ \dots,\ \frac{p-1}{2}a \tag{3}$$

на p, *які більші* $\frac{p}{2}$.

Доведення. Нехай l — число додатних остач від ділення чисел ряду (3) на p, менших за $\frac{p}{2}$. Позначимо ці остачі через $\alpha_1, \alpha_2, \dots, \alpha_l$. Так само позначимо через $\beta_1, \beta_2, \dots, \beta_m$ остачі від ділення чисел ряду (3) на p, більші за $\frac{p}{2}$. Очевидно, що

$$m + l = \frac{p-1}{2}.$$

Через те що всі α_l і β_j конгруентні за модулем p з числами ряду (3), то можемо написати:

$$\alpha_1\alpha_2 \dots \alpha_l\beta_1\beta_2 \dots \beta_m \equiv a \cdot 2a \dots \frac{p-1}{2}\, a = a^{\frac{p-1}{2}} \left(\frac{p-1}{2}\right)! \pmod p.$$

Числа $p-\beta_j$ будуть менші за $\frac{p}{2}$ і різні між собою. Справді, коли б $p-\beta_j = p-\beta_i$, то $\beta_j = \beta_i$, але з цієї рівності випливала б конгруентність двох чисел ряду (3):

$$k_1 a \equiv k_2 a \pmod p,$$

де $k_1,\ k_2 = 1,\ 2,\ \dots .\ \frac{p-1}{2}$, звідки $k_1 \equiv k_2 \pmod p$, що неможливо при $k_1 \neq k_2$.

Покажемо тепер, що ці нові числа $p-\beta_j$ відмінні від чисел α_l. Справді, коли б $\alpha_l = p-\beta_j$, то ми мали б, що $\alpha_l + \beta_j = p$. Остання рівність призвела б до неможливої конгруенції:

$$k_1 a + k_2 a \equiv 0 \pmod p,$$

або

$$k_1 + k_2 \equiv 0 \pmod p,$$

бо

$$0 < k_1 + k_2 < p-1.$$

Отже, $\frac{p-1}{2}$ чисел

$$\alpha_1,\ \alpha_2,\ \dots,\ \alpha_l,\ p-\beta_1,\ p-\beta_2,\ \dots,\ p-\beta_m$$

збігаються з числами ряду 1, 2, ..., $\frac{p-1}{2}$; тому

$$\alpha_1, \alpha_2 \dots \alpha_l (p-\beta_1)(p-\beta_2) \dots (p-\beta_m) = 1 \cdot 2 \dots \frac{p-1}{2} = \left(\frac{p-1}{2}\right)! \quad (4)$$

З другого боку,

$$\alpha_1\alpha_2 \dots \alpha_l (p-\beta_1)(p-\beta_2) \dots (p-\beta_m) \equiv$$
$$\equiv (-1)^m \alpha_1\alpha_2 \dots \alpha_l\beta_1\beta_2 \dots \beta_m \pmod p;$$

але за доведеним вище

$$\prod_{i=1}^{l} \alpha_i \prod_{j=1}^{m} \beta_j = a^{\frac{p-1}{2}} \left(\frac{p-1}{2}\right)!,$$

отже,

$$\alpha_1\alpha_2 \dots \alpha_l (p-\beta_1)(p-\beta_2) \dots (p-\beta_m) \equiv$$
$$\equiv (-1)^m a^{\frac{p-1}{2}} \left(\frac{p-1}{2}\right)! \pmod p.$$

Далі, на підставі рівності (4), знаходимо, що

$$\left(\frac{p-1}{2}\right)! \equiv (-1)^m \left(\frac{p-1}{2}\right)!\, a^{\frac{p-1}{2}} \pmod p.$$

Скорочуючи обидві частини останньої конгруенції на $\left(\frac{p-1}{2}\right)!$, взаємно просте з p, і помножаючи обидві її частини на $(-1)^m$ дістанемо:

$$a^{\frac{p-1}{2}} \equiv (-1)^m \pmod p;$$

на підставі критерію Ейлера

$$a^{\frac{p-1}{2}} \equiv \left(\frac{a}{p}\right) \pmod p.$$

Отже,

$$\left(\frac{a}{p}\right) = (-1)^m.$$

Цим лему Гаусса доведено.

Знайденому виразу для символу Лежандра надамо іншого, більш закінченого вигляду, а саме покажемо, що

$$\left(\frac{a}{p}\right) = (-1)^{\frac{p^2-1}{8}(a-1) + \sum_{k=1}^{\frac{p-1}{2}} \left[\frac{ka}{p}\right]}. \quad (5)$$

Справді, позначимо через q_k і r_k відповідно частку і остачу від ділення ka на p, де $k = 1,\ 2,\ \dots,\ \frac{p-1}{2}$. Тоді, на підставі алгоритму ділення з остачею, можна написати, що

$$ka = q_k p + r_k;\ \ 1 \leqslant r_k \leqslant p-1, \quad (6)$$

причому очевидно, що $q_k = \left[\frac{ka}{p}\right]$ і r_k не може дорівнювати нулю бо $(a,\ p) = 1$ за умовою і $(k,\ p) = 1$; отже, остачі r_k є не що інше, як числа α_l і β_j в доведенні леми Гаусса. Позначимо

$$\alpha = \sum_{l=1}^{l} \alpha_l,\ \ \beta = \sum_{j=1}^{m} \beta_j,$$

Тоді:

$$\sum_{k=1}^{\frac{p-1}{2}} r_k = \alpha + \beta.$$

Далі, ми бачили, що числа

$$\alpha_1,\ \alpha_2,\ \ldots,\ \alpha_t,\ p-\beta_1,\ p-\beta_2,\ \ldots,\ p-\beta_m$$

збігаються з числами ряду $1,\ 2,\ \ldots,\ \frac{p-1}{2}$. Отже,

$$1+2+\cdots+\frac{p-1}{2}=\sum_{i=1}^{t}\alpha_i+\sum_{j=1}^{m}(p-\beta_j),$$

або

$$\frac{\frac{p-1}{2}\left(\frac{p-1}{2}+1\right)}{2}=\sum_{i=1}^{t}\alpha_i-\sum_{j=1}^{m}\beta_j+mp,$$

тобто

$$\frac{p^2-1}{8}=\alpha-\beta+mp. \qquad (7)$$

Додаючи почленно рівності (6), дістанемо:

$$a\cdot\sum_{k=1}^{\frac{p-1}{2}}k=p\cdot\sum_{k=1}^{\frac{p-1}{2}}q_k+\sum_{k=1}^{\frac{p-1}{2}}r_k,$$

або

$$a\cdot\frac{p^2-1}{8}=p\cdot\sum_{k=1}^{\frac{p-1}{2}}\left[\frac{ka}{p}\right]+\alpha+\beta.$$

Віднімаючи від цієї рівності рівність (7), матимемо:

$$\frac{p^2-1}{8}(a-1)=p\cdot\sum_{k=1}^{\frac{p-1}{2}}\left[\frac{ka}{p}\right]+2\beta-mp;$$

звідки

$$\frac{p^2-1}{8}(a-1)\equiv p\cdot\sum_{k=1}^{\frac{p-1}{2}}\left[\frac{ka}{p}\right]-mp\pmod 2,$$

p — непарне число; отже $p\equiv -1\pmod 2$, і тому

$$\frac{p^2-1}{8}(a-1)\equiv-\sum_{k=1}^{\frac{p-1}{2}}\left[\frac{ka}{p}\right]+m\pmod 2,$$

звідки

$$m\equiv\frac{p^2-1}{8}(a-1)+\sum_{k=1}^{\frac{p-1}{2}}\left[\frac{ka}{p}\right]\pmod 2,$$

внаслідок чого

$$(-1)^m=\left(\frac{a}{p}\right)=(-1)^{\frac{p^2-1}{8}(a-1)+\sum_{k=1}^{\frac{p-1}{2}}\left[\frac{ka}{p}\right]},$$

і рівність (5) доведено.

Тепер перейдемо до доведення властивостей 5 і 6.

Доведення властивості 5. У формулі (5) покладемо $a=2$, тоді $\left[\frac{ka}{p}\right]=0$, бо $k=1,\ 2,\ \ldots,\ \frac{p-1}{2}$, і тому дістанемо:

$$\left(\frac{2}{p}\right)=(-1)^{\frac{p^2-1}{8}}.$$

Доведення властивості 6, тобто закону взаємності квадратичних лишків. Припустимо, що у формулі (5) $a=q$, де $q>2$ — просте число, тоді $a-1=q-1$ буде парним числом, значить, у формулі (5) можна відкинути $\frac{p^2-1}{8}(a-1)$. Отже, маємо

$$\left(\frac{q}{p}\right)=(-1)^{\sum_{k=1}^{\frac{p-1}{2}}\left[\frac{kq}{p}\right]};$$

аналогічно

$$\left(\frac{p}{q}\right)=(-1)^{\sum_{l=1}^{\frac{q-1}{2}}\left[\frac{lp}{q}\right]}.$$

Звідси

$$\left(\frac{p}{q}\right)\left(\frac{q}{p}\right)=(-1)^{\sum_{k=1}^{\frac{p-1}{2}}\left[\frac{kq}{p}\right]+\sum_{l=1}^{\frac{q-1}{2}}\left[\frac{lp}{q}\right]}.$$

Покажемо тепер, що

$$\sum_{k=1}^{\frac{p-1}{2}}\left[\frac{kq}{p}\right]+\sum_{l=1}^{\frac{q-1}{2}}\left[\frac{lp}{q}\right]=\frac{p-1}{2}\cdot\frac{q-1}{2}. \tag{8}$$

Для цього розглянемо $\frac{p-1}{2}\cdot\frac{q-1}{2}$ чисел виду $lp-kq$, де $k=1, 2, \ldots, \frac{p-1}{2}$; $l=1, 2, \ldots, \frac{q-1}{2}$. Всі ці числа не дорівнюють нулю. Справді, якщо $lp-kq=0$, то $lp=kq$. З останньої рівності виходить, що lp ділиться на q, але через те що $(p, q)=1$, то l повинно ділитись на q, але це не можливо, бо

$$1\leqslant l\leqslant\frac{q-1}{2}.$$

Отже, серед чисел $lp-kq$ можуть зустрічатись як додатні, так і від'ємні, але такі не дорівнюють нулю. Визначимо, скільки з них додатних і скільки від'ємних.

Припустимо, що $lp-kq>0$ для заданого фіксованого l, тоді $k<\frac{lp}{q}$; разом з тим маємо, що $1\leqslant k\leqslant\frac{p-1}{2}$. Ці нерівності, разом узяті, еквівалентні нерівностям

$$1\leqslant k<\frac{lp}{q} \tag{9}$$

бо

$$\frac{lp}{q}<\frac{\frac{q}{2}\cdot p}{q}=\frac{p}{2},\ \text{тобто}\ \frac{lp}{q}\leqslant\frac{p-1}{2}.$$

Нерівність (9) має щодо k (при фіксованому l) $\left[\frac{lp}{q}\right]$ розв'язків, а саме:

$$k=1, 2, \ldots, \left[\frac{lp}{q}\right],$$

тобто k набуває $\left[\frac{lp}{q}\right]$ значень; але l набуває значення від 1 до $\frac{q-1}{2}$ включно. Звідси виходить, що серед $\frac{p-1}{2}\cdot\frac{q-1}{2}$ чисел виду $lp-kq$ додатних буде

$$\sum_{l=1}^{\frac{q-1}{2}}\left[\frac{lp}{q}\right].$$

Припустимо тепер, що $lp-kq<0$ тоді (при фіксованому k) $l<\frac{kq}{p}$; аналогічно знайдемо, що серед $\frac{p-1}{2}\cdot\frac{q-1}{2}$ чисел виду $lp-kq$ від'ємних буде всього

$$\sum_{k=1}^{\frac{p-1}{2}}\left[\frac{kq}{p}\right].$$

А через те що різних чисел виду $lp-kq$ буде всього $\frac{p-1}{2}\cdot\frac{q-1}{2}$ і кожне з них або додатне, або від'ємне, то й дістанемо рівність (8).

Отже,

$$\left(\frac{p}{q}\right)\left(\frac{q}{p}\right)=(-1)^{\frac{p-1}{2}\cdot\frac{q-1}{2}},$$

або, помножаючи обидві частини рівності на $\left(\frac{p}{q}\right)$ і беручи до уваги, що $\left(\frac{p}{q}\right)^2=1$, дістаємо:

$$\left(\frac{q}{p}\right)=(-1)^{\frac{p-1}{2}\cdot\frac{q-1}{2}}\left(\frac{p}{q}\right),$$

і закон взаємності доведено.

Закон взаємності і властивості 1 і 4 дають змогу обчислення будь-якого символу Лежандра $\left(\frac{a}{p}\right)$ звести до обчислення символів $\left(\frac{1}{p}\right)$, $\left(\frac{-1}{p}\right)$ і $\left(\frac{2}{p}\right)$, значення яких даються властивостями 2, 3, 5.

Приклад. Визначимо, чи має розв'язок конгруенція

$$x^2\equiv 76\ (\mathrm{mod}\ 101).$$

Для цього досить обчислити символ Лежандра $\left(\frac{76}{101}\right)$. Насамперед бачимо, що 101 — число просте; розкладемо чисельник символу на прості множники: $76=2^2\cdot 19$. Тепер, на підставі властивості 4 і висновку з неї, можемо написати:

$$\left(\frac{76}{101}\right)=\left(\frac{2^2}{101}\right)\cdot\left(\frac{19}{101}\right)=\left(\frac{19}{101}\right).$$

Отже, лишається обчислити символ $\left(\frac{19}{101}\right)$. Через те що 19 число просте, то, застосовуючи закон взаємності, дістанемо $\left(\frac{19}{101}\right)=\left(\frac{101}{19}\right)$, бо одне з чисел, а саме 101, є числом виду $4k+1$ $(k=25)$.

В останньому символі чисельник більший від знаменника. Застосовуючи властивість 1, дістанемо:

$$\left(\frac{101}{19}\right) = \left(\frac{6}{19}\right), \text{ бо } 101 \equiv 6 \pmod{19}.$$

Далі, $\left(\frac{6}{19}\right) = \left(\frac{2}{19}\right)\left(\frac{3}{19}\right)$ (властивість 4).

Символ $\left(\frac{2}{19}\right) = -1$ (властивість 5); до символу $\left(\frac{3}{19}\right)$ знову застосовуємо закон взаємності: $\left(\frac{3}{19}\right) = -\left(\frac{19}{3}\right)$ і, на підставі властивості 1, маємо: $-\left(\frac{19}{3}\right) = -\left(\frac{1}{3}\right)$, а далі, застосовуючи властивість 2, дістаємо: $-\left(\frac{1}{3}\right) = -1$.

Звідси матимемо:

$$\left(\frac{76}{101}\right) = +1.$$

Отже, задана конгруенція має два розв'язки.

Контрольні запитання

1. Дайте означення символу Лежандра.
2. Випишіть усі вирази для символу Лежандра.
3. Чому одиниця є квадратичним лишком за будь-яким модулем p?
4. Для простих чисел якого виду -1 є квадратичним лишком? Нелишком?
5. Для яких простих чисел 2 є квадратичним лишком? Нелишком?
6. Сформулюйте закон взаємності квадратичних лишків.
7. Перевірте справедливість леми Гаусса для $a = 6$ і $p = 13$.
8. Які властивості символу Лежандра $\left(\frac{a}{p}\right)$ дають можливість звести його обчислення до обчислення символів $\left(\frac{1}{p}\right)$, $\left(\frac{-1}{p}\right)$, $\left(\frac{2}{p}\right)$, значення яких відомі?

§ 27. Символ Якобі

При обчисленні символу Лежандра доводиться розкладати чисельник символу на прості множники. Якщо чисельник дуже велике число, то таке розкладання становить значні труднощі. Щоб уникнути цього і прискорити обчислення символу Лежандра, розглядають узагальнення символу Лежандра, так званий *символ Якобі*.

Нехай P — довільне непарне число, більше за одиницю, і $P = p_1 p_2 \ldots p_k$ — розклад його на прості множники (серед цих множників можуть бути і однакові). Припустимо, далі, що a —

ціле число, взаємно просте з P, тоді *символ Якобі* $\left(\frac{a}{P}\right)$ *визначається рівністю:*

$$\left(\frac{a}{P}\right) = \left(\frac{a}{p_1}\right)\left(\frac{a}{p_2}\right)\cdots\left(\frac{a}{p_k}\right),$$

де $\left(\frac{a}{p_i}\right)$ — звичайні символи Лежандра. Зокрема, якщо $P = p$ — просте число, то символ Якобі $\left(\frac{a}{P}\right)$ збігається з символом Лежандра $\left(\frac{a}{p}\right)$.

Відомі властивості символу Лежандра дають змогу встановити аналогічні *властивості символу Якобі*.

1. *Якщо*

$$a \equiv a_1 \pmod{P} \text{ то } \left(\frac{a}{P}\right) = \left(\frac{a_1}{P}\right).$$

Справді, згідно з означенням,

$$\left(\frac{a}{P}\right) = \left(\frac{a}{p_1}\right)\left(\frac{a}{p_2}\right)\cdots\left(\frac{a}{p_k}\right),$$

але, якщо $a \equiv a_1 \pmod{P}$, то тим більш

$$a \equiv a_1 \pmod{p_i} \ (i = 1, 2, \ldots, k) \text{ і тому } \left(\frac{a}{p_i}\right) = \left(\frac{a_1}{p_i}\right).$$

Отже, дістаємо:

$$\left(\frac{a}{P}\right) = \left(\frac{a_1}{p_1}\right)\left(\frac{a_1}{p_2}\right)\cdots\left(\frac{a_1}{p_k}\right) = \left(\frac{a_1}{P}\right).$$

2. $\left(\frac{1}{P}\right) = +1$.

Справді,

$$\left(\frac{1}{P}\right) = \left(\frac{1}{p_1}\right)\left(\frac{1}{p_2}\right)\cdots\left(\frac{1}{p_k}\right) = 1, \text{ бо } \left(\frac{1}{p}\right) = 1.$$

3. $\left(-\frac{1}{P}\right) = (-1)^{\frac{P-1}{2}}$.

Справді,

$$\left(\frac{-1}{P}\right) = \left(\frac{-1}{p_1}\right)\left(\frac{-1}{p_2}\right)\cdots\left(\frac{-1}{p_k}\right) = (-1)^{\frac{p_1-1}{2}+\frac{p_2-1}{2}+\cdots+\frac{p_k-1}{2}}. \qquad (1)$$

Але неважко показати, що $\frac{p_1-1}{2}+\cdots+\frac{p_k-1}{2}$ і $\frac{P-1}{2}$ є числа однакової парності. Це випливає з такої рівності:

$$\frac{P-1}{2}=\frac{p_1p_2\cdots p_k-1}{2}=$$

$$=\frac{\left(1+2\frac{p_1-1}{2}\right)\left(1+2\frac{p_2-1}{2}\right)\cdots\left(1+2\frac{p_k-1}{2}\right)-1}{2}=$$

$$=\frac{p_1-1}{2}+\frac{p_2-1}{2}+\cdots+\frac{p_k-1}{2}+2N,$$

де N — ціле число. Тут ми застосували правило множення біномів, які відрізняються тільки другими членами. Отже, з рівності (1) дістанемо:

$$\left(\frac{-1}{P}\right)=(-1)^{\frac{P-1}{2}}.$$

4. $\left(\frac{a_1a_2\cdots a_s}{P}\right)=\left(\frac{a_1}{P}\right)\left(\frac{a_2}{P}\right)\cdots\left(\frac{a_s}{P}\right)$.

Справді, згідно з означенням символу Якобі і властивістю 4 символу Лежандра, матимемо:

$$\left(\frac{a_1a_2\cdots a_s}{P}\right)=\prod_{i=1}^{k}\left(\frac{a_1a_2\cdots a_s}{p_i}\right)=\prod_{i=1}^{k}\prod_{j=1}^{s}\left(\frac{a_j}{p_i}\right)=\prod_{j=1}^{s}\prod_{i=1}^{k}\left(\frac{a_j}{p_i}\right)=$$

$$=\prod_{j=1}^{s}\left(\frac{a_j}{P}\right)=\left(\frac{a_1}{P}\right)\cdots\left(\frac{a_s}{P}\right).$$

Висновок.

$$\left(\frac{ab^2}{P}\right)=\left(\frac{a}{P}\right).$$

5. $\left(\frac{2}{P}\right)=(-1)^{\frac{P^2-1}{8}}$.

Справді, за означенням символу Якобі і властивістю 5 символу Лежандра, дістанемо

$$\left(\frac{2}{P}\right)=\left(\frac{2}{p_1}\right)\left(\frac{2}{p_2}\right)\cdots\left(\frac{2}{p_k}\right)=(-1)^{\frac{p_1^2-1}{8}+\frac{p_2^2-1}{8}+\cdots+\frac{p_k^2-1}{8}},$$

але подібно до того, як у властивості 3, з рівності

$$\frac{P^2-1}{8}=\frac{p_1^2p_2^2\cdots p_k^2-1}{8}=\frac{\left(1+8\frac{p_1^2-1}{8}\right)\cdots\left(1+8\frac{p_k^2-1}{8}\right)-1}{8}=$$

$$=\frac{p_1^2-1}{8}+\frac{p_2^2-1}{8}+\cdots+\frac{p_k^2-1}{8}+2N$$

робимо висновок, що $\frac{P^2-1}{8}$ і $\frac{p_1^2-1}{8}+\frac{p_2^2-1}{8}+\cdots+\frac{p_k^2-1}{8}$ є числа тієї самої парності, отже, виходить:

$$\left(\frac{2}{P}\right)=(-1)^{\frac{P^2-1}{8}}.$$

6. Закон взаємності символу Якобі. *Якщо P і Q додатні непарні взаємно прості числа, більші за 1, то*

$$\left(\frac{Q}{P}\right)=(-1)^{\frac{P-1}{2}\cdot\frac{Q-1}{2}}\left(\frac{P}{Q}\right).$$

Справді, нехай

$$Q=q_1q_2\cdots q_s$$

є розклад Q на прості множники (серед них знов-таки можуть бути й рівні). Внаслідок умови $(P, Q)=1$, всі q_j мають бути відмінні від p_i. Далі, згідно з означенням символу Якобі і властивістю 6 символу Лежандра, послідовно дістанемо:

$$\left(\frac{Q}{P}\right)=\prod_{i=1}^{k}\left(\frac{Q}{p_i}\right)=\prod_{i=1}^{k}\prod_{j=1}^{s}\left(\frac{q_j}{p_i}\right)=$$

$$=(-1)^{\sum_{i=1}^{k}\sum_{j=1}^{s}\frac{p_i-1}{2}\cdot\frac{q_j-1}{2}}\prod_{i=1}^{k}\prod_{j=1}^{s}\left(\frac{p_i}{q_j}\right)=$$

$$=(-1)^{\left(\sum_{i=1}^{k}\frac{p_i-1}{2}\right)\left(\sum_{j=1}^{s}\frac{q_j-1}{2}\right)}\left(\frac{P}{Q}\right).$$

Але при виведенні властивості 3 ми бачили, що

$$\frac{P-1}{2}\text{ і }\sum_{i=1}^{k}\frac{p_i-1}{2}$$

є числа однакової парності; це стосується й чисел

$$\frac{Q-1}{2}\text{ і }\sum_{j=1}^{s}\frac{q_j-1}{2}.$$

Отже,

$$\frac{P-1}{2}\cdot\frac{Q-1}{2}\text{ і }\left(\sum_{i=1}^{k}\frac{p_i-1}{2}\right)\left(\sum_{j=1}^{s}\frac{q_j-1}{2}\right)$$

також числа однакової парності, а тому остаточно дістанемо:

$$\left(\frac{Q}{P}\right) = (-1)^{\frac{P-1}{2}\cdot\frac{Q-1}{2}}\left(\frac{P}{Q}\right).$$

Отже, ми показали, що для символів Якобі справджуються всі властивості символів Лежандра. Тому символи Якобі обчислюються за тими самими правилами, що й символи Лежандра, і при обчисленні їх не слід розрізняти. Це дає можливість при обчисленні символів Лежандра не розкладати чисельники на прості множники; треба тільки виділяти множники, що дорівнюють 2.

Зауваження. При узагальненні Якобі символу Лежандра виконано так званий *принцип перманентності*. Цей принцип потребує, щоб при узагальненні даного поняття залишались правильними основні властивості цього поняття. Здавалося б, природнішим узагальненням символу Лежандра для складеного знаменника було б вважати, що $\left(\frac{a}{P}\right) = +1$, якщо конгруенція $x^2 \equiv a \pmod P$ має розв'язки; в противному разі вважати, що $\left(\frac{a}{P}\right) = -1$. Але, тоді, як неважко побачити, не було б виконано принципу перманентності і таке узагальнення символу Лежандра не мало б жодного практичного значення. Далі побачимо, що для символу Якобі умова $\left(\frac{a}{P}\right) = +1$ необхідна, але не достатня для того, щоб конгруенція $x^2 \equiv a \pmod P$ мала розв'язок.

Приклад. Обчислити символ Лежандра $\left(\frac{2108}{2003}\right)$. Будемо обчислювати, не зважаючи на те, які проміжні символи матимемо — Лежандра чи Якобі; пам'ятатимемо лише, що в чисельнику треба виділяти множники, які дорівнюють 2.

Застосовуючи послідовно властивості 4, 6, 1, 4, 5, 6, 1, 6, 2, знайдемо:

$$\left(\frac{2108}{2003}\right) = \left(\frac{2^2\ 527}{2003}\right) = \left(\frac{527}{2003}\right) = -\left(\frac{2003}{527}\right) = -\left(\frac{422}{527}\right) = -\left(\frac{2}{527}\right)\left(\frac{211}{527}\right) =$$

$$= -\left(\frac{211}{527}\right) = \left(\frac{527}{211}\right) = \left(\frac{105}{211}\right) = \left(\frac{211}{105}\right) = \left(\frac{1}{105}\right) = +1.$$

Цей самий символ можна було обчислити, застосовуючи послідовно властивості 1, 6, 1, 4, 5:

$$\left(\frac{2108}{2003}\right) = \left(\frac{105}{2003}\right) = \left(\frac{2003}{105}\right) = \left(\frac{8}{105}\right) = \left(\frac{2}{105}\right) = +1.$$

Контрольні запитання

1. Дайте означення символу Якобі. Як пов'язані символи Лежандра і Якобі?
2. Перелічіть властивості символу Якобі.
3. Чим відрізняються формулювання законів взаємності символу Якобі і символу Лежандра?
4. Відомо, що $\left(\frac{a}{P}\right) = 1$ (P — складене). Чи можна твердити, що квадратична конгруенція $x^2 \equiv a \pmod P$ має розв'язок?
5. Чого слід уникати при обчисленні символу Лежандра за допомогою символу Якобі?

§ 28. Конгруенції другого степеня за складеним модулем

Конгруенція другого степеня за складеним модулем:

$$x^2 = a \pmod m, \text{ де } m = 2^\alpha p_1^{\alpha_1} p_2^{\alpha_2} \dots p_k^{\alpha_k},\ (a,\ m) = 1 \qquad (1)$$

досліджується і розв'язується згідно з загальними вказівками § 23.

За теоремою 1, § 23, конгруенція (1) еквівалентна системі конгруенцій

$$\begin{cases} x^2 \equiv a \pmod{2^\alpha}, \\ x^2 \equiv a \pmod{p_1^{\alpha_1}}, \\ \dots\dots\dots \\ x^2 \equiv a \pmod{p_k^{\alpha_k}}. \end{cases} \qquad (2)$$

Розглянемо конгруенції виду

$$x^2 \equiv a \pmod{p^\alpha};\ (a,\ p) = 1, \qquad (3)$$

де $\alpha > 1$ — ціле число, а p — просте непарне число.

Ми вже бачили, що розв'язки конгруенції (3) задовольняють і конгруенцію

$$x^2 \equiv a \pmod p. \qquad (4)$$

Позначимо через $f(x)$ вираз $x^2 - a$, тоді $f'(x) = 2x$. Якщо тепер $x \equiv x_1 \pmod p$ є розв'язком конгруенції (4), то, зважаючи на те, що $(a,\ p) = 1$, $(x_1,\ p) = 1$ і p — непарне, дістанемо, що $(2x_1,\ p) = 1$, тобто $f'(x_1)$ не ділиться на p. Тому до знаходження розв'язків конгруенції (3) можна застосувати міркування, викладені в теоремі 2 § 23. За цією теоремою кожний розв'язок конгруенції (4) дає один єдиний розв'язок конгруенції (3). Але остання має два розв'язки тоді і тільки тоді, коли a є квадратичним лишком за модулем p, тобто коли $\left(\frac{a}{p}\right) = +1$. Отже, приходимо до такого результату:

Теорема 1. *Конгруенція* (3) *має два розв'язки або не має жодного залежно від того, чи буде число a квадратичним лишком*

або нелишком за модулем p, *тобто чи буде відповідно* $\left(\frac{a}{p}\right) = +1$ *або* $\left(\frac{a}{p}\right) = -1$.

Зауваження. Неважко побачити, що коли $x \equiv x_\alpha \pmod{p^\alpha}$ є один розв'язок конгруенції (3), то другим її розв'язком буде $-x_\alpha$. Справді,

$$(-x_\alpha)^2 = x_\alpha^2 \equiv a \pmod{p^\alpha};$$

далі, $x_\alpha \not\equiv -x_\alpha \pmod{p^\alpha}$, бо, в противному разі, $2x_\alpha \equiv 0 \pmod{p^\alpha}$, що неможливо, бо ні 2, ні x_α не діляться на p^α, тобто взаємно прості з p^α.

Розглянемо тепер конгруенцію

$$x^2 \equiv a \pmod{2^\alpha};\ \alpha > 0,\ (a,\ 2) = 1. \tag{5}$$

Тут $f'(x_1) = 2x_1$ ділиться на $p = 2$, і тому загальні міркування § 24 незастосовні; їх можна змінити в такий спосіб.

Нехай конгруенція (5) розв'язна, тоді, зважаючи на те, що $(a,\ 2) = 1$, матимемо $(x,\ 2) = 1$, тобто $x = 1 + 2t$, де t — ціле число. Інакше кажучи, розв'язки конгруенції (5) треба шукати серед непарних чисел. Підставляючи $x = 1 + 2t$ в конгруенцію (5), дістанемо нову конгруенцію щодо t:

$$1 + 4t(t + 1) \equiv a \pmod{2^\alpha}.$$

Але одне з чисел t, $t + 1$ — парне, тому $4t(t + 1)$ ділитиметься на 8.

Отже, щоб остання конгруенція мала розв'язок, а разом з тим і конгруенція (5), треба, щоб

$$\begin{aligned} &a \equiv 1 \pmod 4 \text{ при } \alpha = 2; \\ &a \equiv 1 \pmod 8 \text{ при } \alpha > 3. \end{aligned} \tag{6}$$

Припустимо, що справджуються умови (6); розглянемо тоді питання про знаходження розв'язків конгруенції (5) і про їхнє число; при цьому розглянемо окремо такі випадки:

1) $\alpha = 1$, тобто $x^2 \equiv a \pmod 2$.

Тут тільки й може бути, що $a \equiv 1 \pmod 2$, і будь-яке непарне число задовольнятиме нашу конгруенцію. Але всі непарні числа утворюють тільки один клас за модулем 2; отже, в цьому випадку матимемо єдиний розв'язок: $x \equiv 1 \pmod 2$.

2) $\alpha = 2$, тобто $x^2 \equiv a \pmod 4$.

За умовою $a \equiv 1 \pmod 4$. Але легко побачити, що квадрат будь-якого непарного числа конгруентний одиниці за модулем 8, а тому і за модулем 4. Справді, кожне непарне число можна подати у вигляді $4k \pm 1$. Беручи конгруенції за модулем 8, дістанемо:

$$(4k \pm 1)^2 = 16k^2 \pm 8k + 1 \equiv 1 \pmod 8.$$

Отже, в розглядуваному випадку задану конгруенцію задовольнятимуть усі непарні числа. За модулем 4 всі непарні числа утворюють два класи, найменшими невід'ємними лишками яких будуть числа 1 і 3. Отже, в цьому випадку матимемо два розв'язки: $x \equiv 1,\ 3 \pmod 4$.

3) $\alpha = 3$, тобто $x^2 \equiv a \pmod 8$.

Через те що за умовою $a \equiv 1 \pmod 8$ і квадрат всякого непарного числа конгруентний одиниці за модулем 8, то й в цьому випадку всі непарні числа задовольняють задану конгруенцію. Але за модулем 8 непарні числа утворюють чотири класи:

$$x \equiv 1,\ 3,\ 5,\ 7 \pmod 8,$$

вони й будуть розв'язками конгруенції (5) при $\alpha = 3$. При $a = 3$, $5,\ 7 \pmod 8$ конгруенція, очевидно, розв'язків не матиме, бо необхідну умову не буде виконано.

4) $\alpha > 3$. Якщо конгруенція (5) при $\alpha > 3$ має розв'язки, то вони, очевидно, також задовольнятимуть ту саму конгруенцію за модулем 8.

Отже, умова (6) необхідна і при $\alpha > 3$. Доведемо, що ця умова є і достатня. Але спочатку з'ясуємо, скільки всього розв'язків має конгруенція (5), якщо вона взагалі має розв'язки. Нехай b — деякий певний її розв'язок, а x — будь-який її розв'язок. Маємо:

$$b^2 \equiv a \pmod{2^\alpha},\ x^2 \equiv a \pmod{2^\alpha};$$

отже,

$$x^2 - b^2 \equiv 0 \pmod{2^\alpha},$$

або

$$(x - b)(x + b) \equiv 0 \pmod{2^\alpha}.$$

Припустимо, що

$$x - b = 2^\beta \cdot k,\quad x + b = 2^\gamma l,$$

де k і l — непарні числа; тоді додаючи й ділячи на 2, дістанемо:

$$x = 2^{\beta-1} \cdot k + 2^{\gamma-1} \cdot l.$$

Але x як розв'язок конгруенції (5) має бути непарним; отже, або $\beta - 1$, або $\gamma - 1$, дорівнює нулю, тобто одне з чисел β, γ дорівнює одиниці, а друге не менше за $\alpha - 1$, бо добуток $(x - b)(x + b)$ ділиться на 2^α.

Припустимо, що $\gamma = 1$, тоді $\beta \geqslant \alpha - 1$, і ми маємо

$$x - b = 2^{\alpha-1} \cdot s,$$

де s — будь-яке (не обов'язково непарне) число, або

$$x = b + 2^{\alpha-1} \cdot s;$$

і, нарешті,

$$x \equiv b + 2^{\alpha-1} \cdot s \pmod{2^\alpha},$$

бо розв'язки конгруенції (5) визначаються за модулем 2^α. При парному s

$$x \equiv b \pmod{2^\alpha};$$

при непарному s

$$x \equiv b + 2^{\alpha-1} \pmod{2^\alpha}.$$

Ці два розв'язки різні за модулем 2^α.

Нехай тепер $\beta = 1$, значить, $\gamma \geqslant \alpha - 1$ і маємо $x + b = 2^{\alpha-1} \cdot s$, де s — ціле число. У цьому випадку, як і в попередньому, знайдемо ще два такі розв'язки:

$$x \equiv -b \pmod{2^\alpha}, \quad x \equiv -b + 2^{\alpha-1} \pmod{2^\gamma}.$$

Отже, конгруенція (5) має всього чотири розв'язки:

$$b,\ b + 2^{\alpha-1},\ -b,\ -b + 2^{\alpha-1} \text{ (або } -b - 2^{\alpha-1}).$$

Усі ці розв'язки різні за модулем 2^α, у чому легко переконатись.

Доведемо, що *умова* $a \equiv 1 \pmod 8$ *буде достатня для існування розв'язків конгруенції* (5). Ми бачили, що вона достатня при $\alpha = 3$. Застосуємо метод математичної індукції. На підставі сказаного вище досить показати, що при виконанні умови $a \equiv 1 \pmod 8$ конгруенція (5) має хоча б один розв'язок.

Припустимо, що достатність умови (6) доведена для конгруенції

$$x^2 \equiv a \pmod{2^{\alpha-1}}, \qquad (5')$$

тобто при $a \equiv 1 \pmod 8$ ця конгруенція має розв'язки. Якщо $x_{\alpha-1}$ є один з її розв'язків, то, як ми бачили, решта розв'язків буде:

$$x_{\alpha-1} + 2^{\alpha-2},\ -x_{\alpha-1},\ -x_{\alpha-1} - 2^{\alpha-2} \text{ (або } -x_{\alpha-1} + 2^{\alpha-2}).$$

Отже,

$$x_{\alpha-1}^2 \equiv a \pmod{2^{\alpha-1}},$$

тобто $x_{\alpha-1}^2 - a$ ділиться на $2^{\alpha-1}$, або

$$x_{\alpha-1}^2 - a = 2^{\alpha-1} \cdot k.$$

Якщо k — парне, то $x_{\alpha-1} - a$ ділиться на 2^α, тобто $x_{\alpha-1}$ є розв'язком конгруенції (5), і наше твердження доведено. Якщо ж k — непарне, то візьмемо вираз $x_{\alpha-1} + 2^{\alpha-2}$ і покажемо, що він буде розв'язком конгруенції (5) за модулем 2^α, а саме: $(x_{\alpha-1} + 2^{\alpha-2})^2 - a$ за умовою ділиться на $2^{\alpha-1}$, але ми маємо:

$$(x_{\alpha-1} + 2^{\alpha-2})^2 - a = (x_{\alpha-1}^2 - a) + 2^{\alpha-1}x_{\alpha-1} + 2^{2\alpha-4} =$$
$$= 2^{\alpha-1}k + 2^{\alpha-1}x_{\alpha-1} + 2^{2\alpha-4},$$

при $\alpha > 3$, $2\alpha - 4 \geqslant \alpha$; отже,

$$(x_{\alpha-1} + 2^{\alpha-2})^2 - a \equiv 2^{\alpha-1} \cdot (k + x_{\alpha-1}) \pmod{2^\alpha}.$$

Але k і $x_{\alpha-1}$ — непарні: k за умовою, $x_{\alpha-1}$ як розв'язок конгруенції (5) при непарному a, отже,

$$(x_{\alpha-1} + 2^{\alpha-2})^2 - a \equiv 0 \pmod{2^\alpha},$$

тобто $x_{\alpha-1} + 2^{\alpha-2}$ є розв'язком конгруенції (5); наше твердження доведено і в цьому випадку.

Як бачимо, один з розв'язків конгруенції (5′) є неодмінно і розв'язком конгруенції (5). Позначимо його через x_α, решта розв'язків конгруенції (5) будуть:

$$-x_\alpha,\ x_\alpha + 2^{\alpha-1},\ -x_\alpha - 2^{\alpha-1}.$$

Усі ці розв'язки задовольняють і конгруенцію (5′), тільки для цієї конгруенції вони не всі різні, як для конгруенцій (5), але розв'язки x_α і $-x_\alpha$ різні і для (5′).

Підсумовуючи все доведене, дістанемо такий результат:

Теорема 2. 1) *Конгруенція* (5) *завжди має один розв'язок при* $\alpha = 1$; 2) *два розв'язки — при* $\alpha = 2$, *і* $a \equiv 1 \pmod 4$ *і жодного при* $\alpha = 2$ *і* $a \equiv 3 \pmod 4$; 3) *при* $\alpha \geqslant 3$ *конгруенція* (5) *має розв'язки тільки при* $\alpha \equiv 1 \pmod 8$ *і при цьому чотири різних розв'язки; два з них неодмінно задовольняють і конгруенцію*

$$x^2 \equiv a \pmod{2^{\alpha+1}}.$$

Попередні міркування вказують на метод розв'язування конгруенції (5) при $\alpha > 3$.

Приклад. $x^2 \equiv 33 \pmod{64}$.

У цьому випадку маємо:

$$a = 33 \equiv 1 \pmod 8,$$

отже, розв'язків буде чотири. Для їх знаходження розглянемо конгруенції

$$x^2 \equiv 33 \equiv 1 \pmod 8,$$
$$x^2 \equiv 33 \equiv 1 \pmod{16},$$
$$x^2 \equiv 33 \equiv 1 \pmod{32},$$
$$x^2 \equiv 33 \pmod{64}.$$

Розв'язки першої конгруенції будуть 1, 3, 5, 7; з них, наприклад, 1 задовольняє другу конгруенцію. Решта розв'язків другої конгруенції є: $1 + 2^3$, -1, $-1 - 2^3$, тобто розв'язки другої конгруенції будуть 1, 7, 9, 15. З них, наприклад, 1 задовольняє третю конгруенцію; решта її розв'язків буде: $1 + 2^4$, -1, $-1 - 2^4$, тобто, 1, 15, 17, 31 є всі розв'язки третьої конгруенції. З цих розв'язків, наприклад, 15 задовольняє четверту конгруенцію, а решта її розв'язків буде: $15 + 2^5$, -15, $-15 - 2^5$. Отже, маємо всі розв'язки даної конгруенції:

$$x \equiv 15,\ 17,\ 47,\ 49 \pmod{64}.$$

Звичайно, не слід обов'язково починати з конгруенції (5) за модулем 8; краще починати з конгруенції за модулем 2^α, для якої нам відомо хоть один розв'язок x_α, решта три будуть:

$$-x_\alpha,\ x_\alpha + 2^{\alpha-1},\quad -x_\alpha - 2^{\alpha-1}.$$

Так, наприклад, конгруенція

$$x^2 \equiv 57 \pmod{64}$$

має чотири розв'язки, бо $57 \equiv 1 \pmod 8$. Маємо:

$$x^2 \equiv 57 \equiv 1 \pmod 8,$$
$$x^2 \equiv 57 \equiv 9 \pmod{16},$$
$$x^2 \equiv 57 \equiv 25 \pmod{32},$$
$$x^2 \equiv 57 \pmod{64}.$$

У конгруенції

$$x^2 \equiv 25 \pmod{32}$$

25 є точний квадрат, тому один з її розв'язків буде $x \equiv 5 \pmod{32}$; решта будуть:

$$-5,\ 5 + 16 = 21,\ -5 - 16 = -21 \equiv 11 \pmod{32}.$$

Розв'язок 11 задовольняє конгруенцію за модулем 64; отже, розв'язками останньої конгруенції будуть: ± 11, $\pm(11 + 32) = \pm 43$, або

$$x \equiv 11,\ 21,\ 43,\ 53 \pmod{64}.$$

З теорем 1 і 2 та з теореми 1, § 23, маємо таку теорему:

Теорема 3. *Конгруенція*

$$x^2 \equiv a \pmod m;\ m = 2^\alpha p_1^{\alpha_1} \dots p_k^{\alpha_k};\ (a, m) = 1 \qquad (7)$$

має розв'язок тоді і тільки тоді, коли

$$\left(\frac{a}{p_1}\right) = +1,\ \left(\frac{a}{p_2}\right) = +1,\ \dots,\ \left(\frac{a}{p_k}\right) = +1;$$
$$a \equiv 1 \pmod 4 \text{ при } \alpha = 2,$$
$$a \equiv 1 \pmod 8 \text{ при } \alpha \geqslant 3.$$

Якщо жодну з цих умов не порушено, то кількість розв'язків буде

$$2^k \text{ при } \alpha = 0;\ 1,$$
$$2^{k+1} \text{ при } \alpha = 2,$$
$$2^{k+2} \text{ при } \alpha \geqslant 3.$$

Приклад. Визначити, чи має розв'язки конгруенція

$$x^2 \equiv 241 \pmod{360},$$

і якщо має, то скільки.

Знаходимо канонічний розклад модуля; маємо: $360 = 2^3 \cdot 3^2 \cdot 5$; далі,

$$241 \equiv 1 \pmod 8;\quad \left(\frac{241}{3}\right) = \left(\frac{1}{3}\right) = +1;\quad \left(\frac{241}{5}\right) = \left(\frac{1}{5}\right) = +1.$$

Отже, ця конгруенція має $2^{2+2} = 2^4 = 16$ розв'язків, бо тут $k = 2$, $\alpha = 3$.

Зауваження. Якщо m — непарне і конгруенція (7) має розв'язки, то символ Якобі

$$\left(\frac{a}{m}\right) = \left(\frac{a}{p_1}\right)^{\alpha_1}\left(\frac{a}{p_2}\right)^{\alpha_2} \cdots \left(\frac{a}{p_k}\right)^{\alpha_k} = +1,$$

бо всі $\left(\frac{a}{p_i}\right) = +1$. Ця умова необхідна для розв'язності конгруенції (7), але недостатня, бо з $\left(\frac{a}{m}\right) = +1$ не виходить, що всі $\left(\frac{a}{p_i}\right) = +1$. У зв'язку з цим зауважимо ще раз, що застосування символу Якобі та його властивостей лише прискорює обчислення символу Лежандра.

Контрольні запитання

1. Якій системі конгруенцій еквівалентна конгруенція

$$x^2 \equiv a \pmod m,$$

де $m = 2^\alpha \cdot p_1^{\alpha_1} p_2^{\alpha_2} \cdots p_k^{\alpha_k}$ і $(a, m) = 1$?

2. При якій умові кожний розв'язок конгруенції $x^2 \equiv a \pmod p$ дає єдиний розв'язок конгруенції $x^2 \equiv a \pmod{p^\alpha}$, де p — просте непарне число? Чи виконується ця умова при $p = 2$? Чому?

3. Як знайти розв'язок конгруенції $x^2 \equiv a \pmod{2^{\alpha+1}}$, знаючи розв'язки конгруенції $x^2 \equiv a \pmod{2^\alpha}$?

4. Яка умова розв'язності і яке число розв'язків квадратичної конгруенції за модулем p^α, де p — просте непарне число і α — натуральне? За модулем 2^α? За будь-яким модулем $m = 2^\alpha p_1^{\alpha_1} p_2^{\alpha_2} \dots p_k^{\alpha_k}$?

5. Якщо квадратична конгруенція за складеним модулем m розв'язна, то скільки вона має розв'язків?

Вправи

1. За допомогою добору розв'язати конгруенції

а) $x^2 \equiv 3 \pmod{37}$; б) $x^5 - 5 \equiv 0 \pmod 7$;
в) $x^5 - 7x^4 + 11x^3 - 5x + 1 \equiv 0 \pmod{12}$;
г) $2^x \equiv x^2 \pmod 5$, $x > 0$.

Відповідь. а) $x \equiv 15,\ 22 \pmod{37}$; б) $x \equiv 3 \pmod 7$; в) розв'язків немає; г) $x \equiv 2,4 \pmod 5$.

2. Розв'язати конгруенції першого степеня: а) $7x \equiv 13 \pmod{29}$; б) $8x \equiv 15 \pmod{29}$; в) $9x \equiv 17 \pmod{31}$; г) $17x \equiv 13 \pmod{123}$; д) $243x \equiv 271 \pmod{317}$; е) $221x \equiv 111 \pmod{360}$; є) $141x \equiv 73 \pmod{320}$; ж) $139x \equiv 118 \pmod{239}$.

Відповідь: а) $x \equiv 6 \pmod{29}$; б) $x \equiv 20 \pmod{29}$; в) $x \equiv 26 \pmod{31}$; г) $x \equiv 8 \pmod{123}$; д) $x \equiv 112 \pmod{317}$; е) $x \equiv 51 \pmod{360}$; є) $x \equiv 173 \pmod{320}$; ж) $x \equiv 147 \pmod{239}$.

3. Розв'язати конгруенції першого степеня: а) $327x \equiv 78 \pmod{379}$; б) $239x \equiv 302 \pmod{471}$; в) $23x \equiv 667 \pmod{693}$.

Відповідь. а) $x \equiv 188 \pmod{379}$; б) $x \equiv 19 \pmod{471}$; в) $x \equiv 29 \pmod{693}$.

4. Розв'язати конгруенції першого степеня: а) $9x \equiv 15 \pmod{48}$; б) $21x \equiv 15 \pmod{111}$; в) $15x \equiv 120 \pmod{85}$; г) $75x \equiv 62 \pmod{111}$; д) $2560x \equiv 45 \pmod{3605}$; е) $36x \equiv 54 \pmod{18}$.

Відповідь. а) $x \equiv 7,\ 23,\ 39 \pmod{48}$; б) $x \equiv 6,\ 43,\ 80 \pmod{111}$; в) $x \equiv 8,\ 25,\ 42,\ 59,\ 76 \pmod{85}$; г) конгруенція розв'язків не має; д) $x \equiv 100;\ 821,\ 1542,\ 2263,\ 2984 \pmod{3605}$; е) конгруенція тотожна.

5. Скласти конгруенцію першого степеня за модулем 21: а) яка має один розв'язок; б) яка має 3 або 7 розв'язків; в) яка має 2, 10, 15 розв'язків.

Відповідь: а) Шуканою конгруенцією буде $ax \equiv b \pmod{21}$, де $(a, 21) = 1$ і b — ціле; б) для того щоб конгруенція $ax \equiv b \pmod{21}$ мала, наприклад, 3 розв'язки, необхідно і достатньо, щоб $(a, 21) = 3$ і b ділилося на 3; в) такої конгруенції скласти не можна.

6. За допомогою конгруенцій розв'язати в цілих числах такі невизначені рівняння: а) $53x + 17y = 25$; б) $47x - 105y = 4$.

Відповідь. а) $x = 4 + 17t$, $y = -11 - 53t$, б) $x = 47 + 105t$, $y = 21 + 47t$.

7. Безпосередньою перевіркою переконатися, що класи чисел за модулем 7 утворюють поле.

8. Припустимо, що p є просте і $0 < a < p$. Довести, що конгруенція $ax = b \pmod{p}$ має розв'язок.

$$x \equiv b(-1)^{a-1}\frac{(p-1)(p-2)\ldots(p-a+1)}{1\cdot 2\cdot\ldots\cdot a} \pmod{p}.$$

9. Якщо $ax \equiv b \pmod{m}$ і $(a, m) = 1$, то єдиний розв'язок цієї конгруенції символічно позначається як дріб, $x \equiv \frac{b}{a} \pmod{m}$. Довести, що (конгруенції беруться за модулем m):

а) якщо $a \equiv a_1$ і $b \equiv b_1$, то $\frac{b}{a} \equiv \frac{b_1}{a_1}$:

б) $\frac{b}{a} \equiv \frac{bk}{ak}$, якщо $(a, k) = 1$;

в) чисельник b символічного дробу $\frac{b}{a}$ можна замінити конгруентним з ним числом b_0 кратним, a. Тоді символічний дріб $\frac{b}{a}$ буде конгруентний з цілим числом, що подається звичайним дробом $\frac{b_0}{a}$;

г) $\frac{b_1}{a_1} \pm \frac{b_2}{a_2} \equiv \frac{a_2b_1 \pm a_1b_2}{a_1a_2}$ (a_1 і a_2 взаємно прості з m);

д) $\frac{b_1}{a_1} \cdot \frac{b_2}{a_2} \equiv \frac{b_1b_2}{a_1a_2}$ (a_1 і a_2 взаємно прості з m);

е) $\frac{b_1}{a_1} : \frac{b_2}{a_2} \equiv \frac{b_1 \cdot a_2}{a_1 \cdot b_2}$ (a_1, a_2 і b_2 взаємно прості з m);

10. Розв'язати такі системи конгруенцій:

а) $x \equiv 3 \pmod{5}$, $x \equiv 2 \pmod{7}$, $x \equiv 4 \pmod{9}$;

б) $x \equiv 1 \pmod{3}$, $x \equiv 5 \pmod{7}$, $x \equiv 9 \pmod{11}$;

в) $x \equiv 14 \pmod{19}$, $x \equiv 5 \pmod{7}$, $x \equiv 9 \pmod{10}$, $x \equiv 1 \pmod{3}$.

Відповідь. а) $x \equiv 58 \pmod{315}$; б) $x \equiv 229 \equiv -2 \pmod{231}$; в) $x \equiv 2959 \pmod{3990}$.

11. Розв'язати такі системи конгруенцій:

а) $37x \equiv 73 \pmod{91}$, $x \equiv 9 \pmod{16}$, $x \equiv 5 \pmod{7}$;

б) $24x \equiv 20 \pmod{22}$, $13x \equiv 19 \pmod{27}$;

в) $75x \equiv 35 \pmod{40}$, $8x \equiv 12 \pmod{44}$, $51x \equiv 50 \pmod{63}$,

г) $5x \equiv 200 \pmod{251}$, $11x \equiv 192 \pmod{401}$, $3x \equiv -151 \pmod{907}$.

Відповідь: а) $x \equiv 425 \pmod{1456}$; б) $x \equiv 43,\ 340 \pmod{594}$; в) розв'язків немає; г) $x \equiv 7\,777\,777 \pmod{91290457}$.

12. Знайти числа, які: а) при діленні на 4, 5, 7 дають відповідно остачі 2, 3, 4; б) при діленні на 3, 7, 8 дають відповідно остачі 2, 4, 5.

Відповідь. а) $x \equiv 18 \pmod{140}$; б) $x \equiv 53 \pmod{168}$.

13. Знайти найменше натуральне число, яке кратне 7 і дає остачу 1 від ділення на 2, 3, 4, 5 і 6.

Відповідь. 301.

14. Розв'язати такі конгруенції (зводячи їх до конгруенції за простими модулями):

а) $x^4 + 7x + 4 \equiv 0 \pmod{27}$; б) $x^5 - 7x^3 + 2x^2 + x - 4 \equiv 0 \pmod{35}$.

Відповідь. а) $x \equiv 22 \pmod{27}$: б) розв'язків немає.

15. Довести, що коли $(n, m) = 1$, то конгруенцію n-го степеня

$$f(x) = x^n + a_1x^{n-1} + \cdots + a_{n-1}x + a_n \equiv 0 \pmod{m}$$

можна введенням нового невідомого y звести до конгруенції того самого степеня:

$$y^n + b_2y^{n-2} + \cdots + b_{n-1}y + b_n \equiv 0 \pmod{m},$$

де немає члена $(n-1)$-го степеня.

16. Користуючись попередньою задачею, звести конгруенцію

$$x^3 + 5x^2 + 6x - 8 \equiv 0 \pmod{13}$$

до тричленного виду:

$$y^3 + py + q \equiv 0 \pmod{13}.$$

Відповідь. $y^3 + 2y - 2 \equiv 0 \pmod{13}$.

17. Довести, що коли конгруенція n-го степеня $f(x) \equiv 0 \pmod{p}$ має n різних розв'язків і $f(x)$ за модулем p розкладається на два множники $f_1(x)$ і $f_2(x)$ k-го і l-го степенів ($k + l = n$), тобто тотожно $f(x) \equiv f_1(x)\ f_2(x) \pmod{p}$, то конгруенція $f_1(x) \equiv 0 \pmod{p}$ має k різних розв'язків, а конгруенція $f_2(x) \equiv 0 \pmod{p}$ має l різних розв'язків.

18. Довести, що конгруенція $f(x) \equiv 0 \pmod{p}$ степеня $n < p$ тоді і тільки тоді має n різних розв'язків, коли $x^p - x$ ділиться за модулем p на $f(x)$ без остачі, тобто, інакше кажучи, коли всі коефіцієнти остачі від ділення $x^p - x$ на $f(x)$ кратні p.

19. Якій конгруенції степеня нижче за 11 еквівалентна конгруенція

$$6x^{18} + 18x^{15} + 3x^4 - 8x^3 + x^2 + 3 \equiv 0 \pmod{11}?$$

Відповідь. $6x^8 + 7x^5 + 3x^4 + 3x^3 + x^2 + 3 \equiv 0 \pmod{11}$.

20. Звести конгруенцію

$$5x^{24} + 4x^{23} + 4x^{22} + 2x^{21} + x^{20} + 6x^{19} + 4x^{18} + 3x^{17} + 4x^{16} + 6x^{15} + 5x^{14} + 2x^{13} + x^{12} + 2x^{11} + x^{10} + 3x^9 + 4x^8 + 2x^7 + 5x^6 + 6x^5 + 5x^4 + 3x^3 + 4x^2 + 4x + 2 \equiv 0 \pmod{7}$$

до еквівалентної конгруенції степеня нижче 7 і потім розв'язати її.

Відповідь. $x \equiv 2 \pmod{7}$.

21. Знайти частку і остачу від ділення за модулем 17 многочлена $f(x) = 5x^4 - 7x^3 + 5x^2 - 6x + 3$ на многочлен $\varphi(x) = 3x^2 + 7x - 1$.

Відповідь. Частка $q(x) = 13x^2 + 7x + 1$, остача $r(x) = 11x + 4$.

22. Перевірити теорему Вільсона для $p = 11$ і $p = 17$.

23 Користуючись теоремою Вільсона, довести, що конгруенцію

$$x^2 \equiv -1 \pmod{p};\ p = 4n + 1$$

задовольняє число $(2n)!$ Наприклад: $(6!)^2 \equiv -1 \pmod{13}$.

24. Звести такі квадратичні конгруенції до двочленних: а) $4x^2 - 11x - 3 \equiv 0 \pmod{13}$; б) $5x^2 - 11x + 16 \equiv 0 \pmod{45}$; в) $12x^2 + 8x - 15 \equiv 0 \pmod{44}$.

Відповідь. а) $y^2 \equiv 0 \pmod{13}$, $y = x - 3$; б) $y^2 \equiv -16 \pmod{225}$, $y = 5x + 17$; в) $y^2 \equiv 5 \pmod{44}$, $y = 6x + 2$.

25. Знайти всі квадратичні лишки за модулем 53.

Відповідь. 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.

26. Користуючись критерієм Ейлера, визначити, які з чисел 2, 6, 8 — квадратичні лишки, а які — квадратичні нелишки за модулем 19.

Відповідь. 6 — квадратичний лишок, 2, 8 — квадратичні нелишки.

27. Довести, що конгруенції: а) $x^2 \equiv 579 \pmod{821}$, б) $x^2 = 728 \pmod{919}$, в) $x^2 \equiv 847 \pmod{1087}$, г) $x^2 \equiv 3776 \pmod{5987}$ не мають розв'язків.

28. Показати, що конгруенція $x^2 \equiv 3149 \pmod{5987}$ має два розв'язки.

29. Обчислити символи Лежандра і Якобі: а) $\left(\frac{1613}{601}\right)$; б) $\left(\frac{3153}{1201}\right)$; в) $\left(\frac{20\,470}{1847}\right)$; г) $\left(\frac{783\,456}{9\,073\,421}\right)$; д) $\left(\frac{93\,979}{4\,567\,891}\right)$.

Відповідь. а) -1; б) $+1$; в) -1; г) $+1$; д) -1.

30. Розв'язати конгруенції: а) $\left(\frac{x}{15}\right) = +1$; б) $\left(\frac{x}{15}\right) = -1$.

Відповідь: а) $x \equiv 1, 2, 4, 8 \pmod{15}$; б) $x \equiv 7, 11, 13, 14 \pmod{15}$.

31. Розв'язати конгруенції: а) $x^2 \equiv 7 \pmod{27}$; б) $x^2 - 7x + 1 \equiv 0 \pmod{45}$. в) $x^2 \equiv 282 \pmod{343}$; г) $x^2 \equiv 681 \pmod{1024}$; д) $x^2 \equiv 421 \pmod{700}$.

Відповідь. а) $x \equiv \pm 13 \pmod{27}$; б) $x \equiv 11, 26, 41 \pmod{45}$; в) $x \equiv \pm 25 \pmod{343}$; г) $x \equiv \pm 243, \pm 269 \pmod{1024}$; д) $x \equiv \pm 111, \pm 139, \pm 211, \pm 239 \pmod{700}$.

32. *Конгруенцію з n невідомими $x_1, x_2, \ldots, x_n$ називають конгруенцією виду*

$$f(x_1, x_2, \ldots, x_n) \equiv 0 \pmod{m}, \qquad (1)$$

де $f(x_1, x_2, \ldots, x_n)$ — многочлен від $x_1, x_2, \ldots, x_n$ з цілими коефіцієнтами і m — натуральне число.

Розв'язати конгруенцію (1) — означає знайти всі цілі значення невідомих $x_1, x_2, \ldots, x_n$, які задовольняють цю конгруенцію.

Дві конгруенції з тими самими невідомими називаються *рівносильними або еквівалентними*, якщо їх задовольняють ті самі значення невідомих $x_1, x_2, \ldots, x_n$.

Довести:

1) якщо $x_1 = a_1, \ldots, x_n = a_n$ задовольняє конгруенцію (1), то $b_i \equiv a_i \pmod{m}$ $(i = 1, 2, \ldots, n)$ також будуть задовольняти конгруенцію (1).

Класи чисел $x_1 \equiv a_1$, $x_2 \equiv a_2, \ldots, x_n \equiv a_n \pmod{m}$, які задовольняють конгруенцію (1), вважають за один розв'язок цієї конгруенції.

Конгруенцію (1) називають *розв'язною*, якщо вона має хоча б один розв'язок, і *нерозв'язною*, якщо вона не має жодного розв'язку.

2) кожна конгруенція (1), в якій хоча б один з коефіцієнтів $\not\equiv 0 \pmod{m}$, має скінченну множину розв'язків.

33. Довести, що при простому модулі p на систему конгруенцій першого степеня з кількома невідомими

$$a_{i1}x_1 + \cdots + a_{in}x_n \equiv b_i \pmod{p} \quad (i = 1, 2, \ldots, m), \qquad (2)$$

де a_{ij}, b_i — цілі числа, можна поширити всі результати загальної теорії лінійних рівнянь. Якщо через A_{ij} позначити клас, лишком якого є a_{ij}, і через B_i — клас з лишком b_i, то системі конгруенцій (2) відповідатиме система лінійних рівнянь:

$$A_{11}X_1 + \cdots + A_{1n}X_n = B_1,$$
$$\cdots\cdots\cdots\cdots$$
$$A_{m1}X_1 + \cdots + A_{mn}X_n = B_m,$$

де $X_1, X_2, \ldots, X_n$ — класи, лишками яких є невідомі $x_1, x_2, \ldots, x_n$.

34. Користуючись результатами попередньої задачі, дослідити й розв'язати такі системи конгруенцій першого степеня:

$$\text{а)} \begin{cases} x_1 + x_2 + 2x_3 + 3x_4 \equiv 1 \\ 3x_1 - x_2 - x_3 - 2x_4 \equiv -4 \\ 2x_1 + 3x_2 - x_3 - x_4 \equiv -6 \\ x_1 + 2x_2 + 3x_3 - x_4 \equiv 0 \end{cases} \pmod{31};$$

$$\text{б)} \begin{cases} 2x_1 + 5x_2 + 3x_3 \equiv 1 \\ 4x_1 + 6x_2 + 8x_3 \equiv 9 \\ 2x_1 - 8x_2 + x_3 \equiv 1 \end{cases} \pmod{17};$$

$$\text{в)} \begin{cases} x_1 + x_2 + x_3 - x_4 \equiv 1 \\ x_1 + x_2 - x_3 - 2x_4 \equiv 0 \\ 3x_1 + 3x_2 - 8x_3 + 7x_4 \equiv 5 \end{cases} \pmod{31}.$$

Відповідь.

а) $x_1 \equiv 5$, $x_2 \equiv -13$, $x_3 \equiv 15$, $x_4 \equiv -7 \pmod{31}$;

б) $x_1 \equiv 7 - 7x_3$, $x_2 \equiv -6 - 8x_3 \pmod{17}$;

в) система несумісна.

35. Довести, що коли детермінант D системи n лінійних конгруенцій з n невідомими

$$a_{i1}x_1 + \cdots + a_{in}x_n \equiv b_i \pmod{m} \quad (i = 1, 2, \ldots, n)$$

взаємно простий з модулем m, то ця система має єдиний розв'язок. Він визначається за формулами, аналогічними до формул Крамера:

$$x_i \equiv \frac{D_i}{D} \pmod{m} \quad (i = 1, 2, \ldots, n),$$

де D_i — детермінант, який дістаємо заміною в D i-го степеня стовпцем з вільних членів цієї системи.

36. Вказати метод знаходження розв'язків системи конгруенцій:

$$a_{i1}x_1 + \cdots + a_{in}x_n \equiv b_i \pmod{p^\alpha} \quad (i = 1, 2, \ldots, n),$$

де p — просте число; $\alpha > 1$ — ціле число з розв'язків тієї самої системи за модулем $p^{\alpha-1}$.

ІСТОРИЧНІ КОМЕНТАРІ

1. Задачі, які зводяться до розгляду системи конгруенцій 1-го степеня, розглядалися приблизно в 1 ст. китайськими математиками. Незалежно від китайських математиків спосіб розв'язання таких задач дав відомий індійський математик і астроном Брамагупта (VII ст.).

2. Теорему 5 § 24 називають теоремою Лагранжа. Він сформулював і довів її в 1768 р. Доведення, подане в підручнику, близьке до доведення,

яке дав Гаусс. Аналогічне твердження в алгебрі справедливе для рівнянь над довільним числовим полем.

3. Теорему, сформульовану англійським математиком Вільсоном (1714—1786), опублікував Варінг у 1770 р. в своїх «Алгебраїчних роздумах». Варінг і назвав її ім'ям свого учня. Точніше цю теорему можна назвати теоремою Вільсона — Варінга. Подане нами доведення цієї теореми належить Лагранжу. У зв'язку з цією теоремою (критерієм) останнім часом було вивчено подільність чисел $(p-1)!+1$ на p^2, для $p<30000$. З'ясувалося, що $(p-1)!+1$ ділиться на p^2 лише для $p=5$, 13 і 536.

4. У 1798 р. Лежандр опублікував твір: «Essai sur la theorie de nombres», який по суті є першим твором, що був спеціально присвячений теорії чисел і мав великий вплив на дальший її розвиток. У цій книзі Лежандр уперше ввів символ, який ми називаємо тепер символом Лежандра.

5. Властивість 3 символу Лежандра іноді називають першою додатковою теоремою, п'яту властивість — другою додатковою теоремою до закону взаємності; їх сформулював ще Ферма, а довів вперше Ейлер.

6. Закон взаємності (властивість 6) у повному обсязі, хоч і в трохи іншій формі, — вперше був сформульований без доведення ще Ейлером у 1783 р. Незалежно від Ейлера цей закон відкрив і довів Лежандр у 1785 р., але його доведення було неповним. Уперше закон взаємності квадратичних лишків довів Гаусс у 1796 р.; згодом йому вдалося дати сім різних доведень цього закону. Після Гаусса іншими вченими було дано ще понад 50 доведень, серед яких слід зазначити доведення Золотарьова Є. І.

7. Відомі деякі узагальнення закону взаємності на випадки лишків степенів n $(n>2)$.

Закон взаємності квадратичних лишків було перенесено також на конгруенції, які розглядаються в довільних полях. Цікаві результати про закони взаємності загального виду дав у ряді своїх праць І. Р. Шафаревич.

8. У 1918 р. академік І. М. Виноградов і відомий американський математик Пойа (або Поліа), незалежно один від одного дістали нерівність

$$\sum_{0<a<h}\left(\frac{a}{p}\right)\Bigg|<\sqrt{p}\ln p,$$

де $\left(\frac{a}{p}\right)$ — символ Якобі.

Ця нерівність встановлює достатню гладкість розподілу квадратичних лишків і нелишків. Вона була початком серії праць, присвячених розподілу квадратичних лишків і нелишків. Аналогічну нерівність розглядав І. М. Виноградов для лишків n-го степеня. Дослідження І. М. Виноградова з цього питання розвивали у своїх працях як вітчизняні, так і іноземні вчені. Теорію квадратичних лишків можна застосувати для знаходження простих дільників натуральних чисел (див., наприклад, А. А. Бухштаб. Теорія чисел. М., «Просвещение», 1966, стор. 189—191).

9. Символ Якобі був запроваджений у 1837. К. Якобі відомий переважно своїми працями з різних галузей математичного аналізу і механіки. У теорію чисел він зробив великий внесок своїми працями з теорії кубічних і біквадратних лишків.

10. Систему n лінійних конгруенцій з n невідомими вивчав Гаусс. Повне дослідження систем лінійних конгруенцій дав німецький математик Фробеніус (1849—1917) і англійський математик Стейніц (1871—1928) наприкінці XIX ст.

Розділ V

СТЕПЕНЕВІ ЛИШКИ

§ 29. Класи, що належать до даного показника. Основні властивості показників

Припустимо, що a і $m>0$ є цілі числа і $(a, m)=1$; тоді, як відомо, буде справедлива теорема Ейлера:

$$a^{\varphi(m)}\equiv 1 \pmod m. \tag{1}$$

З конгруенції (1) випливає, що існують такі цілі додатні γ, для яких $a^\gamma\equiv 1 \pmod m$ наприклад $\gamma=\varphi(m)$.

Найменше натуральне число δ, для якого

$$a^\delta\equiv 1 \pmod m,$$

називається *показником, до якого належить число a за модулем m.*

Теорема. *Якщо* $a_1\equiv a_2 \pmod m$, то a_1 і a_2 *належать до одного й того самого показника за цим модулем.*

Справді, припустимо, що $a_1\equiv a_2 \pmod m$ (звичайно a_1 і a_2 взаємно прості з m) і припустимо, що a_1 належить до показника δ_1, а a_2 — до показника δ_2 за модулем m. Тоді, піднісши обидві частини конгруенції $a_1\equiv a_2 \pmod m$ до степеня δ_1, дістанемо:

$$a_1^{\delta_1}=a_2^{\delta_1} \pmod m.$$

Але $a_1^{\delta_1}\equiv 1 \pmod m$, тому $a_2^{\delta_1}\equiv 1 \pmod m$, звідки $\delta_2\leqslant\delta_1$. Так само, підносячи обидві частини конгруенції $a_1\equiv a_2 \pmod m$ до степеня δ_2, знайдемо, що $\delta_1\leqslant\delta_2$. Отже, дістанемо, що $\delta_1=\delta_2$. Цим теорему доведено.

Отже, далі, говорячи про число a, яке належить до показника δ за модулем m, завжди матимемо на увазі весь клас чисел за цим модулем, одним з лишків якого є a.

Основні властивості показників. 1. *Якщо a належить до показника* δ *за модулем m, то в ряді степенів*

$$1=a^0,\ a,\ a^2,\ \ldots,\ a^{\delta-1}. \tag{2}$$

всі числа не конгруентні одне з одним за модулем m.

Справді, припустимо супротивне, тобто припустимо, що $a^k\equiv a^l \pmod m$ $(k,\ l=0,\ 1,\ 2,\ \ldots,\ \delta-1)$; нехай для визначеності $k>l$. Скорочуючи обидві частини цієї конгруенції на a^l (за умовою $(a,\ m)=1$), дістанемо: $a^{k-l}\equiv 1 \pmod m$, але $0\leqslant l<k<\delta$, або $0<k-l<\delta$, а це суперечить означенню показника δ.

2. *Якщо a належить до показника* δ *за модулем m, то конгруенція*

$$a^\gamma\equiv a^{\gamma'} \pmod m,$$

де γ *і* γ' *— деякі цілі невід'ємні числа, має місце тоді і тільки тоді, коли*

$$\gamma \equiv \gamma' \pmod{\delta}.$$

Справді, нехай r і r' є найменші невід'ємні лишки чисел γ і γ' за модулем δ; тоді при деяких q і q' матимемо

$$\gamma = \delta q + r, \quad \gamma' = \delta q' + r'.$$

Через те що за умовою

$$a^{\delta} \equiv 1 \pmod{m},$$

то

$$a^{\gamma} = a^{\delta q + r} = (a^{\delta})^{q} \cdot a^{r} \equiv a^{r} \pmod{m}, \quad 0 \leqslant r < \delta;$$
$$a^{\gamma'} = a^{\delta q' + r'} = (a^{\delta})^{q'} \cdot a^{r'} \equiv a^{r'} \pmod{m}, \quad 0 \leqslant r' < \delta.$$

З останніх конгруенцій робимо висновок, що коли $a^{\gamma} \equiv a^{\gamma'} \pmod{m}$, то

$$a^{r} \equiv a^{r'} \pmod{m};$$

але за властивістю 1 всі степені a^{k} $(k = 0, 1, \ldots, \delta - 1)$ неконгруентні між собою за модулем m, тому з останньої конгруенції маємо $r = r'$, а це означає, що

$$\gamma \equiv \gamma' \pmod{\delta}.$$

Навпаки, якщо

$$\gamma \equiv \gamma' \pmod{\delta},$$

то $r = r'$ і $a^{r} \equiv a^{r'} \pmod{m}$, а тому й

$$a^{\gamma} \equiv a^{\gamma'} \pmod{m}.$$

Висновок. *Якщо* a *належить до показника* δ *за модулем* m, *то конгруенція* $a^{\gamma} \equiv 1 \pmod{m}$ *має місце тоді і тільки тоді, коли* γ *ділиться на* δ, *тобто коли* $\gamma \equiv 0 \pmod{\delta}$.

Це твердження є окремий випадок властивості 2 при $\gamma' = 0$.

3. *Якщо* a *належить до показника* δ *за модулем* m, *то* δ *буде дільником числа* $\varphi(m)$.

Справді, за теоремою Ейлера $a^{\varphi(m)} \equiv 1 \pmod{m}$, а на підставі попереднього висновку бачимо, що $\varphi(m)$ ділиться на δ.

Отже, показники δ, до яких можуть належати різноманітні числа a, взаємно прості з модулем m, треба шукати тільки серед дільників числа $\varphi(m)$.

Приклад. Знайти показник, до якого належить число 5 за модулем 44. Знаходимо

$$\varphi(44) = \varphi(4)\,\varphi(11) = 20.$$

Отже, показник δ, до якого належить число 5 за модулем 44, треба шукати серед додатних дільників чисел 20, тобто серед чисел 1, 2, 4, 5, 10, 20. Матимемо:

$$5^{1} \equiv 5, \quad 5^{2} \equiv 25, \quad 5^{4} \equiv 9, \quad 5^{5} \equiv 1 \pmod{44}.$$

Отже, шуканий показник $\delta = 5$.

Контрольні запитання

1. Дайте означення показника, до якого належить число a за модулем m.
2. З якої теореми випливає існування показника, до якого належить a за модулем m, якщо $(a, m) = 1$?
3. Перелічіть основні властивості показників.
4. Серед чисел якого виду міститься показник, до якого належить число a за модулем m?

§ 30. Первісні корені. Теорема про число класів первісних коренів

Особливий інтерес становить випадок, коли показник δ, до якого належить a за модулем m, збігається з числом $\varphi(m)$.

Число a, яке належить до показника $\varphi(m)$ за модулем m, називається *первісним коренем* за цим модулем.

З властивості 1, § 29, безпосередньо випливає таке твердження.

Теорема 1. *Якщо* a *— первісний корінь за модулем* m, *то степені*

$$1 = a^{0}, \ a, \ a^{2}, \ \ldots, \ a^{\varphi(m)-1} \tag{1}$$

утворюють зведену систему лишків за цим модулем.

Справді, згідно з властивістю 1, § 29, ці степені один з одним неконгруентні за модулем m. Крім того, кожен з цих степенів взаємно простий з m, бо $(a, m) = 1$ за умовою; кількість чисел ряду (1) дорівнює $\varphi(m)$. Тоді, за властивістю, 1, § 18, зведеної системи лишків, можна зробити висновок, що $\varphi(m)$ чисел ряду (1) утворюють зведену систему лишків за модулем m.

Припустимо тепер, що модуль $m = p$ є просте число. Тоді первісні корені за модулем p належатимуть до показника $\varphi(p) = p - 1$, а інші показники, до яких належатимуть зведені класи чисел за модулем p, будуть дільниками числа $p - 1$.

Доведемо тепер існування первісних коренів за простим модулем p.

Спочатку доведемо такі два допоміжні твердження.

Лема 1. *Якщо* a *належить до показника* δ *за модулем* p, *то*

$$1 = a^{0}, \ a, \ a^{2}, \ \ldots, \ a^{\delta-1} \tag{2}$$

є всі розв'язки конгруенції

$$x^{\delta} \equiv 1 \pmod{p}. \tag{3}$$

Справді, числа ряду (2), за доведеним, неконгруентні між собою за модулем p і взаємно прості з p, тобто належать до різних зведених класів за цим модулем; кожне з них задовольняє конгруенцію (3), число їх дорівнює δ, а остання конгруенція, як конгруенція за простим модулем p, більш як δ розв'язків мати не може. Отже, числами ряду (2) вичерпуються всі розв'язки конгруенції (3).

Лема 2. *Якщо серед чисел, які не діляться на p, є хоч би одне число a, що належить до показника δ, то всього класів таких чисел буде точно $\varphi(\delta)$.*

Справді, за лемою 1, всяке число x, що належить до показника δ, повинно задовольняти конгруенцію (3), тобто бути конгруентним з одним з чисел ряду (2). Тому числа, які належать, поряд з a, до показника δ, треба шукати серед чисел ряду (2). Припустимо, що будь-яке число a^k ($k = 0, 1, \ldots, \delta - 1$) ряду (2) належить до показника z, тоді z буде найменшим додатним числом, яке задовольняє конгруенцію:

$$(a^k)^z \equiv 1 \pmod p, \text{ або } a^{kz} \equiv 1 \pmod p. \tag{4}$$

Розглянемо тепер два випадки:

1) $(k, \delta) = 1$. Покажемо, що в цьому випадку $z = \delta$, тобто a^k належить до показника δ.

Справді, оскільки за умовою a належить до показника δ, то $a^\delta \equiv 1 \pmod p$. Беручи до уваги конгруенцію (4), внаслідок властивості 2, § 29, робимо висновок, що kz має ділитись на δ. За умовою z є найменше додатне число, що задовольняє конгруенцію

$$(a^k)^z \equiv 1 \pmod p,$$

але $(a^k)^\delta \equiv 1 \pmod p$ за лемою 1, тому δ буде також ділитись на z; отже, $z > 0$ і $\delta > 0$ діляться одне на одне, а це й означає, що $z = \delta$.

2) $(k, \delta) = d > 1$. Покажемо, що в цьому випадку $z \neq \delta$, тобто a^k не належить до показника δ.

Маємо: $k = k_1 d$, $\delta = \delta_1 d$. Але тоді конгруенція (4) буде задовольнятися цілим додатним значенням $z = \frac{\delta}{d}$:

$$(a^k)^z \equiv a^{k_1 d \frac{\delta}{d}} = (a^\delta)^{k_1} \equiv 1 \pmod p,$$

тобто показник z, до якого належить a^k за модулем p, буде вже менший за δ.

З розглянутих випадків можна зробити такий висновок: якщо a належить до показника δ за модулем p, то з ряду чисел (2) до цього показника належатимуть числа a^k ($k = 0, 1, 2, \ldots, \delta - 1$) тоді і тільки тоді, коли $(k, \delta) = 1$; але чисел k, менших за δ і взаємно простих з δ, буде рівно $\varphi(\delta)$; лему 2 доведено повністю.

Теорема 2. (про число класів первісних коренів за простим модулем). *Існує точно $\varphi(\delta)$ класів чисел, що належать до показника δ. Зокрема, точно $\varphi(p-1)$ первісних коренів за простим модулем p.*

Справді, позначимо через $\psi(\delta)$ число зведених класів чисел, що належать до показника δ за модулем p; через те, що всього зведених класів чисел за простим модулем p буде $p - 1$ і кожен з них належить до якого-небудь показника за цим модулем, то можна записати, що

$$\sum_{\delta | p-1} \psi(\delta) = p - 1,$$

де δ пробігає дільники числа $p - 1$ (див. властивість 3, § 29). З другого боку, за теоремою 4, § 14, при $n = p - 1$ маємо

$$\sum_{\delta | p-1} \varphi(\delta) = p - 1,$$

де $\varphi(\delta)$ є функція Ейлера.

Отже, маємо рівність:

$$\sum_{\delta | p-1} \psi(\delta) = \sum_{\delta | p-1} \varphi(\delta). \tag{5}$$

Згідно з лемою 2 для всіх δ, що є дільниками числа $p - 1$, або $\psi(\delta) = \varphi(\delta)$, або $\psi(\delta) = 0$. Але припущення, що $\psi(\delta) = 0$ відпадає, бо коли б який-небудь доданок у лівій частині рівності (5) дорівнював нулю, у правій частині цієї рівності був би зайвий додатний член, бо $\varphi(\delta)$ завжди > 0, і рівність (5) перестала б бути правильною. Отже, $\psi(\delta) = \varphi(\delta)$ для будь-якого δ, що є дільником числа $p - 1$. Теорему доведено.

При $\delta = p - 1$ дістанемо, зокрема, що число первісних коренів за простим модулем p дорівнює $\varphi(p - 1)$.

Практично зручного способу знаходження первісних коренів, тобто принаймні одного первісного кореня, за даним модулем немає; доводиться застосовувати просто спосіб випробувань, який можна тільки трохи удосконалити. Але якщо вже один первісний корінь a за модулем p знайдено, то інші, згідно з лемою 2, визначаються серед чисел, конгруентних з числами a^k, при $0 < k \leqslant p - 2$ і $(k, p - 1) = 1$.

Приклад. Знайти показники, до яких належать зведені класи чисел за простим модулем 19, зокрема знайти всі первісні корені.

Маємо $\varphi(19) = 18$; для δ будуть такі можливі значення: 1, 2, 3, 6, 9, 18. Отже, за теоремою Гаусса, число зведених класів чисел за модулем 19, що належать до показників 1, 2, 3, 6, 9, 18, дорівнюватиме відповідно:

$$\varphi(1) = 1,\ \varphi(2) = 1,\ \varphi(3) = 2,\ \varphi(6) = 2,\ \varphi(9) = 6,\ \varphi(18) = 6.$$

До показника 1 належить очевидно клас чисел з лишком 1, бо $1^1 \equiv 1 \pmod{19}$. Знайдемо, до якого показника належить лишок 2 (конгруенції беремо за модулем 19):

$$2^1 \equiv 2,\ 2^2 \equiv 4,\ 2^3 \equiv 8,\ 2^6 \equiv 7,\ 2^9 \equiv -1,\ 2^{18} \equiv 1.$$

Отже, 2 є первісним коренем за модулем 19. Інші 5 первісних коренів можна знайти, за лемою 2, серед чисел 2^k, де $(k, 18) = 1$ і $0 < k < 17$; останні умови задовольняють значення $k = 1, 5, 7, 11, 13, 17$. Отже, іншими первісними коренями за модулем 19 будуть

$$2^5 \equiv 13,\ 2^7 \equiv 14,\ 2^{11} \equiv 15,\ 2^{13} \equiv 3,\ 2^{17} \equiv 10 \pmod{19}.$$

Цим знайдено всі первісні корені за модулем 19:

$$2,\ 3,\ 10,\ 13,\ 14,\ 15.$$

Будемо шукати тепер показник, до якого належить, наприклад, число 4; з розгляду вже можна виключити показники $\delta = 1; 18$. Маємо:

$$4^2 \equiv 16,\ 4^3 \equiv 7,\ 4^6 \equiv 11,\ 4^9 \equiv 1 \pmod{19};$$

отже, 4 належить до показника 9 за модулем 19. Решта чисел, що належить до цього показника, буде:

$$4^2 \equiv 16,\ 4^4 \equiv 9,\ 4^5 \equiv 17,\ 4^7 \equiv 6,\ 4^8 \equiv 5.$$

Отже, до показника 9 належатимуть числа: 4, 5, 6, 9, 16, 17. Знайдемо тепер наприклад, до якого показника належить число 7 за модулем 19; з розгляду вже можна виключити показники $\delta = 1, 9, 18$. Маємо $7^2 \equiv 11$, $7^3 \equiv 1$; отже 7 належить до показника 3 за модулем 19; другим числом, що належить до цього показника, буде $7^2 \equiv 11 \pmod{19}$.

Далі, бачимо, що, наприклад, 8 не належить до жодного з показників $\delta = 1, 3, 9, 18$. Отже, 8 належить або до показника 2, або до показника 6: $8^2 \equiv 7$, $8^6 \equiv 1$, отже, 8 належить до показника 6 за модулем 19. Другим числом, що належить до цього показника, на підставі тієї самої леми 2, буде $8^5 \equiv 12$. Тепер бачимо, що 18 не належить до жодного з показників $\delta = 1, 3, 6, 9, 18$. Отже, воно належатиме до показника $\delta = 2$, у чому легко переконатися і безпосередньо.

У підсумку дістали: до показника 1 належить число 1, до показника 2 — число 18; до показника 3 — числа 7 і 11; до показника 6 — числа 8, 12; до показника 9 — числа 4, 5, 6, 9, 16, 17, до показника 18 — числа 2, 3, 10, 13, 14, 15, які будуть первісними коренями.

У випадку складеного модуля m первісних коренів може і не бути. Наприклад, легко перевірити, що за модулем 21 немає первісних коренів. Справді, маємо

$$\varphi(21) = 12;\ \delta = 1, 2, 3, 4, 6, 12.$$

Числами, взаємно простими з 21, будуть:

$$1, 2, 4, 5, 8, 10, 11, 13, 16, 17, 19, 20;$$

безпосередньо знаходимо (конгруенції беремо за модулем 21):

$$\begin{array}{llll} 1^1 \equiv 1; & 2^2 \equiv 4; & 2^3 \equiv 8; & 2^4 \equiv 16; \\ 2^6 \equiv 1; & 4^2 \equiv 16; & 4^3 \equiv 1; & 5^2 \equiv 4; \\ 5^3 \equiv -1; & 5^4 \equiv 16; & 5^6 \equiv 1; & 8^2 \equiv 1; \\ 10^2 \equiv 16; & 10^3 \equiv 13; & 10^4 \equiv 4; & 10^6 \equiv 1; \\ 11^2 \equiv 16; & 11^3 \equiv 8; & 11^4 \equiv 4; & 11^6 \equiv 1; \\ 13^2 \equiv 1; & 16^2 \equiv 4; & 16^3 \equiv 1; & 17^2 \equiv 16; \\ 17^3 \equiv -1; & 17^4 \equiv 4; & 17^6 \equiv 1; & 19^2 \equiv 4; \\ 19^3 \equiv 15; & 19^4 \equiv 16; & 19^6 \equiv 1; & 20^2 \equiv 1. \end{array}$$

Отже, до показника 1 належить число 1, до показника 2 — числа 8, 13, 20; до показника 3 — числа 4, 16; до показника 6 — решта чисел: 2, 5, 10, 11, 13, 19. Бачимо, що до показників 4 і 12 за модулем 21 не належить жодний клас чисел, тому за модулем 21 немає первісних коренів.

У випадку складеного модуля $m = p_1^{\alpha_1} p_2^{\alpha_2} \dots p_k^{\alpha_k}$ первісні корені можуть бути тільки для $m = 4$ і модулів виду $m = p^\alpha$ та $m = 2p^\alpha$, де p — просте непарне число. Не спиняючись докладно на всіх випадках, зауважимо, що основна причина цього полягає в тому, що найменше спільне кратне чисел $\varphi(p_1^{\alpha_1})$, $\varphi(p_2^{\alpha_2})$, $\dots$, $\varphi(p_k^{\alpha_k})$, взагалі кажучи, менше, ніж їхній добуток.

Для прикладу доведемо таке твердження.

Теорема 3. *Якщо m непарне складене число, яке містить принаймні два різних простих множники, то за модулем m немає первісних коренів.*

Справді, припустимо, що

$$(a, m) = 1;\quad m = p_1^{\alpha_1} p_2^{\alpha_2} \dots p_k^{\alpha_k},$$

де $k \geqslant 2$ і $p_1, p_2, \dots, p_k$ — різні прості непарні числа. Очевидно, що $(a, p_i^{\alpha_i}) = 1$, звідси, за теоремою Ейлера, дістанемо:

$$a^{\varphi(p_i^{\alpha_i})} \equiv 1 \pmod{p_i^{\alpha_i}},$$

або

$$a^{p_i^{\alpha_i - 1}(p_i - 1)} \equiv 1 \pmod{p_i^{\alpha_i}}. \tag{6}$$

Через те що $p_i - 1$ — парне число, то

$$\frac{1}{2} p_1^{\alpha_1 - 1} p_2^{\alpha_2 - 1} \dots p_k^{\alpha_k - 1} (p_1 - 1)(p_2 - 1) \dots (p_k - 1) = \frac{1}{2}\varphi(m)$$

є цілим і кратним $(p_1^{\alpha_i - 1})(p_i - 1)$, тобто

$$\frac{1}{2}\varphi(m) = p_i^{\alpha_i - 1}(p_i - 1) q_i,$$

де q_i — ціле додатне число. Звідси, підносячи обидві частини конгруенції (6) до q_i-го степеня, матимемо:

$$a^{\frac{1}{2}\varphi(m)} \equiv 1 \pmod{p_i^{\alpha_i}} \quad (i = 1, 2, \dots, k).$$

З останньої системи конгруенцій випливає, що $a^{\frac{1}{2}\varphi(m)} \equiv 1 \pmod{m}$, тобто число a за модулем m належить до показника, який не перевищує $\frac{1}{2}\varphi(m)$.

Отже, будь-яке a, взаємно просте з m, не може бути первісним коренем за модулем m. Теорему доведено.

З теорем 2 і 3 та з задачі № 5, 6, 7, 8, 9, 11 випливатиме, що первісні корені існують лише за модулем $m = 2,\ 4,\ p^\alpha,\ 2p^\alpha$, де p — просте непарне число і α — ціле, не менше за 1.

Контрольні запитання

1. Яке число a називається первісним коренем за модулем m?
2. Чи достатньо конгруенції $a^{\varphi(m)} \equiv 1 \pmod m$ для того, щоб число a було — первісним коренем за модулем m?
3. Чому числа ряду $1 = a^0,\ a,\ a^2,\ \dots,\ a^{\varphi(m)-1}$ не конгруентні між собою за модулем m, якщо a — первісний корінь?
4. Які числа належать показнику δ за простим модулем p, коли відомо що a належить показнику δ за цим модулем?
5. Чи можна з леми 2 зробити висновок про існування первісного кореня за простим модулем p.
6. Чому дорівнює число первісних коренів за модулем p?

§ 31. Індекси та їхні властивості[1]

Нехай g — первісний корінь за простим модулем p, отже, належить до показника $\varphi(p) = p - 1$; тоді, на підставі теореми 1, § 30, числа

$$1 = g^0,\ g,\ g^2,\ \dots,\ p^{p-2} \qquad (1)$$

утворюють зведену систему лишків за модулем p, тобто числами (1) подано всі зведені класи чисел за цим модулем.

Внаслідок цього, виконуючи операції над числами за модулем p, можна користуватись зведеною системою лишків (1) нарівні із зведеною системою найменших невід'ємних лишків 1, 2, 3, ..., $p - 1$. Щодо дій множення, ділення, піднесення до степеня і добування кореня, то це дає такі самі переваги, як і при переході до подання чисел у показниковій формі, тобто при користуванні логарифмами. Введемо тепер поняття індексу, яке відіграє в теорії конгруенцій роль, аналогічну до ролі логарифма.

Припустимо, що a є деяке ціле число, яке не ділиться на p, тобто $(a,\ p) = 1$, тоді a буде конгруентне з одним з чисел ряду (1). *Індексом числа a за модулем p при основі g називається таке ціле невід'ємне число γ, що*

$$g^\gamma \equiv a \pmod p.$$

Індекс числа a при основі g позначають символом

$$\gamma = \operatorname{ind}_g a, \text{ або } \gamma = \operatorname{ind} a.$$

[1] Поняття індексів і їхніх основних властивостей дав Гаусс.

На підставі сказаного, всяке a, взаємно просте з p, має деякий єдиний індекс γ' за модулем p серед чисел ряду

$$\gamma' = 0,\ 1,\ 2,\ \dots,\ p - 2.$$

Знаючи один з індексів, можемо вказати і всі індекси числа a за модулем p.

Справді, маємо $g^{\gamma'} \equiv a \pmod p$, припустимо, що γ є інший будь-який індекс числа a, тобто $g^\gamma \equiv a \pmod p$ отже,

$$g^\gamma \equiv g^{\gamma'} \pmod p;$$

але остання конгруенція виконується тоді і тільки тоді, коли (див. властивість 2, § 29):

$$\gamma \equiv \gamma' \pmod{p - 1}. \qquad (2)$$

Отже, *всі індекси заданого числа a за простим модулем p утворюють клас чисел* (2) *за модулем $p - 1$.*

Із самого означення індексу виходить, що числа одного й того самого класу за модулем p мають одні й ті самі індекси при основі g за модулем p.

Основні властивості індексів. 1. *Індекс добутку конгруентний із сумою індексів окремих множників за модулем $p - 1$, тобто*

$$\operatorname{ind}(a_1 a_2 \dots a_k) \equiv \operatorname{ind} a_1 + \operatorname{ind} a_2 + \dots + \operatorname{ind} a_k \pmod{p - 1}.$$

Справді, за означенням:

$$\begin{aligned} a_1 &\equiv g^{\operatorname{ind} a_1} \pmod p, \\ a_2 &\equiv g^{\operatorname{ind} a_2} \pmod p, \\ &\dots\dots\dots \\ a_k &\equiv g^{\operatorname{ind} a_k} \pmod p, \end{aligned}$$

звідки, перемножуючи, знаходимо:

$$a_1 a_2 \dots a_k \equiv g^{\operatorname{ind} a_1 + \operatorname{ind} a_2 + \dots + \operatorname{ind} a_k} \pmod p.$$

Користуючись доведеним раніше [див. конгруенцію (2)], дістанемо:

$$\operatorname{ind}(a_1 a_2 \dots a_k) \equiv \operatorname{ind} a_1 + \operatorname{ind} a_2 + \dots + \operatorname{ind} a_k \pmod{p - 1}.$$

Висновок.

$$\operatorname{ind} a^k \equiv k \operatorname{ind} a \pmod{p - 1}.$$

2. *Індекс дробу за модулем p: $\frac{b}{a} \pmod p$, тобто індекс розв'язку конгруенції $ax \equiv b \pmod p$, зокрема індекс звичайної частки $\frac{b}{a}$, якщо b ділиться на a, конгруентний з різницею індексів чисельника й знаменника за модулем $p - 1$.*

Справді, якщо $ax \equiv b \pmod p$ і a та b взаємно прості з p, то за властивістю 1 дістанемо:

$$\operatorname{ind} a + \operatorname{ind} x \equiv \operatorname{ind} b \pmod{p-1};$$

отже,

$$\operatorname{ind} x \equiv \operatorname{ind} b - \operatorname{ind} a \pmod{p-1}.$$

3. *Індекс одиниці завжди конгруентний з нулем, індекс основи конгруентний з одиницею* (за модулем $p-1$).

Ці твердження безпосередньо випливають з очевидних конгруенцій:

$$g^0 \equiv 1 \pmod p, \quad g^1 \equiv g \pmod p;$$

маємо:

$$\operatorname{ind} 1 \equiv 0 \pmod{p-1}, \quad \operatorname{ind} g \equiv 1 \pmod{p-1}.$$

Ми бачимо, що індекси мають багато аналогій з логарифмами. Можна сказати, що індекси — це логарифми за модулем. Зважаючи на практичну користь індексів, для простих модулів (звичайно, не надто великих) складено таблиці індексів. Це дві таблиці: одна для знаходження індексу за числом, а друга — для знаходження числа за індексом. Таблиці містять найменші невід'ємні лишки чисел (зведена система) і їхні найменші індекси (повна система) відповідно за модулями p і $p-1$. Кожна з таблиць має вигляд прямокутника; в рядку стоять цифри 0, 1, 2, ... , 9; у стовпчику цифр 0, 1, 2, ... ; номер рядка вказує число десятків, номер стовпчика — число одиниць числа (або індексу). У графі, спільній вказаним рядку й стовпчику, міститься відповідний індекс (число).

Для прикладу складемо таблиці індексів за модулем 23. Як неважко перевірити безпосередньо, число 5 є одним з первісних коренів за модулем 23. Визначаємо (конгруенції беремо за модулем 23):

$5^0 \equiv 1$;	$5^5 \equiv 20$;	$5^{10} \equiv 9$;	$5^{15} \equiv 19$;	$5^{20} \equiv 12$;
$5^1 \equiv 5$;	$5^6 \equiv 8$;	$5^{11} \equiv 22$;	$5^{16} \equiv 3$;	$5^{21} \equiv 14$;
$5^2 \equiv 2$;	$5^7 \equiv 17$;	$5^{12} \equiv 18$;	$5^{17} \equiv 15$;	(тут $p-2=21$).
$5^3 \equiv 10$;	$5^8 \equiv 16$;	$5^{13} \equiv 21$;	$5^{18} \equiv 6$;	
$5^4 \equiv 4$;	$5^9 \equiv 11$;	$5^{14} \equiv 13$;	$5^{19} \equiv 7$;	

Тому описані нами таблиці матимуть вигляд:

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							

1	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								

Приклад 1. Знайти індекс числа 21 за модулем 23.

На перетині рядка з номером 2 і стовпчика з номером 1 знаходимо за першою таблицею число 13, тобто $\operatorname{ind} 21 = 13$.

Приклад 2. $\operatorname{ind} N = 18$. Знайти N. За другою таблицею на перетині рядка за номером 1 і стовпчика з номером 8 знаходимо $N = 6$. У додатку 2 наведено таблицю індексів для простих чисел у межах першої сотні.

Зауваження. Таблицю індексів можна будувати і для зведеної системи лишків складеного модуля m, що має первісний корінь, причому, як неважко бачити, індекси будуть визначені тут з точністю до кратного $\varphi(m)$, а всі виведені властивості індексів будуть характерні і для цього випадку.

Контрольні запитання

1. Якщо g — первісний корінь за простим модулем p, то чи утворюють числа $g^0, g, g^2, \ldots, g^{p-2}$ зведену систему лишків за цим модулем? У чому переваги цієї зведеної системи лишків над будь-якою іншою?
2. Яке число називається індексом числа a за простим модулем p при основі g?
3. На підставі яких міркувань можна твердити, що всяке число a, взаємно просте з p, має єдиний індекс γ' менший від p?
4. Знаючи один індекс γ числа a за модулем p, назвати всі індекси цього числа a. За яким модулем вони утворюють клас чисел?
5. Назвіть основні властивості індексів.
6. Що являють собою таблиці індексів для даного простого числа p?
7. Чи можна побудувати таблиці індексів для складеного модуля m?

§ 32. Розв'язування двочленних конгруенцій з допомогою індексів

Конгруенція виду

$$ax^n \equiv b \pmod m, \tag{1}$$

де $a \not\equiv 0 \pmod m$ і n є натуральне число, називається *двочленною конгруенцією* з одним невідомим.

Зважаючи на те, що всяка конгруенція за складеним модулем зводиться до конгруенцій за простими модулями, ми обмежимось розглядом двочленної конгруенції:

$$ax^n \equiv b \pmod p, \quad (a, p) = 1, \tag{1'}$$

де p — просте число.

Покажемо, як з допомогою таблиць індексів можна розв'язати конгруенцію (1').

Застосовуючи властивості індексів до конгруенції (1'), дістанемо еквівалентну конгруенцію:

$$\operatorname{ind} a + n \operatorname{ind} x \equiv \operatorname{ind} b \pmod{p-1},$$

або

$$nz \equiv c \pmod{p-1}, \tag{2}$$

де $z = \operatorname{ind} x$, $c = \operatorname{ind} b - \operatorname{ind} a$. Отже, розв'язування конгруенції (1′) зводиться до розв'язування конгруенції (2) першого степеня.

Відомо, що коли $d = (n, p-1)$ і c *ділиться на* d, *то конгруенція* (2), *а отже, і конгруенція* (1′) *має* d *розв'язків; якщо ж* c *не ділиться на* d, *то конгруенція* (2), *а тому й конгруенція* (1′), *розв'язків мати не буде*.

Приклад. Розв'язати конгруенцію $15x^4 \equiv 17 \pmod{23}$.

Беремо індекси від обох частин конгруенції:

$$\operatorname{ind} 15 + 4 \operatorname{ind} x \equiv \operatorname{ind} 17 \pmod{22}.$$

З першої таблиці § 32 знаходимо, що $\operatorname{ind} 15 = 17$, $\operatorname{ind} 17 = 7$. Отже, маємо конгруенцію першого степеня відносно $\operatorname{ind} x$:

$$4 \operatorname{ind} x \equiv 12 \pmod{22}.$$

Ця конгруенція має два розв'язки, а саме:

$$\operatorname{ind} x \equiv 3; 14 \pmod{22}.$$

Тепер, за другою таблицею, знаходимо, що

$$x = 10, 13 \pmod{23}.$$

Зауважимо, що з допомогою таблиць індексів можна розв'язувати й конгруенції першого степеня за простим модулем. Для прикладу розв'яжемо конгруенцію $48x = 59 \pmod{83}$.

Переходячи від цієї конгруенції до співвідношень між індексами, дістанемо:

$$\operatorname{ind} 48 + \operatorname{ind} x \equiv \operatorname{ind} 59 \pmod{82}.$$

З таблиць індексів (див. додаток 2) знаходимо:

$$\operatorname{ind} 48 = 64, \quad \operatorname{ind} 59 = 20,$$

отже,

$$\operatorname{ind} x \equiv 20 - 64 \equiv 38 \pmod{82}.$$

З другої таблиці для $p = 83$ знайдемо:

$$x \equiv 41 \pmod{83}.$$

З а у в а ж е н н я. Цілком аналогічно можна застосовувати теорію індексів і для розв'язування конгруенцій

$$ax^n \equiv b \pmod{m} \qquad (1)$$

у випадку складеного модуля m, якщо для цього модуля існує хоча б один первісний корінь, то беручи його за основу, можна побудувати систему індексів.

При $m > 2$ матимемо конгруенцію

$$n \operatorname{ind} x \equiv \operatorname{ind} b - \operatorname{ind} a \pmod{\varphi(m)},$$

з якої знаходимо значення $\operatorname{ind} x$ (якщо, вони, звичайно, є), а за ними значення невідомого x.

Особливий інтерес становить двочленна конгруенція виду

$$x^n \equiv a \pmod{p}, \quad (a, p) = 1 \qquad (3)$$

Якщо ця конгруенція має розв'язки, то a називають *лишком степеня* n за модулем p, в противному разі a називають *нелишком степеня* n. Зокрема, при $n = 2$, як ми вже говорили, лишки і нелишки називають *квадратичними*; при $n = 3$ — *кубічними*; при $n = 4$ — *біквадратичними*.

Легко побачити, що конгруенцію (1′) завжди можна звести до двочленної конгруенції виду (3). Для цього досить обидві частини конгруенції (1′) помножити на таке α, щоб $a\alpha \equiv 1 \pmod{p}$. Поклавши $b\alpha \equiv a \pmod{p}$, ми дістанемо конгруенцію (3).

Теорема 1. *Конгруенція* (3) *розв'язна* (і тим самим a є лишок степеня n за модулем p) *тоді і тільки тоді, коли* $\operatorname{ind} a$ *кратний* $d = (n, p-1)$.

При розв'язності конгруенція (3) має d розв'язків. У зведеній системі лишків за модулем p число лишків степеня n дорівнює $\frac{p-1}{d}$.

Справді, конгруенція (3) еквівалентна конгруенції

$$n \operatorname{ind} x \equiv \operatorname{ind} a \pmod{p-1},$$

яка, як відомо, розв'язна тоді і тільки тоді, коли $\operatorname{ind} a$ ділиться на d, причому, у випадку її розв'язності ми знайдемо d значень для $\operatorname{ind} x$, їм відповідатимуть d розв'язків конгруенції (3).

Далі, серед чисел $0, 1, 2, \ldots, p-2$, що є найменшими індексами лишків зведеної системи за модулем p, буде $\frac{p-1}{d}$, кратних d. Їм відповідатимуть лишки степеня n. Отже, теорема повністю доведена.

Критерій розв'язності (теорема 1) конгруенції (3) можна подати і в іншій, більш закінченій формі.

Теорема 2. *Число* a *є лишком степеня* n *за простим модулем* p *тоді і тільки тоді, коли*

$$a^{\frac{p-1}{d}} \equiv 1 \pmod{p}. \qquad (4)$$

Справді, умова теореми 1 ($\operatorname{ind} a$ кратний d), тобто $\operatorname{ind} a \equiv 0 \pmod{d}$ еквівалентна тому, що

$$\frac{p-1}{d} \cdot \operatorname{ind} a \equiv 0 \pmod{p-1}.$$

Ми помножили обидві частини попередньої конгруенції і модуль на $\frac{p-1}{d}$. Але, переходячи тепер від індексів до чисел, дістанемо еквівалентну конгруенцію (4). Навпаки, з конгруенції (4) виходить,

що $\frac{p-1}{d}\operatorname{ind} a \equiv 0 \pmod{p-1}$; ділячи обидві частини останньої конгруенції і модуль на ціле число $\frac{p-1}{d}$, дістанемо $\operatorname{ind} a \equiv 0 \pmod{d}$, тобто $\operatorname{ind} a$ кратний d.

При $n=2$ завжди і $d=2$, бо якщо p є число непарне, то $p-1$ є парне, і умова (4) перетворюється в критерій Ейлера.

Зауваження. Знаючи таблицю індексів за простим модулем p, можна знайти всі лишки степеня n, відібравши числа, в яких індекси діляться на $d=(n, p-1)$; решта чисел будуть нелишками степеня n.

Приклад 1. Знайти всі біквадратичні лишки за модулем 29. Тут $d=(4, 28)=4$. Вибираємо з таблиці індексів ті числа, індекси яких кратні 4: 1, 7, 8, 16, 20, 23, 25. Це означає, що конгруенція $x^4 \equiv a \pmod{29}$ має розв'язки (чотири) тільки при $a \equiv 1, 7, 8, 16, 20, 23, 25 \pmod{29}$.

Приклад 2. Знайти всі лишки п'ятого степеня за модулем 17. Тут $d=(5, 16)=1$. Це означає, що всі подані лишки за модулем 17 будуть лишками п'ятого степеня, тобто конгруенція $x^5 \equiv a \pmod{17}$ має один розв'язок при будь-якому a.

Тепер розглянемо розв'язання двочленних показникових конгруенцій за допомогою індексів

Обмежимось розглядом показникової конгруенції виду

$$a \cdot c^x \equiv b \pmod{p}, \tag{5}$$

де p — просте число, $(a, p)=1$ і $(c, p)=1$.

Застосовуючи властивості індексів до конгруенції (5), дістанемо еквівалентну конгруентність

$$\operatorname{ind} a + x \operatorname{ind} c \equiv \operatorname{ind} b \pmod{(p-1)}. \tag{6}$$

Конгруенція (6) є конгруенцією першого степеня за модулем $p-1$. Якщо $d=(\operatorname{ind} c, p-1)$ і $\operatorname{ind} b - \operatorname{ind} a$ ділиться на d, то конгруенція (6), а тому і конгруенція (5) має d розв'язків, а якщо $\operatorname{ind} b - \operatorname{ind} a$ не ділиться на d, то конгруенція (6), а отже, і конгруенція (5) не має розв'язків.

Зауваження. Якщо $a \vdots p$ або $c \vdots p$, а b не $\vdots p$, то конгруенція (5) неможлива і, отже, не матиме розв'язків; якщо при цьому і $b \vdots p$, то конгруенція (5) зводитиметься до тотожної конгруенції виду $0^x \equiv 0 \pmod{p}$, і її задовольнятиме будь-яке значення x.

Приклад 1. Розв'язати рівняння $3 \cdot 8^x \equiv 7 \pmod{23}$.

Маємо

$$\operatorname{ind} 3 + x \operatorname{ind} 8 \equiv \operatorname{ind} 7 \pmod{22},$$
$$6x \equiv 3 \pmod{22}.$$

Оскільки $(6,22)=2$ і $3 \not\vdots 2$, то остання конгруенція не має розв'язків, а тому і задана конгруенція також не матиме розв'язків.

Приклад 2. Розв'язати конгруенцію $15 \cdot 7^{2x} \equiv 8 \cdot 3^{3x} \pmod{31}$. Маємо:

$$\operatorname{ind} 15 + 2x \operatorname{ind} 7 \equiv \operatorname{ind} 8 + 3x \operatorname{ind} 3 \pmod{30},$$
$$53x \equiv -9 \equiv 21 \pmod{30} \quad \text{або} \quad 23x \equiv 21 \pmod{30}.$$

Розв'язуючи цю конгруенцію, дістанемо: $x=27 \pmod{30}$. Цей розв'язок і буде єдиним розв'язком заданої конгруенції.

Перевірка: $15 \cdot 7^{54} \equiv 15 \cdot 7^{24} \equiv 15 \cdot 18^{12} \equiv 15 \cdot 10^3 \equiv 15 \times 10 \cdot 7 \equiv 27 \pmod{31}$; $8 \cdot 3^{81} \equiv 8(-4)^7 = 8(-2)^2(-4) \equiv 8 \times 4(-4) \equiv 27 \pmod{31}$.

Тут ми скористались теоремою Ейлера, що $7^{\varphi(31)} \equiv 1$ і $3^{\varphi(31)} \equiv 1 \pmod{31}$, де $\varphi(31)=30$.

Контрольні запитання

1. До розв'язання якої конгруенції першого степеня зводиться розв'язання конгруенції $ax^n \equiv b \pmod{p}$, де $(a, p)=1$?
2. Скільки розв'язків має конгруенція $ax^n \equiv b \pmod{p}$ і при якій умові?
3. Яке число називається лишком степеня n за простим модулем p?
4. Яка умова буде необхідною і достатньою для того, щоб a було лишком степеня n за простим модулем p?
5. Скільки розв'язків має конгруенція $a \cdot c^x \equiv b \pmod{p}$ і при якій умові?

Вправи

1. Знайти показник, до якого належать: а) 25 за модулем 31; б) 18 за модулем 29; в) 5 за модулем 61.

Відповідь. а) 3; б) 28; в) 30.

2. Знайти найменші первісні корені для чисел: а) 23; б) 41; в) 71.

Відповідь. а) 5; б) 6; в) 7.

3. Довести, що коли a і b — два цілих числа, які не діляться на просте число p, і a належить до показника α, а b — до показника β за модулем p, причому $(\alpha, \beta)=1$, то ab належатиме до показника $\alpha\beta$ за модулем p.

4. На підставі попереднього твердження, довести існування первісних коренів за простим модулем p.

5. Довести, що коли g — первісний корінь за простим непарним модулем p, то можна знайти таке ціле t, щоб ціле u, яке визначається рівністю $(g+pt)^{p-1}=1+pu$ не ділилося б на p; при такому t число $g+pt$ буде первісним коренем за модулем p^α при будь-якому $\alpha \geqslant 1$. (Теорема існування первісного кореня за модулем p^α).

6. Припустимо, що $\alpha \geqslant 1$ — ціле число і g — первісний корінь за модулем p^α, де p — просте непарне число. Довести, що з чисел g і $g+p^\alpha$ буде первісним коренем за модулем $2p^\alpha$ те число, яке непарне (звідси на підставі попередньої задачі випливає існування первісного кореня за модулем $2p^\alpha$).

7. Довести, що первісні корені за модулем 2^α бувають тільки при $\alpha = 1, 2$.

8. Довести, що немає первісних коренів за модулем $m=2^\alpha p$, де $\alpha > 1$ і $p > 2$ є просте число.

9. Довести, що коли $m=2^\alpha p_1^{\alpha_1} p_2^{\alpha_2} \dots p_k^{\alpha_k}$ — канонічний розклад числа m і $k \geqslant 2$, то за модулем m немає первісних коренів.

10. Довести, що коли $c = \varphi(m)$ і q_1 і q_2, ... , q_k є різні прості дільники числа c, то для того, щоб число g, взаємно просте з m, було первісним коренем за модулем m, необхідно і достатньо, щоб це g не задовольняло жодної з конгруенцій.

$$g^{\frac{c}{q_1}} \equiv 1 \pmod m, \quad g^{\frac{c}{q_2}} \equiv 1 \pmod m, \ \dots\ , \quad g^{\frac{c}{q_k}} \equiv 1 \pmod m.$$

11. Довести, що непарне число a, яке ділиться на просте число p, належить до одного й того самого показника за модулем p^α, і за модулем $2p^\alpha$. Зокрема, всякий непарний первісний корінь числа p^α є первісним коренем числа $2p^\alpha$.

12. Знаючи, що 4 належить до показника 14 за модулем 29, знайти решту чисел, які належать до цього показника.

Відповідь. 5, 6, 9, 13, 22.

13. Знаючи, що 3 є одним з первісних коренів за модулем 29, знайти решту первісних коренів за цим модулем.

Відповідь. 2, 8, 10, 11, 14, 15, 18, 19, 21, 26, 27.

14. Знайти всі первісні корені за модулем: а) 49; б) 81.

Відповідь. а) 3, 5, 10, 12, 17, 19, 24, 26, 38, 40, 45, 47. б) 2, 5, 11, 14, 20, 23, 29, 32, 38, 41, 47, 50, 56, 59, 65, 68, 74, 77.

15. Користуючись твердженням задачі 10, довести, що: а) 7 є первісним коренем за модулем 79; б) 5 є первісним коренем за модулем 162.

16. Припустимо, що $(a, m) = 1$; $m = p_1^{\alpha_1} p_2^{\alpha_2} \dots p_k^{\alpha_k}$ — канонічний розклад числа m на прості множники. Довести, що показник δ, до якого належить a за модулем m, є найменше спільне кратне показників, до яких належить a за модулями $p_1^{\alpha_1}$, $p_2^{\alpha_2}$, ... , $p_k^{\alpha_k}$.

17. Нехай $(a, p^\alpha) = 1$, де $\alpha > 1$ — ціле і p — просте число, і покладемо, що δ — показник, до якого належить a за модулем $p^{\alpha-1}$. Тоді, якщо $a^\delta \equiv 1 \pmod{p^\alpha}$, то a належить до показника δ за модулем p^α, а якщо $a^\delta \not\equiv 1 \pmod{p^\alpha}$, то a належить до показника p^δ за модулем p^α. Довести це твердження.

18. Користуючись твердженнями задач 16 і 17, знайти показник, до якого належить число $a = 16$ за модулем $m = 5929$.

Відповідь. 1155.

19. Довести, що коли p — просте число виду $4k + 1$ і g — первісний корінь за модулем p, то $p - g$ є також первісний корінь за модулем p.

20. Довести, що коли g і g_1 — два первісних корені простого числа p, то справедливі конгруенції:

$$\operatorname{ind}_g a \equiv \operatorname{ind}_{g_1} a \cdot \operatorname{ind}_g g_1 \pmod{p-1},$$
$$\operatorname{ind}_{g_1} a \equiv \operatorname{ind}_g a \cdot \operatorname{ind}_{g_1} g \pmod{p-1}.$$

Зокрема,

$$\operatorname{ind}_{g_1} g \cdot \operatorname{ind}_g g_1 \equiv 1 \pmod{p-1}.$$

Ці формули аналогічні формулам для переходу від однієї системи логарифмів до іншої.

21. Скласти таблицю індексів за модулями 29, 31 і 59.

22. Визначити число розв'язків конгруенцій: а) $x^{16} \equiv 10 \pmod{37}$; б) $x^5 \equiv 3 \pmod{71}$; в) $x^{21} \equiv 5 \pmod{71}$.

Відповідь. а) 4; б) розв'язків немає; в) 7.

23. Користуючись таблицями індексів, розв'язати конгруенцію: а) $15x^4 \equiv 26 \pmod{29}$; б) $25x^5 \equiv 15 \pmod{73}$; в) $x^{48} \equiv 2 \pmod{97}$; г) $15x \equiv 19 \pmod{59}$.

Відповідь. а) $x \equiv 3$, 7, 22, 26 (mod 29); б) $x \equiv 5 \pmod{73}$; в) розв'язків немає; г) $x \equiv 17 \pmod{59}$.

24. З допомогою таблиць індексів розв'язати показникові конгруенції а) $17^x \equiv 7 \pmod{53}$; б) $6 \cdot 11^x \equiv 56 \pmod{61}$.

Відповідь. а) $x \equiv 17$, 43 (mod 52); б) $x \equiv 3$, 7, 11, 15, 19, 23, 27, 31, 35, 39, 43, 47, 51, 55, 59 (mod 60).

25. Знаючи, що 2 є первісним коренем за модулями 101 і 163, розв'язати показникові конгруенції.

а) $3 \cdot 5^x \equiv 4 \cdot 3^{2x+1} \pmod{101}$; б) $2^x \equiv 3 \cdot 5^{3x} \pmod{163}$.

Відповідь. а) $x \equiv 7$, 57 (mod 100); б) розв'язків немає.

26. Знайти індекс числа -1 за простим модулем $p > 2$ при довільній основі g.

Відповідь. $\frac{1}{2}(p-1)$.

27. Довести, що добуток двох первісних коренів за простим модулем $p > 2$ не може бути первісним коренем за тим самим модулем.

28. Користуючись теорією індексів, довести теорему Вільсона для простого $p > 2$.

29. Користуючись теорією індексів, вивести критерій Ейлера для квадратичних лишків.

30. Користуючись таблицею індексів, серед зведеної системи лишків за модулем 19 вказати: а) квадратичні лишки; б) кубічні лишки.

Відповідь. а) 1, 4, 5, 6, 7, 9, 11, 16, 17; б) 1, 7, 8, 11, 12, 18.

31. Серед зведеної системи лишків за модулем 43 вказати: а) числа, що належать до показника 6; б) первісні корені.

Відповідь. а) 7, 37; б) 3, 5, 12, 18, 19, 20, 26, 28, 29, 30, 33, 34.

32. Скласти таблицю індексів для модуля 27, взявши за основу первісний корінь 2; з допомогою цієї таблиці розв'язати конгруенції а) $5x \equiv 13 \pmod{27}$; б) $x^2 \equiv 10 \pmod{27}$.

Відповідь. а) $x \equiv 8 \pmod{27}$; б) $x \equiv \pm 8 \pmod{27}$.

33. Скласти таблицю індексів для модуля 50, взявши за основу первісний корінь 3; з допомогою цієї таблиці розв'язати конгруенції: а) $17x \equiv 39 \pmod{50}$; б) $x^2 \equiv 29 \pmod{50}$.

Відповідь. а) $x \equiv 17 \pmod{50}$; б) $x \equiv \pm 23 \pmod{50}$.

ІСТОРИЧНІ КОМЕНТАРІ

1. Теорія степеневих лишків грунтується на теоремі Ейлера про лишки, які утворюються від ділення степенів (1755). Поняття показника, індексів і їх основних властивостей ввів Гаусс.

2. Поняття первісного кореня запровадив Ейлер. Теорема 2, § 30 називається теоремою Гаусса; її сформулював (без доведення) німецький математик, фізик і астроном (за походженням француз) Ламберт (1728—1777). Її доведення зустрічається в Ейлера, проте він не дав його в досить чіткій формі. Гаусс дав два різні доведення цієї теореми.

3. П. Л. Чебишов у ряді теорем розглядав деякі класи простих чисел, для яких можна легко знайти первісний корінь.

Твердження, що первісні корені бувають лише за модулями $m = 2$, 4, p^α, $2p^\alpha$, де p — просте непарне число, зустрічається у Гаусса в його «Арифметичних дослідженнях».

4. Спинимось на класичних працях І. М. Виноградова, присвячених розподілу первісних коренів, індексів, лишків або нелишків того чи іншого степеня і т. д. в арифметичних прогресіях і в інтервалах заданої довжини. За допомогою простих оцінок тригонометричних сум І. М. Виноградов довів ряд теорем фундаментального значення, таких як:

1) *найменший первісний додатний корінь за простим модулем p менший за $2\sqrt[2k]{p}\ln p$, де k — число різних простих дільників $p-1$;*

2) *найменший додатний квадратичний нелишок для простого модуля* p *буде менший, від* $p^{\frac{1}{2\sqrt{e}}}(\ln p)^2$ *при* p, *більшому від деякого* p_0, *де* e — основа натуральних логарифмів.

Методи Виноградова мали велике значення у теорії чисел, бо до появи його праць не було ніякого уявлення про розподіл цих величин.

Зазначимо тут, що є припущення, за яким прості числа p, для яких 2 є первісним коренем, мають додатну щільність у множині простих чисел. Це означає, що коли позначити через $T(x)$ число таких $p \leqslant x$ а через $\pi(x)$ загальне число простих чисел $p \leqslant x$, то при деякому $\alpha > 0$ для всіх x виконується нерівність $T(x) \geqslant \alpha\pi(x)$. Це припущення ще не доведене і не спростоване.

Розділ VI

АРИФМЕТИЧНІ ЗАСТОСУВАННЯ ТЕОРІЇ КОНГРУЕНЦІЙ

§ 33. Обчислення остач при діленні на дане число

Нехай треба знайти невід'ємну остачу x від ділення деякого цілого числа N на натуральне число m; через те що дане число N і шукана остача x належать одному й тому самому класу чисел за модулем m, то ця задача зводиться до знаходження найменшого невід'ємного лишку x того класу чисел, до якого належить N за модулем m, тому

$$N \equiv x \pmod m,$$

де

$$0 \leqslant x < m. \tag{1}$$

Найчастіше N є степенем якого-небудь цілого числа або степенем многочлена від цілих чисел. Останній випадок зводиться до першого, а саме коли $N = a^k$. У цьому разі завжди можна вважати, що $0 \leqslant a < m$; далі, якщо $(a, m) = 1$, то за теоремою Ейлера $a^{\varphi(m)} \equiv 1 \pmod m$, і тому в конгруенції $a^k \equiv x \pmod m$, k можна замінити числом r, яке є остачею від ділення k на $\varphi(m)$.

Приклад. Знайти остачу від ділення $N = (86^{143} - 31^{547})^{62}$ на 21. Зауважимо тут, що $\varphi(21) = 12$, тому для будь-якого a, взаємно простого з 21 справедлива теорема Ейлера:

$$a^{12} \equiv 1 \pmod{21}.$$

На підставі теореми 2, § 16, дістанемо (конгруенції беремо за модулем 21): $86^{143} \equiv 2^{143} \equiv (2^{12})^{11} \cdot 2^{11}$, але через те що $(2,21) = 1$, то за теоремою Ейлера $2^{12} \equiv 1 \pmod{21}$ і тому $86^{143} \equiv 2^{11}$. Далі: $2^{11} \equiv (2^5)^2 \cdot 2 \equiv 16 \cdot 2 \equiv 11$. Отже, $86^{143} \equiv 11 \pmod{21}$.

Аналогічно, беручи до уваги, що на підставі теореми Ейлера $10^{12} \equiv 1 \pmod{21}$, послідовно дістанемо:

$$31^{547} \equiv 10^{547} \equiv (10^{12})^{45} \cdot 10^7 \equiv (10^2)^3 \cdot 10 \equiv (-5)^3 \cdot 10 \equiv 10 \pmod{21}.$$

Шукана невід'ємна остача x від ділення числа N на 21 має задовольняти конгруенцію (1). Знайдемо:

$$x \equiv (86^{143} - 31^{547})^{62} \equiv (11 - 10)^{62} = 1^{62} = 1 \pmod{21}.$$

Отже, шукана остача дорівнює 1.

Зауваження. Якщо для модуля m є таблиця індексів, то для обчислення остач від ділення на m добутків кількох співмножників і, зокрема, натуральних степенів, можна застосувати індекси. А саме, щоб знайти остачу x від ділення добутку $a_1 a_2 \dots a_k$ на m, де всі a_l взаємно прості з m, запишемо

$$x \equiv a_1 a_2 \dots a_k \pmod m, \text{ де } 0 \leqslant x < m.$$

Звідси

$$\operatorname{ind} x \equiv \operatorname{ind} a_1 + \operatorname{ind} a_2 + \dots + \operatorname{ind} a_k \pmod{\varphi(m)}.$$

За таблицею індексів знайдемо

$$s = \operatorname{ind} a_1 + \operatorname{ind} a_2 + \dots + \operatorname{ind} a_n,$$

звідки

$$\operatorname{ind} x \equiv s \pmod{\varphi(m)}.$$

Далі знаходимо число, індекс якого дорівнює s, тобто таке r, що

$$\operatorname{ind} x \equiv \operatorname{ind} r \pmod{\varphi(m)},$$

звідки

$$x \equiv r \pmod m.$$

Зокрема, якщо $a_1 = a_2 = \dots a_k = a$, ми дістанемо прийом для обчислення остачі від ділення на модуль m числа a^k.

Якщо $m = p_1^{\alpha_1} p_2^{\alpha_2} \dots p_k^{\alpha_k}$, то, щоб знайти остачу від ділення на m добутку або степеня, можна знайти остачі r_1, r_2, ... r_k при діленні на модулі $p_1^{\alpha_1}$, $p_2^{\alpha_2}$, ... , $p_k^{\alpha_k}$, а потім розв'язати систему конгруенцій

$$\begin{aligned} x &\equiv r_1 \pmod{p_1^{\alpha_1}}, \\ x &\equiv r_2 \pmod{p_2^{\alpha_2}}, \\ &\dots\dots\dots \\ x &\equiv r \pmod{p_k^{\alpha_k}}. \end{aligned}$$

Приклад. Знайти остачу від ділення $N = 13^{37} \cdot 12^{41}$ на $35 = 5 \cdot 7$. 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 лівій і правій частинах конгруенції, дістанемо:

$$\operatorname{ind} r_1 \equiv 37 \operatorname{ind} 3 + 41 \operatorname{ind} 2 \equiv \operatorname{ind} 3 + \operatorname{ind} 2 \equiv 3 + 1 \equiv 0 \pmod 4,$$

звідки

$$r_1 \equiv 1 \pmod 5.$$

Аналогічно знайдемо остачу від ділення N на 7:

$$r_2 \equiv 13^{37} \cdot 12^{41} \equiv 6^{37} \cdot 5^{41} \pmod 7; \quad \operatorname{ind} r_2 \equiv 37 \operatorname{ind} 6 + 41 \operatorname{ind} 5 \equiv$$
$$\equiv \operatorname{ind} 6 + 5 \operatorname{ind} 5 \equiv 3 + 5 \cdot 5 = 4 \pmod 6,$$

звідки $r_2 \equiv 4 \pmod 7$. Розв'язуючи систему конгруенцій

$$x = 1 \pmod 5,$$
$$x = 4 \pmod 7,$$

дістанемо

$$x \equiv 11 \pmod{35}.$$

Отже, шукана остача дорівнює 11.

Контрольні запитання

1. До якої задачі зводиться знаходження невід'ємної остачі від ділення цілого числа N на натуральне число m?
2. Чи можна для знаходження остачі від ділення $2^{27} + 3^{150}$ на 30 застосувати теорему Ейлера?
3. Як застосувати таблицю індексів для обчислення остач від ділення?

§ 34. Встановлення ознак подільності за допомогою конгруенцій

Ознакою подільності натурального числа N на натуральне число d називається необхідна й достатня умова подільності N на d, застосування якої потребує меншого числа дій, ніж процес ділення.

Нехай треба дізнатись, чи ділиться натуральне число N на натуральне число d. Ця задача, по суті, зводиться до побудови числової функції $f(N)$, яка задовольняє такі вимоги:

1) задане число N і $f(N)$ одночасно діляться або одночасно не діляться на d:

2) $|f(N)| < N$;

3) при заданому N функцію $f(N)$ можна визначити досить просто.

Якщо число $|f(N)|$ ще велике, то з ним роблять те саме, що й з заданим числом N, і т. д. доти, поки не буде знайдено такого малого числа, що буде беспосередньо видно, чи ділиться воно на d чи ні.

Взагалі, досить знати тільки ознаки подільності на числа $d = p^\alpha$, де p — просте число і α — ціле $\geqslant 1$, бо N ділитиметься на $d = p_1^{\alpha_1} p_2^{\alpha_2} \dots p_k^{\alpha_k}$ тоді і тільки тоді, коли воно ділиться на всі $p_i^{\alpha_i}$ окремо.

Розглянемо деякі способи побудови функції $f(N)$.

Відомо, що кожне натуральне число N при основі числення g має вигляд:

$$N = a_0 + a_1 g + a_2 g^2 + \dots + a_n g^n = \overline{a_n a_{n-1} \dots a_1 a_0},$$

де $a_0, a_1, \dots, a_n$ — «цифри», тобто цілі числа, які більші або дорівнюють нулю і менші від g. Позначимо через r_k абсолютний найменший лишок числа g^k за модулем d тоді буде справедливим таке твердження:

Теорема 1. *Якщо $N = a_0 + a_1 g + a_2 g^2 + \dots + a_n g^n$ ділиться на d, то $M = a_0 + a_1 r_1 + \dots + a_n r_n$ ділиться на d і навпаки.*

Це твердження беспосередньо випливає з властивостей конгруенції (див. окремий випадок теореми 2, § 15). Спосіб побудови функції $f(N) = M$, що грунтується на цій теоремі, називають способом Паскаля.

Отже, дослідження подільності числа N на d ми звели до дослідження подільності числа $|M| < N$ на d.

Тут $M = f(N) \equiv N \pmod d$, *це навіть більше, ніж нам було потрібно, бо остання конгруенція показує не тільки те, що N і M одночасно діляться або не діляться на d, а й те, що їхні остачі від ділення на d однакові.*

Ця теорема дає змогу встановити практично зручні ознаки подільності на ряд натуральних чисел, якщо число N записане в десятковій системі числення, тобто при основі $g = 10$:

$$N = a_0 + a_1 \cdot 10 + a_2 \cdot 10^2 + \dots + a_n \cdot 10^n.$$

Розглянемо деякі окремі випадки.

1. d = 2; 5. Тут $r_k \equiv 10^k \equiv 0 \pmod{2;\ 5}$ для всіх $k = 1, 2, \dots, n$, отже,

$$N \equiv M = a_0 \pmod{2;\ 5}$$

— це відомі ознаки подільності на 2 і 5. *Число N ділиться на 2 (відповідно на 5) тоді і тільки тоді, коли число одиниць a_0, тобто остання цифра, ділиться на 2 (відповідно на 5).*

2. d = 3; 9. Тут $r_k \equiv 10^k \equiv 1 \pmod{3;\ 9}$ для всіх $k = 1, 2, \dots, n$; отже,

$$N \equiv M = a_0 + a_1 + \dots + a_n \pmod{3;\ 9},$$

тобто *N ділиться на 3 (відповідно на 9) тоді і тільки тоді, коли сума цифр, які його зображають, ділиться на 3 (відповідно на 9).*

3. d = 11. Тут $r_0 = -1$, $r_2 = 1$, $r_3 = -1, \dots$, отже

$$N \equiv M = a_0 - a_1 + a_2 - a_3 + \dots = (a_0 + a_2 + a_4 + \dots) -$$
$$- (a_1 + a_3 + a_5 + \dots) \pmod{11},$$

тобто *число ділиться на 11 тоді і тільки тоді, коли різниця між сумою цифр, які стоять на непарних* (рахуючи справа наліво) *місцях, і сумою цифр, які стоять на парних місцях, ділиться на 11.*

Приклад. 2 975 841 ділиться на 11, бо $(1+8+7+2)-(4+5+9)=0$ ділиться на 11.

4. $\mathbf{d=4}$. Тут $r_1=\pm 2$, $r_2=r_3=\cdots=r_n=0$, отже,

$$N\equiv M=a_0\pm 2a_1 \pmod 4.$$

Приклад. 368 ділиться на 4, бо $8+2\cdot 6=20$ або $8-2\cdot 6=-4$ ділиться на 4.

5. $\mathbf{d=7}$. Тут $r_1=3$, $r_2=2$, $r_3=-1$, $r_4=-3$, $r_5=-2$, $r_6=1$, $r_7=3$ (далі величини остач повторюватимуться періодично); отже,

$$N\equiv M=(a_0+3a_1+2a_2)-(a_3+3a_4+2a_5)+\cdots \pmod 7.$$

У цій формі ознака подільності на 7 досить складна і відрізняється від шкільного формулювання.

Приклад. 24 829 ділиться на 7, або $9+3\cdot 2+2\cdot 8-(4+3\cdot 2)=21$ ділиться на 7.

Зауваження. При виконанні обчислень у правих частинах конгруенцій можна відкидати числа, кратні d. Результат дає не тільки відповідь на запитання про подільність, а й величину остачі від ділення N на d, якщо N не ділиться на d.

6. Беручи за основу числення $g=\mathbf{100}$, вивести ознаки подільності на $\mathbf{d=4;\ 25;\ 50}$. Маємо:

$$N=b_0+b_1\cdot 100+b_2\cdot 100^2+\cdots+b_l\cdot 100^l,$$

де $b_0=\overline{a_1a_0}$ — цифра одиниць першого розряду, $b_1=\overline{a_3a_2}$ — цифра одиниць другого розряду і т. д. У цьому випадку всі $r_k=0\,(k=1,\ \ldots,\ l)$; отже,

$$N\equiv M=b_0=\overline{a_1a_0} \pmod d,$$

тобто число N ділиться на 4 (відповідно на 25 і 50), якщо дві його останні цифри утворюють число, яке ділиться на 4 (відповідно на 25 і 50).

Розглянемо окремий випадок теореми 1, а саме, доведемо таке твердження:

Нехай $(d,\ 10)=1$, *число 10 належить показнику* δ *за модулем d і записане в системі числення з основою* 10^δ. *Число N ділиться на d тоді і тільки тоді, коли на d ділиться сума чисел, які утворюються при розбитті справа наліво цифрового запису числа N на грані по* δ *цифр у кожній грані.*

Справді, маємо:

$$N=c_0+c_1\cdot 10^\delta+c_2\cdot(10^\delta)^2+\cdots+c_m(10^\delta)^m,\ (10^\delta)^k\equiv 1,$$
$$(k=1,\ 2,\ \ldots,\ m)$$
$$N\equiv M=c_0+c_1+c_2+\ldots+c_m \pmod d;\ \text{тут } 0\leqslant c_k<10^\delta-1.$$

З останньої конгруенції й випливає, що N і M при діленні на d дають однакові остачі і, отже, одночасно або діляться на d, або ні. Тут $c_0,\ c_1,\ \ldots,\ c_n$ — числа, які утворюються при розбитті справа наліво числа N на грані по δ цифр у кожній.

Отже, *якщо за модулем d число* 10 *належить показнику* δ, тоді *в системі числення з основою* 10^δ *ознака подільності для d* така *сама, як для чисел* 3 *і* 9 *у десятковій системі.*

Далі зауважимо, що *у випадку, коли за модулем d* 10 *належить парному показнику* δ, *тоді при основі* 10 *для d ознака подільності аналогічна до ознаки подільності на* 11 *у десятковій системі, оскільки* $10^{\delta/2}\equiv -1 \pmod d$.

7. Помічаючи, що $10^2\equiv 1 \pmod{11}$, можна дістати іншу ознаку подільності числа N на $d=11$. Маємо: $N=b_0+b_1\cdot 10^2+\cdots+b_l\cdot(10^2)^l$, де $b_0=a_1a_0$ — цифра одиниць 1-го розряду, $b_1=a_3a_2$ — цифра одиниць 2-го розряду і т. д.; враховуючи, що $(10^2)^k\equiv 1 \pmod{11}$, $k=1,\ 2,\ \ldots,\ l$, дістанемо

$$N\equiv M=b_0+b_1+\cdots+b_l \pmod{11}.$$

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.*

Так, для розглянутого вище прикладу $N=2\,975\,841$ матимемо: $N\equiv M=41+58+97+2\equiv 8+3-2+2\equiv 0 \pmod{11}$, тобто що N ділиться на 11.

8. Легко перевірити, що 10 належить показнику $\delta=3$ за модулем 37, тобто $10^3=1 \pmod{37}$. Записуючи число N в системі числення $g=10^3$, дістанемо: $N=c_0+c_1\cdot 10^3+c_2(10^3)^2+\cdots+c_n\cdot(10^3)^n$, де $c_0=\overline{a_2a_1a_0}$ — цифра одиниць 1-го розряду, $c_1=\overline{a_5a_4a_3}$ — цифра одиниць 2-го розряду і т. д.; $N\equiv M=c_0+c_1+\cdots+c_m \pmod{37}$, тобто *N ділиться на 37 тоді і тільки тоді, коли на 37 ділиться сума трицифрових чисел, утворених відповідними гранями числа N при його розбитті справа наліво.*

Так для $N=256\,300\,147$ матимемо: $N\equiv M=147+300+256\equiv -1+4-3\equiv 0 \pmod{37}$, отже, число 256 300 147 ділиться на 37.

9. Безпосередньою перевіркою знаходимо, що 10 належить показнику $\delta=6$ за модулями 7, 11 і 13. Згідно із розробленим раніше зауваженням при основі $g=10^3$ дістанемо ознаки подільності на 7, 11 і 13 аналогічні до ознаки подільності на 11 в десятковій системі, тобто

$$N\equiv M=(c_0+c_2+\cdots)-(c_1+c_3+\cdots) \pmod{7;\ 11;\ 13},$$

отже, N ділиться на одне з чисел 7, 11 і 13, якщо M ділиться на одне з цих чисел.

Візьмемо, наприклад, число $N = 11\,673\,207$. Тоді матимемо $N \equiv M = (207 + 11) - 673 \equiv 455 \pmod{7, 11, 13}$. Тепер безпосередньо впевнюємось, що 455 ділиться на 7 і 13 і не ділиться на 11, а тому і задане число N ділиться на 7 і 13 і не ділиться на 11.

Контрольні запитання

1. Що називається ознакою подільності натурального числа N на натуральне число d?
2. Яким умовам має задовольняти функція $f(N)$?
3. У чому суть способу Паскаля побудови функції $f(N)$?
4. Сформулюйте ознаки подільності на 2 і 5 на 3 і 9, на 7, 11, 13, 37.

§ 35. Визначення члена цифр періоду при перетворенні звичайного дробу в десятковий

З елементарної арифметики відомо, що звичайний нескоротний дріб $\frac{a}{b}$ перетворюється в скінченний десятковий дріб тоді і тільки тоді, коли канонічний розклад знаменника не містить простих множників відмінних від 2 і 5 [1].

Нехай $\frac{a}{b}$ нескоротний дріб і канонічний розклад знаменника b містить прості числа, відмінні від 2 і 5; перетворюватимемо такий дріб у десятковий.

Нагадаємо, що нескінченний десятковий дріб, десяткові знаки якого періодично повторюються, називається *періодичним десятковим дробом*. Якщо десяткові знаки повторюються, починаючи з першого, то десятковий дріб називається *чистим періодичним*, у противному разі він називається *мішаним періодичним дробом*.

Теорема 1. Якщо $\frac{a}{b}$ — *нескоротний дріб і* $(b, 10) = 1$, *то цей дріб перетворюється у чистий періодичний десятковий дріб; число цифр у періоді дробу дорівнює* δ, *де* δ — *показник, до якого належить число 10 за модулем* b.

[1] Справді нехай $b = 2^\alpha \cdot 5^\beta$, де $\alpha \geqslant 0$, $\beta \geqslant 0$, $\alpha + \beta > 0$. Помножаючи чисельник і знаменник на $2^\beta \cdot 5^\alpha$, дістанемо $\frac{a}{b} = \frac{a \cdot 2^\beta \cdot 5^\alpha}{10^{\alpha+\beta}}$, а цей дріб, знаменник якого є степенем 10, подаємо скінченним десятковим дробом. Навпаки, нехай $\frac{a}{b} = N, q_1 q_2 \ldots q_n$, де N — ціла частина, $q_1, q_2, \ldots, q_n$ — десяткові знаки скінченного десяткового дробу: тоді $\frac{a}{b} = N + \frac{\overline{q_1 q_2 \ldots q_n}}{10^n}$, де $\overline{q_1 q_2 \ldots q_n}$ означає число, зображене цифрами $q_1, q_2, \ldots, q_n$. Якщо цей дріб скоротний, то, оскільки канонічний розклад знаменника є $2^n \cdot 5^n$, після скорочення в знаменнику дістанемо число, яке не містить у своєму розкладі простих чисел, відмінних від 2 і 5.

Справді, не порушуючи загальності міркувань, можна нескоротний дріб $\frac{a}{b}$ вважати правильним (якщо він неправильний, тобто $a > b$, то ми спочатку виділимо цілу частину); отже, a можна вважати рівним одному з $\varphi(b)$ чисел, менших b і взаємно простих з b.

Перетворюватимемо дріб $\frac{a}{b}$ у десятковий за загальними правилами; для цього поділимо спочатку $10a$ на b; позначаючи через a_1 частку і через r_1 — остачу від цього ділення, дістанемо:

$$10a = ba_1 + r_1, \quad 0 < r_1 < b.$$

Тепер поділимо $10r_1$ на b:

$$10r_1 = ba_2 + r_2, \quad 0 < r_2 < b;$$

далі ділимо $10r_2$ на b:

$$10r_2 = ba_3 + r_3, \quad 0 < r_3 < b$$

і т. д. Такий процес нескінченний, бо щоразу будуть остачі $r_1, r_2, r_3, \ldots$, менші від b і взаємно прості з b. Справді, $(a, b) = 1$, $(10, b) = 1$ за умовою, тому $(10a, b) = 1$ і $(r_1, b) = 1$; аналогічно $(10r_1, b) = 1$, а тому $(r_2, b) = 1$ і т. д.

Звідси випливає, що різних остач при зазначеному діленні буде не більш, як $\varphi(b)$. Це означає, що не пізніш як через $\varphi(b)$ кроків ми дістанемо повторення остач, а отже, й повторення цифр частки.

Для доведення теореми залишається показати, що перше повторення настане після δ ділень, де δ — показник, до якого належить 10 за модулем b, причому перша остача, яка повторюється, саме й буде a. Тому знайдений дріб буде чистим періодичним з числом цифр у періоді, яке дорівнює δ.

Але для доведення цих тверджень досить встановити, що коли δ — найменший показник, для якого

$$10^\delta \equiv 1 \pmod{b}, \tag{1}$$

то при діленні на b будь-якого числа $r < b$ і взаємно простого з b, остача r повториться тільки після визначення δ цифр частки.

Справді, конгруенція (1) еквівалентна конгруенції:

$$10^\delta \cdot r \equiv r \pmod{b}. \tag{2}$$

Ця конгруенція саме й показує, що приписавши до числа r δ нулів, що відповідає визначенню δ послідовних цифр частки, дістанемо при діленні $10^\delta \cdot r$ на b остачу r. Через те що δ — найменше невід'ємне число, для якого мають місце конгруенції (1) і (2), то жодна остача не може повторитись раніш як через δ ділень. Зокрема, при діленні $a < b$ на b перша остача, що повторюється,

саме й буде a, причому вона повториться точно через δ ділень. Цим теорему доведено.

Бачимо, що δ залежить тільки від знаменника нашого дробу і, звичайно, від основи нашої системи числення, тобто від числа $g = 10$. Тому два дроби $\frac{a}{b}$ і $\frac{a_1}{b}$, які задовольняють умову теореми 1, матимуть одну й ту саму довжину періоду при перетворенні їх у десяткові дроби.

Зауваження. З конгруенції $10^\delta \equiv 1 \pmod b$ випливає, що $\underbrace{99\ldots9}_{\delta \text{ раз}} \equiv 0 \pmod b$; тому δ можна знайти так: ділимо 9 на b, потім 99 на b і т. д., поки не дістанемо в остачі нуль. Число дев'яток у цьому діленні, а отже, й число цифр частки, дорівнюватимуть шуканому показнику δ.

Приклад. Знайти довжину періоду, який утворюється при перетворенні дробів $\frac{a_i}{21}$, де a_i — будь-яке ціле, взаємно просте з 21, у десяткові. Тут $b = 21$; ділимо:

$$\begin{array}{l|l} 99 & 21 \\ \hline 159 & 047619 \\ 129 & \\ \hline 39 & \\ 189 & \\ \hline 0 & \end{array}$$

У частці маємо 6 цифр, беручи до уваги й 0, який відповідає першій дев'ятці. Отже, $\delta = 6$, тобто шуканий період складається з 6 цифр.

Теорема 2. Якщо $\frac{a}{b}$ — *нескоротний дріб і* $b = 2^\alpha 5^\beta \cdot b_1$, *де* $(b_1, 10) = 1$, *то цей дріб перетворюється у мішаний періодичний десятковий дріб; число цифр у періоді дробу дорівнює* δ, *де* δ — *показник, якому належить 10 за модулем* b_1; *число цифр до періоду дорівнює* γ; *де* γ — *найбільше з чисел* α *або* β.

Справді, нехай дріб $\frac{a}{b}$ — нескоротний, причому

$$b = 2^\alpha \cdot 5^\beta \cdot b_1, \quad (b_1, 10) = 1, \quad \gamma = \max(\alpha, \beta).$$

Помножимо $\frac{a}{b}$ на 10^γ; після скорочення в знаменнику множників 2 і 5 дістанемо:

$$\frac{10^\gamma a}{b} = \frac{a_1}{b_1},$$

де дріб $\frac{a_1}{b_1}$ — нескоротний і $(b_1, 10) = 1$. За теоремою 1, цей дріб перетворюється у чистий періодичний з числом цифр у періоді, яке дорівнює δ, де δ — показник, до якого належить 10 за модулем b_1. Щоб з нього дістати початковий дріб $\frac{a}{b}$, треба $\frac{a_1}{b_1}$ поділити на 10^γ, тобто перенести кому в знайденому періодичному дробу на γ знаків ліворуч. У результаті дістанемо мішаний періодичний дріб з числом цифр до періоду, що дорівнює γ. Цим теорему доведено.

Приклад. $b = 140 = 2^2 \cdot 5 \cdot 7$; маємо $\gamma = 2$. Знайдемо δ, тобто показник, до якого належить 10 за модулем 7. Маємо:

$$\varphi(7) = 6;\ \delta = 1, 2, 3, 6;\ 10 \equiv 3,\ 10^2 \equiv 9,\ 10^3 \equiv -1,\ 10^6 \equiv 1 \pmod 7.$$

Отже, $\delta = 6$ (δ можна було знайти і згідно з зауваженням, зробленим вище). Таким способом усі дроби виду $\frac{a}{140}$, де $(a, 140) = 1$, перетворюються в мішані періодичні дроби з числом цифр у періоді, яке дорівнює 6, і з числом цифр до періоду, яке дорівнює 2. Так, наприклад, безпосередньо переконуємось, що

$$\frac{187}{140} = 1{,}33\,(571428).$$

Розглянемо обернену задачу: *знайти звичайний дріб, який відповідав заданому періодичному дробу.*

Нехай дано чистий періодичний дріб: $x = N,\ (a_1 a_2 \ldots a_\delta)$, де N — ціла частина, тобто

$$x = N + \left(\frac{a_1}{10} + \frac{a_2}{10^2} + \cdots + \frac{a_\delta}{10^\delta}\right) + \frac{1}{10^\delta}\left(\frac{a_1}{10} + \frac{a_2}{10^2} + \cdots + \frac{a_\delta}{10^\delta}\right) + \frac{1}{10^{2\delta}}\left(\frac{a_1}{10} + \frac{a_2}{10^2} + \cdots + \frac{a_\delta}{10^\delta}\right) + \cdots,$$

або

$$x = N + (10^{\delta-1}a_1 + 10^{\delta-2}a_2 + \cdots + a_\delta)\left(\frac{1}{10^\delta} + \frac{1}{10^{2\delta}} + \cdots\right);$$

але

$$\frac{1}{10^\delta} + \frac{1}{10^{2\delta}} + \cdots = \frac{1}{10^\delta - 1},$$

де число $10^\delta - 1$ зображається δ дев'ятками. Отже, дістанемо:

$$x = N + \frac{10^{\delta-1}a_1 + 10^{\delta-2}a_2 + \cdots + a_\delta}{10^\delta - 1}.$$

тобто для того, щоб перетворити чистий періодичний дріб у звичайний, треба період дробу зробити чисельником, а в знаменнику написати стільки дев'яток, скільки цифр у періоді, і знайдений дріб додати до цілої частини.

Нехай тепер дано мішаний періодичний дріб:

$$x = N,\ \overline{b_1, b_2 \ldots b_\gamma (c_1 c_2 \ldots c_\delta)}.$$

Його можна подати так:

$$x = [\overline{Nb_1b_2 \dots b_\gamma}, \overline{(c_1c_2 \dots c_\delta)}] : 10^\gamma = \left[\overline{Nb_1b_2 \dots b_\gamma}, \frac{\overline{c_1c_2 \dots c_\delta}}{10^\delta - 1}\right] : 10^\gamma =$$

$$= N + \frac{b_1 10^{\gamma-1} + b_2 10^{\gamma-2} + \dots + b_\gamma}{10^\gamma} + \frac{c_1 10^{\delta-1} + c_2 10^{\delta-2} + \dots + c_\delta}{10^\gamma (10^\delta - 1)} =$$

$$= N + [(b_1 10^{\delta+\gamma-1} + b_2 10^{\delta+\gamma-2} + \dots + b_\gamma \quad 10^\delta + c_1 10^{\delta-1} + \dots + c_\delta) -$$

$$- (b_1 10^{\gamma-1} + b_2 10^{\gamma-2} + \dots + b_\gamma)] \cdot \frac{1}{10^\gamma (10^\delta - 1)}.$$

Звідси виводимо таке п р а в и л о: щоб перетворити мішаний періодичний дріб у звичайний, треба від числа, що стоїть між комою і другим періодом (тобто від числа $\overline{b_1b_2 \dots b_\gamma c_1c_2 \dots c_\delta}$), відняти число, яке стоїть між комою і першим періодом (тобто число $\overline{b_1b_2 \dots b_\gamma}$), і цю різницю зробити чисельником; у знаменнику треба написати стільки дев'яток, скільки цифр у періоді, й після них — стільки нулів, скільки цифр між комою й першим періодом, і цей дріб додати до цілої частини N.

З а у в а ж е н н я. Можна відразу перетворити періодичний дріб у звичайний неправильний дріб (не виділяючи цілої частини). Для цього треба цифри цілої частини вважати цифрами, що стоять до періоду, й застосувати правило для перетворення мішаного періодичного дробу в звичайний. При такій побудові знаменника цифри цілої частини враховувати не слід.

Приклад.

$$3{,}1\,(54) = 3\frac{154-1}{990} = 3\frac{153}{990} = 3\frac{17}{110}, \text{ або } 3{,}1\,(54) = \frac{3154-31}{990} =$$

$$= \frac{3123}{990} = \frac{347}{110} = 3\frac{17}{110}.$$

Контрольні запитання

1. Скільки цифр у періоді, при перетворенні звичайного дробу $\frac{a}{b}$, де $(a, b) = 1$ і $(b, 10) = 1$, у десятковий?
2. З якою метою при доведенні теореми 1 використовують умову $(b, 10) = 1$?
3. Як розуміти, що δ — показник, до якого належить 10 за модулем b?
4. Чому два дроби $\frac{a}{b}$ і $\frac{a_1}{b}$, які задовольняють умову теореми 1, мають однакове число цифр у періоді?
5. У який десятковий дріб перетворюється дріб $\frac{a}{b}$, де $(a, b) = 1$, $b = 2^\alpha \cdot 5^\beta \cdot b_1$ і вже $(b_1, 10) = 1$?

§ 36. Перевірка результатів арифметичних дій

Перевірка арифметичних дій (додавання, віднімання, множення) над цілими числами грунтується на такому твердженні, яке безпосередньо випливає з теореми 2, § 15.

Теорема. *Якщо*

$$N = f(N_1, N_2, \dots, N_k), \qquad (1)$$

де f — многочлен від цілих чисел $N_1, N_2, \dots, N_k$, то має місце конгруенція $N = f(N_1, N_2, \dots, N_k) \pmod m$ (2), *де m є будь-яке натуральне число.*

Конгруенція (2) показує, що з рівності (1) випливає рівність остач від ділення N і $f(N_1, N_2, \dots, N_k)$ на m, але обернене твердження, взагалі, несправедливе. Інакше кажучи, справедливість конгруенції (2) є умова, необхідна для рівності (1), але недостатня.

Найбільш поширена перевірка арифметичних дій числами $m = 9$ і 11. Справа в тому, що коли позначати через M суму цифр числа N, то очевидно матиме місце конгруенція: $N \equiv M \pmod 9$ (див. § 34, п. 2). Позначаючи тепер через M_i суму цифр числа N_i $(i = 1, 2, \dots, k)$, дістанемо таке твердження:

Для того щоб результат арифметичних дій (1) *був правильним, необхідно (проте недостатньо), щоб мала місце конгруенція*

$$M \equiv f(M_1, M_2, \dots, M_k) \pmod 9.$$

Приклад 1. $1042 \cdot 10\,182 + 42\,932 - 18\,265 = 10\,634\,311$.

Для перевірки правильності виконаних дій замінимо цю рівність типу (1) конгруенцією (2) за модулем 9;

$$7 \cdot 12 + 20 - 22 \equiv 19 \pmod 9, \text{ або } 1 \equiv 1 \pmod 9.$$

Взагалі, якщо числа $M_1, M_2, \dots, M_k$ великі, то до них можна застосувати ту саму теорему. Із сказаного вище випливає, що коли не виконано умов контролю, тобто конгруенції (2), то обчислення зроблено неправильно, але виконання умов контролю ще не гарантує правильності обчислень.

Легко побачити, що при перевірці числом 9 не виявилось би помилки, яка сталася з таких причин: а) не взято до уваги нуль у множеному або множнику; б) в результаті записано цифри не в тому порядку; в) неповні добутки було записано не на своїх місцях; г) взагалі, якщо помилка становить число, кратне 9.

Приклад 2. $4325 \cdot 897 = 451\,425$; перевіримо числом 9:

$$14 \cdot 24 \equiv 21 \pmod 9;$$

застосовуючи ще раз зазначене вище правило, дістанемо: $5 \cdot 6 \equiv 3 \pmod 9$, або $3 \equiv 3 \pmod 9$. Отже, перевірка числом 9 не виявляє помилки в цьому прикладі. Щоб мати більше гарантій у правильності виконаних арифметичних дій, треба перевірити цей результат будь-яким іншим числом m, найкраще числом 11.

Припустимо, що

$$N = \overline{a_n a_{n-1} \dots a_1 a_0} = a_n 10^n + a_{n-1} 10^{n-1} + \dots + a_1 10 + a_0;$$

тоді, позначаючи через P вираз

$$P = a_0 - a_1 + a_2 - a_3 + \dots = (a_0 + a_2 + \dots) - (a_1 + a_3 + \dots);$$

аналогічно до попереднього, дістанемо конгруенцію:

$$N \equiv P \pmod{11},$$

(див. § 34, п. 3) і, так само, якщо справедлива рівність (1), то матиме місце конгруенція:

$$P \equiv f(P_1, P_2, \ldots, P_k) \pmod{11},$$

де P_i — сума цифр числа N_i, узятих по черзі із знаком «плюс» і «мінус» (а не навпаки!).

Перевіримо результат арифметичних дій у прикладах 1 і 2. Відповідно маємо:

1) $(-3)(-4) + 10 + 6 \equiv -5$; $6 \equiv -5 \pmod{11}$;

2) $2 \cdot 6 \not\equiv 7 \pmod{11}$.

Отже, можемо твердити, що в прикладі 2 вказані дії виконано неправильно. Щодо правильності дій у прикладі 1 є вже велика гарантія. А коли все-таки допущено помилку в обчисленнях у цьому прикладі, то вона буде кратною 9 і 11, тобто кратна 99.

Результат ділення перевіряють за допомогою множення (ділене дорівнює дільнику, помноженому на частку плюс остача). *Взагалі, слід мати на увазі, що додержання контролю при неправильних обчисленнях пов'язане принаймні з двократною помилкою в обчисленнях, тому треба визнати контроль* (навіть одним числом) *ефективним.*

Контрольні запитання

1. На якому твердженні грунтується перевірка арифметичних дій за допомогою конгруенцій?

2. Яка умова є необхідною для того, щоб результат арифметичних дій $N = f(N_1, N_2, \ldots, N_k)$, де f — многочлен від цілих чисел $N_1, N_2, \ldots, N_k$ був правильним? Чи є ця умова достатньою? Чому?

3. Сформулюйте необхідну умову перевірки результатів дій додавання, віднімання і множення числами 9 і 11.

4. Як перевірити правильність результату ділення?

Вправи

1. Знайти остачу від ділення: а) $7^{100} + 11^{100}$ на 13; б) $8^{80} + 13^{90}$ на 17; в) $(85^{70} + 19^{32})^{17}$ на 21; г) $(84^{80} - 23^{40})^{15}$ на 25; д) $(15\,728 + 19^{30})^7$ на 57; е) $(12\,371^{56} + 34)^{28}$ на 243.

Відповідь. а) 12; б) 0; в) 17; г) 0; д) 51; е) 130.

2. Які остачі може давати сотий степінь цілого числа N при діленні на 125?

Відповідь. Якщо $N \vdots 5$, то остача дорівнює нулю; якщо $(N, 5) = 1$, то остача дорівнює 1.

3. Знайти останню цифру числа: а) 9^{9^9}; б) 2^{3^4}.

Відповідь. а) 9; б) 2.

4. Знайти дві останні цифри числа: а) 2^{999}; б) 3^{999}.

Відповідь. а) 88; б) 67.

5. Знайти три останні цифри числа 243^{402}.

Відповідь. 049.

6. Користуючись таблицею індексів, знайти остачу від ділення: а) 12^{12} на 73; б) $85 \cdot 79$ на 97.

Відповідь. а) 64; б) 22.

7. Методом конгруенцій довести такі твердження:

1) при будь-якому натуральному n: а) $n^7 + 6n$ ділиться на 7; б) $10^n(9n - 1) + 1$ ділиться на 9; в) $3 \cdot 5^{2n+1} + 2^{3n+1}$ ділиться на 17; г) $2^{5n} - 1$ ділиться на 31.

2) а) $2222^{5555} + 5555^{2222}$ ділиться на 7; б) $43^{23} + 23^{43}$ ділиться на 66.

3) Довести, що коли ціле число N взаємно просте з 10, то й 101-й степінь числа N закінчується тими самими трьома цифрами, що й N.

8. 13-й степінь деякого одноцифрового числа має цифрою одиниць 7. Користуючись таблицями індексів, знайти це число.

Відповідь 7.

9. Вивести ознаки подільності на 13 у десятковій системі числення.

Відповідь. Якщо

$$N = \overline{a_n a_{n-1} \ldots a_1 a_0} = a_n 10^n + a_{n-1} 10^{n-1} + \cdots + a_1 10 + a_0,$$

то N ділиться на 13 тоді і тільки тоді, коли

$$(a_0 + 10a_1 + 9a_2) - (a_3 + 10a_4 + 9a_5) + \cdots \equiv 0 \pmod{13}.$$

10. Довести, що число, записане в системі числення з основою g, ділиться на $g - 1$ тоді і тільки тоді, коли сума його цифр ділиться на $g - 1$.

11. Вказати системи числення, для яких ознаки подільності на 3 і 11 ті самі, що й для десяткової системи числення (див. § 35).

Відповідь. Системи числення з основою $g \equiv 10 \pmod{33}$.

12. Беручи за основу системи числення $g = 1000$, вивести ознаки подільності на $d = 3, 9, 27, 111, 333, 999$.

Відповідь. $N \equiv M = \overline{a_2 a_1 a_0} = c_0 \pmod{d}$, тобто N ділиться на d, якщо три його останні цифри становлять число M, яке ділиться на d.

Зауваження. При $d = 3; 9$ до числа M знову можна застосувати відому для них ознаку подільності: $M \equiv M_1 = a_0 + a_1 + a_3 \pmod{3,9}$.

13. Нехай $(d, 10) = 1$; тоді конгруенція $10M \equiv N \pmod{d}$ відносно M має єдиний розв'язок. Довести, що в цьому випадку N і M одночасно або діляться, або не діляться на d, тобто M задовольняє вимоги функції $f(N)$.

14. Знайти ознаки подільності на 2, 3, 4, 5, 7, 9 для вісімкової системи числення.

Відповідь. На 2 ділиться число, яке закінчується парною цифрою, включаючи і 0; на 3 і на 9 ділиться число, для якого різниця між сумою цифр, що стоять на парних місцях, і сумою цифр, що стоять на непарних місцях, ділиться на 3 або на 9; на 4 ділиться число, яке закінчується нулем або цифрою 4; на 5 ділиться число $N = a_0 + 8a_1 + 8^2 a_2 + 8^3 a_3 + \cdots$, якщо вираз

$$a_0 - 2a_1 - a_2 + 2a_3 + a_4 - 2a_5 - a_6 + \cdots$$

ділиться на 5; на 7 ділиться число, сума цифр якого ділиться на 7.

15. Знайти ознаки подільності на 2, 3, 4, 5, 6, 7, 8, 9, 11, 13 для дванадцяткової системи числення.

Відповідь. На 2 ділиться число, яке закінчується парною цифрою, включаючи і 0; на 3 ділиться число, яке закінчується цифрою 0, 3, 6, або 9; на 4 ділиться число, яке закінчується цифрою 0, 4, або 8; на 5 ділиться число $N = a_0 + 12a_1 + 12^2 a_2 + \cdots$, якщо число

$$a_0 + 2a_1 - 2a_3 + a_4 + 2a_5 - \cdots$$

ділиться на 5; на 6 ділиться число, яке закінчується нулем або цифрою 6; на 7 ділиться число $N = a_0 + 12a_1 + 12^2 a_2 + \cdots$, якщо число

$$a_0 - 2a_1 - 3a_2 - a_3 + 2a_4 + 3a_5 + a_6 - 2a_7 - 3a_8 + \cdots$$

ділиться на 7; на 8 ділиться число N, якщо $a_0 + 4a_1$ ділиться на 8; на 9 ділиться число N, якщо $a_0 + 3a_1$ ділиться на 9; на 11 ділиться число, сума цифр

якого ділиться 11; ознака подільності на 13 така сама, як і в десятковій системі на 11.

16. Припустимо, що $p \neq 2; 5$ — просте число. Розбиваючи число N на грані по $\frac{p-1}{2}$ цифр у кожній грані, тобто переходячи до системи числення з основою $g = 10^{\frac{p-1}{2}}$, ми дістанемо ознаку подільності на p, аналогічну до ознаки подільності на 9 або 11, залежно від того, чи буде 10 відповідно квадратичним лишком, чи нелишком за модулем p. Довести це твердження.

17. Нехай $N = a_0 + a_1 g + \cdots + a_n g^n$ — число, написане при основі системи числення g якщо $(d, g) = 1$ і μ — розв'язок конгруенції $gx \equiv -1 \pmod d$, то $M = \left[\frac{N}{g}\right] - \mu a_0$ задовольняє вимоги функції $f(N)$, тобто M і N одночасно або діляться на d, або одночасно не діляться на d. Довести це твердження.

18. Нехай, як і в попередньому твердженні, $N = a_0 + a_1 g + \cdots + a_n g^n$, якщо $(d, g) = 1$ і μ — розв'язок конгруенції $gx \equiv 1 \pmod d$, то $M = \left[\frac{N}{g}\right] + \mu a_0$ задовольняє вимоги функції $f(N)$.

19. На підставі твердження задачі 17 довести, що число $N = 10a + b$ ділиться на число d виду:

а) $d = 10c + 1$, якщо $a - bc$ ділиться на d;
б) $d = 10c + 3$, якщо $a + b(3c + 1)$ ділиться на d;
в) $d = 10c + 7$, якщо $a - b(3c + 2)$ ділиться на d;
г) $d = 10c + 9$, якщо $a + b(c + 1)$ ділиться на d.

Зауважимо тут, що ці ознаки подільності застосовані для будь-якого простого числа, крім 2 і 5, бо всі прості числа крім 2 і 5, у десятковій системі числення закінчуються цифрами 1, 3, 7, 9.

20. Використовуючи ознаки подільності попередньої задачі, знайти канонічний розклад чисел: а) 90 799; б) 3 058 487.

Відповідь. а) $29 \cdot 31 \cdot 101$; б) $17^2 \cdot 19 \cdot 557$.

21. Методом конгруенцій виявити цифру a, якої невистачає у восьмицифровому числі $\overline{37a\,10201}$ і яким числом треба замінити букву x у виразі $[11(492 + x)]^2$, щоб рівність $[11(492 + x)]^2 = \overline{37a\,10201}$ була справедливою.

Відповідь. $a = 8$; $x = 67$.

22. Перевірити, чи ділиться число $372654^{500} + 72 \cdot 10^7$ на 18.

Відповідь. Ділиться.

23. Довести, що при будь-яких цілих m і n вираз $mn(m^{60} - n^{60})$ ділиться на 56 786 730.

Вказівка. Методом конгруенцій показати, що такий вираз ділиться на всі прості дільники цього числа.

24. Довести, що вираз $20^n + 16^n \cdot 3^n - 1$ ділиться на 323, якщо n — парне.

25. Число, що записується в десятковій системі числення як $\overline{7x\,36y\,5}$, ділиться на 1375. Знайти x і y.

Відповідь. $x = 1$, $y = 2$.

26. Число, що записується в десятковій системі числення як $\overline{13xy\,45z}$, ділиться на 792. Знайти x, y, z.

Відповідь. $x = 8$, $y = 0$, $z = 6$.

27. Знайти число цифр у періоді десяткових дробів, в які перетворюються нескоротні звичайні дроби із знаменниками: 3, 7, 11, 17, 19, 21.

Відповідь. 1, 6, 2, 16, 18, 6.

28. Довести, що коли 10 є первісним коренем за модулем m, то періоди всіх нескоротних дробів із знаменником m складатимуться з кругових перестановок однієї й тієї самої системи $k = \varphi(m)$ цифр.

29. Припустимо, що $z_1, z_2, \ldots, z_k$ — період дробу $\frac{1}{m}$, де $(m, 10) = 1$, і 10 є первісним коренем за модулем m. Довести, що число цифр q, на яке треба відступати праворуч, щоб знайти період $z_{q+1}, z_{q+2}, \ldots, z_q$ дробу $\frac{n}{m}$, дорівнює $q = \operatorname{ind}_{10} n$.

30. Користуючись результатом попередньої задачі і знаючи, що $\frac{1}{7} = 0,(142857)$, знайти $\frac{2}{7}, \frac{3}{7}, \frac{4}{7}, \frac{5}{7}, \frac{6}{7}$.

Відповідь. $\frac{2}{7} = 0,(285714)$; $\frac{3}{7} = 0,(428571)$; $\frac{4}{7} = 0,(571428)$; $\frac{5}{7} = 0,(714\,285)$; $\frac{6}{7} = 0,(857142)$.

31. Знайти знаменник дробу, який перетворюється в чистий періодичний дріб з трьома цифрами в періоді.

Відповідь. 27, 37, 111, 333, 999.

32. Довести, що коли 10 є квадратичним нелишком за простим модулем $p \neq 2, 5$, то при перетворенні $\frac{1}{p}$ у нескінченний десятковий дріб, утворюється парне число цифр у періоді. При цьому, якщо p — просте число виду $4k + 3$, то парне число цифр у періоді буде тільки тоді, коли 10 — квадратичний нелишок.

33. Довести, що коли p — просте число, відмінне від 2 і 5, і дріб $\frac{1}{p}$ перетворюється у чистий періодичний десятковий дріб з парним числом цифр у періоді, то цифри другої половини періоду доповнюють до дев'яти цифри першої половини періоду. Наприклад, $0,(142\,857)$ і $1 + 8 = 9$, $4 + 5 = 9$, $2 + 7 = 9$.

34. За допомогою таблиць індексів визначити кількість цифр у періоді розкладу дробів $\frac{1}{43} \cdot \frac{1}{89} \cdot \frac{1}{97}$ у нескінченний десятковий дріб.

Відповідь. 21, 44, 96.

35. Перетворити такі періодичні десяткові дроби в звичайні: а) $0,3\overline{5}\,(6\overline{2})$; б) $5,1\,(538)$; в) $3\,(27)$; г) $11,12\,(31)$.

Відповідь. а) $\frac{3527}{9900}$; б) $\frac{51\,487}{9900}$; в) $\frac{3\overline{6}}{11}$; г) $\frac{110\,119}{9900}$.

36. Перевірити правильність результату обчислень числом 9.

а) $12\,376\,(809\,376 - 745\,934) + 43^2 \cdot 97\,215 = 964\,908\,727$;
б) $(378^3 - 7\,298\,348) \cdot 10 + (427\,019 - 451^2) \cdot 50 = 578\,298\,940$.

37. Перевірити правильність результату обчислень числом 11:

а) $(2\,708^2 - 8\,513\,874) \cdot 18 - 37^3 \cdot 179 = 276\,181\,597$;
б) $437 \cdot 86 + 16\,384 = 54\,866$.

38. Перевірити правильність виконання арифметичних дій числами 9 і 11:

а) $3125 \cdot 256 = 800\,000$; б) $4325 \cdot 897 = 454\,125$; в) $6735 \cdot 324 = 2\,178\,900$;
г) $(574\,339 + 831 \cdot 991) \cdot 12 - 1277^2 = 15\,044\,591$.

ІСТОРИЧНІ КОМЕНТАРІ

1. Блез Паскаль (1623 — 1662) — видатний французький математик, фізик і філософ. Математичні інтереси Паскаля були дуже різноманітні: він зробив істотний внесок у розвиток аналізу нескінченно малих; разом з Ферма Паскаль є основоположником теорії ймовірностей; йому належить загальна ознака подільності будь-якого цілого числа на будь-яке інше ціле число, яка грунтується на знанні суми цифр числа, а також спосіб обчислення біноміальних

коефіцієнтів («арифметичний трикутник»); він вперше точно визначив і застосував для доведення метод повної математичної індукції.

2. Перевірка арифметичних дій числом 9 була поширена до кінця XVIII ст.; нею користувалися ще на початку нашої ери в Індії.

Розділ VII

АПРОКСИМАЦІЯ ІРРАЦІОНАЛЬНИХ ЧИСЕЛ РАЦІОНАЛЬНИМИ

§ 37. Збіжність нескінченних неперервних дробів

Теорія неперервних дробів є одним з найважливіших засобів аналізу, теорії ймовірностей, механіки й особливо теорії чисел.

Нескінченним неперервним дробом називається вираз виду:

$$q_0 + \cfrac{1}{q_1 + \cfrac{1}{q_2 + \ddots}},$$

або символічно

$$[q_0;\ q_1,\ q_2,\ \ldots]. \qquad (1)$$

Букви q_0, q_1, $q_2 \ldots$ залежно від спеціальних потреб можна вважати дійсними або комплексними числами, функціями однієї або кількох змінних і т. п.

Збережемо термінологію § 8 і 9, де ми розглядали скінченні неперервні дроби. Зокрема, дроби:

$$\frac{P_0}{Q_0} = q_0,\ \frac{P_1}{Q_1} = q_0 + \frac{1}{q_1},\ \ldots,\ \frac{P_k}{Q_k} = q_0 + \cfrac{1}{q_1 + \cfrac{1}{q_1 + \ddots + \cfrac{1}{q_k}}} \qquad (2)$$

$$(k = 0, 1, 2, \ldots)$$

називатимемо *підхідними дробами* до дробу (1).

Нескінченний неперервний дріб (1) називається *збіжним*, якщо нескінченна послідовність (2) підхідних дробів збігається, тобто має певну границю α; цю границю α називають значенням неперервного дробу (1) і записують:

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

Якщо послідовність (2) підхідних дробів границі не має, то неперервний дріб (1) називають *розбіжним*.

Надалі вважатимемо $q_1, q_2, \ldots$ — натуральними, а q_0 — будь-яким цілим числом, тоді, яке б велике не було k, підхідні дроби (2) до нескінченного дробу (1) є разом з тим підхідними дробами до скінченного неперервного дробу. Тому всі властивості підхідних дробів, доведені в § 8 для скінченних неперервних дробів, будуть справедливі і для нескінченних неперервних дробів такого типу.

Теорема 1. *Нескінченний неперервний дріб (1) завжди збігається.*

Справді, відомо (див. теорему 3, § 8), що підхідні дроби парного порядку утворюють зростаючу, а непарного порядку — зустрічну спадну послідовність, так що будь-який підхідний дріб парного порядку менший від будь-якого підхідного дробу непарного порядку, тобто:

$$\frac{P_0}{Q_0} < \frac{P_2}{Q_2} < \frac{P_4}{Q_4} < \cdots < \frac{P_5}{Q_5} < \frac{P_3}{Q_3} < \frac{P_1}{Q_1}.$$

За відомою теоремою про обмежені монотонні послідовності можна твердити, що існує кожна з границь:

$$\lim_{k\to\infty} \frac{P_{2k}}{Q_{2k}} \text{ і } \lim_{k\to\infty} \frac{P_{2k+1}}{Q_{2k+1}}.$$

Покажемо, що ці границі рівні між собою. Справді, починаючи з $k = 1$, $Q_{k+1} = Q_k q_{k+1} + Q_{k-1}$ (див. теорему 1, § 8), отже,

$$Q_{k+1} \geqslant Q_k + Q_{k-1} > Q_k,$$

бо $q_i \geqslant 1$ для всіх $i = 1, 2, 3, \ldots$, тому послідовність натуральних чисел $Q_0, Q_1, Q_2, \ldots$ зростаюча, і $\lim\limits_{k\to\infty} Q_k = \infty$, отже

$$\lim_{k\to\infty} \frac{1}{Q_{2k} Q_{2k+1}} = 0.$$

Тепер легко побачити, що

$$\lim_{k\to\infty} \left| \frac{P_{2k+1}}{Q_{2k+1}} - \frac{P_{2k}}{Q_{2k}} \right| = \lim_{k\to\infty} \frac{1}{Q_{2k} Q_{2k+1}} = 0$$

(див. теорему 2, § 8).

Цим і доведено твердження про існування границі $\lim\limits_{n\to\infty} \frac{P_n}{Q_n} = \alpha$, коли n пробігає послідовно усі натуральні, парні й непарні, значення.

З теореми 3, § 8 для збіжних нескінченних неперервних дробів випливає таке твердження:

Теорема 2. *Значення збіжного нескінченного неперервного дробу (1) більше від будь-якого підхідного дробу парного порядку і менше від будь-якого підхідного дробу непарного порядку.*

Контрольні запитання

1. Який вираз називається нескінченним неперервним дробом?
2. Які дроби називаються підхідними дробами до неперервного дробу типу (1)?
3. Який неперервний дріб називається збіжним?
4. На якій теоремі з математичного аналізу грунтується доведення теореми 1?

§ 38. Подання ірраціональних чисел нескінченними неперервними дробами

Надалі символ

$$[q_0;\ q_1;\ q_2,\ \ldots,\ q_k,\ \ldots] = \alpha \qquad (1)$$

завжди позначатиме збіжний неперервний дріб α.

Неперервний дріб виду

$$\alpha_k = [q_k,\ q_{k+1},\ \ldots]$$

називають k-ою *повною часткою*, або *остачею*, нескінченного неперервного дробу (1). При цій умові завжди можна написати такий вираз для α:

$$\alpha = [q_0,\ q_1,\ \ldots,\ q_{k-1},\ \alpha_k]. \qquad (2)$$

Справді, для скінченного неперервного дробу це співвідношення очевидне. Якщо границя послідовності підхідних дробів до нескінченного неперервного дробу $[q_k,\ q_{k+1},\ \ldots]$ дорівнює α_k, то $\alpha_k > 1$, і, за відомими теоремами про границю суми і частки, дістанемо:

$$\lim_{l\to\infty}[q_0;\ q_1,\ \ldots,\ q_k,\ q_{k+1},\ \ldots,\ q_{k+l}] = [q_0;\ q_1,\ \ldots,\ q_{k-1}],\ \lim_{l\to\infty}[q_k,$$

$$q_{k+1},\ \ldots,\ q_{k+l}],$$

тобто матимемо рівність (2).

Зауважимо тут, що за означеннями $q_k = [\alpha_k]$ для всіх $k = 0, 1, 2, \ldots$

Теорема 1. Якщо α — значення неперервного дробу (скінченого або нескінченного), то для будь-якого $k > 1$ справджується рівність:

$$\alpha = \frac{P_{k-1}\alpha_k + P_{k-2}}{Q_{k-1}\alpha_k + Q_{k-2}} \qquad (3)$$

(для скінченного дробу $k \leqslant n$, де n — довжина дробу).

Справді, за законом утворення підхідних дробів (теорема 1, § 8) маємо:

$$\frac{P_k}{Q_k} = \frac{P_{k-1}q_k + P_{k-2}}{Q_{k-1}q_k + Q_{k-2}};$$

але неперервний дріб $[q_0;\ q_1,\ \ldots,\ q_{k-1},\ \alpha_k] = \alpha$ можна дістати з $[q_0;\ q_1,\ \ldots,\ q_{k-1},\ q_k] = \frac{P_k}{Q_k}$, замінивши неповну частку q_k повною часткою α_k, і ми дістанемо формулу (3).

Теорема 2. *Всякому дійсному ірраціональному числу відповідає єдиний нескінченний неперервний дріб, що має це число своїм значенням. Навпаки, всякий нескінченний неперервний дріб визначає одне і тільки одне дійсне ірраціональне число.*

Доведення цієї теореми розіб'ємо на дві частини.

1) Припустимо, що ω — довільне дійсне число. Виділимо цілу частину числа ω; нехай $q_0 = [\omega]$, тоді

$$\omega = q_0 + x_0,\ 0 \leqslant x_0 < 1,$$

де q_0 — ціле число, більше або менше 0. Для того щоб мати можливість повторити операцію виділення цілої частини, розглянемо число $\omega_1 = \frac{1}{x_0}$, обернене до x_0. Припустимо, що

$$\omega_1 = q_1 + x_1,\ 0 \leqslant x_1 < 1,$$

де $q_1 = [\omega_1]$ — натуральне число. Тоді

$$x_0 = \frac{1}{q_1 + x_1} \quad \text{і} \quad \omega = q_0 + \frac{1}{q_1 + x_1}.$$

Роблячи так само й далі, на n-й стадії процесу прийдемо до рівності:

$$\omega = q_0 + \cfrac{1}{q_1 + \cfrac{1}{q_2 + \ddots + \cfrac{1}{q_n + x_n}}}, \qquad (4)$$

де $q_0, q_1, q_2, \ldots, q_n$ — цілі числа, додатні, починаючи з q_1, а $0 \leqslant x_n < 1$. Якщо ω — раціональне число, то описаний процес буде скінченним, тобто при деякому n дістанемо, що $x_n = 0$ (див. теорему § 7). А коли ω — ірраціональне число, то описаний процес породжує нескінченну послідовність неповних часток $q_0, q_1, q_2, \ldots$ і відповідну послідовність підхідних дробів, тобто ω розкладається в нескінченний неперервний дріб типу (1), який за доведеним має єдине значення, що дорівнює $\lim_{n\to\infty}\frac{P_n}{Q_n} = \alpha$. Справді, оскільки ω — ірраціональне, то ніколи не матимемо $x_n = 0$, бо число x_n як дробова частина ірраціонального числа саме буде ірраціональним при будь-якому $n = 0, 1, 2, \ldots$

Покажемо тепер, що

$$\omega = \lim_{n\to\infty}\frac{P_n}{Q_n} = \alpha.$$

Справді, якщо $0 < x_n < 1$ і $\omega_{n+1} = \frac{1}{x_n}$, то з рівності (4) випливатиме, що ω_{n+1} буде повною часткою в розкладі ω, за теоремою 1 маємо:

$$\omega = \frac{P_n\omega_{n+1} + P_{n-1}}{Q_n\omega_{n+1} + Q_{n-1}},$$

тоді

$$\left|\omega - \frac{P_n}{Q_n}\right| = \left|\frac{P_n\omega_{n+1} + P_{n-1}}{Q_n\omega_{n+1} + Q_{n-1}} - \frac{P_n}{Q_n}\right| =$$

$$= \left|\frac{P_{n-1}Q_n - P_nQ_{n-1}}{Q_n(Q_n\omega_{n+1} + Q_{n-1})}\right| = \frac{1}{Q_n(Q_n\omega_{n+1} + Q_{n-1})} < \frac{1}{Q_n^2\omega_{n+1}} < \frac{1}{Q_n^2},$$

бо $\omega_{n+1} > 1$.

Звідси при $n > N$ і при будь-якому $\varepsilon > 0$ дістанемо:

$$\left|\omega - \frac{P_n}{Q_n}\right| < \varepsilon, \text{ а це означає, що } \omega = \lim_{n\to\infty}\frac{P_n}{Q_n} = \alpha.$$

Доведемо тепер, що для будь-якого дійсного ірраціонального числа ω є один і лише один неперервний дріб, що дорівнює ω.

Справді, припустимо супротивне, тобто припустимо, що

$$\omega = [q_0;\ q_1,\ q_2, \ldots] = [q_0',\ q_1',\ q_2', \ldots],$$

де q_i і q_i' — цілі числа, причому при $i \geqslant 1$ всі q_i і q_i' — натуральні. Припустимо, що ці два неперервні дроби відрізняються хоча б одним елементом. Позначимо через k перший по порядку номер, такий, що $q_k \neq q_k'$, тобто припустимо:

$$q_0 = q_0',\ q_1 = q_1', \ldots,\ q_{k-1} = q_{k-1}',\ \text{але } q_k \neq q_k'.$$

Позначимо через

$$\omega_k = [q_k,\ q_{k+1}, \ldots] \text{ і } \omega_k' = [q_k',\ q_{k+1}', \ldots].$$

З припущення і рівності (2) випливатиме, що

$$\omega = [q_0,\ q_1, \ldots,\ q_{k-1},\ \omega_k] = [q_0';\ q_1', \ldots,\ q_{k-1}',\ \omega_k'];$$

звідси дістанемо, що $\omega_k = \omega_k'$, але оскільки $q_k = [\omega_k]$ і $q_k' = [\omega_k']$, то $q_k = q_k'$, а це суперечить умові.

2) Раніш уже було доведено (теорема 1, § 37), що нескінченний неперервний дріб (1) визначає деяке цілком певне число $\alpha = \lim_{n\to\infty}\frac{P_n}{Q_n}$. Справді, α є дійсне число, бо воно є границею нескінченної послідовності дійсних чисел.

Покажемо тепер, що, коли $[q_0;\ q_1,\ q_2, \ldots] = \alpha$, то сам неперервний дріб $[q_0;\ q_1,\ q_2, \ldots]$ дістаємо з α за допомогою виділення цілої частини.

Справді, припустимо, що, розкладаючи α в неперервний дріб за допомогою виділення цілої частини, дістанемо

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

Тут $q_0' = [\alpha]$ з другого боку, за формулою (2) можна написати: $\alpha = [q_0,\ \alpha_1]$, де $\alpha_1 = [q_1,\ q_2, \ldots]$ — перша повна частка, тобто $\alpha = q_0 + \frac{1}{\alpha_1}$. Оскільки $q_1 \geqslant 1$, то всі підхідні дроби для α_1 будуть більші від 1, а тому й $\alpha_1 > 1$, отже, $\frac{1}{\alpha_1} < 1$. Отже, q_0 визначається

однозначно як ціла частина числа α, тобто $q_0 = [\alpha]$. Але $q_0' = [\alpha]$, тому $q_0' = q_0$, і з рівностей

$$\alpha = q_0 + \frac{1}{\alpha_1},\ \alpha = q_0' + \frac{1}{\alpha_1'},$$

де $\alpha_1' = [q_1',\ q_2', \ldots]$, маємо тепер $\alpha_1 = \alpha_1'$. Далі, аналогічно знайдемо, що $q_1 = q_1'$ і т. д.

Тепер уже ірраціональність числа α відразу випливає з нескінченності процесу виділення цілої частини з α, бо коли б α було раціональним, то такий процес виділення цілої частини був би, як ми знаємо, скінченним (теорема § 7). Отже, теорему доведено.

У § 7 ми показали, що коли поставити вимогу, щоб останній знаменник q_n був більший одиниці, то кожне раціональне число єдиним способом можна розкласти в скінченний неперервний дріб. За щойно доведеною теоремою кожне ірраціональне число єдиним способом розкладається в нескінченний неперервний дріб. Щодо цього розклади дійсних чисел у неперервні дроби характеризують природу дійсних чисел краще, ніж розклади їх у систематичні дроби.

Розклад раціонального числа у систематичний дріб, наприклад у десятковий, може бути скінченним і нескінченним (див. § 35), причому характер такого розкладу істотно залежить від основи системи числення.

Через те що між дійсними числами і неперервними дробами встановлено взаємно однозначну відповідність, то у випадку, коли $\alpha = [q_0;\ q_1,\ q_2, \ldots]$, підхідні дроби $\frac{P_k}{Q_k}$ до цього неперервного дробу називають також, для спрощення, підхідними дробами до числа α.

Контрольні запитання

1. Який неперервний дріб називають k-ою повною часткою неперервного дробу типу (1).
2. Як зв'язані між собою значення неперервного дробу і k-а повна частка цього дробу?
3. Яким способом будь-яке дійсне ірраціональне число можна подати у вигляді нескінченного неперервного дробу?
4. Чому ірраціональне число подається нескінченним неперервним дробом?

§ 39. Порядок наближення ірраціональних чисел підхідними дробами[1]

У ряді обчислень доводиться дійсні числа α подавати у вигляді звичайного раціонального дробу. Для цього можна скористатись підхідними дробами розкладу α у неперервний дріб.

[1] Взагалі, всі твердження щодо наближення ірраціональних чисел підхідними дробами $\frac{P_k}{Q_k}$ $(k = 0, 1, 2, \ldots)$ справедливі і для раціональних чисел, тільки в цьому випадку треба вважати, що $k \leqslant n$, де n — довжина скінченного неперервного дробу.

Теорема 1. *Якщо замість точного значення неперервного дробу взяти його k-й підхідний дріб, то за межу похибки зверху можна взяти:*

$$\frac{1}{Q_kQ_{k+1}} \text{ або } \frac{1}{Q_k(Q_k+Q_{k-1})}, \text{ або } \frac{1}{Q_k^2}.$$

Це твердження є не що інше, як теорема 4, § 8. Воно еквівалентне нерівності (5), § 8.

$$\left|\alpha-\frac{P_k}{Q_k}\right| \leqslant \frac{1}{Q_kQ_{k+1}} \leqslant \frac{1}{Q_k(Q_k+Q_{k-1})} < \frac{1}{Q_k^2}.$$

Але можна дістати ще точніший висновок про міру наближення, якщо додатково скористатись такою теоремою про оцінку похибки модуля різниці знизу.

Теорема 2. *Для всякого* $k \geqslant 0$ і $\alpha \neq P_k/Q_k$ *має місце нерівність:*

$$\left|\alpha-\frac{P_k}{Q_k}\right| > \frac{1}{Q_k(Q_{k+1}+Q_k)},$$

тобто *за оцінку похибки знизу можна взяти число*

$$\frac{1}{Q_k(Q_{k+1}+Q_k)}.$$

Справді, для $k=0$ ця нерівність очевидна, бо з розкладу $\alpha = [q_0; q_1, q_2, \ldots]$ числа α у неперервний дріб випливає, що

$$\left|\alpha-\frac{P_0}{Q_0}\right| = \alpha - q_0 = \frac{1}{q_1+\cfrac{1}{q_2+\cdots}} > \frac{1}{q_1+1} = \frac{1}{Q_0(Q_1+Q_0)}.$$

1) Припустимо тепер, що k є парне число не менше за 2, тоді внаслідок властивості 3 підхідних дробів (див. § 8):

$$\frac{P_k}{Q_k} < \frac{P_{k+2}}{Q_{k+2}} < \alpha.$$

Покажемо, що дріб $\frac{P_k+P_{k+1}}{Q_k+Q_{k+1}}$ міститься між $\frac{P_k}{Q_k}$ і $\frac{P_{k+2}}{Q_{k+2}}$.

Справді,

$$\frac{P_{k+2}}{Q_{k+2}} - \frac{P_k+P_{k+1}}{Q_k+Q_{k+1}} = \frac{(P_{k+2}Q_k - P_kQ_{k+2}) + (P_{k+2}Q_{k+1} - P_{k+1}Q_{k+2})}{(Q_k+Q_{k+1})Q_{k+2}} = \frac{(-1)^k q_{k+2} + (-1)^{k+1}}{(Q_k+Q_{k+1})Q_{k+2}}$$

(див. властивості 3 і 2, § 8). І через те що k — парне за умовою, матимемо:

$$\frac{P_{k+2}}{Q_{k+2}} - \frac{P_k+P_{k+1}}{Q_k+Q_{k+1}} = \frac{q_{k+2}-1}{(Q_k+Q_{k+1})Q_{k+2}} > 0, \text{ бо } q_{k+2} > 1.$$

Аналогічно знайдемо:

$$\frac{P_k+P_{k+1}}{Q_k+Q_{k+1}} - \frac{P_k}{Q_k} = \frac{P_{k+1}Q_k - P_kQ_{k+1}}{Q_k(Q_k+Q_{k+1})} = \frac{(-1)^k}{Q_k(Q_k+Q_{k+1})} > 0.$$

Отже, дістанемо:

$$\frac{P_k}{Q_k} < \frac{P_k+P_{k+1}}{Q_k+Q_{k+1}} \leqslant \frac{P_{k+2}}{Q_{k+2}} < \alpha,$$

звідки

$$0 < \frac{P_k+P_{k+1}}{Q_k+Q_{k+1}} - \frac{P_k}{Q_k} < \alpha - \frac{P_k}{Q_k}$$

і

$$\left|\alpha-\frac{P_k}{Q_k}\right| > \frac{P_k+P_{k+1}}{Q_k+Q_{k+1}} - \frac{P_k}{Q_k} = \frac{1}{Q_k(Q_k+Q_{k+1})}.$$

2) Нехай k є непарне число, тоді, за властивістю 3 підхідних дробів (див. § 8):

$$\frac{P_k}{Q_k} > \frac{P_{k+2}}{P_{k+2}} > \alpha.$$

Покажемо, що дріб $\frac{P_k+P_{k+1}}{Q_k+Q_{k+1}}$ міститься між $\frac{P_{k+2}}{Q_{k+2}}$ і $\frac{P_k}{Q_k}$.

Справді, тут внаслідок непарності k аналогічно дістанемо:

$$\frac{P_k+P_{k+1}}{Q_k+Q_{k+1}} - \frac{P_k}{Q_k} = \frac{(-1)^k}{Q_k(Q_k+Q_{k+1})} < 0,$$

$$\frac{P_{k+2}}{Q_{k+2}} - \frac{P_k+P_{k+1}}{Q_k+Q_{k+1}} = \frac{-q_{k+2}+1}{(Q_k+Q_{k+1})Q_{k+2}} \leqslant 0,$$

звідки випливає, що

$$\frac{P_{k+2}}{Q_{k+2}} \leqslant \frac{P_k+P_{k+1}}{Q_k+Q_{k+1}} < \frac{P_k}{Q_k}.$$

Звідси:

$$0 < \frac{P_k}{Q_k} - \frac{P_k+P_{k+1}}{Q_k+Q_{k+1}} < \frac{P_k}{Q_k} - \alpha$$

і

$$\left|\alpha-\frac{P_k}{Q_k}\right| > \frac{P_k}{Q_k} - \frac{P_k+P_{k+1}}{Q_k+Q_{k+1}} = \frac{1}{Q_k(Q_k+Q_{k+1})}.$$

Отже, теорему доведено.

Зауважимо, що можна розкладати у неперервні дроби не тільки дані дійсні числа, а й невідомі нам дійсні числа, наприклад, корені алгебраїчних або трансцендентних рівнянь. Для цього треба тільки вміти виділяти цілі частини коренів таких рівнянь. При цьому розкладуване в неперервний дріб ірраціональне число можна наближено знайти у вигляді раціонального числа з будь-якою наперед заданою точністю. Цим раціональним числом може бути один

з підхідних дробів. На підставі теорем 1 і 2 можна робити висновок про межу похибки зверху і знизу[1].

Щоб знайти раціональне наближення дійсного числа α з точністю до $\varepsilon > 0$, можна підібрати підхідний дріб $\frac{P_k}{Q_k}$ з таким найменшим номером k, щоб Q_kQ_{k+1} або $Q_k(Q_k + Q_{k-1})$, або Q_k^2 було більше від $\frac{1}{\varepsilon}$, і тоді матимемо

$$\left|\alpha - \frac{P_k}{Q_k}\right| < \varepsilon.$$

Приклад 1. Розкласти у неперервний дріб $\sqrt{42}$ і знайти раціональне наближення до нього з точністю до 0,0001.

Маємо:

$$\sqrt{42} = 6 + \frac{1}{\alpha_1}, \text{ де } \alpha_1 > 1.$$

Звідси:

$$\alpha_1 = \frac{1}{\sqrt{42} - 6} = \frac{\sqrt{42} + 6}{6} = 2 + \frac{1}{\alpha_2};\ \alpha_2 > 1;$$

$$\alpha_2 = \frac{6}{\sqrt{42} - 6} = \sqrt{42} + 6 = 12 + \frac{1}{\alpha_3};\ \alpha_3 > 1;$$

$$\alpha_3 = \frac{1}{\sqrt{42} - 6} = \alpha_1.$$

Отже, далі повторюватимуться ті самі повні частки, а тому і відповідні неповні частки також періодично повторюватимуться, починаючи з q_1. В результаті дістанемо такий розклад $\sqrt{42}$ у неперервний дріб:

$$\sqrt{42} = [6, (2, 12)].$$

У круглих дужках стоять ті неповні частки розкладу $\sqrt{42}$ у неперервний дріб, які періодично повторюються. Щоб дати відповідь на друге запитання задачі, треба знайти такий підхідний дріб $\frac{P_k}{Q_k}$ у цьому розкладі, щоб

$$\frac{1}{Q_kQ_{k+1}} \text{ або } \frac{1}{Q_k(Q_k+Q_{k-1})}, \text{ або } \frac{1}{Q_k^2}$$

---

[1] Зауважимо, що коли за наближення до α взяти підхідний дріб $\frac{P_k}{Q_k}$, то про межу похибки зверху завжди можемо зробити висновок на підставі теореми 1, а про нижню — ні, щоб зробити висновок і про нижню межу похибки, треба знати ще Q_{k+1}, яке не завжди можна легко знайти.

були менші, ніж 0,0001 (див. теорему 1). Маємо:

k		0	1	2	3	4
q_k		6	2	12	2	12
P_k	1	6	13	162	337	
Q_k	0	1	2	25	52	649

Тепер легко побачити, що підхідний дріб $\frac{P_3}{Q_3} = \frac{337}{52}$ задовольняє умову задачі, і ми можемо записати, що $\sqrt{42} \approx \frac{337}{52}$ (з точністю до 0,0001). Тут похибка не перевищує навіть $\frac{1}{52 \cdot 649}$, що значно менше від 0,0001. За теоремою 2 можна сказати, що ця похибка більша від $\frac{1}{52(52+649)}$. Зрозуміло, що будь-який наступний за $\frac{P_3}{Q_3}$ підхідний дріб буде раціональним наближенням до $\sqrt{42}$ з ще більшою точністю. Проте звичайно краще вибирати за потрібне наближення той з підхідних дробів, в якого знаменник найменший.

Приклад 2. Знайти четвертий підхідний дріб у розкладі в неперервний дріб кореня рівняння $f(x) = x^4 - x - 1 = 0$, що міститься в інтервалі (1; 2).

З умови задачі відразу випливає що

$$x = 1 + \frac{1}{x_1}, \text{ де } x_1 > 1.$$

Щоб визначити $[x_1]$, знайдемо рівняння, коренем якого є x_1; для цього розкладемо $f(x)$ за степенями $x - 1 = \frac{1}{x_1}$, наприклад, за схемою Горнера

	1	0	0	−1	−1
1	1	1	1	0	−1
1	1	2	3	3	
1	1	3	6		
1	1	4			
1	1				

Отже, дістанемо:

$$\frac{1}{x_1^4} + 4 \cdot \frac{1}{x_1^3} + 6 \cdot \frac{1}{x_1^2} + 3 \cdot \frac{1}{x_1} - 1 = 0,$$

або звівши до спільного знаменника,

$$\varphi_1(x_1) = x_1^4 - 3x_1^3 - 6x_1^2 - 4x_1 - 1 = 0.$$

Відомими з алгебри прийомами знаходимо, що корінь останнього рівняння лежить в інтервалі (4; 5); отже, припускаємо, що $x_1 = 4 + \frac{1}{x_2}$, і, розклавши $\varphi_1(x_1)$ за степенями $x_1 - 4 = \frac{1}{x_2}$, після аналогічних перетворень дістанемо рівняння для x_2:

$$\varphi_2(x_2) = 49x_2^4 - 60x_2^3 - 54x_2^2 - 13x_2 - 1 = 0.$$

Знаходимо, що корінь x_2 лежить в інтервалі (1; 2); нехай $x_2 = 1 + \frac{1}{x_3}$. Після аналогічних перетворень многочлена $\varphi_2(x_2)$ дістанемо, що x_3 буде коренем рівняння

$$\varphi_3(x_3) = 79x_3^4 + 105x_3^3 - 60x_3^2 - 136x_3 - 49 = 0.$$

Корінь цього рівняння також лежить в інтервалі (1; 2); тоді $x_3 = 1 + \frac{1}{x_4}$. Після вказаних вище перетворень дістанемо, що x_4 буде коренем рівняння

$$\varphi_4(x_4) = 64x_4^4 - 375x_4^3 - 729x_4^2 - 421x_4 - 79 = 0.$$

Знаходимо, що x_4 лежить в інтервалі (6; 7); звідси $x_4 = 6 + \frac{1}{x_5}$ і т. д. На цьому спинимось, бо ми вже знайшли достатню кількість неповних часток, щоб визначити $\frac{P_4}{Q_4}$ у розкладі кореня заданого рівняння в неперервний дріб. Маємо:

$$x = 1 + \frac{1}{x_1} = 1 + \cfrac{1}{4 + \frac{1}{x_2}} = 1 + \cfrac{1}{4 + \cfrac{1}{1 + \frac{1}{x_3}}} =$$

$$= 1 + \cfrac{1}{4 + \cfrac{1}{1 + \cfrac{1}{1 + \frac{1}{x_4}}}} = 1 + \cfrac{1}{4 + \cfrac{1}{1 + \cfrac{1}{1 + \cfrac{1}{6 + \frac{1}{x_5}}}}},$$

або

$$x = [1; 4, 1, 1, 6, x_5].$$

де x_5 — корінь рівняння, яке можна вивести з $\varphi_4(x_4) = 0$ за допомогою перетворень, аналогічних попереднім. Далі маємо:

k		0	1	2	3	4
q_k		1	4	1	1	6
P_k	1	1	5	6	11	72
Q_k	0	1	4	5	9	59

Отже, $\frac{P_4}{Q_4} = \frac{72}{59}$ наближено виражає корінь заданого рівняння з точністю, яка принаймні не перевищує $\frac{1}{59(59+9)} = \frac{1}{59 \cdot 68} = \frac{1}{4012}$. Тут уже ми не можемо за верхню межу похибки взяти $\frac{1}{Q_k Q_{k+1}} = \frac{1}{Q_4 Q_5}$, бо Q_5 нам невідоме. Це ми й мали на увазі, коли в § 8 зауважили, що хоч межі похибки $\frac{1}{Q_k(Q_k + Q_{k+1})}$ і $\frac{1}{Q_k^2}$ гірші, ніж $\frac{1}{Q_k Q_{k+1}}$, але вони зручніші.

Приклад 3. З якою точністю визначає четвертий підхідний дріб корінь рівняння:

$$10^x = 5?$$

Очевидно, що x лежить в інтервалі (0; 1). Отже, $x = 0 + \frac{1}{x_1}$.

Маємо:

Легко побачити, що x_1 лежить в інтервалі (1; 2); отже, $x_1 = 1 + \frac{1}{x_2}$. Маємо:

$$5^{1+\frac{1}{x_2}} = 10; \quad 5 \cdot 5^{\frac{1}{x_2}} = 10; \quad 5^{\frac{1}{x_2}} = 2; \quad 2^{x_2} = 5.$$

Очевидно x_2 лежить в інтервалі (2; 3); звідси $x_2 = 2 + \frac{1}{x_3}$.

$$2^{2+\frac{1}{x_3}} = 5; \quad 2^2 \cdot 2^{\frac{1}{x_3}} = 5; \quad 2^{\frac{1}{x_3}} = \frac{5}{4}; \quad \left(\frac{5}{4}\right)^{x_3} = 2.$$

Випробуваннями знаходимо, що x_3 лежить в інтервалі (3; 4), тоді $x_3 = 3 + \frac{1}{x_4}$. Маємо:

$$\left(\frac{5}{4}\right)^{3+\frac{1}{x_4}} = 2; \quad \frac{125}{64}\left(\frac{5}{4}\right)^{\frac{1}{x_4}} = 2; \quad \left(\frac{5}{4}\right)^{\frac{1}{x_4}} = \frac{128}{125}; \quad \left(\frac{128}{125}\right)^{x_4} = \frac{5}{4},$$

або $(1{,}024)^{x_4} = 1{,}25$.

Випробуваннями знаходимо, що x_4 лежить в інтервалі (9; 10); звідси $x_4 = 9 + \frac{1}{x_5}$ і т. д.

Отже, дістанемо:

$$x = \log_{10} 5 = [0; 1, 2, 3, 9, x_5].$$

Далі знаходимо: $\frac{P_4}{Q_4}$:

k	—	0	1	2	3	4
q_k		0	1	2	3	9
P_k	1	0	1	2	7	65
Q_k	0	1	1	3	10	93

Отже, $\frac{P_4}{Q_4} = \frac{65}{93}$ визначає $x = \log_{10} 5$ з точністю $\frac{1}{93(93+10)} = \frac{1}{9579}$.

Так можна обчислювати логарифми за допомогою неперервних дробів; але цей спосіб незручний, бо потребує громіздких обчислень.

Контрольні запитання

1. Які три числа можна взяти для визначення межі похибки зверху, яка утворюється при заміні точного значення неперервного дробу k-им підхідним дробом?
2. Яке з чисел попереднього запитання дає кращу оцінку наближення? Яке найзручніше?
3. Яке число можна взяти для визначення межі похибки знизу, яка утворюється при заміні точного значення неперервного дробу k-им підхідним дробом?
4. Для розв'язання яких задач застосовували неперервні дроби?
5. У чому суть способу Лагранжа наближеного обчислення дійсних коренів алгебраїчного рівняння?

§ 40. Підхідні дроби як найкращі наближення

З попереднього параграфа відомо, що підхідні дроби $\frac{P_k}{Q_k}$ ($k = 0, 1, 2, \ldots$) розкладу дійсного числа α у неперервний дріб можна використати як раціональні наближення до цього числа. Оскільки $\lim\limits_{k\to\infty} \frac{P_k}{Q_k} = \alpha$, то підхідні дроби при зростанні k дають дедалі точніші наближення до числа α, причому точність підвищується внаслідок збільшення знаменника Q_k, а разом з ним і чисельника P_k підхідного дробу (див. теореми 1 і 2, § 39). Більш того, виявляється,

що підхідні дроби є найкращими наближеннями до числа α в тому розумінні, що жоден раціональний дріб $\frac{x}{y}$ із знаменником, який не перевищує Q_k не може відрізнятись від α менш, ніж $\frac{P_k}{Q_k}$. Іншими словами, тут справедлива така теорема:

Теорема про найкраще наближення. *Якщо α — будь-яке дійсне число, $\frac{P_k}{Q_k}$ — k-й підхідний дріб розкладу α у неперервний дріб, $\frac{x}{y}$ — довільний раціональний дріб із знаменником y, меншим від Q_k, то виконується нерівність:*

$$\left|\alpha - \frac{P_k}{Q_k}\right| < \left|\alpha - \frac{x}{y}\right|. \tag{1}$$

Справді, α завжди міститься в інтервалі $\left(\frac{P_{k-1}}{Q_{k-1}}, \frac{P_k}{Q_k}\right)$ (див. теорему 2, § 40), довжина якого дорівнює:

$$\left|\frac{P_{k-1}}{Q_{k-1}} - \frac{P_k}{Q_k}\right| = \frac{1}{Q_{k-1}Q_k}.$$

Нехай для визначеності

$$\frac{P_k}{Q_k} < \alpha < \frac{P_{k-1}}{Q_{k-1}}. \tag{2}$$

Покажемо спочатку, що дріб $\frac{x}{y}$ не може бути в зазначеному інтервалі. Справді, це випливає з очевидної нерівності:

$$\left|\frac{x}{y} - \frac{P_{k-1}}{Q_{k-1}}\right| = \frac{|xQ_{k-1} - yP_{k-1}|}{yQ_{k-1}} > \frac{1}{yQ_{k-1}} > \frac{1}{Q_kQ_{k-1}}, \tag{3}$$

бо $y < Q_k$ за умовою і $\frac{x}{y} \neq \frac{P_{k-1}}{Q_{k-1}}$.

Подивимось тепер, що вийде у випадку співвідношення (2); якщо $\frac{x}{y} > \frac{P_{k-1}}{Q_{k-1}}$, тоді $\frac{P_{k-1}}{Q_{k-1}}$ міститься між α і $\frac{x}{y}$ і тому

$$\left|\alpha - \frac{x}{y}\right| > \left|\frac{x}{y} - \frac{P_{k-1}}{Q_{k-1}}\right| > \frac{1}{Q_{k-1}Q_k};$$

але

$$\left|\alpha - \frac{P_k}{Q_k}\right| < \frac{1}{Q_{k-1}Q_k},$$

бо α міститься всередині інтервалу

$$\left(\frac{P_{k-1}}{Q_{k-1}}, \frac{P}{Q_k}\right).$$

Отже, й поготів

$$\left|\alpha-\frac{P_k}{Q_k}\right|<\left|\alpha-\frac{x}{y}\right|.$$

А коли $\frac{x}{y}<\frac{P_k}{Q_k}$, то відразу ж дістанемо, що

$$\left|\alpha-\frac{P_k}{Q_k}\right|<\left|\alpha-\frac{x}{y}\right|,$$

бо $\frac{P_k}{Q_k}$ міститься між $\frac{x}{y}$ і α.

Аналогічно доводиться нерівність (1) тоді, коли

$$\frac{P_{k-1}}{Q_{k-1}}<\alpha<\frac{P_k}{Q_k}.$$

Контрольні запитання

1. Як розуміти, що k-ий підхідний дріб розкладу дійсного числа α у неперервний дріб є найкращим наближенням до числа α?
2. Сформулювати теорему про найкраще наближення.
3. Чому число α лежить між двома послідовними підхідними дробами розкладу α в неперервний?
4. Довести нерівність (1) для випадку, коли

$$\frac{P_{k-1}}{Q_{k-1}}<\alpha<\frac{P_k}{Q_k}.$$

§ 41. Наближення ірраціонального числа раціональними дробами з заданим обмеженням для знаменника

Використання підхідних дробів як раціональних наближень ірраціонального числа приводить до такої оцінки наближення раціональними дробами із заданим обмеженням для знаменника.

Теорема (Діріхле). *Для всякого дійсного числа α при заданому $\tau\geqslant 1$ можна знайти такий нескоротний дріб $\frac{x}{y}$ із знаменником, що не перевищує τ, який відрізняється від α не більш як на $\frac{1}{y\tau}$, так що:*

$$\left|\frac{x}{y}-\alpha\right|<\frac{1}{y\tau}\leqslant\frac{1}{y^2},$$

або

$$\alpha=\frac{x}{y}+\frac{\theta}{y\tau},$$

де $0<y\leqslant\tau$, $|\theta|<1$ і x, y — *взаємно прості.*

Справді, розкладаючи α у неперервний дріб, виберемо $\frac{P_k}{Q_k}$ так, щоб Q_k було найбільшим із знаменників підхідних дробів, який не перевищує ще τ, тобто $Q_k\leqslant\tau$. Як дріб $\frac{x}{y}$, що задовольняє умови теореми, можна взяти $\frac{P_k}{Q_k}$, тобто припустити $x=P_k$, $y=Q_k$.

Справді, розглянемо два можливі випадки.

1. Q_k не є знаменником останнього підхідного дробу в розкладі числа α (ця умова виконується для будь-якого ірраціонального α, але може бути і для раціонального α), тобто існує Q_{k+1} таке, що $Q_k\leqslant\tau<Q_{k+1}$.

Тоді згідно з теоремою 4, § 8 дістанемо:

$$\left|\frac{x}{y}-\alpha\right|=\left|\frac{P_k}{Q_k}-\alpha\right|\leqslant\frac{1}{Q_kQ_{k+1}}<\frac{1}{Q_k\tau}=\frac{1}{y\tau}\leqslant\frac{1}{y^2},$$

бо $Q_k\leqslant\tau$, $Q_{k+1}>\tau$ за побудовою.

2. Q_k — знаменник останнього підхідного дробу в розкладі числа α, тобто $\alpha=\frac{P_k}{Q_k}$, тоді при $x=P_k$, $y=Q_k$ матимемо

$$\left|\alpha-\frac{P_k}{Q_k}\right|=0<\frac{1}{y\tau}\leqslant\frac{1}{y^2},\ \text{бо}\ y=Q_k\leqslant\tau.$$

Коли $\alpha=\frac{a}{b}$ є раціональне число, наведене міркування допустиме лише при $\tau\leqslant b$. Формально ця теорема справедлива і для $\tau>b$, бо тоді можна припустити, що $x=a$, $y=\beta$, $\theta=0$.

Цю характеристику наближення до дійсного числа α виражають іноді в зручнішій для ряду застосувань формі.

Для всякого α і будь-якого $\tau\geqslant 1$ можна знайти таку пару взаємно простих чисел x і y, з яких останнє не перевищує τ, що

$$|x-\alpha y|<\frac{1}{\tau}.$$

Тут оцінка наближення дробу $\frac{x}{y}$ до числа α дається у формі обмеження різниці $x-\alpha y$, яке не залежить від x і y, числом $\frac{1}{\tau}$ при одночасній вимозі $y<\tau$.

В останньому формулюванні теорему Діріхле можна використати для розв'язування невизначених рівнянь з двома невідомими в цілих числах; за допомогою цієї самої теореми можна також довести, що всяке просте число виду $4n+1$ є сума двох квадратів [1].

Теорема про найкраще наближення і теорема Діріхле мають велике значення. У математиці для наближеного подання ірраціональних чисел і, взагалі, величин найчастіше застосовують десяткові дроби,

[1] Докладніше про це див., наприклад; В. Арнольд. Теория чисел. М., Учпедгиз, 1939, стор. 194 і далі.

проте іноді використовують і прості дроби. В таких випадках саме підхідні дроби є найпростішими і найточнішими наближеннями з знаменником, який не перевищує деякої даної межі.

Приклад. Знайти найкраще раціональне наближення до $\sqrt{7}$ з знаменником, який не перевищує $\tau = 60$.

Розкладемо $\sqrt{7}$ у неперервний дріб:

$$\alpha = \sqrt{7} = 2 + (\sqrt{7} - 2) = 2 + \frac{3}{\sqrt{7}+2} = 2 + \frac{1}{\frac{\sqrt{7}+2}{3}};\ \alpha_1 = \frac{\sqrt{7}+2}{3}.$$

$$\frac{\sqrt{7}+2}{3} = 1 + \frac{\sqrt{7}-1}{3} = 1 + \frac{2}{\sqrt{7}+1} = 1 + \frac{1}{\frac{\sqrt{7}+1}{2}};\ \alpha_2 = \frac{\sqrt{7}+1}{2}.$$

$$\frac{\sqrt{7}+1}{2} = 1 + \frac{\sqrt{7}-1}{2} = 1 + \frac{3}{\sqrt{7}+1} = 1 + \frac{1}{\frac{\sqrt{7}+1}{3}};\ \alpha_3 = \frac{\sqrt{7}+1}{3}.$$

$$\frac{\sqrt{7}+1}{3} = 1 + \frac{\sqrt{7}-2}{3} = 1 + \frac{1}{\sqrt{7}+2};\ \alpha_4 = \sqrt{7}+2.$$

$$\sqrt{7}+2 = 4 + (\sqrt{7}-2) = 4 + \frac{1}{\frac{\sqrt{7}+2}{3}};\ \alpha_5 = \frac{\sqrt{7}+2}{3} = \alpha_1.$$

Отже, дістаємо: $\sqrt{7} = [2;\ (1, 1, 1, 4)]$.

За доведеним, найкращими наближеннями є підхідні дроби. Отже, треба знайти такий підхідний дріб $\frac{P_k}{Q_k}$, щоб $Q_k \leqslant 60$, але вже $Q_{k+1} > 60$.

Маємо:

q_k		2	1	1	1	4	1	1	1	4
P_k	1	2	3	5	8	37	45	82	127	
Q_k	0	1	1	2	3	14	17	31	48	223

Отже, шукане наближення до $\sqrt{7}$ буде $\frac{127}{48}$.

Можна, навіть, згідно з теоремами 1, 2, § 40, оцінити ступінь цього наближення:

$$\frac{1}{48 \cdot 271} < \left|\sqrt{7} - \frac{127}{48}\right| < \frac{1}{48 \cdot 223},$$

або

$$0{,}00007 < \left|\sqrt{7} - \frac{127}{48}\right| < 0{,}0001.$$

Контрольні запитання

1. Сформулюйте теорему Діріхле про наближення ірраціонального числа раціональними дробами з заданим обмеженням для знаменника.
2. Чи справедлива теорема Діріхле для раціонального числа $\alpha = \frac{a}{b}$?
3. Якщо обмежити числом $\tau \geqslant 1$ знаменник раціонального наближення $\frac{x}{y}$ до дійсного числа α, то яка буде похибка при такому наближенні?
4. Наведіть інше формулювання теореми Діріхле, яке іноді зручніше для ряду її застосувань?
5. Яке практичне значення мають теореми про найкраще наближення і теорема Діріхле?

§ 42. Квадратичні ірраціональності і періодичні неперервні дроби. Теорема Лагранжа

Нескінченний неперервний дріб називається *періодичним*, якщо неповні частки періодично повторюються, починаючи з деякого q_k. Якщо це повторення одного й того самого періоду починається з q_0, то дріб називається *чистим періодичним;* а якщо повторення неповних часток починається з деякого q_k $(k \geqslant 1)$, то дріб називається *мішаним періодичним*.

Для скорочення запису найменший період беруть у круглі дужки, як ми вже робили у прикладі 1, § 39 і в прикладі § 41.

Дійсне ірраціональне число ω називається *квадратичною ірраціональністю*, якщо ω є коренем квадратного рівняння з цілими коефіцієнтами[1]. Другий корінь ω' цього рівняння називається *спряженою з ω квадратичною ірраціональністю.*

Наприклад, числа $\sqrt{42}$ і $\sqrt{7}$, які ми розглянули в двох попередніх параграфах, є квадратичними ірраціональностями як корені квадратних рівнянь $x^2 - 42 = 0$ і $x^2 - 7 = 0$ з цілими коефіцієнтами. Взагалі, всяка дійсна квадратична ірраціональність має вигляд: $\frac{A \pm \sqrt{D}}{B}$, де A, B, D — цілі і D — додатне число, яке не є повним квадратом. Це випливає безпосередньо з формули коренів квадратного рівняння і з означення дійсної квадратичної ірраціональності.

Ми вже бачили на прикладах, що $\sqrt{42}$ і $\sqrt{7}$ розкладаються у періодичні неперервні дроби; це не випадково, а саме справедлива така теорема, яка відіграє важливу роль у багатьох питаннях теорії чисел.

Теорема (Лагранжа). *Всяка дійсна квадратична ірраціональність розкладається у періодичний неперервний дріб.*

---

[1] Звичайно, це рівняння буде незвідним у полі раціональних чисел, у противному разі його корені були б раціональні.

Взагалі, цю теорему досить довести для додатної квадратичної ірраціональності ω, бо коли ω — від'ємне, то $\omega = [\omega] + \frac{1}{\omega_1}$, де $\omega_1 > 1$ — додатна квадратична ірраціональність; отже, якщо ω_1 розкладається в періодичний неперервний дріб, то й ω також розкладатиметься в періодичний дріб.

Тому припустимо, що ω є додатна квадратична ірраціональність. Не порушуючи загальності, припустимо, що ω є коренем квадратного рівняння з цілими коефіцієнтами:

$$a_1x^2 - 2b_0x + a_0 = 0, \tag{1}$$

тобто $\omega = \frac{b_0 + \sqrt{b_0^2 - a_0a_1}}{a_1}$, де $b_0^2 - a_0a_1 = D > 0$ — дискримінант цього рівняння, причому D не є повним квадратом.

Розкладатимемо ω у неперервний дріб. Позначаючи $[\omega] = q_0$, дістанемо:

$$\omega = q_0 + \frac{1}{\omega_1}, \text{ де } \omega_1 > 1.$$

Припускаючи тепер у рівнянні (1) $x = q_0 + \frac{1}{x_1}$, дістанемо:

$$a_1\left(q_0 + \frac{1}{x_1}\right)^2 - 2b_0\left(q_0 + \frac{1}{x_1}\right) + a_0 = 0,$$

або

$$a_2x_1^2 - 2b_1x_1 + a_1 = 0, \tag{2}$$

де

$$a_2 = a_1q_0^2 - 2b_0q_0 + a_0 \text{ і } b_1 = b_0 - q_0a_1.$$

Маємо квадратне рівняння (2) з цілими коефіцієнтами, коренем якого є $\omega_1 > 1$.

Позначаючи $[\omega_1] = q_1$, дістаємо:

$$\omega_1 = q_1 + \frac{1}{\omega_2};\ \omega_2 > 1.$$

Припускаючи тепер у рівнянні (2) $x_1 = q_1 + \frac{1}{x_2}$, аналогічно дістанемо рівняння з цілими коефіцієнтами, коренем якого є ω_2:

$$a_3x_2^2 - 2b_2x_2 + a_2 = 0,$$

де $a_3 = a_2q_1^2 - 2b_1q_1 + a_1$, $b_2 = b_1 - q_1a_2$ і т. д.

Отже, повна частка $\omega_i > 1$ задовольнятиме таке рівняння з цілими коефіцієнтами:

$$a_{i+1}x_i^2 - 2b_ix_i + a_i = 0, \tag{3}$$

де

$$a_{i+1} = a_iq_{i-1}^2 - 2b_{i-1}q_{i-1} + a_{i-1}, \tag{4}$$

$$b_i = b_{i-1} - q_{i-1}a_i. \tag{5}$$

Зауважимо, що всі рівняння типу (3) при будь-якому i мають один і той самий дискримінант D. Справді, маємо:

$$b_i^2 - a_ia_{i+1} = (b_{i-1} - q_{i-1}a_i)^2 - a_i(a_iq_{i-1}^2 - 2b_{i-1}q_{i-1} + a_{i-1}) =$$

$$= b_{i-1}^2 - a_{i-1}a_i.$$

тобто дискримінант i-го рівняння дорівнює дискримінанту $(i-1)$-го рівняння і, отже, при будь-якому i:

$$b_i^2 - a_ia_{i+1} = b_0^2 - a_0a_1 = D > 0.$$

Доведемо тепер, що знаки чисел $a_1, a_2, a_3, \ldots$, починаючи з довільного a_k, не можуть бути одні й ті самі. Зауважимо відразу, що $a_i \neq 0$, бо інакше рівняння (3) мало б раціональні корені і ω розкладалося б у скінченний неперервний дріб, що суперечило б теоремі 1, § 38.

Справді, припустимо, що, починаючи з a_k, числа $a_k, a_{k+1}, \ldots$ додатні, тоді внаслідок рівності (5) дістанемо: $a_iq_{i-1} = b_{i-1} - b_i$ і, отже, починаючи з $i = k$, $b_{i-1} > b_i$. Значить, числа b_i, які є цілі, необмежено зменшуються і, починаючи з деякого j, $b_j < 0$ $(i \geqslant j)$. Через те, що $j \geqslant k$, то $a_i > 0$ при $i \geqslant j$ (за умовою).

Отже, починаючи з номера j, ліва частина рівняння (3) при $x_j = \omega_j > 0$ буде строго додатною, бо $a_{i+1} > 0$, $-2b_i > 0$, $a_i > 0$, а це суперечить тому, що $\omega_j > 0$ є коренем цього рівняння.

Аналогічно доводиться, що числа a_i, починаючи з деякого a_k, не можуть бути всі від'ємні. Отже, знак чисел a_i, повинен при необмеженому збільшенні i змінюватись нескінченне число разів. Таким чином, є безліч пар чисел $a_m, a_{m+1}; a_n, a_{n+1}; \ldots$, які мають протилежні знаки. Для таких чисел обидва доданки алгебраїчної суми $b_i^2 - a_ia_{i+1} = D > 0$ будуть додатними числами, тому $b_i^2 < D$ і $|a_ia_{i+1}| < D$. Отже, числа

$$a_m, a_{m+1}, a_n, a_{n+1}, \ldots, b_m, b_n, \ldots$$

обмежені, а тому трійки чисел

$$b_m, a_m, a_{m+1}; b_n, a_n, a_{n+1}; \ldots$$

не можуть бути всі різними.

Так, мають бути однакові трійки:

$$b_s = b_t,\ a_s = a_t,\ a_{s+1} = a_{t+1}.$$

Але тоді рівняння (3), які їм відповідають, збігатимуться, і корені їх відповідно будуть рівними, тобто $\omega_s = \omega_t$. Це означає, що в розкладі ω у неперервний дріб зустрінуться дві однакові повні частки ω_s і ω_t; звідси випливатиме, що $\omega_{s+1} = \omega_{t+1}$; $\omega_{s+2} = \omega_{t+2}, \ldots$. З рівності повних часток випливає рівність відповідних неповних часток:

$$q_s = q_t,\ q_{s+1} = q_{t+1},\ q_{s+2} = q_{t+2}, \ldots$$

Отже, квадратична ірраціональність ω розкладатиметься у періодичний неперервний дріб, що й треба було довести.

Справедлива й обернена теорема.

Теорема, обернена до теореми Лагранжа. *Всякий періодичний неперервний дріб є розкладом дійсної квадратичної ірраціональності.*

Справді, нехай дано будь-який періодичний неперервний дріб: його значення позначимо через ω (отже, ω є ірраціональне) і покажемо, що ω є квадратична ірраціональність. Оскільки ω за умовою розкладається в періодичний дріб, то періодично разом з неповними частками повторюватимуться й повні частки; тобто існують такі n і $k\,(k \geqslant 1)$, що $\omega_{n+k} = \omega_n$. Тоді за формулою 3 (теорема 1 § 38) матимемо:

$$\omega = \frac{P_{n-1}\omega_n + P_{n-2}}{Q_{n-1}\omega_n + Q_{n-2}}; \quad \omega = \frac{P_{n+k-1}\omega_{n+k} + P_{n+k-2}}{Q_{n+k-1}\omega_{n+k} + Q_{n+k-2}}.$$

Звідси, наприклад, з першої рівності, знайдемо

$$\omega_n = \omega_{n+k} = \frac{-Q_{n-2}\omega + P_{n-2}}{Q_{n-1}\omega - P_{n-1}} = \frac{-Q_{n+k-2}\omega + P_{n+k-2}}{Q_{n+k-1}\omega - P_{n+k-1}}. \qquad (6)$$

Рівність (6) після зведення до спільного знаменника дає рівняння з цілими коефіцієнтами виду:

$$A\omega^2 + B\omega + C = 0, \qquad (7)$$

де $A = Q_{n-1}Q_{n+k-2} - Q_{n-2}Q_{n+k-1}$.

Щоб довести, що ω є квадратичною ірраціональністю, залишається показати, що рівняння (7) квадратне, тобто його старший коефіцієнт $A \neq 0$. Зокрема, при $n=1$ $A = Q_0Q_{k-1} - Q_{-1}Q_{k-2} = Q_{k-1} \neq 0$, оскільки $Q_0 = 1$, $Q_{-1} = 0$ $\left(\text{під } \frac{P_{-1}}{Q_{-1}} \text{ розуміють неіснуючий дріб } \frac{1}{0}!\right)$.

Доведемо від супротивного, що $A \neq 0$ при $n \geqslant 2$. На підставі співвідношення (2), § 8 випливає, що в послідовності

$$Q_{-1} = 0,\ Q_0 = 1 \leqslant Q_1 < Q_2 < \ldots. \qquad (8)$$

Будь-які два сусідні знаменники взаємно прості. Коли припустити, що $A = 0$ при $n \geqslant 2$, то $\frac{Q_{n-2}}{Q_{n-1}} = \frac{Q_{n+k-2}}{Q_{n+k-1}}$.

З рівності цих двох нескоротних дробів випливає, що

$$Q_{n+k-2} = Q_{n-2},\quad Q_{n+k-1} = Q_{n-1},$$

а це суперечить тому, що в послідовності (8) є найбільше два однакові знаменники.

Приклад 1. Розкласти в неперервний дріб $\omega = \frac{7-\sqrt{3}}{3}$ і обчислити з точністю до 0,00001.

Застосовуючи послідовно процес виділення цілої частини, матимемо:

$$\omega = \frac{7-\sqrt{3}}{3} = 1 + \frac{4-\sqrt{3}}{3} = 1 + \frac{13}{3(4+\sqrt{3})} = 1 + \frac{1}{\frac{12+3\sqrt{3}}{13}};$$

$$\omega_1 = \frac{12+3\sqrt{3}}{13}.$$

$$\frac{12+3\sqrt{3}}{13} = 1 + \frac{3\sqrt{3}-1}{13} = 1 + \frac{26}{13(3\sqrt{3}+1)} = 1 + \frac{1}{\frac{1+3\sqrt{3}}{2}};$$

$$\omega_2 = \frac{1+3\sqrt{3}}{2}.$$

$$\frac{1+3\sqrt{3}}{2} = 3 + \frac{3\sqrt{3}-5}{2} = 3 + \frac{2}{2(3\sqrt{3}+5)} = 3 + \frac{1}{3\sqrt{3}+5};$$

$$\omega_3 = 3\sqrt{3} + 5.$$

$$5 + 3\sqrt{3} = 10 + (3\sqrt{3} - 5) = 10 + \frac{2}{3\sqrt{3}+5} = 10 + \frac{1}{\frac{3\sqrt{3}+5}{2}};$$

$$\omega_4 = \frac{5+3\sqrt{3}}{2}.$$

$$\frac{3\sqrt{3}+5}{2} = 5 + \frac{3\sqrt{3}-5}{2} = 5 + \frac{2}{2(3\sqrt{3}+5)} = 5 + \frac{1}{3\sqrt{3}+5};$$

$$\omega_5 = 3\sqrt{3} + 5 = \omega_3.$$

Отже, дістали такий розклад квадратичної ірраціональності ω у неперервний дріб:

$$\omega = \frac{7-\sqrt{3}}{3} = [1;\ 1,3,\ (10,5)].$$

Далі маємо:

		1	1	3	10	5	10
1	1	2	7	72	367		
0	1	1	4	41	209	2131	

На підставі значення верхньої межі похибки $\frac{1}{Q_kQ_{k+1}}$ робимо висновок, що

$$\frac{7-\sqrt{3}}{3} \approx \frac{367}{209} \text{ (з точністю до 0,00001).}$$

Приклад 2. Розв'яжемо тепер обернену задачу. Знайдемо квадратичну ірраціональність $x = [1;\ 1{,}3\ (10{,}5)]$.

Позначимо $[(10{,}5)]$ через y, тоді

$$x = [1;\ 1{,}3,\ y] = \frac{P_2 y + P_1}{Q_2 y + Q_1} = \frac{7y + 2}{4y + 1};$$

$$y = 10 + \frac{1}{5 + \frac{1}{y}} = 10 + \frac{y}{5y + 1} = \frac{51y + 10}{5y + 1},$$

звідки

$$5y^2 - 50y - 10 = 0;\quad y^2 - 10y - 2 = 0;\quad y = 5 + \sqrt{27},$$

де квадратний корінь беремо із знаком плюс, бо y — додатна квадратична ірраціональність.

Підставляючи тепер знайдене значення y у вираз для x, знайдемо:

$$x = \frac{7(5 + \sqrt{27}) + 2}{4(5 + \sqrt{27}) + 1} = \frac{37 + 21\sqrt{3}}{21 + 12\sqrt{3}} = \frac{21 - 3\sqrt{3}}{9} = \frac{7 - \sqrt{3}}{3}.$$

Отже, шукана квадратична ірраціональність буде:

$$x = \frac{7 - \sqrt{3}}{3}.$$

Приклад 3. Неперервний дріб $x = [1;\ 1{,}1,\ \ldots]$ заданий послідовністю неповних часток 1, 1, 1, ... Щоб знайти його значення, можна відразу записати, що

$$x = [1,\ x],\ \text{або}\ x = 1 + \frac{1}{x},$$

звідки

$$x^2 - x - 1 = 0\ \text{і}\ x = \frac{1 + \sqrt{5}}{2}.$$

Чисельники і знаменники підхідних дробів у розкладі числа $x = \frac{1 + \sqrt{5}}{2}$ будуть, очевидно, суміжними числами ряду

$$1,\ 1,\ 2,\ 3,\ 5,\ 8,\ 13,\ 21,\ 34,\ 55,\ \ldots,$$

де *кожний член дорівнює сумі двох попередніх. Цей ряд називається рядом Фібоначчі.*

З елементарної геометрії відомо, що при «поділі відрізка в крайньому і середньому відношенні» (так званий «золотий переріз») відношення більшої частини до меншої саме й дорівнює $\frac{1 + \sqrt{5}}{2}$. Тому відношення двох послідовних чисел ряду Фібоначчі можна використати для наближеного здійснення «золотого перерізу».

Контрольні запитання

1. Який нескінченний неперервний дріб називають періодичним? Чистим періодичним? Мішаним періодичним?
2. Яке ірраціональне число називають квадратичною ірраціональністю? Дати означення спряженої квадратичної ірраціональності.
3. У який неперервний дріб розкладається дійсна квадратична ірраціональність?
4. Чи розкладається ірраціональне число, яке не є квадратичною ірраціональністю, в періодичний неперервний дріб? Чому?
5. Сформулюйте теорему, обернену теоремі Лагранжа.

Вправи

1. Знайти другий підхідний дріб у розкладі $\sqrt[3]{2}$.

Відповідь. $\frac{5}{4}$.

2. Знайти третій підхідний дріб у розкладі кореня рівняння

$$x^3 - x^2 - 2x + 1 = 0,$$

що міститься в інтегралі (0; 1).

Відповідь. $\frac{81}{182}$.

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

Відповідь. $\frac{65}{28}$.

4. Розкласти в нескінченний неперервний дріб: а) $\sqrt{5}$; б) $\sqrt{6}$; в) $\sqrt{8}$; г) $\sqrt{10}$; д) $\sqrt{11}$.

Відповідь. а) $[2; (4)]$; б) $[2; (2,4)]$; в) $[2; (1,4)]$; г) $[3; (6)]$; д) $[3; (3,6)]$.

5. За допомогою неперервних дробів обчислити обидва корені рівняння $x^2 + 9x + 6 = 0$ з точністю до 0,0001.

Відповідь. $x_1 \approx -\frac{29}{40}$; $x_2 \approx -\frac{331}{40}$.

6. За допомогою неперервних дробів обчислити з точністю до 0,0001 корінь рівняння $x^3 - x^2 - 2x + 1 = 0$, що міститься в інтервалі $(-2; -1)$.

Відповідь. $x \approx -\frac{101}{81}$.

7. Беручи значення $\pi \approx 3{,}1416$ з точністю до четвертого знака після коми, з'ясувати, чи є дріб $\frac{22}{7}$ підхідним дробом розкладу π у неперервний дріб.

Відповідь. Так.

8. За допомогою неперервних дробів обчислити $\lg 500$ з точністю до 0,0001.

Відповідь. $\lg 500 \approx \frac{251}{93}$.

9. Розкласти у нескінченний неперервний дріб і обчислити з точністю до 0,0001: а) $\sqrt{13}$; б) $\sqrt{14}$; в) $\sqrt{30}$; г) $\sqrt{59}$.

Відповідь. а) $[3; (1, 1, 1, 1, 6)] \approx \frac{393}{109}$; б) $[3; (1, 2, 1, 6)] \approx \frac{333}{89}$; в) $[5; (2, 10)] \approx \frac{241}{44}$; г) $[7; (1, 2, 7, 2, 1, 14)] \approx \frac{530}{69}$.

10. Розкласти у нескінченний неперервний дріб і обчислити з точністю до 0,0001: а) $\frac{3 + \sqrt{7}}{2}$; б) $\frac{1 + \sqrt{11}}{4}$; в) $\frac{7 - \sqrt{5}}{3}$; г) $\frac{76 + \sqrt{285}}{94}$.

Відповідь. а) $[2; (1, 4, 1, 1)] \approx \frac{271}{96}$; б) $[(1; 12, 1, 1, 1, 2, 1, 1)] \approx \frac{109}{101}$; в) $[1; 1, 1, (2, 2, 1, 12, 1, 2)] \approx \frac{343}{216}$; г) $[2; 1, 4, (5, 3)] \approx \frac{217}{83}$.

11. Знайти квадратичну ірраціональність x, якщо: а) $x = [6; (1, 5, 1, 12)]$; б) $x = [4; (1, 1, 5)]$; в) $x = [4; 3, (2, 1, 3, 1)]$; г) $x = [3; 2, 1, (3, 1)]$.

Відповідь. а) $\sqrt{47}$; б) $\frac{3+\sqrt{37}}{2}$; в) $\frac{25-\sqrt{61}}{4}$; г) $\frac{29+\sqrt{21}}{10}$

12. У яких рівняннях корені розкладаються у такі неперервні періодичні дроби: а) $[(2; 4, 1, 3)]$; б) $[2; 1, 2, (1, 1, 3)]$; в) $[9; (1, 1, 2, 4, 2, 1, 1, 18)]$; г) $[10; (10, 20)]$.

Відповідь. а) $19x^2 - 37x - 11 = 0$; б) $2x^2 - 15x + 26 = 0$; в) $x^2 - 92 = 0$; г) $x^2 - 102 = 0$.

13. Знайти квадратичну ірраціональність x, якщо: а) $x = [q; (2q)]$; б) $x = [q; (q; 2q)]$.

Відповідь. а) $x = \sqrt{q^2+1}$; б) $x = \sqrt{q^2+2}$.

14. Розкласти у неперервний періодичний дріб: а) $\sqrt{q^4+2q}$; б) $\sqrt{(q+1)^2-2}$ (q — натуральне число).

Відповідь. а) $[q^2; (q, 2q^2)]$; б) $[q; (1, q-1, 1, 2q)]$.

15. Знайти найкраще наближення до $\sqrt{29}$ з знаменником, що не перевищує 140, й оцінити похибку.

Відповідь. $\frac{P_5}{Q_5} = \frac{727}{135}$ і похибка $< \frac{1}{135 \cdot 283} < \frac{1}{135^2}$.

16. Знайти краще наближення до $\lg 11$ з знаменником, що не перевищує 400 і оцінити похибку.

Відповідь. $\frac{P_3}{Q_3} = \frac{327}{314}$ і похибка $< \frac{1}{314^2}$.

17. Довести: якщо $k > 1$, то принаймні одна з двох нерівностей $\left|\alpha - \frac{P_k}{Q_k}\right| < \frac{1}{2Q^2_k}$, $\left|\alpha - \frac{P_{k-1}}{Q_{k-1}}\right| < \frac{1}{2Q^2_{k-1}}$ виконується для заданого дійсного додатного α.

18. Довести, що коли α — дійсне додатне число і p, q — натуральні взаємно прості числа, такі, що $\alpha \neq \frac{p}{q}$ і $\left|\alpha - \frac{p}{q}\right| < \frac{1}{2q^2}$, то $\frac{p}{q}$ є підхідним дробом розкладу α у неперервний дріб.

19. Два ірраціональні числа ω і ω', зв'язані співвідношенням

$$\omega = \frac{a\omega' - b}{c\omega' + d},$$

де a, b, c, d — цілі і $ad - bc = \pm 1$, називають *еквівалентними*. Довести:

а) коли $\omega' > 1$ і $c \geqslant d > 0$, то $\frac{b}{d}$ і $\frac{a}{c}$ *є двома послідовними підхідними дробами до* ω, *а* ω' *є відповідна повна частка;*

б) *для того щоб у двох нескінченних неперервних дробів послідовності неповних часток, починаючи з деяких місць, збігались, необхідно і достатньо, щоб ці дроби визначали еквівалентні числа (теорема* Серре).

20. Довести, що коли ω є корінь рівняння

$$a\omega^2 + 2b\omega + c = 0 \quad (D = b^2 - ac > 0)$$

з цілими коефіцієнтами, то всяка еквівалентна їй ірраціональність ω' задовольнятиме такого самого типу рівняння з цілими коефіцієнтами і тим самим дискримінантом D.

21. Довести, що для всякого ірраціонального x еквівалентними завжди будуть $-x$ і $\frac{1}{x}$.

ІСТОРИЧНІ КОМЕНТАРІ

1. Є припущення, що ще Архімед застосовував неперервні дроби до добування квадратного кореня з 3.

У римлян зустрічалися дроби, в яких чисельник не ціле число, а дробове, наприклад, $\frac{1\frac{1}{2}}{12}$ унції, тобто всього $\frac{3}{24}$. Ці дроби грунтуються на тому, що чисельник може бути не тільки цілим числом, а й мішаним, тобто римлянам ідея неперервних дробів була зрозуміла і доступна.

Процес розкладання деяких дійсних чисел окремого виду (квадратних коренів з даних чисел) вперше зустрічається в італійського математика Бомбеллі (1530 — ?) в його «Алгебрі» (1572), але не в сучасних позначеннях. Сучасні позначення вперше зустрічаються в 1613 р. в італійського математика Катальді (1548—1616), тільки він замість знака «+» писав «et».

Англійський математик Броункер (1620—1684) перший звернув увагу на застосування неперервних дробів. Він подав у вигляді неперервного дробу валісове число $\frac{4}{\pi} = 1 + \frac{1}{2} + \frac{9}{2} + \frac{25}{2} + \cdots$, однак невідомо, як він це зробив. Броункер і Валліс (1616—1703) знайшли (щоправда громіздкий) розв'язок рівняння $ax^2 + 1 = y^2$ у цілих числах, пізніше приписаний Ейлером Пеллю. У Валліса вперше з'явився і сам термін «неперервний дріб». Він обчислив 35 перших елементів розкладу π у неперервний дріб. Загальний вигляд елементів розкладу π у неперервний дріб невідомий.

Голландський механік, фізик і математик Христіан Гюйгенс (1629—1695) широко застосував неперервні дроби.

Саме при будуванні планетарія (моделі сонячної системи) Гюйгенсу треба було, щоб відношення обертів зчеплених між собою зубчастих коліс виражались дробами заданими і притому великими чисельниками і знаменниками. Через те що точне здійснення цієї умови потребувало б нездійсненного в конструкції великого числа зубців, то виникла проблема про заміну таких незручних відношень якомога точнішими відношеннями менших чисел. Ця задача саме і розв'язується за допомогою розкладу у неперервний дріб і утворення підхідних дробів і дуже зв'язаних з ними так званих проміжних дробів типу:

$$\frac{P_{k-2} + lP_{k-1}}{Q_{k-2} + lQ_{k-1}} \quad (k = 1, 2, \ldots, q_{k-1}).$$

Теорію неперервних дробів систематизували Ейлер, а потім Лагранж. Зокрема останньому належить спосіб наближеного обчислення коренів алгебраїчних рівнянь за допомогою неперервних дробів (див. приклад 3, § 39).

2. Вкажемо, ще на деякі застосування неперервних дробів.

Про один з таких прикладів, а саме про з'єднання двох валів зубчастими колесами, ми згадували. Ця задача, взагалі, розв'язується наближено. Справді, якщо позначити через α відношення кутових швидкостей таких валів, то кутові швидкості коліс будуть обернено пропорційні числам зубців; отже, обернене відношення чисел зубців дорівнює α. Але числа зубців — цілі і не дуже великі, тоді як α може бути й ірраціональним. Отже, щоб розв'язати задану задачу, треба взяти для α наближене значення у формі простого дробу і з не дуже великим знаменником.

Календарний стиль[1]. З астрономії відомо, що рік має 365,24220... так званих «середніх» діб. Звичайно, таке складне відношення року до доби в практичному житті дуже незручне; треба замінити його простішим, хоч і менш точним. Розклавши 365,24220... у неперервний дріб, дістанемо:

$$365{,}24220\ldots = [365; 4, 7, 1, 3, \ldots].$$

[1] Див. А. К. Сушкевич Теория чисел, Харьков, 1954, стор. 44—45.

Перші підхідні дроби тут будуть:

$$365;\ 365\frac{1}{4};\ 365\frac{7}{29};\ 365\frac{8}{33}.$$

Наближення до $365\frac{1}{4}$ знали ще стародавні народи (єгиптяни, ассіровавілоняни, китайці), хоч вони й не мали регулярних високосних років. 7 березня 238 р. до нашої ери вийшов Канопський декрет Птолемея Евергета, в якому вказувалось, що кожний четвертий рік має не 365, а 366 діб. Але через 40 років цей декрет забули і тільки в 47 р. до н. е. Юлій Цезар за участю Сосігена відновив його і встановив у кожний четвертий рік зайвий день у лютому. Цей день назвали bissextilis, звідки походить і назва «високосний» рік. Це так званий *старий*, або *юліанський*, стиль.

Новий, або *григоріанський*, *стиль* дає наближення $365\frac{97}{400}$; воно трохи точніше, ніж $365\frac{7}{29}$ і $365\frac{8}{33}$. Цей стиль відрізняється від юліанського тим, що в ньому кожний сотий рік — не високосний, крім тих, число сотень яких ділиться без остачі на 4. Так, 1700, 1800, 1900 — не високосні, тоді як 1600, 2000 роки — високосні, тобто 400 років мають 97 зайвих днів, а не 100, як в юліанському стилі.

Вже у XV ст. було помічено відставання юліанського стилю (тоді на 10 діб), внаслідок чого були пропозиції зробити реформу календаря. Але цю реформу було проведено тільки в кінці XVI ст. У католицьких країнах її було здійснено буллою папи Григорія XIII від 1 березня 1582 р. Десять діб — з 5 по 14 жовтня — було викреслено, тобто 5 жовтня наказано було вважати за 15 жовтня 1582 р.

Найбільш точний календар запровадив у Персії у 1079 р. знаменитий поет, астроном, математик і філософ Омар Хайям[1]. Він запровадив цикл з 33 років, в якому 7 раз високосний рік вважався четвертим, а 8-й раз високосний був не четвертий, а п'ятий рік. Отже, тут є вісім зайвих діб за 33 роки, тобто для кожного року маємо $365\frac{8}{33}$ доби; це є саме третій підхідний дріб.

3. Теорему про те, що всяка додатна квадратична ірраціональність розкладається в неперервний періодичний дріб довів Лагранж. Йому належать істотні дослідження в теорії неперервних дробів і застосування їх до розв'язання в цілих числах невизначених рівнянь 2-го степеня. Лагранж вивчав загальні питання квадратичних форм, зокрема дав перше доведення теореми про подання чисел у вигляді суми чотирьох квадратів, яку висловив ще Баше де Мезаріак, поклав початок вивченню відносних мінімумів форм і дав багато доведень раніше знайдених закономірностей.

Розкладом квадратичних ірраціональностей у періодичні неперервні дроби займався також геніальний французький математик-алгебраїст Еваріст Галуа (1811—1832), зокрема, він довів таку теорему:

Квадратична ірраціональність $\alpha = \frac{A+\sqrt{D}}{B}$, де A, B і $D>1$ — *цілі (і D не є повним квадратом), розкладається в чисто періодичний неперервний дріб тоді і тільки тоді, коли* $\alpha>1$ *і спряжена ірраціональність* $\alpha' = \frac{A-\sqrt{D}}{B}$ *лежить в інтервалі* $(-1;\ 0)$.

Галуа довів так само, що при суто періодичному розкладі квадратичної ірраціональності α спряжена їй ірраціональність α' має ті самі елементи, але розміщені вони в зворотному порядку.

[1] Омар Хайям за національністю таджик.

4. Зауважимо, що квадратична ірраціональність є окремий випадок ірраціональності n-го степеня ($n \geqslant 2$). Під ірраціональністю n-го степеня звичайно розуміють дійсний корінь алгебраїчного рівняння n-го степеня з цілими коефіцієнтами, незвідного в полі раціональних чисел. Внаслідок теореми Лагранжа і оберненої до неї теореми тільки дійсні квадратичні ірраціональності розкладаються у періодичний неперервний дріб. Для ірраціональностей вищих степенів такий розклад уже неможливий. Це спонукало багатьох видатних математиків XIX ст. шукати таке узагальнення алгоритму неперервних дробів, яке б забезпечило періодичний розклад кубічних ірраціональностей. Таке узагальнення зробив видатний український математик Г. Ф. Вороний; воно було опубліковане в 1896 р. у праці «Про одне узагальнення алгоритму неперервних дробів».

5. Багато математиків цікавилось питанням про те, чи в ряді Фібоначчі безліч простих чисел, чи ні. Це питання й досі не розв'язане.

6. Твердження задачі № 19 називається теоремою Серре за ім'ям французького математика Жозефа Серре (1819—1885), який працював у різних галузях математики і механіки. Великою популярністю користувались його курси вищої алгебри і диференціального й інтегрального числень, які неодноразово перевидавались і були перекладені на інші мови.

Розділ VIII

АЛГЕБРАЇЧНІ І ТРАНСЦЕНДЕНТНІ ЧИСЛА

§ 43. Ірраціональні числа

Поняття раціональності й ірраціональності дуже істотно характеризують будову дійсного числа. Так, наприклад, раціональні числа і тільки вони розкладаються в періодичні десяткові дроби (скінченні десяткові дроби розглядаються при цьому як періодичні десяткові дроби з періодом 0) і в скінченні неперервні дроби. Ірраціональні числа і тільки вони розкладаються в нескінченні неперіодичні десяткові дроби і в нескінченні неперервні дроби.

Зазначені факти можуть, очевидно, бути критеріями для визначення раціональності чи ірраціональності заданого дійсного числа, але не завжди ці критерії можна безпосередньо застосувати.

Наведемо деякі інші критерії раціональності й ірраціональності заданих дійсних чисел. При цьому зауважимо, що доведення ірраціональності будь-якого дійсного числа α можна звести до доведення того, що нема цілих чисел a і b, таких, що $b\alpha = a$.

У § 4 на підставі теореми 4 ми встановили, що корінь n-го степеня з натурального числа не може дорівнювати нескоротному дробу. Можна довести загальніше твердження.

Теорема 1. *Якщо N і k — натуральні числа, причому N не є k-тим степенем цілого числа, то $\sqrt[k]{N}$ — число ірраціональне.*

Припустимо супротивне, тобто, що $\sqrt[k]{N} = \frac{a}{b}$ — число раціональне, $(a, b) = 1$ і $b > 1$ (інакше N було б k-тим степенем цілого

числа a). Тоді $a^k = b^k N$, звідки $a^k : b$ і $a^k : p$, де p — простий дільник числа b. Але в такому разі a також має ділитися на p і тоді $(a, b) = p > 1$, що суперечить умові $(a, b) = 1$. Отже теорема доведена.

Ця теорема еквівалентна твердженню, що рівняння $x^k = y^k \cdot N$ нерозв'язне в цілих взаємно простих числах.

Теорема 2. *Якщо α — дійсний корінь рівняння*

$$f(x) = x^n + c_1 x^{n-1} + \cdots + c_n = 0 \qquad (1)$$

з цілими коефіцієнтами і з старшим коефіцієнтом, що дорівнює одиниці, то α будь-яке ціле або ірраціональне число.

При доведенні обмежимось випадком, коли $c_n \neq 0$. Припустимо супротивне: α не є ірраціональним числом, а раціональним дробом, тобто $\alpha = \frac{a}{b}$, $(a, b) = 1$ і $b > 1$; підставляючи в многочлен (1), дістанемо:

$$a^n + c_1 a^{n-1} b + \cdots + c_n b^n = 0 \text{ або } a^n = -b(c_1 a^{n-1} + \cdots + c_n b^{n-1}).$$

З останньої рівності випливає, що $a^n : b$, тобто ми прийшли до суперечності.

Теорема 2 твердить, що дійсне число α, неявно визначене рівнянням (1), не будучи цілим числом є число ірраціональне, при цьому з алгебри відомо, що цілі розв'язки рівняння (1) слід шукати серед дільників вільного члена c_n.

Для деяких дійсних чисел питання про раціональність чи ірраціональність з'ясовуємо за допомогою таких двох теорем.

Теорема 3. *Для всякого раціонального числа α існує таке додатне число c, що нерівність*

$$\left|\alpha - \frac{a}{b}\right| \geqslant \frac{c}{b} \qquad (2)$$

виконується для будь-якого раціонального дробу $\frac{a}{b} \neq \alpha$.

Справді, нехай $\alpha = \frac{p}{q} \neq \frac{a}{b}$ (так що $pb - aq \neq 0$) і $q \geqslant 1$. Тоді

$$\left|\alpha - \frac{a}{b}\right| = \left|\frac{p}{q} - \frac{a}{b}\right| = \frac{|pb - aq|}{bq} \geqslant \frac{1}{bq} = \frac{\frac{1}{q}}{b} = \frac{c}{b},$$

де $c = \frac{1}{q} > 0$, і нерівність (2) доведена.

У теоремі 3 міститься необхідна ознака раціонального числа. Число, яке не задовольняє цю ознаку має бути ірраціональним, і ми приходимо до такої теореми.

Теорема 4. *Якщо для будь-якого додатного c можна знайти хоча б одну пару цілих чисел a і b таких, що*

$$\left|\alpha - \frac{a}{b}\right| < \frac{c}{b}, \qquad (3)$$

то α ірраціональне.

Справді, якщо α було б раціональним, то існувало б таке $c > 0$, що для зазначеного дробу $\frac{a}{b}$ виконувалася б нерівність (2), і тоді для цього c не могла б виконуватись нерівність (3). Отже, α — ірраціональне число і теорему доведено.

Приклад. Довести ірраціональність числа α:

$$\alpha = 1 - \frac{1}{2^1} + \frac{1}{2^4} - \frac{1}{2^9} + \cdots + \frac{(-1)^n}{2^{n^2}} + \cdots$$

Візьмемо довільне $c > 0$ і n таке велике, що $2^{2n+1} > \frac{1}{c}$. Покладемо

$$b = 2^{n^2}, \quad a = 2^{n^2}\left[1 - \frac{1}{2^1} + \frac{1}{2^4} + \cdots + \frac{(-1)^n}{2^{n^2}}\right].$$

Тут a і b — цілі числа. При таких a і b

$$\left|\alpha - \frac{a}{b}\right| = \left|\frac{1}{2^{(n+1)^2}} - \frac{1}{2^{(n+2)^2}} + \cdots\right| < \frac{1}{2^{(n+1)^2}} = \frac{1}{b 2^{2n+1}} < \frac{c}{b},$$

тобто за теоремою 4 α — ірраціональне число.

Теорему 4 можна застосувати і для доведення *ірраціональності числа e*. Але ще простіше скористатися таким міркуванням.

Припустимо супротивне, тобто припустимо, що e — раціональне число, а саме $e = \frac{a}{b}$, де a і b цілі, і розглянемо при $k \geqslant b$ вираз

$$c = k!\left(e - 1 - \frac{1}{1!} - \frac{1}{2!} - \cdots - \frac{1}{k!}\right).$$

Оскільки при $k \geqslant b$ добуток $k!$ ділиться на b, то c повинно бути цілим числом (оскільки $k!\,e$ — ціле, а інші доданки в дужках при множенні на $k!$ також дають цілі числа). Але, з другого боку, оскільки $e = 1 + \frac{1}{1!} + \frac{1}{2!} + \cdots + \frac{1}{k!} + \cdots$, то

$$0 < c = \frac{1}{k+1} + \frac{1}{(k+1)(k+2)} + \cdots < \frac{1}{(k+1)} + \frac{1}{(k+1)^2} + \cdots = \frac{1}{k},$$

тобто c — дробове число. Знайдена суперечність і доводить ірраціональність числа e.

Ірраціональність числа π довести значно складніше. Наведемо одне з доведень *ірраціональності числа π*.

Припустимо супротивне, тобто, що π раціональне і $\pi = \frac{a}{b}$, де a і b — цілі. Розглянемо многочлени

$$f(x) = \frac{b^n x^n (\pi - x)^n}{n!} = \frac{x^n (a - bx)^n}{n!} \tag{4}$$

$$F(x) = f(x) - f^{II}(x) + f^{IV}(x) - \cdots + (-1)^n f^{(2n)}(x). \tag{5}$$

Оскільки x входить у чисельник многочлена $f(x)$ з показниками від n до $2n$, то $f(x)$ можна записати в такому вигляді:

$$f(x) = \frac{1}{n!} \sum_{l=n}^{2n} a_{l-n} x^l,$$

звідки видно, що

$$f(0) = f'(0) = \cdots = f^{(n-1)}(0) = 0$$

і що в похідній $f^{(k)}(x)$, $n \leqslant k \leqslant 2n$ при $x = 0$ зберігається лише доданок, утворений членом многочлена $f(x)$, який містить x^k. Тому

$$f^k(0) = \frac{k!}{n!} a_{k-n}.$$

Отже, для $0 \leqslant l \leqslant 2n$, $f^l(0)$ — ціле число, оскільки, очевидно, що a_{l-n} — числа цілі. Але з рівності (4) дістанемо:

$$f(\pi - x) = f\left(\frac{a}{b} - x\right) = \frac{\left(\frac{a}{b} - x\right)^n \left[a - b\left(\frac{a}{b} - x\right)\right]^n}{n!} = f(x).$$

Отже, при будь-якому j, $f^{(j)}(x) = f^{(j)}(\pi - x)$ і $f^{(j)}(\pi) = f^{(j)}(0)$ — також ціле число. Тому $F(0)$ і $F(\pi)$ — цілі числа.

Ураховуючи тепер, що з

$$\frac{d}{dx}(F'(x)\sin x - F(x)\cos x) = F''(x)\sin x + F(x)\sin x = f(x)\sin x$$

випливає

$$I = \int_0^\pi f(x)\sin x\,dx = [F'(x)\sin x - F(x)\cos x]_0^\pi = F(\pi) + F(0),$$

приходимо до висновку: I — число ціле, притому додатне, бо в інтервалі $(0, \pi)$ підінтегральна функція додатна. Але для $0 < x < \pi$ з рівності (4) матимемо: $f(x)\sin x < \frac{\pi^n a^n}{n!}$. Остання нерівність показує, що для досить великих n підінтегральна функція, а разом з тим і сам інтеграл можуть стати як завгодно малими. Ця суперечність і доводить ірраціональність числа π.

Контрольні запитання

1. Чим відрізняються розклади раціональних та ірраціональних чисел у десяткові і неперервні дроби?
2. У якому випадку $\sqrt[k]{N}$, де k і N — натуральні числа, буде числом ірраціональним?
3. У якому випадку дійсний корінь α рівняння $x^n + c_1 x^{n-1} + \cdots + c_n = 0$ з цілими коефіцієнтами буде числом ірраціональним?
4. Сформулюйте необхідну ознаку раціональності числа α.
5. Сформулюйте достатню ознаку ірраціональності числа α.

§ 44. Алгебраїчні числа та їхні основні властивості. Поле алгебраїчних чисел

З вищої алгебри відомо, що будь-яке алгебраїчне рівняння n-го степеня з раціональними коефіцієнтами має в полі комплексних чисел n коренів, з яких кілька, або навіть усі, можуть не належати полю раціональних чисел. Проте не всяке комплексне або дійсне число є коренем деякого алгебраїчного рівняння з раціональними коефіцієнтами.

Комплексне або дійсне число α називається *алгебраїчним числом*, якщо воно є коренем деякого многочлена з раціональними коефіцієнтами. Будь-яке неалгебраїчне число називається *трансцендентним*.

Якщо α — алгебраїчне число, то воно буде коренем навіть деякого алгебраїчного рівняння з цілими коефіцієнтами. Припустимо, що $p(x) = 0$ є рівняння найнижчого степеня серед усіх алгебраїчних рівнянь з цілими коефіцієнтами, що мають α своїм коренем. Неважко побачити, що тоді многочлен $p(x)$, який є лівою частиною цього рівняння, буде незвідним над полем раціональних чисел і визначатиметься однозначно з точністю до сталого множника, відмінного від нуля.

Справді, перше твердження відразу ж випливає з того, що $p(x) = 0$ є рівняння найменшого степеня, коренем якого є число α.

Для доведення однозначності $p(x)$ припустимо, що α є також коренем незвідного над полем раціональних чисел рівняння $q(x) = 0$ з цілими коефіцієнтами. Тоді многочлени $p(x)$ і $q(x)$ ділитимуться на $x - \alpha$. Отже, $p(x)$ і $q(x)$ матимуть найбільший спільний дільник $d(x)$, вищий від нульового степеня, який, як відомо, не залежить від того, чи розглядаємо ми многочлени над даним полем P, чи над будь-яким його розширенням $\overline{P}$. Внаслідок незвідності многочлени $p(x)$ і $q(x)$ збігаються з $d(x)$ з точністю до сталого множника, який не дорівнює нулю, а тому $p(x)$ і $q(x)$ також відрізнятимуться один від одного тільки сталим множником, відмінним від нуля.

Якщо n — степінь незвідного над полем [1] R рівняння $p(x) = 0$

[1] Буквою R позначатимемо поле раціональних чисел.

з цілими коефіцієнтами, то корінь α з цього рівняння називається *алгебраїчним числом степеня* n; усі корені цього рівняння, відмінні від α, називаються *спряженими* з α. Очевидно, що степінь спряжених алгебраїчних чисел один і той самий.

До алгебраїчних чисел належать усі раціональні числа як корені рівнянь першого степеня: $ax = b\,(a \neq 0)$ з цілими (раціональними) коефіцієнтами, а також будь-який радикал виду $\sqrt[n]{a}$, де a є раціональне, як корінь двочленного рівняння: $x^n - a = 0$.

Всяке раціональне число як корінь рівняння першого степеня не має спряжених чисел, відмінних від нього, і ця властивість є для раціональних чисел характерною. Всяке алгебраїчне число, яке не є раціональним, буде коренем незвідного многочлена (рівняння), степінь якого більший від одиниці, і тому для нього існують спряжені числа, відмінні від його самого.

Вкажемо тепер такі основні властивості алгебраїчних чисел.

Властивість 1. *Сума, різниця, добуток і частка алгебраїчних чисел є числа алгебраїчні. Інакше кажучи, сукупність усіх алгебраїчних чисел утворює поле, яке є підполем поля комплексних чисел.*

Справді, нехай дано алгебраїчні числа α і β відповідно степеня $n \geqslant 1$ і $m \geqslant 1$. Позначимо через $\alpha_1 = \alpha, \alpha_2, \ldots, \alpha_n$ усі числа, спряжені з α, через $\beta_1 = \beta, \beta_2, \ldots, \beta_m$ — усі числа, спряжені з β через $f(x)$ і $g(x)$ — незвідні многочлени з раціональними коефіцієнтами, що мають своїми коренями відповідно α і β. Очевидно, що многочлен $f(x) \cdot g(x)$ також має раціональні коефіцієнти і його коренями є

$$\gamma_1 = \alpha_1, \ \ldots, \ \gamma_n = \alpha_n, \ \gamma_{n+1} = \beta_1, \ \ldots, \ \gamma_{n+m} = \beta_m.$$

Складемо тепер многочлен, коренями якого є всі можливі суми $\gamma_i + \gamma_j$, де $i \neq j$ і $i, j = 1, 2, \ldots, m+n$. Це буде, очевидно, многочлен:

$$F(x) = \prod_{i,\,j=1}^{m+n} [x - (\gamma_i + \gamma_j)].$$

Коефіцієнти цього многочлена не змінюватимуться при переставлянні чисел $\gamma_1, \gamma_2, \ldots, \gamma_{n+m}$, отже, вони будуть симетричними многочленами від $\gamma_1, \gamma_2, \ldots, \gamma_{n+m}$. Звідси, внаслідок основної теореми про симетричні многочлени, випливає, що коефіцієнти многочлена $F(x)$ є многочленами від основних симетричних многочленів $\sigma_1 = \gamma_1 + \cdots + \gamma_{n+m}, \ \ldots, \ \sigma_{n+m} = \gamma_1\gamma_2 \cdots \gamma_{n+m}$ над тим самим полем раціональних чисел, які з точністю до знака є коефіцієнтами многочлена $f(x) \cdot g(x)$. Отже, коефіцієнти многочлена $F(x)$ будуть раціональними числами, і тому число $\alpha + \beta = \gamma_1 + \gamma_{n+1}$, яке є одним з його коренів, буде алгебраїчним.

Так само за допомогою многочлена

$$G(x) = \prod_{i,\,j=1}^{n+m} (x - \gamma_i\gamma_j) \ (i \neq j)$$

доводиться алгебраїчність числа $\alpha\beta$.

Далі легко переконатись, що разом з β буде алгебраїчним числом і $-\beta$. Для цього, припускаючи, що у многочлені $g(x)$ $x = -y$, дістанемо, очевидно, многочлен з раціональними коефіцієнтами, коренем якого буде $-\beta$, тобто $-\beta$ буде алгебраїчним числом, а тому $\alpha + (-\beta) = \alpha - \beta$, за доведеним, буде числом алгебраїчним.

Нарешті, покладемо, що $\beta \neq 0$ є коренем рівняння

$$g(x) = b_0x^m + b_1x^{m-1} + \cdots + b_{m-1}x + b_m = 0 \ \ (b_0 \neq 0).$$

Припускаючи, що $x = \frac{1}{y}$, дістанемо рівняння з раціональними коефіцієнтами:

$$b_my^m + b_{m-1}y^{m-1} + \ \ldots \ + b_1y + b_0 = 0,$$

яке має корінь $\frac{1}{\beta}$. Отже, $\frac{1}{\beta}$ є алгебраїчне число, а тому і $\alpha \cdot \frac{1}{\beta} = \frac{\alpha}{\beta}$ буде числом алгебраїчним. Отже, наше твердження доведено повністю.

Наслідок. *Сукупність усіх дійсних алгебраїчних чисел утворює поле, яке, в свою чергу, є підполем поля всіх алгебраїчних чисел.*

З цієї властивості випливає, що будь-яка сума раціонального числа і радикала з раціонального числа, наприклад $7 + \sqrt[5]{3}$, а також будь-яка сума радикалів, наприклад $\sqrt[3]{2} + \sqrt[8]{7}$, будуть алгебраїчними числами. І взагалі, *будь-яка комбінація простих радикалів з раціональних чисел і раціональних чисел, добута внаслідок застосування скінченного числа дій додавання, віднімання, множення і ділення, є числом алгебраїчним.* Наприклад, число $\dfrac{\sqrt{2} + 3\sqrt[3]{3} - \sqrt[7]{5}}{\sqrt[11]{4}\ \sqrt[5]{2} - 2}$ буде алгебраїчним. Проте ми поки що не можемо стверджувати алгебраїчності чисел, які записують у вигляді «багатоповерхових» (складних) радикалів, наприклад, числа $\sqrt{2 + \sqrt[3]{3}}$. Це випливатиме лише з такої властивості:

Властивість 2. *Якщо ω — корінь рівняння,*

$$\varphi(x) = x^n + a_1x^{n-1} + \ldots + a_n = 0 \ (n \geqslant 1),$$

коефіцієнти якого є алгебраїчними числами, то ω також буде алгебраїчним числом.

Справді, ми можемо вважати, що $\alpha_1, \alpha_2, \ldots, \alpha_n$ є коренями одного й того самого многочлена

$$h(x) = \varphi_1(x) \ldots \varphi_n(x)$$

з раціональними коефіцієнтами, де $\varphi_i(x)$ $(i = 1, 2, \ldots, n)$ є многочлен, коренем якого є α_i. Взагалі, степінь m многочлена $h(x)$ може бути більший від n, або $\alpha_1, \alpha_2, \ldots, \alpha_n$ можуть і не вичерпувати всіх коренів многочлена $h(x)$. Тому позначимо всі корені многочлена $h(x)$ через $\gamma_1, \gamma_2, \ldots, \gamma_m (m \geqslant n)$, серед них, звичайно, будуть $\alpha_1, \alpha_2, \ldots, \alpha_n$, і складемо допоміжний многочлен:

$$H(x) = \prod_{i_1, \ldots, i_n} (x^n + \gamma_{i_1} x^{n-1} + \ldots + \gamma_{i_n}), \qquad (1)$$

де кожний з індексів $i_1, i_2, \ldots, i_n$ пробігає значення 1, 2, 3, ..., m і $i_1, i_2, \ldots, i_n$ попарно різні. Так само, як і при доведенні властивості 1, робимо висновок, що коефіцієнти многочлена $H(x)$ є симетричні многочлени від $\gamma_1, \gamma_2, \ldots \gamma_m$ над полем раціональних чисел, а тому, згідно з основною теоремою про симетричні многочлени, вони є раціональними числами. Оскільки $\varphi(x)$ є, очевидно, одним з множників добутку (1), то ω буде коренем многочлена $H(x)$ з раціональними коефіцієнтами. Отже ω — алгебраїчне число. Цим теорему доведено.

Застосуємо цю властивість до числа $\omega = \sqrt{2 + \sqrt[3]{3}}$. Число $\alpha = 2 + \sqrt[3]{3}$ згідно з властивістю 1 алгебраїчне, а тому й число ω буде алгебраїчне, як корінь многочлена $x^2 - \alpha$ з алгебраїчними коефіцієнтами (властивість 2). Взагалі, застосовуючи кілька разів властивості 1 і 2, прийдемо до такого висновку:

Усяке число, яке записується в радикалах над полем раціональних чисел R (тобто число, яке становить як завгодно складну скінченну комбінацію радикалів,[1] *в загальному випадку «багатоповерхових»), буде алгебраїчним числом.*

Алгебраїчні числа, які записуються в радикалах, утворюють, очевидно, поле. Це поле буде, звичайно, тільки частиною поля всіх алгебраїчних чисел. До нього, зокрема, не ввійдуть ті алгебраїчні числа, які є коренями рівнянь з раціональними коефіцієнтами, що не розв'язуються в радикалах.

У вищій алгебрі числове поле P називається *алгебраїчно замкненим*, якщо будь-який многочлен з коефіцієнтами з P має в самому полі P стільки коренів, який його степінь. Отже, властивості 1 і 2 алгебраїчних чисел означають, що *множина всіх алгебраїчних чисел утворює алгебраїчно замкнене поле.*

---

[1] Тут мається на увазі чотири арифметичні дії над радикалами, піднесення до степеня і добування кореня з раціональним показником. Проте, наприклад, комбінація $2^{\sqrt{2}}$ буде неалгебраїчним числом.

Контрольні запитання

1. Які числа називаються алгебраїчними?
2. Яке число називається алгебраїчним числом степеня n?
3. Які числа називаються спряженими між собою алгебраїчними числами?
4. Сформулювати основні властивості алгебраїчних чисел.
5. Яким числом буде будь-яка комбінація радикалів над полем раціональних чисел?

§ 45. Теорема Ліувілля. Трансцендентні числа. Побудова трансцендентних чисел

У попередньому параграфі було показано, що поле алгебраїчних чисел є алгебраїчно замкненим полем. За основною теоремою алгебри поле комплексних чисел також алгебраїчно замкнене. Виникає природне запитання, чи вичерпується алгебраїчними числами поле комплексних чисел.

Як ми вже зазначили, всяке число ω, яке не є алгебраїчним, називається *трансцендентним*, тобто інакше кажучи, комплексне (зокрема дійсне) число ω називається *трансцендентним*, якщо воно не є коренем жодного алгебраїчного рівняння степеня $n \geqslant 1$ з раціональними коефіцієнтами. Коротко кажучи, число ω, яке не є алгебраїчним, називається *трансцендентним*.

З цього означення випливає, що дійсне трансцендентне число повинно бути ірраціональним. Обернене твердження неправильне. Наприклад, $\sqrt{7}$ — ірраціональне число, але воно, як ми бачили вище, є алгебраїчним.

Усередині минулого століття було дано конструктивне доведення існування трансцендентних чисел.

Ліувілль довів таку теорему.

Теорема 1 (Ліувілля). *Якщо α — дійсне алгебраїчне число степеня $n \geqslant 2$, то для будь-якої пари цілих чисел a і $b > 0$ справедлива нерівність:*

$$\left|\alpha - \frac{a}{b}\right| > \frac{C}{b^n},$$

де C — додатна стала, яка не залежить від a та b.

Справді, припустимо, що α є дійсний корінь многочлена

$$f(x) = a_0 x^n + a_1 x^{n-1} + \ldots + a_{n-1} x + a_n \; (a_0 \neq 0)$$

з цілими коефіцієнтами, незвідного в полі раціональних чисел. За теоремою Безу, многочлен $f(x)$ повинен ділитись на $x - \alpha$; позначаючи через $f_1(x)$ частку від цього ділення, дістанемо:

$$f(x) = (x - \alpha) f_1(x),$$

де $f_1(x)$ — многочлен $(n-1)$-го степеня з дійсними алгебраїчними коефіцієнтами. Припускаючи, що $x=\frac{a}{b}$, дістанемо

$$f\left(\frac{a}{b}\right)=\left(\frac{a}{b}-\alpha\right)f_1\left(\frac{a}{b}\right),$$

звідки

$$\left|f\left(\frac{a}{b}\right)\right|=\left|\alpha-\frac{a}{b}\right|\cdot\left|f_1\left(\frac{a}{b}\right)\right|. \tag{1}$$

З другого боку, через те що $f(x)$ незвідний у полі раціональних чисел, то він не може мати раціональних коренів, тому

$$\left|f\left(\frac{a}{b}\right)\right|=\frac{|a_0a^n+a_1a^{n-1}b+\ldots+a_nb^n|}{b^n}\neq 0;$$

чисельник останнього дробу є цілим числом, але не дорівнює нулю. Значить, абсолютна величина чисельника не менша від 1 і

$$\left|f\left(\frac{a}{b}\right)\right|>\frac{1}{b^n}.$$

Отже, замінюючи у лівій частині рівності (1) $\left|f\left(\frac{a}{b}\right)\right|$ величиною $\frac{1}{b^n}$, дістанемо нерівність:

$$\left|\alpha-\frac{a}{b}\right|\cdot\left|f_1\left(\frac{a}{b}\right)\right|>\frac{1}{b^n}; \tag{2}$$

якщо $\left|\alpha-\frac{a}{b}\right|>1$, то й поготів

$$\left|\alpha-\frac{a}{b}\right|>\frac{1}{b^n}. \tag{3}$$

Тому залишається розглянути тільки такі пари чисел a і b, для яких

$$\left|\alpha-\frac{a}{b}\right|\leqslant 1. \tag{4}$$

Легко побачити, що для таких пар a, b дріб $\frac{a}{b}$ обмежений [1], але оскільки $f_1(x)$ — неперервна в сегменті $[\alpha-1,\ \alpha+1]$, то, отже,

[1] Тобто $\left|\frac{a}{b}\right|\leqslant M$, де M — деяка додатна стала (яка не залежить від чисел a і b), що задовольняє умову (4). Справді, через те що $\left|\frac{a}{b}\right|-\left|\alpha\right|\leqslant\left|\alpha-\frac{a}{b}\right|$, то й поготів $\left|\frac{a}{b}\right|-\left|\alpha\right|\leqslant 1$, звідки $\left|\frac{a}{b}\right|\leqslant\left|\alpha\right|+1$, тобто роль сталої M відіграє $|\alpha|+1$.

на цьому сегменті $f_1(x)$ буде обмеженою, тобто $\left|f_1\left(\frac{a}{b}\right)\right|<N$, де N є деяка додатна стала.

Отже, нерівність (2) можна підсилити, замінивши $\left|f_1\left(\frac{a}{b}\right)\right|$ більшою величиною N:

$$\left|\alpha-\frac{a}{b}\right|N>\frac{1}{b^n},$$

звідки

$$\left|\alpha-\frac{a}{b}\right|>\frac{1}{Nb^n}, \tag{5}$$

якщо a і b задовольняють умову (4). Припускаючи тепер, що C дорівнює найменшому з чисел 1 і $\frac{1}{N}$, згідно з нерівностями (3) і (5), дістанемо, що

$$\left|\alpha-\frac{a}{b}\right|>\frac{C}{b^n}$$

для всіх цілих a і $b>0$ та сталої C, яка не залежить від a і b, це й доводить нашу теорему.

Зауваження. Якщо α алгебраїчне число степеня $n=1$, тобто $\alpha=\frac{a}{b}$ — раціональне число, то ми дістанемо теорему 3 § 43.

Теорема Ліувілля показує, що наближення будь-якого алгебраїчного числа обмежене знизу.

За допомогою теореми Ліувілля можна довести існування трансцендентних чисел.

Теорема 2. Нехай ω — дійсне число. Якщо для будь-якого натурального $n\geqslant 1$ і будь-якого дійсного $C>0$ хоча б один раціональний дріб $\frac{a}{b}\left(\frac{a}{b}\neq\omega\right)$ такий, що

$$\left|\omega-\frac{a}{b}\right|<\frac{C}{b^n}, \tag{6}$$

то ω — *трансцендентне число.*

Справді, якби α було алгебраїчним, то за теоремою Ліувілля і теоремою 3, § 43 знайшлися б натуральне n і дійсне $C>0$ такі, що для будь-якого дробу $\frac{a}{b}$ було б $\left|\omega-\frac{a}{b}\right|>\frac{C}{b^n}$.

Це суперечить тому, що згідно з умовою теореми для цих n і C існує дріб $\frac{a}{b}$ такий, що справджується нерівність (6). Припущення, що ω — алгебраїчне, привело нас до суперечності, отже, ω — трансцендентне число.

Числа ω, для яких при будь-яких $n \geqslant 1$ і $c > 0$ нерівність (6) має розв'язок у цілих a і b, називаються *трансцендентними числами Ліувілля*.

Теорема 3. *Трансцендентні числа існують.*

Справді, припустимо, що q_0 і q_1 — довільні цілі додатні числа. Утворимо неповні частки за таким правилом:

$$q_2 > Q_1,\ q_3 > Q_2^2,\ q_4 > Q_3^3,\ \ldots,\ q_{k+1} > Q_k^k,\ \ldots$$

Оскільки $\frac{P_1}{Q_1} = \frac{q_0 q_1 + 1}{q_1}$, то q_2 вибираємо так, щоб $q_2 > q_1 = Q_1$. Знаючи q_0, q_1, q_2, обчислюємо $\frac{P_2}{Q_2}$ і вибираємо q_3 так, щоб $q_3 > Q_2^2$ і т. д.

Покажемо, що нескінченний неперервний дріб

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

визначає трансцендентне число ω. Припустимо супротивне, тобто нехай ω — алгебраїчне число степеня $n \geqslant 2$. На підставі теореми 1, § 39 маємо:

$$\left|\omega - \frac{P_k}{Q_k}\right| < \frac{1}{Q_k Q_{k+1}} = \frac{1}{Q_k(Q_k q_{k+1} + Q_{k-1})} < \frac{1}{Q_k^2 q_{k+1}} < \frac{1}{Q_k^{k+2}},$$

бо $q_{k+1} > Q_k^k$ за умовою.

Але, за теоремою Ліувілля, таке додатне число C, що $\left|\omega - \frac{a}{b}\right| > \frac{C}{b^n}$ при будь-яких цілих a і $b > 0$. Зокрема, $\left|\omega - \frac{P_k}{Q_k}\right| > \frac{C}{Q_k^n}$ при будь-якому натуральному k.

Оскільки

$$\frac{1}{Q_k^{k+2}} > \left|\omega - \frac{P_k}{Q_k}\right| > \frac{C}{Q_k^n},$$

то

$$\frac{1}{Q_k^{k+2}} > \frac{C}{Q_k^n} \quad \text{і при} \quad k \geqslant n \quad \frac{1}{Q_k^2} > C,$$

але $\lim\limits_{k \to \infty} \frac{1}{Q_k^2} = 0$ і при досить великому k $\frac{1}{Q_k^2} < C$.

Ця суперечність говорить про те, що ω не може бути алгебраїчним числом степеня $n \geqslant 2$. Але ω не може бути і раціональним числом (тобто алгебраїчним першого степеня); отже, ω — число трансцендентне. Цим ми не тільки довели теорему, а й вказали на метод побудови трансцендентних чисел Ліувілля. Клас чисел, які дістаємо таким способом, цікавий як історичний приклад конкретного задання явно трансцендентних чисел.

А тим часом можна будувати трансцендентні числа, їх не користуючись алгоритмом неперервних дробів. Так, наприклад, справедливе таке твердження:

Теорема 4. *Число* $\omega = \sum\limits_{m=1}^{\infty} \frac{1}{2^{m!}}$ *є трансцендентним.*

Справді, розглянемо раціональне число

$$\frac{p}{q} = \sum_{m=1}^{k} \frac{1}{2^{m!}};$$

матимемо

$$0 < \omega - \frac{p}{q} = \sum_{m=k+1}^{\infty} \frac{1}{2^{m!}} < \sum_{t=1}^{\infty} \frac{1}{2^{(k+1)!\,t}} = \frac{1}{2^{(k+1)!} - 1} < \frac{2}{2^{(k+1)!}},$$

бо $\sum\limits_{t=1}^{\infty} \frac{1}{2^{(k+1)!\,t}}$ є сума нескінченної спадної прогресії, знаменник 1 перший член якої дорівнюють $\frac{1}{2^{(k+1)!}}$. Але для довільно заданих $C > 0$ і $n \geqslant 1$ завжди можна вказати таке досить велике додатне число l, щоб для всіх $k > l$ виконувалась нерівність

$$\frac{2}{2^{(k+1)!}} < \frac{C}{q^n}. \tag{6}$$

Справді, через те, що $q = 2^{k!}$, то нерівність (6) можна переписати у вигляді $\frac{2}{q^{k+1}} < \frac{C}{q^n}$. Ця сама нерівність при досить великих значеннях k, очевидно, справджується.

Отже, для довільно заданих $C > 0$ і $n \geqslant 1$ і при досить великих значеннях k матимемо, що

$$0 < \omega - \frac{p}{q} < \frac{C}{q^n}.$$

Звідси, за теоремою Ліувілля, випливає, що ω не може бути алгебраїчним числом степеня $n \geqslant 2$, бо тоді при довільно заданих $C > 0$ і $n \geqslant 2$ і при досить великих k виконувалась би нерівність:

$$\left|\omega - \frac{p}{q}\right| > \frac{C}{q^n}.$$

Залишається показати, що ω не є алгебраїчним числом степеня $n = 1$, тобто не є число раціональне. Припустимо, що ω — раціональне і $\omega = \frac{a}{b}$, де a і b — деякі цілі додатні числа. Тоді для $n = 2$ і $C = 1$ при досить великих k з нерівностей $0 < \frac{a}{b} - \frac{p}{q} < \frac{1}{q^2}$ ми дістали б, що

$$0 < \frac{aq - bp}{bq} < \frac{1}{q^2};\ 0 < aq - bp < \frac{b}{q} < 1,$$

бо $q = 2^{k!}$ можна зробити як завгодно великим. Але це неможливо, оскільки $aq - bp$ — ціле додатне число. Цим ми довели наше твердження [1].

Як приклад розглянемо трансцендентне число, задане десятковим розкладом.

Приклад. Число $\omega = \frac{a_1}{10^{1!}} + \frac{a_2}{10^{2!}} + \frac{a_3}{10^{3!}} + \dots =$ $= 0, a_1 a_2 000 a_3 000\,000\,000\,000\,000\,0 a_4 00 \dots$, де a_i позначають довільні цифри від 1 до 9 (найпростіше припустити, що всі a_i дорівнюють 1) будуть трансцендентними.

Справді, візьмемо довільні натуральне n і дійсне $C > 0$. Припустимо $a^{k!}\left(\frac{a_1}{10^{1!}} + \frac{a_2}{10^{2!}} + \dots + \frac{a_k}{10^{k!}}\right)$, $b = 10^{k!}$, де k вибрано таким великим, що $10^{(k-1)!} \geqslant \frac{2}{C}$ і $k > n$, тоді

$$\left|\omega - \frac{a}{b}\right| = \frac{a_{k+1}}{10^{(k+1)!}} + \frac{a_{k+2}}{10^{(k+2)!}} + \dots < \frac{10}{10^{(k+1)!}} + \frac{10}{10^{(k+2)!}} +$$

$$+ \dots < \frac{1}{10^{(k+1)!-1}} + \frac{1}{10^{(k+2)!-1}} + \dots < \frac{1}{10^{k!}} + \frac{1}{10^{(k+1)!}} +$$

$$+ \dots < \frac{1}{10^{k!}}\left(1 + \frac{1}{2} + \frac{1}{2^2} + \dots\right) = \frac{2}{10^{k!}} = \frac{2}{10^{(k-1)!}} \cdot \frac{1}{10^{(k-1)!\,(k-1)}} \leqslant \frac{C}{b^n}.$$

Оскільки для довільних натурального n і дійсного $C > 0$ ми підібрали дріб $\frac{a}{b}$ такий, що $\left|\omega - \frac{a}{b}\right| < \frac{C}{b^n}$, то ω — трансцендентне число.

Контрольні запитання

1. Які числа називаються трансцендентними?
2. Чи завжди трансцендентне число ірраціональне? Чи правильне обернене твердження?
3. Сформулюйте теорему Ліувілля.
4. З якою метою при доведенні теореми Ліувілля використовують умову, що α дійсне алгебраїчне число степеня $n \geqslant 2$?
5. Які трансцендентні числа називаються числами Ліувілля?
6. Чи справедлива теорема Ліувілля для алгебраїчних чисел степеня $n = 1$, тобто для раціональних чисел? Як треба сформулювати теорему в цьому випадку?
7. Наведіть приклад трансцендентного числа, заданого десятковим розкладом.

---

[1] Цю теорему можна узагальнити так: усі числа виду $\omega \sum_{m=1}^{\infty} \frac{a_m}{l^{m!}}$, де a_m і l — цілі числа, $l > 1$ і $0 \leqslant a_m \leqslant l - 1$, є трансцендентні числа.

§ 46. Сучасний стан питання про трансцендентні числа; результати Гельфонда

Через 20—25 років після досліджень Ліувілля німецький математик Георг Кантор (1845—1918) дав просте і оригінальне доведення існування трансцендентних чисел, яке грунтується зовсім на інших принципах. Він показав, що множина всіх дійсних алгебраїчних чисел є зчисленною множиною, а множина всіх дійсних чисел незчисленна. Звідси випливає, що є незчисленна множина дійсних неалгебраїчних, тобто трансцендентних чисел. Слід зазначити, що доведення Кантора не дає можливості побудувати будь-яке конкретне трансцендентне число. З цього погляду доведення існування трансцендентних чисел Ліувілля є ефективнішим.

У 1873 р. французькому математику Ерміту вдалося встановити трансцендентність числа e. Доведення трансцендентності числа e з використанням інтеграла $\int_0^x e^{-t} f(t)\,dt$, де $f(t)$ — многочлен, можна провести аналогічно доведенню ірраціональності числа π.

У 1882 р. німецький математик Ліндеман, користуючись методом Ерміта, довів трансцендентність числа π. Цим самим було доведено неможливість розв'язання славнозвісної проблеми квадратури круга, тобто неможливість побудувати за допомогою циркуля й лінійки, квадрата, рівновеликого кругу з радіусом, що дорівнює одиниці, або, що те саме, — відрізка завдовжки π. До цієї задачі зводиться також задача про спрямлення кола.

Взагалі, Ліндеман довів загальніше припущення, з якого відразу ж випливає трансцендентність числа π.

Теорема Ліндемана. *Якщо*

$$\alpha_1, \alpha_2, \dots, \alpha_n$$

є різні між собою алгебраїчні числа, а

$$\beta_1, \beta_2 \dots, \beta_n$$

є довільні алгебраїчні числа, які не всі дорівнюють нулю одночасно, то рівність

$$\beta_1 e^{\alpha_1} + \beta_2 e^{\alpha_2} + \dots + \beta_n e^{\alpha_n} = 0$$

неможлива [1].

Ми не наводимо доведення цієї теореми, бо воно досить складне. З цієї теореми легко довести трансцендентність чисел e і π. Справді,

---

[1] Цей результат виражають, говорячи, що $e^{\alpha_1}, e^{\alpha_2}, \dots, e^{\alpha_n}$ при зазначених α_i лінійно незалежні над полем алгебраїчних чисел.

через те, що ціле раціональне число є окремим випадком алгебраїчного числа, то за теоремою Ліндемана співвідношення

$$a_0e^n + a_1e^{n-1} + \cdots + a_{n-1}e + a_ne^0 = 0,\ n \geqslant 1,$$

де a_0, a_1, ..., a_n — цілі числа, неможливе. Інакше кажучи, e не може бути коренем жодного многочлена $f(x) = a_0x^n + a_1x^{n-1} + \cdots + a_{n-1}x + a_n$ степеня $n \geqslant 1$ з цілими коефіцієнтами, тобто e — трансцендентне.

Трансцендентність числа π тепер можна довести так. З відомої формули Ейлера $e^{i\varphi} = \cos\varphi + i\sin\varphi$ при $\varphi = \pi$ виходить, що $e^{\pi i} = -1$, або $e^{\pi i} + e^0 = 0$. Звідси, за теоремою Ліндемана, дістаємо, що πi, а тому й π не може бути алгебраїчним, тобто π є трансцендентне.

З теореми Ліндемана, зокрема, випливають і такі твердження:

1) *e^α трансцендентне для всякого алгебраїчного $\alpha \neq 0$;*

2) *натуральний логарифм всякого дійсного алгебраїчного числа (крім 1) є трансцендентним числом;*

3) *всяке відмінне від 1 число, що має раціональний натуральний логарифм, — трансцендентне;*

4) $\sin\alpha$, $\cos\alpha$ і $\operatorname{tg}\alpha$ *є трансцендентними при дійсному алгебраїчному $\alpha \neq 0$.*

Справді, щоб довести твердження (1), припустимо супротивне, тобто, що e^α — алгебраїчне, тоді воно має бути коренем деякого многочлена

$$f(x) = a_0x^n + \cdots + a_{n-1}x + a_n$$

степеня $n \geqslant 1$ з цілими коефіцієнтами, тобто мали б

$$a_0e^{\alpha n} + a_1e^{\alpha(n-1)} + \cdots + a_ne^0 = 0.$$

Але ця рівність суперечить теоремі Ліндемана.

Щоб довести твердження (2), також припустимо супротивне, тобто що $\ln\alpha = \beta$ — алгебраїчне число, тоді $\alpha = e^\beta$ за тільки що доведеним має бути трансцендентним, але за умовою α — алгебраїчне.

3) Припустимо, що $\beta \neq 1$ — будь-яке дійсне число і $\ln\beta = \frac{m}{n}$ є раціональне число; тоді з рівності $\beta = e^{\frac{m}{n}}$ безпосередньо випливає трансцендентність числа β.

4) Доведемо трансцендентність $\sin\alpha$ у випадку дійсного алгебраїчного $\alpha \neq 0$. Припустимо супротивне, нехай $\sin\alpha = \beta$ — алгебраїчне число. Через те що

$$\sin\alpha = \frac{e^{i\alpha} - e^{-i\alpha}}{2i},$$

то

$$\frac{e^{i\alpha} - e^{-i\alpha}}{2i} = \beta,$$

звідки $(e^{i\alpha})^2 - 2i\beta e^{i\alpha} - 1 = 0$, тобто $e^{i\alpha}$ є коренем квадратного рівняння $x^2 - 2i\beta x - 1 = 0$ з алгебраїчними коефіцієнтами і тому за властивістю 2 алгебраїчних чисел $e^{i\alpha}$ має бути алгебраїчним. Але це неможливо, бо $i\alpha$ — алгебраїчне число, відмінне від нуля. Аналогічно доводиться трансцендентність $\cos\alpha$ і $\operatorname{tg}\alpha$ при дійсному алгебраїчному $\alpha \neq 0$.

Ці результати протягом майже 50 років були єдиними, які стосувались арифметичної природи чисел.

У 1900 р. на Паризькому міжнародному математичному конгресі один з найвидатніших німецьких математиків Гільберт (1862—1943) вказав на 23 найважчі математичні проблеми, розв'язання яких істотно сприяло б дальшому розвитку математики. Серед цих проблем була проблема (під № 7) про арифметичну природу чисел виду α^β, де α — алгебраїчне число, відмінне від 0 і 1, а β — алгебраїчне число, не нижче від другого степеня, тобто ірраціональне алгебраїчне число.

Довгий час цю проблему не могли розв'язати, і тільки в 1936 р. Гельфонд повністю розв'язав цю проблему, тобто довів таку теорему:

Теорема Гельфонда. *Всяке число виду α^β, де α — алгебраїчне число, відмінне від 0 і 1, і β — алгебраїчне число не нижче другого степеня, є число трансцендентне.*

Методи, створені Гольфондом, дали змогу встановити і трансцендентність ряду інших чисел. Вони сприяють дальшому розвитку теорії трансцендентних чисел, яка є однією з найскладніших розділів математики.

Як наслідок з теореми Гельфонда випливає така важлива теорема, яку ще інтуїтивно сформулював Ейлер.

Логарифм алгебраїчного числа $\alpha \neq 0$ при алгебраїчній основі β ($0 \neq \beta \neq 1$) є число трансцендентне, якщо α не дорівнює раціональному степеню основи, тобто $\alpha \neq \beta^{\frac{p}{q}}$, де p і q ($q > 0$) — *цілі числа.*

З цієї теореми безпосередньо випливає, що *десяткові логарифми всіх натуральних чисел $N \neq 10^k$ (k — ціле число) є трансцендентні числа.*

Цей факт має велике принципове значення. Десятковими логарифмами в науці і практиці користуються понад 300 років, і тільки в 40-х роках нашого століття, завдяки блискучим успіхам радянської школи теорії чисел, удалось цілком розкрити арифметичну природу цього класу чисел і довести їх трансцендентність.

Взагалі, проблеми про арифметичну природу конкретно заданих чисел належать і досі до найважчих математичних задач, що потребують майже в кожному окремому випадку особливого методу розв'язання їх.

Контрольні запитання

1. Хто й коли довів трансцендентність чисел e і π?
2. Сформулюйте теорему Ліндемана і наслідки з неї.
3. У чому полягала проблема Гільберта під № 7?
4. Сформулюйте теорему Гельфонда.
5. Яким числом буде десятковий логарифм натурального числа $N \neq 10^k$?

Вправи

1. Довести, що коли неповні частки розкладу додатного ірраціонального числа ω у нескінченний неперервний дріб задовольняють умову

$$q_{k+1} \geqslant 2^{k^2} q_1^k q_2^k \ldots q_k^k \ (k = 1, 2, \ldots),$$

то число ω трансцендентне.

2. Довести, що коли неповні частинні розклади додатного ірраціонального числа ω у нескінченний неперервний дріб мають вигляд $q_k = 2^{(k)!^2}$, $(k = 0, 1, 2, \ldots)$, то число ω трансцендентне.

3. Довести, що коли $\alpha > 0$ — алгебраїчне дійсне число і $\log_{10} \alpha$ — ірраціональне число, то $\log_{10} \alpha$ трансцендентне число.

4. Довести, що $\log_{10} 2$ — трансцендентне число.

5. Довести, що $\log_{10} e$ — ірраціональне число.

ІСТОРИЧНІ КОМЕНТАРІ

1. Теорема 2 § 43 належить Гауссу.

2. Ірраціональність числа π вперше довів у 1761 р. Ламберт. Доведення Ламберта грунтується на застосуванні неперервних дробів. Його уточнив Лежандр. Доведення, подане в § 43, дав американський математик Нівен у 1947 р. Доведення Ламберта і Лежандра можна знайти у книзі акад. С. Н. Бернштейна «Про квадратуру круга» з додатками історії питання, складеними Ф. Рудіо (вид. 3, М. — Л, 1936).

3. Докладне вивчення властивостей алгебраїчних чисел становить предмет теорії алгебраїчних чисел, який стоїть на межі алгебри і теорії чисел і є дуже змістовним. Деякі нові задачі, поставлені ще в XVII ст., потребували для їх розв'язання узагальнення поняття цілого числа. Однією з задач, яка відіграла неабияку роль в узагальненні поняття цілого числа, є так звана велика теорема Ферма. Вона твердить, що рівняння $x^n + y^n = z^n$ нерозв'язне в цілих числах, відмінних від нуля, при $n > 2$.

Цікаве походження великої теореми Ферма. На полях «Арифметики» Діофанта Ферма написав: «... навпаки, не можна поділити ні куб на два куби, ні біквадрат на два біквадрати, ні взагалі степінь, більший від квадрата, на два степені з тим самим показником; я відкрив цьому, по правді кажучи, чудове доведення, яке через брак місця не можна розмістити на цих полях». З того часу і досі, незважаючи на старанні зусилля видатних математиків майже трьох століть, цю теорему у загальному вигляді не доведено, хоч її доведено для багатьох значень n (в тому числі для всіх $n \leqslant 4003$).

Зрозуміло, що перевіряються тільки прості числа, а не кратні. Останні результати щодо доведення теореми були добуті за допомогою електронно-обчислювальних машин. У свій час великий інтерес до спроб довести цю теорему навіть серед неспеціалістів у галузі математики був викликаний великою міжнародною премією, анульованою ще в кінці першої світової війни. Спроби довести цю теорему привели до відкриття так званих цілих алгебраїчних чисел.

Першим розширенням поняття цілого числа були цілі гауссові числа, тобто числа виду $a + bi$, де $i = \sqrt{-1}$ і a, b — цілі раціональні числа. Гаусс

довів, що для цих чисел має місце алгоритм ділення з остачею, а тому справедливі всі теореми подільності, аналогічні теоремам подільності в кільці цілих раціональних чисел. Це узагальнене поняття цілого числа дало змогу розв'язати ряд важливих проблем теорії чисел. Ціле гауссове число $a + bi$ є коренем квадратного рівняння $x^2 - 2ax + (a^2 + b^2) = 0$ з цілими раціональними коефіцієнтами. Природно, що далі дослідження вчених були присвячені вивченню властивостей коренів алгебраїчних рівнянь степеня $n \geqslant 1$ з цілими раціональними коефіцієнтами, тобто алгебраїчним числом. При вивченні властивостей алгебраїчних чисел було введено поняття про ціле алгебраїчне число, яке стало розширенням поняття про ціле число.

4. Проблеми, що стосуються теорії трансцендентних чисел, виникли вперше в працях Ейлера, який поставив зокрема задачу доведення трансцендентності ірраціональних значень логарифмічної функції. Він ввів назву «трансцендентні числа». Латинське слово «transcendere» в перекладі на українську мову означає «переходити» або «перевищувати». Ейлер назвав такі числа трансцендентними тому, що вони ніби перевищують можливість алгебраїчних методів».

5. Питання існування трансцендентних чисел до Г. Кантора розглянув Ліувілль у працях, опублікованих у 1844 і 1851 рр.

6. Теорема Ліндемана є окремим випадком загальних теорем німецького математика К. Л. Зігеля (н. 1896) і радянського математика А. Б. Шидловського (н. 1915) про алгебраїчну незалежність значень так званих E — функцій при алгебраїчних значеннях аргументу.

7. Проблему Гільберта під № 7 висловив в дещо іншій формі ще Ейлер у 1748 р.

8. Свою теорему О. Й. Гельфонд опублікував у 1934 р. До цього (в 1929 р.) цю теорему було доведено для окремого випадку, коли β чисто уявна квадратична ірраціональність, тобто $\beta = i\sqrt{Q}$, де Q — додатне раціональне число.

Продовжуючи свої дослідження, Гельфонд довів, зокрема, нерівність

$$\left| \frac{\ln \alpha}{\ln \beta} - \theta \right| > e^{-\ln^{\lambda} H}, \quad \lambda = \text{const},$$

встановив скінченність числа розв'язків при змінних n і m конгруенції

$$\alpha^n - \beta^m \equiv 0 \pmod{p^s}, \quad s = \ln^{\gamma} m, \quad \gamma = \text{const},$$

де α і β — числа алгебраїчні; $\frac{\ln \alpha}{\ln \beta}$ — ірраціональне; θ — алгебраїчне число фіксованого степеня q і висоти H[1]; m і n — цілі раціональні і p — будь-який простий ідеал поля, який не входить в α і β. Крім того, у цій конгруенції $\alpha^n \neq \beta^m$ жодним цілим m і n. З цих тверджень випливає, наприклад, теорема:

Рівняння

$$\alpha^x + \beta^y = \gamma^z$$

має лише скінченне число розв'язків у цілих числах x, y, z, якщо α, β, γ — алгебраїчні числа, і хоча б одне з них не є алгебраїчною одиницею.

9. Зазначимо, нарешті, що теорія алгебраїчних і трансцендентних чисел тісно пов'язана з рядом найважливіших проблем теорії чисел і, зокрема, з проблемою розв'язування алгебраїчних і трансцендентних рівнянь у цілих числах.

Одним з повчальних прикладів цього роду є, на перший погляд незначне, уточнення теореми Ліувілля, зроблене в 1908 р. норвезьким математиком А. Туе (1863—1922 рр). Він довів таку теорему.

---

[1] *Висотою* H алгебраїчного числа θ називають максимальний з модулів коефіцієнтів того незвідного у полі раціональних чисел рівняння, яке задовольняється θ, коли всі коефіцієнти цього рівняння цілі і їхній найбільший спільний дільник дорівнює одиниці.

Теорема 1 (Туе). *Для всякого алгебраїчного числа* α степеня $n \geqslant 3$ нерівність $\left|\alpha - \frac{a}{b}\right| < \frac{c}{b^n}$ *допускає при будь-якому* $c > 0$ *лише скінченне число розв'язків у цілих числах* a і $b > 0$.

Доведення цієї теореми, на відміну від теореми Ліувілля, потребувало дуже тонких міркувань.

Дальші результати в цьому напрямі дістали К. Зігель, А. О. Гельфонд та ін. Найточнішу оцінку нерівності в теоремі 1 дістав у 1955 р. англійський математик Рот. Іменем Туе—Зігеля—Рота названо таку теорему:

Нехай α — алгебраїчне число степеня $n \geqslant 2$; тоді при будь-якому $\varepsilon > 0$ існує тільки скінченне число раціональних дробів $\frac{a}{b}$ таких, що

$$\left|\alpha - \frac{a}{b}\right| < \frac{1}{b^{2+\varepsilon}}.$$

З цієї теореми випливає, що для будь-якого алгебраїчного числа α степеня $n \geqslant 2$ і довільного $\varepsilon > 0$ можна знайти таке $c > 0$, що для будь-якого раціонального дробу $\frac{a}{b}$ справджуватиметься рівність:

$$\left|\alpha - \frac{a}{b}\right| \geqslant \frac{c}{b^{2+\varepsilon}}.$$

Користуючись цією теоремою можна довести таку теорему.

Теорема 2 (Туе). *Якщо*

$$f(z) = a_0 z^n + a_1 z^{n-1} + \cdots + a_n \quad (a_0 \neq 0)$$

незвідний у полі раціональних чисел многочлен з цілими коефіцієнтами степеня $n \geqslant 3$ і m *в ціле число, то невизначене рівняння*

$$g(x, y) = a_0 x^n + a_1 x^{n-1} y + \cdots + a_{n-1} x y^{n-1} + a_n y^n = m$$

або нерозв'язне, або має скінченну множину розв'язків у цілих числах.

Цей результат Туе є одним з небагатьох тверджень, встановлених для невизначених рівнянь вищих степенів.

Розділ IX

РОЗПОДІЛ ПРОСТИХ ЧИСЕЛ У НАТУРАЛЬНОМУ РЯДІ

§ 47. Нерівності Чебишова для функції $\pi(x)$

Числова функція $\pi(x)$ визначає число простих чисел, що не перевищують дійсного числа $x > 1$. Ця числова функція відіграє велику роль у теорії розподілу простих чисел, теорії, багато проблем якої ще й тепер не розв'язані.

У § 10 було доведено теорему Евкліда про нескінченність множини простих чисел у натуральному ряді, тобто що $\lim\limits_{x \to \infty} \pi(x) = \infty$.

Безпосереднє вивчення таблиць простих чисел, а також деякі відомі тепер теореми показують, що розподіл простих чисел у натуральному ряді відрізняється тією самою іррегулярністю, яка взагалі характерна для мультиплікативних властивостей чисел. Так, наприклад, у межах від 1 до 10 000 прості числа розподілені так:

від	до	простих чисел
1	100	25
101	200	21
201	300	16
301	400	16
401	500	17
501	600	14
601	700	16
701	800	14
801	900	15
901	1000	14

Всього в першій	тисячі	168	простих чисел
» » другій	»	135	» »
» » третій	»	127	» »
» » четвертій	»	120	» »
» » п'ятій	»	119	» »
» » шостій	»	114	» »
» » сьомій	»	117	» »
» » восьмій	»	107	» »
» » дев'ятій	»	110	» »
» » десятій	»	112	» »
Всього від 1 до 10 000		1229	простих чисел

Незважаючи на загальну тенденцію до зменшення кількості простих чисел, які припадають на відрізок $[a, a+h]$ довжини h, із збільшенням a при заданому h можна вказати впереміжку розміщені відрізки однієї й тієї самої довжини з порівняно малою і порівняно великою кількістю простих чисел. Наприклад, поділяючи відрізок від 1 до 100 000 на сотні, можна побачити, що в ньому буде: одна сотня з 21 простим числом, дві сотні з 17 простими числами, шість сотен з 4 простими числами, три сотні, в яких є тільки три простих числа, і т. д. Усі ці сотні розміщені при цьому аж ніяк не в порядку спадання кількості простих чисел у них. Відрізок тієї самої довжини між 8 900 000 і 9 000 000 містить вже одну сотню, в якій немає жодного простого числа.

А взагалі справедливе таке загальне твердження.

Існують як завгодно довгі відрізки натурального ряду, які зовсім не містять простих чисел.

Наприклад, для довільного натурального $n > 1$ можна вказати такий відрізок натурального ряду завдовжки $n-1$, який не містить жодного простого числа, наприклад:

$$n! + 2,\ n! + 3,\ \ldots,\ n! + n.$$

Справді, при $2 \leqslant k \leqslant n$ число $n! + k$ ділиться на k, і через те що $k < n! + k$, то $n! + k$ буде складеним.

Безпосереднє визначення того, чи є дане число простим чи складеним, становить задачу, яка для великих чисел в загальному випадку практично нерозв'язна. Спроби математиків визначити n-е просте число як функцію його номера за допомогою якого-небудь простого аналітичного виразу, або рівнозначної задачі про аналітичний вираз функції $\pi(x)$ досі не привели до мети. Навіть розв'язання простіших, ніж ця, задач, пов'язаних з розподілом простих чисел у натуральному ряді, становить і досі величезні труднощі.

Природними були спроби математиків знайти для функції $\pi(x)$ наближений вираз у вигляді простої аналітичної функції від x, дослідити зростання якої було б не важко. Але й ці спроби аж до середини XIX ст. не дали істотного результату. Вперше теоретично обгрунтував зв'язок між функцією $\pi(x)$ і елементарною функцією $\frac{x}{\ln x}$ наш великий співвітчизник П. Л. Чебишов. Треба зазначити, що в цьому питанні П. Л. Чебишов не мав попередників і всі ідеї і методи доведень він створив заново, він дістав також свої найважливіші результати елементарними арифметичними прийомами, не вдаючись до засобів вищої математики.

Зокрема, в 1850 р. він довів таку визначну теорему, яка характеризує порядок зростання функції $\pi(x)$.

Теорема. *Для всіх дійсних $x \geqslant 2$ можна вказати такі дві додатні сталі a і b $(a < b)$, що*

$$a\frac{x}{\ln x} < \pi(x) < b\frac{x}{\ln x}. \qquad (1)$$

Нерівності (1) називають *нерівностями Чебишова.*

Доведення. Припустимо, що n — натуральне число, не менше 2; розглянемо вираз

$$\alpha(n) = \frac{(2n)!}{(n!)^2},$$

Можна оцінити величину цього виразу двояко:

1) З одного боку, $\alpha(n)$ є коефіцієнт при x^n у біноміальному розкладі $(1 + x)^{2n}$, тому

$$\frac{(2n)!}{(n!)^2} = C_{2n}^n = \alpha(n) < (1+1)^{2n} = 2^{2n},\ \alpha(n) < 2^{2n};$$

з другого боку:

$$\alpha(n) = \frac{(n+1)\ldots 2n}{1\cdot 2\ldots n} = \frac{n+1}{1}\cdot\frac{n+2}{2}\cdot\ldots\frac{n+n}{n} > 2^n.$$

Отже,

$$2^n < \alpha(n) < 2^{2n}.$$

2) Тепер уведемо в розгляд прості числа, не забуваючи, що $\alpha(n)$ як біноміальний коефіцієнт є число ціле.

З одного боку, всяке просте число p, більше від n і менше від $2n$, ділить чисельник, але не ділить знаменника виразу $\alpha(n)$, тому $\alpha(n)$ ділиться на добуток усіх $\pi(2n) - \pi(n)$ простих чисел, які містяться між n і $2n$, і, оскільки кожне з цих чисел більше від n, то

$$\alpha(n) > n^{\pi(2n)-\pi(n)}.$$

З другого боку, в канонічний розклад $\alpha(n) = \prod_{n<p<2n} p^r$ можуть входити тільки прості числа p, які не перевищують $2n$, і кожне таке число, очевидно, ввійде в розклад $\alpha(n)$ з показником

$$\sum_{m=1}^{r}\left(\left[\frac{2n}{p^m}\right] - 2\left[\frac{n}{p^m}\right]\right),$$

де r є найбільше число, для якого ще $p^r < 2n$ (див. теорему 1, § 12)

Легко побачити, що при парному x вираз $[x] - 2\left[\frac{x}{2}\right] = 0$, а при непарному x маємо $[x] - 2\left[\frac{x}{2}\right] = 1$, так що в обох випадках

$$[x] - 2\left[\frac{x}{2}\right] \leqslant 1.$$

Застосовуючи це співвідношення до всіх чисел написаної вище суми, знайдемо, що ця сума не перевищує r одиниць, через те всяке просте число p увійде в розклад $\alpha(n)$ з показником, що не перевищує числа r, для якого все ще $p^r < 2n$.

Замінимо тепер не меншим числом $2n$ усі степені p^r простих чисел p, які входять у канонічний розклад числа $\alpha(n)$. Ми дістанемо добуток множників, які дорівнюють $2n$, у числі, що не перевищує загального числа $\pi(2n)$ простих чисел на відрізку від 1 до $2n$. Отже,

$$\alpha(n) < (2n)^{\pi(2n)}.$$

Таким чином, можна написати:

1) $2^n < \alpha(n) < 2^{2n}$;
2) $n^{\pi(2n)-\pi(n)} < \alpha(n) < (2n)^{\pi(2n)}$.

З цих нерівностей внаслідок транзитивності співвідношення нерівності дістанемо:

$$n^{\pi(2n)-\pi(n)} < 2^{2n},\ 2(n)^{\pi(2n)} > 2^n.$$

Логарифмуючи, знайдемо, що, по-перше:

$$[\pi(2n) - \pi(n)] \ln n < 2n \ln 2,$$

$$\pi(2n) - \pi(n) < 2 \ln 2 \frac{n}{\ln n}; \qquad (2)$$

по-друге:

$$\pi(2n) \ln(2n) > n \ln 2;$$

$$\pi(2n) > \ln 2 \frac{n}{\ln(2n)}. \qquad (3)$$

Але при $n \geqslant 2$ очевидно

$$2n \leqslant n^2, \ \ln(2n) \leqslant 2 \ln n,$$

отже,

$$\pi(2n) \geqslant \frac{\ln 2}{2} \cdot \frac{n}{\ln n}. \qquad (3')$$

Припускаючи, що $n = \left[\frac{x}{2}\right]$ і користуючись нерівністю (3'), дістанемо:

$$\pi(x) \geqslant \pi\left(2\left[\frac{x}{2}\right]\right) \geqslant \frac{\ln 2}{2} \cdot \frac{\left[\frac{x}{2}\right]}{\ln\left[\frac{x}{2}\right]} > \frac{\ln 2}{2} \cdot \frac{\frac{x}{2} - 1}{\ln x}$$

при $x \geqslant 4$. Але коли $x \geqslant 4$, то, як легко перевірити, $\frac{1}{2}x - 1 \geqslant \frac{1}{4}x$, тому при $x \geqslant 4$:

$$\pi(x) > \frac{\ln 2}{8} \cdot \frac{x}{\ln x}.$$

Якщо $2 \leqslant x < 4$, $\pi(x) \geqslant 1$, а $\frac{x}{\ln x}$, досягаючи мінімуму в точці $x = e$, де e є неперове число, буде $\leqslant \frac{2}{\ln 2} = \frac{4}{\ln 4} < 3$. Отже,

$$\pi(x) > \frac{1}{3} \frac{x}{\ln x} > \frac{\ln 2}{8} \cdot \frac{x}{\ln x}$$

при $2 \leqslant x < 4$.

Таким чином, при будь-якому $x \geqslant 2$:

$$\pi(x) > a \cdot \frac{x}{\ln x},$$

де $a = \frac{\ln 2}{8}$. Цим встановлено потрібну межу $\pi(x)$ знизу.

Тепер встановимо межу $\pi(x)$ зверху.

Насамперед доведемо, що можна знайти таке c, що

$$\pi(x) - \pi\left(\frac{x}{2}\right) < c \cdot \frac{x}{\ln x}$$

при будь-якому $x \geqslant 2$, не тільки при $x = 2n$, як це показує нерівність (2). Справді, припускаючи, що $\left[\frac{x}{2}\right] = n$, знайдемо при $x = 2n$ і $x = 2n + 1$, що

$$\pi(x) \leqslant \pi(2n) + 1 \ \text{ і } \ \pi\left(\frac{x}{2}\right) \geqslant \pi(n).$$

Віднімаючи від першої нерівності другу, дістанемо

$$\pi(x) - \pi\left(\frac{x}{2}\right) \leqslant \pi(2n) - \pi(n) + 1 < c_1 \frac{n}{\ln n} + 1,$$

де $c_1 \geqslant 2 \ln 2$ (див. нерівність 2).

Якщо $\left[\frac{x}{2}\right] = n$, то нескінченно велика величина $\frac{n}{\ln n}$, зростаючи при $x \to \infty$, дедалі більше відстає за своїми значеннями від нескінченно великої $\frac{x}{\ln x}$. Тому легко вибрати c так, що й додана одиниця не заважатиме виконанню нерівності

$$c_1 \frac{n}{\ln n} + 1 < c \frac{x}{\ln x},$$

тоді матимемо

$$\pi(x) - \pi\left(\frac{x}{2}\right) < c \frac{x}{\ln x}$$

при будь-якому $x \geqslant 2$.

Зауважимо, що при встановленні нерівності такого типу можна не турбуватись про початкові значення x, бо значення c завжди можна відповідно збільшити так, щоб нерівності виконувались для всіх значень x, починаючи з $x = 2$.

Тепер можна написати:

$$\ln x \cdot \pi(x) - \ln \frac{x}{2} \cdot \pi\left(\frac{x}{2}\right) = \ln x \cdot \pi(x) - \ln x \cdot \pi\left(\frac{x}{2}\right) + \ln 2 \cdot \pi\left(\frac{x}{2}\right) =$$

$$= \ln x \left\{\pi(x) - \pi\left(\frac{x}{2}\right)\right\} + \ln 2 \cdot \pi\left(\frac{x}{2}\right) < \ln x \cdot c \cdot \frac{x}{\ln x} + \frac{x}{2} = d \cdot x,$$

де $d = c + \frac{1}{2}$, причому ми скористались очевидними нерівностями

$$\pi\left(\frac{x}{2}\right) < \frac{x}{2} \ \text{ і } \ \ln 2 < 1.$$

Отже,

$$\ln x \cdot \pi(x) - \ln \frac{x}{2} \cdot \pi\left(\frac{x}{2}\right) < d \cdot x. \qquad (4)$$

Покладемо тут, що $x = \frac{z}{2^m}$, тоді матимемо:

$$\ln \frac{z}{2^m} \cdot \pi\left(\frac{z}{2^m}\right) - \ln \frac{z}{2^{m+1}} \cdot \pi\left(\frac{z}{2^{m+1}}\right) < d \cdot \frac{z}{2^m}.$$

Надаючи m значень від 0 до k, де k таке, що ще $\frac{z}{2^{k+1}} > 1$, дістанемо такі нерівності:

$$\text{при } m = 0 \ln z \cdot \pi(z) - \ln \tfrac{z}{2} \cdot \pi\left(\tfrac{z}{2}\right) < d \cdot z,$$

$$\text{при } m = 1 \ln \tfrac{z}{2} \cdot \pi\left(\tfrac{z}{2}\right) - \ln \tfrac{z}{2^2} \cdot \pi\left(\tfrac{z}{2^2}\right) < d \cdot \tfrac{z}{2},$$

. . . . . .

$$\text{при } m = k \ln \tfrac{z}{2^k} \cdot \pi\left(\tfrac{z}{2^k}\right) - \ln \tfrac{z}{2^{k+1}} \cdot \pi \tfrac{z}{2^{k+1}} < d \cdot \tfrac{z}{2^k}.$$

Додаючи ці нерівності, дістанемо:

$$\ln z \pi(z) - \ln \tfrac{z}{2^{k+1}} \cdot \pi\left(\tfrac{z}{2^{k+1}}\right) < d\left(1 + \tfrac{1}{2} + \cdots + \tfrac{1}{2^k}\right) z < 2d \cdot z;$$

але при вказаному виборі k

$$2^{\frac{z}{k+2}} < 1, \quad 2^{\frac{z}{k+1}} < 2,$$

і тому $\pi\left(\frac{z}{2^{k+1}}\right) = 0.$

Остаточно дістаємо: $\ln z \cdot \pi(z) < 2d \cdot z$, або, змінюючи позначення z на x:

$$\pi(x) < b \cdot \frac{x}{\ln x}.$$

Цим встановлено потрібну межу зверху і тим самим теорему Чебишова доведено повністю. Чебишов для сталих a і b знайшов значення: $a = 0{,}92129 \ldots$; $b = \frac{6}{5} a$.

Нерівності Чебишова дають змогу порівнювати число простих чисел у заданих межах і число чисел якої-небудь іншої підпослідовності натуральних чисел.

Контрольні запитання

1. Що визначає функція $\pi(x)$?
2. Дайте характеристику розподілу простих чисел у натуральному ряді.
3. Що можна сказати про порядок зростання функції $\pi(x)$?
4. Чи існує аналітичний вираз для функції $\pi(x)$?

§ 48. Розбіжність ряду величин, обернених до простих чисел

Після Евкліда Ейлер перший намітив новий підхід до дослідження питання про розподіл простих чисел у натуральному ряді. Він знайшов друге доведення теореми Евкліда, яке грунтується

на застосуванні понять і теорем з математичного аналізу (найпростіший приклад застосування аналітичного методу). Розглянемо доведення Ейлера теореми Евкліда.

Припустимо, що p є довільне просте число. Оскільки $p \geqslant 2$, то $0 < \frac{1}{p} < 1$ і ряд $1 + \frac{1}{p} + \frac{1}{p^2} + \cdots$ буде збіжним як сума нескінченно спадної геометричної прогресії з першим членом 1 і з знаменником $\frac{1}{p}$. Матимемо:

$$\frac{1}{1 - \frac{1}{p}} = 1 + \frac{1}{p} + \frac{1}{p^2} + \cdots = \sum_{m=0}^{\infty} \frac{1}{p^m}. \qquad (1)$$

Припустимо тепер, що число простих чисел скінченне і найбільше з них не перевищує N. Тоді і рівностей типу (1) буде скінченне число. Через те що в правих частинах цих рівностей ми маємо збіжні ряди з додатними членами, то на підставі відомої з аналізу теореми про множення рядів[1] всі ці рівності можна перемножити. В результаті вийде збіжний ряд з додатними членами, які можна розмістити в будь-якому порядку. Очевидно, що при перемноженні рядів $\sum_{m=0}^{\infty} \frac{1}{p^m}$ дістанемо члени виду:

$$\frac{1}{p_1^{\alpha_1} p_2^{\alpha_2} \ldots p_k^{\alpha_k}}, \qquad (2)$$

де $p_1, p_2, \ldots p_k$ — усі прості числа, які не перевищують N; $\alpha_1, \alpha_2, \ldots \alpha_k$ — довільна система цілих невід'ємних чисел. Оскільки за основною теоремою арифметики (див. § 10) всяке натуральне число $n > 1$ можна розкласти на прості множники і притому тільки єдиним способом і оскільки знаменники членів (2) знайденого ряду будуть добутками можливих комбінацій простих чисел, то вони являтимуть собою всі натуральні числа n. Отже, ми дістанемо в результаті перемноження рядів (1) таку рівність:

$$\prod_p \frac{1}{1 - \frac{1}{p}} = \sum_{n=1}^{\infty} \frac{1}{n}.$$

Але ця рівність неможлива, бо в правій частині маємо розбіжний (гармонічний) ряд, а в лівій — скінченне число (число множників скінченне). Ця суперечність і доводить теорему Евкліда.

---

[1] За цією теоремою добуток скінченного числа абсолютно збіжних рядів (зокрема рядів з додатними членами) визначають як добуток скінченних сум, помножаючи кожний член кожного співмножника на кожний член кожного з решти співмножників.

З доведення Ейлера теореми Евкліда як наслідок випливає така властивість простих чисел.

Теорема про розбіжність ряду величин, обернених до простих чисел. *Ряд*

$$\frac{1}{2}+\frac{1}{3}+\frac{1}{5}+\ldots+\frac{1}{p}+\ldots=\sum_p\frac{1}{p},$$

де p набуває значення всіх простих чисел, розбігається.

Справді, з наведеного вище доведення теореми Евкліда випливає, що нескінченний добуток $\prod_p \frac{1}{1-\frac{1}{p}}$ розбігається, тобто розбігається і ряд $-\sum \ln\left(1-\frac{1}{p}\right)$, при цьому його сума прямує до $+\infty$.

Але

$$-\ln(1-\eta)=\eta+\frac{\eta^2}{2}+\frac{\eta^3}{3}+\ldots<\eta+\eta^2+\eta^3+\ldots=\frac{\eta}{1-\eta}\leqslant 2\eta$$

при $\eta=\frac{1}{p}<1$; тому ряд $2\sum_p\frac{1}{p}$, тобто і ряд $\sum_p\frac{1}{p}$, розбігається, що й доводить теорему.

Розглянемо друге доведення цього твердження, яке грунтується на нерівностях Чебишова.

Покажемо спочатку, як за допомогою нерівностей Чебишова можна дістати оцінку зростання n-го простого числа p_n, а саме: *n-е просте число p_n при всякому цілому $n\geqslant 1$ задовольняє нерівність:*

$$\alpha\cdot n\ln n<p_n<\beta\cdot n\ln n, \qquad (3)$$

де α і β — деякі додатні константи.

Справді, припускаючи, в нерівностях Чебишова $x=p_n$ і покладаючи, що $\pi(p_n)=n$, дістанемо:

$$a\frac{p_n}{\ln p_n}<n<b\frac{p_n}{\ln p_n}.$$

Звідси, по-перше, матимемо:

$$p_n>\frac{1}{b}n\ln p_n>\frac{1}{b}n\ln n=\alpha\cdot n\ln n,$$

де $\alpha=\frac{1}{b}$, оскільки $p_n>n$.

По-друге, дістанемо, що

$$p_n<\frac{1}{a}n\ln p_n. \qquad (4)$$

Границя величини $\frac{\ln p_n}{\sqrt{p_n}}$ при $n\to\infty$ дорівнює нулю. Отже, для досить великих n:

$$\frac{\ln p_n}{\sqrt{p_n}}<a,$$

звідки при досить великих n

$$\frac{1}{a}\ln p_n<\sqrt{p_n};$$

і ми можемо нерівність (4) підсилити при досить великих n:

$$p_n<n\sqrt{p_n},$$

звідки

$$p_n<n^2,\ \ln p_n<2\ln n$$

при досить великих значеннях n. Підставляючи у праву частину нерівності (4) замість $\ln p_n$ більшу величину $2\ln n$, тільки нідсилимо нерівність:

$$p_n<\frac{2}{a}n\ln n \qquad (5)$$

при досить великих n. Очевидно, що при потребі можна сталу $\frac{2}{a}$ збільшити настільки, щоб нерівність (5) справджувалась уже для всіх значень $n\geqslant 1$.

Отже, для всіх $n\geqslant 1$:

$$\alpha\cdot n\ln n<p_n<\beta\cdot n\ln n,$$

де α і β — деякі додатні сталі.

Знайдена оцінка (3) зростання n-го простого числа p_n дає змогу дуже просто виявити розбіжність ряду $\sum_p\frac{1}{p}$ з величин, обернених до простих чисел.

Справді, з математичного аналізу відомо, що ряд $\sum_{n=2}^{\infty}\frac{1}{n\ln n}$ розбігається. Оскільки $\frac{1}{p_n}>\frac{1}{\beta}\cdot\frac{1}{n\ln n}$, то звідси і поготів розбігається ряд

$$\sum_{n=1}^{\infty}\frac{1}{p_n}=\sum_p\frac{1}{p}.$$

Разом з цим знову доведено нескінченність числа простих чисел. Розбіжність ряду $\sum_p\frac{1}{p}$ свідчить про те, що у відповідному сумар-

ному розумінні слова прості числа густіше розміщені в натуральному ряді, ніж повні квадрати n^2 цілих чисел, бо відомо, що ряд $\sum_{n=1}^{\infty} \frac{1}{n^2}$ збігається. І все-таки прості числа розміщені досить рідко. Точніше кажучи, справджується така теорема, яку також вперше сформулював і довів Ейлер.

Теорема Ейлера. *При необмеженому зростанні дійсного числа* $x > 1$ *границя відношення* $\frac{\pi(x)}{x}$ *дорівнює нулю.*

Відношення $\frac{\pi(x)}{x}$ можна розглядати як «середню щільність» простих чисел на відрізку $[1; x]$. Отже, теорема Ейлера твердить, що при необмеженому зростанні x середня щільність простих чисел прямує до нуля.

Це твердження є прямим наслідком нерівностей Чебишова. Справді, маємо $\frac{\pi(x)}{x} < \frac{b}{\ln x}$. При $x \to \infty$, $\frac{b}{\ln x} \to 0$, отже $\frac{\pi(x)}{x} \to 0$.

Контрольні запитання

1. Сформулюйте теорему про множення абсолютно збіжних рядів. З якою метою використовується ця теорема при доведенні Ейлером теореми Евкліда?
2. Сформулюйте теорему про розбіжність ряду величин, обернених простим числам.
3. До якого значення прямує відношення $\frac{\pi(x)}{x}$ при $x \to \infty$.

§ 49. Сучасний стан питання про розподіл простих чисел у натуральному ряді і арифметичних прогресіях

У попередніх двох параграфах ми вже ознайомилися з деякими питаннями, пов'язаними з розподілом простих чисел у натуральному ряді. Одним з напрямів, який бере початок від теореми Евкліда про нескінченність числа простих чисел, є спроба встановити нескінченність множини простих чисел в тій чи іншій частині натурального ряду, тобто серед натуральних чисел того чи іншого певного виду. Тут також не розв'язано ряд проблем, в яких треба дати загальне доведення або спростувати загальність навіть найпростіших емпірично спостережуваних на табличному матеріалі закономірностей.

Спинимось на прикладах.

1. Ще Ферма висловив припущення, що числа виду $F_n = 2^{2^n} + 1$ при цілому невід'ємному n є прості. Числа Ферма мають значення для задачі про поділ кола; це, наприклад, такі числа: $F_0 = 2^{2^0} + 1 = 3$, $F_1 = 2^{2^1} + 1 = 5$, $F_2 = 2^{2^2} + 1 = 17$, $F_3 = 2^{2^3} + 1 = 257$, $F_4 = 65537$. Але вже Ейлер у 1732 р. показав, що при $n = 5$ виходить складене число, яке ділиться на 641:

$$F_5 = 2^{2^5} + 1 = 4\,294\,967\,297 = 641 \cdot 6\,700\,417.$$

Згодом було виявлено, що при $n = 6, 7, 8, 9, 10, 11, 12, 13, 15, 16, 18, 23, 36, 38$ і 73 виходять складені числа. Для кожного з цих F_n, крім $n = 7$ і 8, відомий один дільник.

Найбільше з наведених чисел Ферма F_{1945} має простий дільник $5 \cdot 2^{1947} + 1$. З перших 118 натуральних чисел F_n ($n = 0, 1, \ldots, 117$) відомо 19 складених; на триста з лишком чисел після F_{117} відомо тільки 10 складених. Усього відомо поки що 36 складених чисел Ферма F_n.

Твердження німецького математика Ейзенштейна (1823—1852) про те, що вираз $2^{2^n} + 1$ дає, хоч і не підряд, але все ж таки безліч простих чисел, і досі не доведене.

Цікаво, що для $n > 4$ досі не відомі прості числа Ферма.

2. Французький математик Мерсенн (1588—1648) розглядав числа виду $M_p = 2^p - 1$, де p — просте (числа Мерсенна). Ці числа мають особливе значення, бо вони пов'язані з проблемою досконалих чисел. Натуральне число n називається досконалим, якщо сума всіх його власних дільників дорівнює n. Наприклад, відоме твердження, що число $p = 2^{k+1} - 1$ може бути простим тоді і тільки тоді, коли показник $k + 1$ — просте число.

Той факт, що числа M_{17} і M_{19} — прості, встановив італійський математик Катальді до Мерсенна.

Отже, не говорячи вже про те, що немає загальної відповіді на питання, чи існує скінченна, чи нескінченна множина простих чисел Мерсенна, характер числа M_p не з'ясований навіть для порівняно невеликих окремих значень p.

Як довів І. М. Первушин у 1883 р., число $2^{61} - 1 = 2\,305\,843\,009\,213\,693\,951$ — просте; довгий час його вважали найбільшим з відомих простих чисел. Тепер відомо, що числа M_p при $p = 2, 3, 5, 7, 13, 17, 19, 31, 61, 89, 107, 127, 521, 607, 1279, 2203, 2281, 3217, 4423$ — прості. Найбільшим відомим простим числом Мерсенна є M_{4423}.

До 1953 р. було припущення, що коли $p = 2^n - 1$ просте, то і $M_p = 2^p - 1 = 2^{2^n - 1} - 1$ просте. У 1953 р. це припущення було спростоване для $n = 13$.

Тепер деякі дослідники дійшли висновку, що чисел Мерсенна, а, отже, і досконалих чисел, не безліч, а скінченне число.

3. Як поправку до твердження Ферма про числа $2^{2^n} + 1$ було висловлено припущення, що числа $2 + 1$, $2^2 + 1$, $2^{2^2} + 1$, $2^{2^{2^2}} + 1$, ... — прості.

Недавно було доведено, що це припущення неправильне. Серед чисел цього виду є й складені. Складеним є, наприклад, число $2^{2^{2^2}} - 1$.

4. Шукаючи формулу, яка давала б виключно прості числа, Ейлер указав кілька многочленів з цілими коефіцієнтами, значення яких для порівняно великого числа початкових значень $x = 0, 1, 2, 3, \ldots$ становлять тільки прості числа. Це наприклад, такі многочлени:

$$x^2 + x + 17,\ 2x^2 + 29,\ x^2 + x + 41,\ x^2 - 79x + 1601,$$

що дають відповідно 16, 29, 40 і 80 простих чисел при підставлянні замість x значень $0, 1, \ldots, 15$; $0, 1, \ldots, 28$; $0, 1, \ldots, 39$; $0, 1, \ldots, 79$.

Однак уже Ейлер дав загальне доведення того, що *жодний многочлен від x з цілими коефіцієнтами*

$$f(x) = a_0x^n + a_1x^{n-1} + \ldots + a_n$$

не може при всіх без винятку цілих значеннях x набувати значень, які становлять (хоча б за абсолютною величиною) прості числа.

Справді, припустимо, що при $x = x_0$ маємо просте число $f(x_0) = p$. При $x = x_0 + py$, де y — будь-яке ціле число, $f(x)$ ділиться на p, бо

$$f(x_0 + py) = f(x_0) + pg(y) = p + pg(y) = p[1 + g(y)],$$

де $g(y)$ — многочлен відносно y з цілими коефіцієнтами. Оскільки $f(x)$ відмінний від сталого, то многочлен $g(y)$ не перетворюється тотожно в нуль. Тому при всіх цілих значеннях y, крім скінченного числа коренів рівняння $g(y) = 0$, цей многочлен набуває значень, відмінних від нуля. Множник $1 + g(y)$ при цьому буде цілим числом, відмінним від одиниці, і число $f(x_0 + py)$ буде складеним при всіх значеннях x, крім лише скінченного числа.

5. У 1845 р. французький математик Жозеф Бертран (1822—1900) для доведення однієї теореми з теорії скінченних груп скористався таким твердженням: якщо $n > 3$ — ціле число, то є принаймні одне просте число, що лежить між n і $2n - 2$. Незважаючи на всі зусилля, Бертрану не вдалось довести це твердження (хоч він і перевірив його справедливість для всіх $n \leqslant 3\,000\,000$) і він прийняв його як постулат. Цей постулат вперше довів у 1852 р. Чебишов. Метод доведення його дуже дотепний і порівняно елементарний. Чебишов розглядає функцію $\theta(x)$, що є натуральним логарифмом добутку всіх простих чисел, які не перевищують дійсного числа $x > 0$, і розглядає зростання $\theta(x)$ при зростанні x. Він знаходить такі нерівності:

$$Ax - \frac{12}{5}Ax^{\frac{1}{2}} - \frac{5}{8\ln 6}\ln^2 x - \frac{15}{4}\ln x - 3 < \theta(x) < \frac{6}{5}Ax - Ax^{\frac{1}{2}} + \frac{5}{4\ln 6}\ln^2 x + \frac{5}{2}\ln x + 2,$$

де

$$A = \ln \frac{2^{\frac{1}{2}} \cdot 3^{\frac{1}{3}} \cdot 5^{\frac{1}{5}}}{30^{\frac{1}{30}}} = 0{,}92129\ldots.$$

За допомогою цих нерівностей Чебишов довів ряд теорем, пов'язаних з законом розподілу простих чисел у натуральному ряді, зокрема, не тільки довів постулат Бертрана, а й дістав кращий результат.

Найпростішими нескінченними підпослідовностями натуральних чисел є арифметичні прогресії. У 1788 р. Лежандр висловив, а в 1837 р. Діріхле довів таку теорему.

Теорема Діріхле. *Усяка арифметична прогресія, перший член якої і різниця взаємно прості числа, містить безліч простих чисел.*

Для деяких окремих випадків, наприклад, для чисел виду $6k - 1$, $4k - 1$ (див. приклади 25 і 26, розд. I), $4k + 1$, $8k + 5$, цю теорему легко довести. Доведення теореми в загальному випадку дуже складне і потребує використання спеціального аналітичного апарату, зв'язаного з рядами типу

$$\sum_{n=1}^{\infty} \frac{a_n}{n^s},$$

які називаються тепер *рядами Діріхле*. У 1949 р. норвезький математик Сельберг опублікував перше елементарне доведення цієї теореми. У 1956 р. Гельфонд опублікував друге елементарне доведення теореми Діріхле. Ця теорема твердить, що коли числа a і b взаємно прості, то існує безліч простих чисел виду $ax + b$ (x — ціле).

Умова $(a, b) = 1$ істотна, бо коли $(a, b) = d > 1$, то всі члени прогресії ділитимуться на d, і тоді прогресія матиме щонайбільше одне просте число (саме d, якщо d — просте).

Наступним природним кроком було б дослідження в тому самому розумінні виразів другого степеня, тобто виразів виду $ax^2 + bx + c$. Проте у цьому напрямі нічого зробити не вдалось. Сучасна наука не знає жодного підходу навіть до найпростішого випадку цієї задачі — до питання про те, чи безліч простих чисел виду $x^2 + 1$, тобто в ряду чисел, 2, 5, 10, 17, 26, 37, ...

Ще важчою стає проблема, якщо перейти до многочленів вищого степеня. Досі для жодного многочлена $f(x) = a_0x^n + a_1x^{n-1} + \ldots + a_{n-1}x + a_n$ з цілими коефіцієнтами степеня $n > 1$ не вдалося встановити існування безлічі простих чисел у послідовності $f(1)$, $f(2)$, $f(3)$, ... Отже, сучасна теорія чисел може дослідити розподіл простих чисел тільки в арифметичних прогресіях, та й то далеко не повністю.

Питання розподілу простих чисел розглядають, як бачимо, і за допомогою елементарних методів і методів математичного аналізу. Особливо плодотворним є метод, що грунтується на використанні тотожності:

$$\prod_p \frac{1}{1-\frac{1}{p^s}} = \sum_{n=1}^{\infty} \frac{1}{n^s}$$

(добуток поширюється на всі прості числа), на яку вперше вказав Л. Ейлер. Ця тотожність для дійсного $s \geqslant 1$ виходить після формального перемножування збіжних рядів:

$$\frac{1}{1-\frac{1}{p^s}} = 1 + \frac{1}{p^s} + \frac{1}{p^{2s}} + \ldots$$

(пор. § 47). Вона справедлива і при всіх комплексах s з дійсною частиною, більшою від одиниці. На підставі цієї тотожності питання розподілу простих чисел зводяться до вивчення спеціальної так званої *дзета-функції*, яка визначається рядом

$$\zeta(s) = \sum_{n=1}^{\infty} \frac{1}{n^s} \quad (Re\, s > 1).$$

Контрольні запитання

1. Які числа називаються числами Ферма? Що відомо про ці числа тепер?
2. Які числа називаються числами Мерсенна? Їх число скінченне чи нескінченне?
3. Чи можна побудувати многочлен від одного невідомого x з цілими коефіцієнтами, який набував би значень простих чисел при всіх цілих значеннях x?
4. Сформулюйте постулат Бертрана.
5. Сформулюйте теорему Діріхле про розподіл простих чисел в арифметичних прогресіях.

§ 50. Асимптотичні оцінки функції $\pi(x)$

Дві додатні функції $g(x)$ і $h(x)$, означені для дійсних додатних значень x, називають *асимптотично рівними* якщо

$$\lim_{x\to\infty} \frac{g(x)}{h(x)} = 1.$$

Асимптотичну рівність функцій $g(x)$ і $h(x)$ записують знаком $\sim$. Приклади: $\sin\frac{1}{x} \sim \frac{1}{x}$; $x^3 + 4x^2 + 2\sqrt{x} \sim x^3$.

Природно, що перед ученими XIX ст. виникла проблема знаходження досить простої аналітичної функції $f(x)$, яка асимптотично дорівнювала б $\pi(x)$. Іншими словами, шукана аналітична функція $f(x)$ має бути наближеним виразом функції $\pi(x)$ з як завгодно малою відносною похибкою при досить великих значеннях x, тобто має бути:

$$\lim_{x\to\infty} \frac{\pi(x) - f(x)}{\pi(x)} = \lim_{x\to\infty} \left(1 - \frac{f(x)}{\pi(x)}\right) = 0.$$

Але ця умова еквівалентна такій: $\lim\limits_{x\to\infty} \frac{\pi(x)}{f(x)} = 1$, тобто функції $f(x)$ і $\pi(x)$ повинні бути асимптотично рівні.

Вивчаючи таблиці простих чисел, Лежандр і Гаусс висловили припущення, що функція $\frac{x}{\ln x}$ асимптотично дорівнює $\pi(x)$. Але всі зусилля як Лежандра і Гаусса, так і багатьох інших видатних учених того часу, були марні. У 1849 р. Чебишов показав, що емпірична формула Лежандра

$$\pi(x) \approx \frac{x}{\ln x - 1{,}08366},$$

яка визначає наближено кількість простих чисел, що не перевищують заданого числа x, неправильна. Але основним результатом роботи Чебишова було твердження, що *від $x = 2$ до $x = \infty$ функція $\pi(x)$ задовольняє безліч разів і нерівність*

$$\pi(x) > \int_2^x \frac{du}{\ln u} - \frac{\alpha x}{\ln^n x},$$

і нерівність

$$\pi(x) < \int_2^x \frac{du}{\ln u} + \frac{\alpha x}{\ln^n x},$$

де α — як завгодно мале додатне число і n — *як завгодно велике додатне число.*

Зміст цієї теореми полягає в тому, що функція $\pi(x)$ зростає не повільніше, ніж функція

$$\int_2^x \frac{du}{\ln u} - \frac{\alpha x}{\ln^n x},$$

і не швидше, ніж функція

$$\int_2^x \frac{du}{\ln u} + \frac{\alpha x}{\ln^n x}$$

при як завгодно малому $\alpha > 0$ і як завгодно великому цілому $n > 0$. Звідси, зокрема, випливає, що коли границя

$$\lim_{x \to \infty} \left[\pi(x) : \int_2^x \frac{du}{\ln u} \right],$$

то вона обов'язково дорівнює одиниці.

Отже, Чебишов уперше вказав на зв'язок функції $\pi(x)$ з трансцендентними функціями $\frac{x}{\ln x}$ і $\int_2^x \frac{du}{\ln u}$ («інтегральним логарифмом»). Цей зв'язок саме й полягає в тому, що при великих значеннях x функції $\frac{x}{\ln x}$ і $\int_2^x \frac{du}{\ln u}$ дають значення функції $\pi(x)$ з відносною похибкою, яка прямує до нуля, тобто

$$\lim_{x \to \infty} \left[\pi(x) : \frac{x}{\ln x} \right] = 1$$

$$\lim_{x \to \infty} \left[\pi(x) : \int_2^x \frac{du}{\ln u} \right] = 1. \qquad (1)$$

При цьому похибка при користуванні інтегральним логарифмом менша, ніж для функції $\frac{x}{\ln x}$.

Твердження, що границя відношення $\pi(x) : \frac{x}{\ln x}$ дорівнює одиниці, називають *асимптотичним законом розподілу простих чисел.*

Для прикладу наведемо таку таблицю [1]:

x	$\pi(x)$	$\int_2^x \frac{du}{\ln u}$	$\pi(x) : \int_2^x \frac{du}{\ln u}$	$\pi(x) : \frac{x}{\ln x}$
1 000	168	178	0,94 ...	1,159...
10 000	1 229	1 246	0,98 ...	1,132...
100 000	9 592	9 630	0,996 ...	1,104...
10 000 000	664 579	664 918	0,9994 ...	1,071...
100 000 000	5 761 455	5 762 209	0,99986...	1,061...
1 000 000 000	50 847 478	50 849 534	0,99996...	1,053...

[1] Див.: А. Е. Ингам Распределение простых чисел. Онти, 1936. Подане в цій книзі значення $\pi(10^9) = 50\,847\,478$ неточне. За допомогою електронно-обчислювальної машини було встановлено, що $\pi(10^9) = 50\,847\,534$; знайдено також, що $\pi(10^{10}) = 455\,052\,512$.

Асимптотичні закони (1) розподілу простих чисел тільки в 1896 р. точно довели незалежно один від одного французький математик Адамар і бельгійський математик ла Валле Пуссен. Вони, власне, довели існування границь (1), звідки, згідно з твердженням Чебишова, випливає рівність їх одиниці.

Зауважимо, що методи, якими користувалися Адамар і ла Валле Пуссен, були значно складніші, ніж елементарний метод Чебишова. Основну роль у їхніх побудовах відігравала ріманова аналітична *дзета — функція* $\zeta(s) \sum_{s=1}^{\infty} \frac{1}{n^s}$, де s — комплексне змінне.

Протягом тривалого часу зусилля багатьох математиків були спрямовані на те, щоб спростити доведення Адамара і ла Валле Пуссена. Початкове доведення було дуже спрощене, однак до останнього часу не було відомо доведення асимптотичного закону розподілу простих чисел, яке б не використовувало методів теорії функцій комплексного змінного. Було навіть висловлено припущення, що такого доведення взагалі немає. Тим більшою сенсацією були результати норвезького математика Сельберга (н. 1917) і угорського математика Ердьоша, яким у 1949 р. вдалося дати елементарне (тобто без застосування теорії функцій комплексного змінного) доведення асимптотичного закону розподілу простих чисел.

Зауважимо, що елементарне доведення Сельберга і Ердьоша дуже складне. Це доведення, незважаючи на те, що знайдено ряд його спрощень, і досі залишається більш довгим і заплутаним, ніж доведення, яке використовує теорію функцій комплексного змінного. Однак, принципіальна можливість такого доведення сама по собі цікава. Дальше його спрощення — справа майбутнього.

Дальший розвиток методів, пов'язаних з встановленням такого роду асимптотичних формул, привів до створення *аналітичної теорії чисел*, що включає й такі досягнення, як доведення ряду властивостей системи простих чисел, які до останніх років не досліджувались за допомогою інших засобів.

Контрольні запитання

1. Які функції називаються асимптотично рівними?
2. Чи будуть функції $\sqrt{x^2 + 3x + 5}$ і $x + 7$ асимптотично рівними?
3. У чому полягають асимптотичні закони розподілу простих чисел?

§ 51. Адитивні задачі з простими числами. Проблема Гольдбаха — Ейлера і простих чисел-«близнят»

Адитивна теорія чисел вивчає питання про розбиття чисел на доданки того чи іншого виду. До таких задач належить, наприклад, проблема Е. Варінга (див. «Вступ»). Особливе значення

у теорії простих чисел мають задачі, які групуються навколо славнозвісної проблеми Гольдбаха — Ейлера.

Гольдбах у листі до Л. Ейлера (від 7 червня 1742 р.) висловив припущення, що *кожне натуральне число $n \geqslant 6$ є сумою трьох простих чисел.*

У листі-відповіді Ейлер (30 червня 1742 р.) вказав, що для розв'язання цієї проблеми досить довести, що *кожне парне число $n \geqslant 4$ є сумою двох простих чисел.*

Ці твердження, відомі тепер під назвою проблеми Гольдбаха—Ейлера, або просто проблеми Гольдбаха, можна сформулювати так:

Всяке парне число $n \geqslant 4$ є сумою двох, а непарне $n \geqslant 7$ є сумою трьох простих чисел.

Незважаючи на те, що експериментальною перевіркою цілком підтверджується це твердження, протягом майже двох століть його не вдавалось довести.

Відомий спеціаліст з теорії чисел Ландау поставив таку проблему: довести, що кожне натуральне число можна подати як суму простих чисел, кількість яких не перевищує якогось певного числа; однак і в такому вигляді задача була дуже важкою. Перший істотний внесок у розв'язання цієї проблеми зробив у 1930 р. Шнірельман, який довів, що всяке натуральне число можна подати у вигляді суми не більш як C простих чисел, де C — деяке фіксоване число. Стала C у дослідженнях Шнірельмана була дуже велика, але незабаром у працях різних математиків її вдалося знизити до 67. Тепер методом Шнірельмана знайдено $C = 20$, а якщо брати натуральні числа, починаючи з деякого $N > N_0$, то $C = 18$. Праця Шнірельмана, яка в той час зробила сенсацію в математиці, цікава особливо тим, що розроблені в ній методи стали основою нового напряму в теорії чисел.

Метод доведення Шнірельмана грунтується на запровадженні поняття про «щільність» послідовності натуральних чисел $n_1, n_2, \ldots, n_\nu, \ldots$, по відношенню до чисел натурального ряду. Якщо можна твердити, що відношення $\frac{N(x)}{x}$ числа елементів послідовності $n_1, n_2, \ldots, n_\nu, \ldots$ на відрізку $[1, x]$ до всієї кількості x натуральних чисел залишається не меншим від деякого сталого додатного α, то найбільше α тут називається *щільністю послідовності* $n_1, n_2, \ldots, n_\nu, \ldots$. Невиконання умови $\frac{N(x)}{x} \geqslant \alpha$ для скінченного числа початкових значень істотної ролі не відіграє в одному випадку можна приєднати до послідовності скінченне число нових членів так, щоб умова $\frac{N(x)}{x} \geqslant \alpha$ справджувалась, починаючи з $x = 1$. Елементарно можна показати, що:

1) *всяке натуральне число можна подати у вигляді одного або суми двох елементів будь-якої послідовності, щільність якої більша від $\frac{1}{2}$;*

2) *всяке натуральне число можна подати у вигляді суми обмеженого числа членів будь-якої послідовності додатної щільності.*

Далі основна трудність полягає в тому, що *послідовність простих чисел є послідовністю нульової щільності* (див. § 47). Проте Шнірельману вдалось довести, що послідовність, складена з попарних сум $p_i + p_j$ простих чисел, після приєднання до неї 1, має додатну щільність. Звідси й випливає твердження про подання натуральних чисел у вигляді суми скінченного числа простих чисел.

Метод Шнірельмана застосовується не тільки в задачі Гольдбаха — Ейлера, а й в інших задачах адитивної теорії чисел. Цікаві результати, зв'язані з застосуванням цього методу, дістав Романов, який дослідив множину натуральних чисел, що подаються у вигляді простого числа і числа виду a^n при заданому $a > 1$; він довів, що коли до множини натуральних чисел, які можна подати в зазначеному вигляді, додати число 1, то вийде множина додатної щільності. Він довів, що буде те саме, коли замість степенів заданої основи взяти k-ті степені натуральних чисел ($k \geqslant 1$ — будь-яке ціле число).

У 1937 році була опублікована стаття І. М. Виноградова «Про подання непарного числа сумою трьох простих чисел», де він з допомогою створеного ним аналітичного методу показав, що *будь-яке досить велике непарне число можна подати у вигляді суми трьох, а будь-яке парне число — у вигляді суми не більш як чотирьох простих чисел.*

Цей новий аналітичний метод Виноградова полягає в точній оцінці сум виду

$$\sum_{p<N} e^{2\pi i F(p)},$$

де $F(x)$ — дійсна функція змінного x, а p пробігає прості числа, які не перевищують N. Це є один з найпотужніших методів теорії простих чисел, що відкриває великі можливості для розв'язання багатьох складних проблем. Зокрема, метод Виноградова дає змогу розв'язати ряд задач, які узагальнюють проблему Гольдбаха. Враховуючи історичну важливість проблеми Гольдбаха і величезну кількість затрачених на неї в усьому світі зусиль, слід визнати, що цей результат Виноградова є одним з найвидатніших у теорії чисел за весь час її існування. Інші доведення теореми про подання досить великого непарного числа у вигляді суми трьох простих чисел пізніше дали Лінник і Чудаков (див. «Вступ»). Задача про розбиття парного числа на суму двох простих ще не розв'язана. Слід зауважити, що в деяких своїх частинах ця праця Виноградова йде значно далі від проблеми Гольдбаха — Ейлера. Саме поряд із точним доведенням можливості розкласти ціле число у вигляді суми простих чисел Виноградов знайшов асимптотичну формулу для визначення числа найрізноманітніших зображень натурального числа у вигляді суми простих чисел. Знаходження цієї наближеної формули є значно важча задача, ніж сама проблема Гольдбаха — Ейлера.

Як проблема Гольдбаха — Ейлера, так і проблема чисел-«близнят» тісно пов'язані з питаннями розподілу простих чисел.

Два прості числа, різниця між якими дорівнює двом, називаються *«близнятами»*. Наприклад, числа 3 і 5, 5 і 7, 11 і 13, 17 і 19, 29 і 31 — «близнята»[1]. Серед чисел від 1 до 100 000 є 1224 пари «близнят», а проміжок від 1 до 1 000 000 містить їх 8164 пари. Кількості простих чисел відповідно дорівнюють 9592 і 78 498.

Проблема «близнят» полягає в тому, щоб дізнатись: *скінченною чи нескінченною є множина простих чисел-«близнят»*. Інакше кажучи, *треба або довести, або спростувати, що невизначене рівняння*

$$x - y = 2$$

має безліч розв'язків у простих числах x і y.

Таблиці простих чисел (доведені Голубєвим до 15 з лишком мільйонів) показують, що є дуже великі числа-«близнята» (наприклад, 1 016 957 і 1 016 959) однак це не є доведенням нескінченності їх числа. Проблему «близнят» і тепер не розв'язано, але встановлено (норвезьким математиком Віго Бруном), *що ряд величин, обернених простим числам-«близнятам»*,

$$\frac{1}{3}+\frac{1}{5}+\frac{1}{7}+\frac{1}{11}+\frac{1}{13}+\frac{1}{17}+\frac{1}{19}+\frac{1}{29}+\frac{1}{31}+\cdots,$$

збігається[2]. Це означає, що «близнят», або скінченна множина, або вони в середньому розміщенні порівняно рідко. Відомо, що відношення числа «близнят», які не перевищують N, до числа усіх простих $p \leqslant N$ прямує до нуля із зростанням N.

Проблема «близнят» і проблема будь-якого парного числа у вигляді суми двох простих чисел тісно пов'язані між собою, так що з розв'язання однієї з них випливатиме розв'язання другої.

Зауважимо, що прості числа-«близнята» можна виділити з натурального ряду способом, цілком аналогічним до ератосфенового решета[3]. Цікаве застосування знайшло так зване «велике решето» Лінника.

Нарешті, зазначимо, що задачі адитивної теорії чисел поряд з розподілом простих чисел утворюють другий великий напрям в аналітичній теорії чисел. Тут основними методами є метод утворюючих функцій, який бере свій початок у працях Ейлера, і метод тригонометричних сум, створений Виноградовим. До аналітичної

[1] Неважко довести теорему про те, що числа n і $n+2$ тоді і тільки тоді є числами-«близнятами», коли

$$4[(n-1)!+1]+n \equiv 0 \pmod{n(n+2)},\quad n>1$$

(див., наприклад: Ернст Трост. Простые числа. М., Физматгиз, 1959, стор. 30—31).

[2] Див. Трост Э. Простые числа. М., Физматгиз, 1959.

[3] Див. Бухштаб А. А. Теория чисел, изд. 2. М., «Просвещение», 1966.

теорії чисел належать геометричні числові задачі, задачі підрахунку точок з цілочисловими координатами у плоских або просторових фігурах.

На закінчення наведемо ще ряд задач теорії простих чисел, які чекають свого розв'язання.

1. *Довести, що існує стала k така, що нерівність $p-q<k$ має безліч розв'язків у простих числах p і q.*

2. *Знайти стале число k таке, щоб було безліч пар простих чисел p і q таких, що*

$$p-q=k.$$

3. *Довести, що кожне парне натуральне число являє собою різницю двох простих чисел.*

3. *Довести існування безлічі простих чисел p таких, що $q=\frac{p-1}{2}$ — також просте число.*

5. *Довести, що для будь-якого, як завгодно великого числа n існує n простих чисел p_i таких, що*
$p_{i_2}-p_{i_1}=p_{i_3}-p_{i_2}=\cdots=p_{i_n}-p_{i_{n-1}}$ (запропонував Ердеш).

6. *Довести, що при будь-якому $\varepsilon>0$ кожне натуральне число N, починаючи з деякого N, $N \geqslant N_0$, де $N_0=N(\varepsilon)$, можна подати у вигляді: $N=m+n$, де всі прості дільники чисел m і n не перевищують N^{ε}.*

7. *Довести, що кожне досить велике натуральне число N або саме є квадратом, або подається у вигляді суми $N=p+s^2$, де p — просте число.*

8. *Довести існування безлічі простих чисел, що становлять суму трьох кубів натуральних чисел.*

Останні дві проблеми запропонували Харді і Літлвуд.

Контрольні запитання

1. Сформулюйте проблему Гольдбаха — Ейлера.
2. Яка роль академіка Виноградова в розв'язанні проблеми Гольдбаха — Ейлера?
3. У чому полягає проблема чисел-«близнят»? Чи розв'язана ця проблема?

ІСТОРИЧНІ КОМЕНТАРІ

1. Ще в 1798 р. Лежандр у першому виданні своєї книги «Essai sur la theorie de nombres» опублікував наближену формулу для $\pi(x)$ у вигляді

$$\frac{x}{A\ln x+B}$$

У другому виданні цієї книги він уточнив свою формулу, взявши за A число 1.

Свої міркування про величину функції при великих значеннях x Гаусс повідомив лише в 1849 р., а опублікував у 1863 р., вже після праці Рімана.

У 1849 р. П. Л. Чебишов написав книгу «Теорія конгруенцій». Ця книга являє собою оригінальний і дуже глубокий для того часу курс основ теорії чисел. Як один з додатків до цього курсу є праця П. Л. Чебишова «Про визначення числа простих чисел, які не перевищують даної величини», в якій доводиться теорема про те, що границя відношення $\pi(x)$ до $\frac{x}{\ln x}$ не може бути відмінна від 1.

Праця П. Л. Чебишова «Прості числа», в якій він дає нерівності для функції $\pi(x)$ і доведення постулату Бертрана, опублікована Петербурзькою АН у 1850 р.

2. Теорему про розбіжність ряду величин, обернених простим числам, уперше довів Ейлер у 1737 р.

3. На підставі теореми про те, що $\lim_{x\to\infty}(\pi(x):x)=0$, недавно було доведено, що відношення $\frac{N}{\pi(N)}$ набуває всіх натуральних значень, починаючи з 2. Подано таблицю перших 22-х натуральних чисел N, які діляться на $\pi(N)$.

4. Імовірне припущення про те, що між двома послідовними квадратами x^2 і $(x+1)^2$ завжди знайдеться хоча б одне просте число, залишається досі не доведеним і не спростованим. Інгам довів, що для всіх досить великих x між x^3 і $(x+1)^3$ лежить просте число.

5. Гаусс довів, що правильний m-кутник тоді і тільки тоді можна побудувати за допомогою циркуля й лінійки, коли в канонічному розкладі числа m кожне просте число $p>2$ входить з показником, що дорівнює одиниці і є простим числом Ферма. Серед перших 1000 значень $m\,(m>1)$ є тільки 54 числа такого виду: $2^\alpha p_1 p_2 \ldots p_s$, де всі p_i — прості числа Ферма.

6. У 1878 р. уральський математик І. М. Первушин (1827—1900) довів, що F_{23} ділиться на $5\cdot 2^{25}+1=167772161$. Число F_{23} містить 2 525 223 цифри. Щоб надрукувати це число звичайним шрифтом, потрібен був би рядок завдовжки 5 *км* або книжка звичайного формату в 1000 сторінок.

Німецький математик Зельгоф (1829—1896) показав, що число F_{36} ділиться на $5\cdot 2^{39}+1=2\,748\,779\,069\,441$. Французький математик Люка (1842—1891) знайшов, що це число в десятковому зображенні містить понад 20 млрд. цифр. Запис цього числа був би більший від довжини екватора. Якщо число F_{73} записати в рядок, де кожна цифра матиме ширину в один міліметр, то воно буде в $6\cdot 10^9$ довше, ніж земний екватор. Якщо на кожну цифру, щоб її написати, затрачати хоч півсекунди і писати число протягом цілої доби, то для цього потрібно буде $2\cdot 10^4$ років.

За допомогою електронно-обчислювальних машин було знайдено, що числа F_n при $n=39,\ 55,\ 63,\ 117,\ 125,\ 144,\ 150,\ 207,\ 226,\ 228,\ 268,\ 284,\ 316,\ 452$— складені.

Цікаво зазначити, що для $n>4$ досі невідомі прості числа Ферма F_n.

7. Відомо, що M_p для всіх $p\leqslant 257$, крім вищезазначених ($p=2,\ 3,\ 5,\ 7,\ 13,\ 19,\ 31,\ 61,\ 107,\ 127$), є складеними. Між M_{127} і M_{521} є 66 скадених чисел M_p. Встановлено, що в межах $2300<p<3300$ всі M_p — складені, крім M_{3127}, яке є простим. Це 18-те просте число Мерсенна; його знайшов шведський математик Різель у 1957 р. за допомогою електронно-обчислювальної машини. Відповідне досконале число $S_{18}=2^{3216}(2^{3217}-1)$ див. задачу № 13, розд. II).

8. Відомо, ряд деяких функцій $f(x)$, які набувають при всіх натуральних значеннях аргументу x тільки простих значень. Так, наприклад, Мілле у 1947 р. довів, що дійсне α таке, що $f(x)=[\alpha^{3^x}]$ при всіх натуральних x набуває значень, які являють собою прості числа. У 1951 р. Нівен дещо уточнив цю теорему, показавши, що для будь-якого $c>\frac{8}{3}$ α таке, що $[\alpha^{c^x}]$ при всіх натуральних x завжди просте число.

9. П. Л. Чебишов не тільки довів постулат Бертрана, а й дістав кращий результат, а саме: він довів, що число простих чисел в інтервалі $(n,\ 2n-2)$ необмежено збільшується при збільшенні величини n

10. Теорему Діріхле для випадку $b=1$ висловив у 1755 р. Ейлер. Лежандр у своїй книзі «Theorie des nombres» (1808) навів доведення так званої теореми Діріхле, однак це доведення спиралось на одне допоміжне припущення, яке, як було з'ясовано пізніше, виявилось неправильним.

Доведення Діріхле істотно спростив німецький математик Ландау (1877—1938).

Перше елементарне доведення теореми Діріхле, для загального випадку, дав А. Сельберг. Елементарні доведення існування безлічі простих чисел для дуже багатьох арифметичних прогресій окремого виду були знайдені до Сельберга різними авторами, наприклад, було відоме елементарне доведення для всіх прогресій виду $ax\pm 1$ $(x=1,\ 2,\ 3\ldots)$.

Особливо цікавим є питання про найменше просте число, що входить в дану арифметичну прогресію. Ю. В. Лінник дістав такий важливий результат: існує така абсолютна стала c_0, що для будь-якого натурального a в кожній арифметичній прогресії $ax+b$, де $(a,\ b)=1$ є просте число $p<a^{c_0}$. Тепер обчислено, що для досить великих a стала c_0 така, що $c_0<10^4$ і навіть $1<c_0<5448$.

Згідно з гіпотезою Човла найменше просте число в прогресії $ax+b$ не перевищує $b^{1+\varepsilon}$ для будь-якого $\varepsilon>0$ і всіх досить великих a.

Таблиці простих чисел у широких межах показують переважання кількості простих чисел $4x+3$ над числами виду $4x+1$. Проте було з'ясовано, що таке переважання не триватиме необмежено довго.

11. П. Л. Чебишов перший застосував ξ-функцію і за її допомогою дістав нові результати з питання розподілу простих чисел. Він розглядав поводження функції $\xi(s)$ поблизу від її єдиного полюса $s=1$ при дійсних значеннях s і користувався похідними від $\xi(s)$ і $\ln\xi(s)$.

Ріман вказав на важливість вивчення $\xi(s)$ при комплексних s. Він висловив гіпотезу про те, що всі корені рівняння $\zeta(s)=0$, які лежать у правій півплощині, мають дійсну частину, що дорівнює $\frac{1}{2}$. Цю гіпотезу й досі не доведено; її доведення дало б багато в розв'язанні питання про розподіл простих чисел.

12. Ще Ріман вивів формулу, яка встановила безпосередній зв'язок між $\pi(x)$ і нулями $\xi(s)$, що лежать у критичній смузі. Формулу Рімана повністю обгрунтував у 1894 р. Мангольд.

Оцінка різниці між $\pi(x)$ і $\int_2^x \frac{du}{\ln u}$ залежить від того, наскільки віддалені від прямої $\sigma=1$ нулі $\xi(s)$.

Дальші зусилля досі були спрямовані на якомога точнішу оцінку різниць:

$$\left[\pi(x):\frac{x}{\ln x}\right]-1 \quad \text{і} \quad \left[\pi(x):\int_2^x\frac{du}{\ln u}\right]-1,$$

які, згідно з сказаним вище, нескінченно малі при $x\to\infty$. Визначних результатів у цьому питанні досягла за останні роки радянська школа теорії чисел, яку очолює І. М. Виноградов. Так, наприклад, М. Г. Чудаков у 1936 р. довів, що

$$\pi(x)=\int_2^x\frac{du}{\ln u}+O\left(xe^{-\alpha(\ln x)^\mu}\right),\quad \mu=\frac{1}{2}+\frac{1}{42}-\varepsilon,$$

де α — додатна стала, а символ O має такий зміст: припустимо, що $f(x)$ і $g(x)$ є функція дійсного змінного x, означені при $x \geqslant a$, і функція $g(x)$ додатна; якщо відношення $\frac{|f(x)|}{g(x)}$ для всіх досить великих значень x менше від деякої сталої C, яка не залежить від x, то записують $f(x) = O(g(x))$.

Останні праці Виноградова і Коробова дали таку оцінку:

$$\pi(x) \int_2^x \frac{du}{\ln u} + O\left(xe^{-\alpha(\ln x)^{\frac{3}{5}}}\right).$$

Якщо позначити через $\pi_b(a, x)$ кількість простих чисел у прогресії $ay + b$, $(a, b) = 1$ $(b, b+a, b+2a, \ldots)$, менших або таких, що дорівнюють x, то за теоремою Діріхле матимемо: $\lim_{x \to \infty} \pi_b(a, x) = \infty$. Для функції $\pi_b(a, x)$ так само як і для функції $\pi(x)$ ставиться проблема визначення порядку зростання при збільшенні x. Методи, за допомогою яких було визначено порядок зростання $\pi(x)$, були застосовані до функції $\pi_b(a, x)$, і ла Валле Пуссен довів таку теорему:

При будь-яких сталих взаємно простих a і b справедлива асимптотична рівність

$$\pi_b(a, x) \sim \frac{1}{\varphi(a)} \int_2^x \frac{du}{\ln u}, \tag{1}$$

де $\varphi(a)$ — *функція Ейлера.*

З цієї теореми випливає також, що

$$\pi_b(a, x) \sim \frac{1}{\varphi(a)} \frac{x}{\ln x}. \tag{2}$$

Проте оцінка (1) точніша, ніж (2), у тому розумінні, що різниця між лівою і правою частинами в (1) за модулем менша, ніж у (2). Доведення асимптотичного закону розподілу простих чисел, подане А. Сельбергом і П. Ердьошем, грунтується на використанні тотожності

$$\sum_{p \leqslant x} \ln^2 p + \sum_{pq \leqslant x} \ln p \ln q = 2x \ln x + 0(x),$$

де p і q прості числа. Ця тотожність називається тотожністю Сельберга. З часу виходу в світ праці Сельберга і Ердьоша з'явилось кілька різних варіантів елементарного доведення асимптотичного закону розподілу простих чисел.

13. У 1931 р. Естерман довів, що кожне натуральне число, більше за 1, можна подати у вигляді суми простого числа і числа, вільного від квадратів, і дав асимптотичну формулу виразів для зображень такого числа.

14. У 1952 р. К. Прахар довів, що нескінченна множина чисел k таких, що рівняння $x - y = 2k$ має нескінченну множину розв'язків у простих числах x і y.

15. У 1959 р. Лінник розв'язував проблему, поставлену в 1923 р. англійськими математиками Харді і Літлвудом, тобто, йому вдалося довести теорему: кожне досить велике натуральне число n можна подати у вигляді суми простого числа і суми двох квадратів цілих чисел, тобто у вигляді

$$n = p + k^2 + l^2.$$

16. У 1963 р. Б. М. Бредіхін, розвиваючи метод Лінника, довів узагальнення теореми Лінника, а саме, що кожне досить велике число N можна подати у вигляді $N = p + f(k, l)$, де p — просте число $f(k, l) = ak^2 + bkl + cl^2$ — примітивна додатно визначена форма, $0 < f(k, l) < N$. Він же сформулював і ряд інших теорем такого типу.

17. Існує алгоритм (решето) для знаходження чисел — «близнят» і для розв'язання рівняння Гольдбаха — Ейлера $p + p' = 2N$.

Аналогічне решето можна побудувати і для інших адитивних задач з простими числами. Таке решето часто називають подвійним ератосфеновим решетом (для «просіювання» кожного з простих чисел $p_i \leqslant \sqrt{N}$). Таке решето вперше побудував французький математик Марлінг (він загинув на фронті під час першої світової війни; і праця його залишилась незакінченою).

У 1957 р. за допомогою електронно-лічильної машини дістали найбільшу з відомих тепер пар «близнят»: 157131437 і 157131439. У 1959 р. було опубліковано таблицю простих чисел — «близнят» до 1000000.

Багато зробив щодо розв'язання проблеми чисел «близнят» О. В. Голубєв. Він узагальнив її також на «згущення простих чисел», а саме на «трійки», «четвірки», «п'ятірки» і т. д. простих чисел з мінімальними інтервалами між ними, як, наприклад, трійка 11, 13, 17 або трійка 37, 41, 43; четвірка 7, 11, 13, 17 і т. д. Голубєв висловив гіпотезу, яка грунтується на спостереженнях, що «близнята» розподілені серед простих чисел за тим самим законом, що й прості числа серед натуральних чисел.

18. Грунтуючись на своєму узагальненні «великого решета» Ю. В. Лінника, угорському математикові Реньї у 1948 р. вдалося показати існування такої сталої e, що будь-яке досить велике парне число $2N$ можна подати у вигляді: $2N = p + n$, де p — просте, а n складається не більш як з l простих множників.

У 1964 р. А. А. Бухштаб довів теорему Реньї для значення $l = 3$. Аналогічну теорему він довів і для простих чисел-«близнят».

Методом решета можна довести: кожне досить велике парне число $2N$ допускає вираження у формі $2N = a^{(r)} + b^{(s)}$, де $a^{(r)}$ — складене число, що складається не більш як з r простих множників ($a^{(1)} = p$, $a^2 = p^2$ або $p_1 p_2$ і т. д.

ВКАЗІВКИ І РОЗВ'ЯЗАННЯ ДЕЯКИХ ЗАДАЧ

Розділ 1

1. Припустимо, що n, $n+1$ і $n+2$ — три послідовні цілі числа. Якщо n і $n+1$ не діляться на 3, то

$$n = 3k + 1,\ n + 1 = 3k + 2,\ n + 2 = 3k + 3 = 3(k + 1),$$

тобто $n + 2$ ділиться на 3.

2. Число $N = n(n+1))(n+2)$ за доведеним ділиться на 3. Далі, N ділиться на 2, бо одне з двох послідовних цілих чисел n, $n+1$ — парне. Тому N ділиться на 6.

21. Позначимо суму $\frac{1}{2} + \frac{1}{3} + \cdot \cdot \cdot + \frac{1}{n}$ через S. Нехай k — ціле невід'ємне число, для якого $2^k \leqslant n$, але $2^{k+1} > n$. Позначимо через P добуток усіх непарних чисел, які не перевищують n. Оскільки S можна записати у вигляді $S = S_1 + \frac{1}{2^k}$, де S_1 — сума усіх доданків, крім $\frac{1}{2^k}$, то

$$2^{k-1} PS = 2^{k-1} PS_1 + \frac{1}{2} P.$$

Але $2^{k-1}\,PS_1$ — ціле, $\frac{1}{2}\,P$ — не ціле внаслідок непарності P. Отже, $2^{k-1}PS$ не може бути цілим. Звідси S тим більше не може бути цілим.

22. Позначимо суму $\frac{1}{3}+\frac{1}{5}+\cdots+\frac{1}{2n+1}$ через S. Нехай k — найбільше ціле при умові $3^k \leqslant 2n+1$ і P — добуток усіх взаємно простих з 6 чисел, які не перевищують $2n+1$. Як і в попередній задачі, число $3^{k-1}PS$ можна подати сумою, всі доданки якої крім $\frac{P}{3}$, — цілі числа.

23. Якщо $n=ab$, b — непарне >1, то

$$2^n+1=2^{ab}+1=(2^a+1)\,[2^{a(b-1)}-2^{a(b-2)}+\cdots-2^a+1],$$

а тому 2^n+1 — складене число.

24. Якщо $n=ab$, $a>1$, $b>1$, то

$$2^n-1=2^{ab}-1=(2^a-1)\,[2^{a(b-1)}+2^{a(b-2)}+\cdots+2^a+1].$$

25. Всяке просте число, починаючи з 5, є число виду $6m+1$ або $6m-1$; припустимо всупереч висловленому твердженню, що існує найбільше число $p=P$ виду $6m-1$ і позначимо через π добуток усіх простих чисел, які не перевищують P. Потім напишемо

$$N=\pi-1=2\cdot 3\cdot 5\ldots P-1.$$

Це число є число виду $6m-1$, всі його прості дільники виду $6m+1$ або $6m-1$. Оскільки добуток чисел виду $6m+1$ є число також виду $6m+1$, то число N має простий дільник p^* виду $6m-1$. З другого боку, N не ділиться на жодне з простих чисел $2, 3, \ldots, P$. Тому $p^*>P$, що суперечить нашому припущенню.

26. Доведення аналогічне попередньому.

29. Для $k=2$, 3 твердження перевіряється безпосередньо. Нехай наше твердження справедливе для k, покажемо його справедливість для $k+1$. З припущення випливає, що число $n=p_1^{\alpha_1}p_2^{\alpha_2}\cdots p_k^{\alpha_k}\,2^{k-1}$ способами розкладається на добуток двох взаємно простих множників. Нехай одна з пар таких множників буде a і b. Тоді для числа

$$n_1=p_1^{\alpha_1}p_2^{\alpha_2}\cdots p_k^{\alpha_k}p_{k+1}^{\alpha_{k+1}}$$

дістанемо відповідно дві пари таких множників: ap_{k+1}, b і a, bp_{k+1}, тобто всього множників матимемо: $2^{k-1}\cdot 2=2^k$.

31. Нехай

$$\frac{a_1}{b_1}\pm\frac{a_2}{b_2}\pm\cdots\pm\frac{a_n}{b_n}=q$$

ціле число. Помножаючи на $b_2b_3\ldots b_n$, дістанемо, що $\frac{a_1b_2\cdots b_n}{b_1}$ — ціле, що неможливо, бо $a_1, b_2, \ldots, b_n$ взаємно прості з b_1 за умовою.

32. Без обмеження загальності можна вважати $(x, y)=1$ і x непарним: тоді

$$z^2-y^2=(z-y)(z+y)=x^2.$$

Припускаючи, що

$$z+y=a\delta^2,\quad z-y=b\delta^2,$$

де $(a, b)=1$, дістанемо, що $ab\delta^2=x^2$, отже, $a=u^2$, $b=v^2$, де u і v — непарні натуральні числа, причому $u>v$.

Отже, матимемо:

$$\ldots+\ldots$$

$$x=\delta uv,\quad y=\delta\frac{u^2-v^2}{2},\quad z=\delta\frac{u^2+v^2}{2}.$$

Оскільки за припущенням $(x, y)=1$, то $\delta=1$, і ми дістанемо шукані формули.

Розділ II

11. а) Справді при цій умові матимемо:

$$S(n)=S(2^k\cdot p)=\frac{2^{k+1}-1}{2-1}\;\frac{p^2-1}{p-1}=(2^{k+1}-1)(p+1)=p\cdot 2^{k+1}=2n,$$

тобто $S(n)=2n$, а це й доводить наше твердження.

б) Справді, припустимо, що $n=2^k\cdot u$, $k\geqslant 1$ і u — непарне число, тоді

$$S(n)=(2^{k+1}-1)\;S(u).$$

Припустимо тепер, що n — досконале, тобто $S(n)=2n$, тоді матимемо:

$$2^{k+1}\cdot u=(2^{k+1}-1)\cdot S(u),\quad \text{або}\quad \frac{u}{S(u)}=\frac{2^{k+1}-1}{2^{k+1}}.$$

У правій частині останньої рівності стоїть нескоротний дріб, а тому

$$u=(2^{k+1}-1)\cdot t, \tag{1}$$

$$S(u)=2^{k+1}\cdot t, \tag{2}$$

де t — деяке натуральне число. Оскільки u є числом виду (1), то до суми дільників $S(u)=\sum_{d\mid n} d$, безперечно, входять як доданки два різних дільники: t і $(2^{k+1}-1)\,t>t$. Але вже їхня сума дає значення $2^{k+1}\cdot t$, яке дорівнює, згідно з (2), сумі $S(u)$. Тому u не має жодних інших натуральних дільників, крім t і $(2^{k+1}-1)\,t=u$.

Але тільки прості числа p мають точно два натуральних дільники 1 і p, отже, $u=p=2^{k+1}-1$ є просте число. Звідси й випливає справедливість нашого твердження.

Отже, досконалі числа n виду $n=2^k\cdot p$ утворюватимуться тільки при таких значеннях k, які перетворюють вираз $2^{k+1}-1$ у просте число p.

в) Справді, нехай $p_{k+1}=a\;\;b$; $a>0$, $b>0$. Тоді

$$2^{k+1}-1=2^{ab}-1=(2^a-1)(1+2^a+\cdots+2^{a(b-1)})$$

буде складеним числом.

12. Усіх натуральних чисел від 1 до x буде, очевидно, $[x]$; натуральних $\leqslant x$ і кратних деякому простому p_i, буде $\left[\frac{x}{p_i}\right]$ (див. властивість 3, § 11). Отже, щоб знайти шукану кількість $B(x; p_1, p_2, \ldots, p_k)$, треба скласти різницю:

$$[x]-\left[\frac{x}{p_1}\right]-\left[\frac{x}{p_2}\right]-\cdots-\left[\frac{x}{p_k}\right]. \tag{3}$$

Проте цей вираз ще не відповідає шуканому значенню $B(x; p_1, p_2\ldots, p_k)$, бо числа, кратні одночасно двом простим числам p_i і p_j, ми враховували не один раз, а двічі, а саме: вперше, коли розглядали $\left[\frac{x}{p_i}\right]$, і вдруге, коли

розглядали $\left[\frac{x}{p_j}\right]$. Отже треба внести поправку — додати ще вирази $\left[\frac{x}{p_1p_2}\right]$, $\left[\frac{x}{p_1p_3}\right], \ldots, \left[\frac{x}{p_{k-1}p_k}\right]$, де $\left[\frac{x}{p_ip_j}\right]$ — кількість натуральних чисел, які кратні добутку p_ip_j і не перевищують x. Але й після цього ще не буде шуканого значення $B(x; p_1, \ldots, p_k,)$ бо, додаючи додаткові члени $\left[\frac{x}{p_ip_j}\right]$, ми знов таким способом не виключили ті числа, які одночасно діляться на три простих числа. Тому, щоб виправити допущену похибку, слід відняти

$$\left[\frac{x}{p_1p_2p_3}\right], \left[\frac{x}{p_1p_2p_4}\right], \ldots, \left[\frac{x}{p_{k-2}p_{k-1}p_k}\right]$$

і т. д.

Діючи так, внесемо останню поправку:

$$(-1)^k\left[\frac{x}{p_1p_2\cdots p_k}\right].$$

Вносячи цю поправку, ми справді виключимо всі натуральні числа, що перевищують x і діляться принаймні на одне з простих чисел $p_1, p_2, \ldots, p_k$. Отже, припустимо, що деяке натуральне $a \leqslant x$ кратне, наприклад, кожному з перших s простих чисел $p_1, p_2, \ldots, p_s$, а на решту простих чисел $p_{s+1}, \ldots, p_k$ вже не ділиться ($s \leqslant k$). Через те що $1 \leqslant a \leqslant x$, то в першому рядку правої частини рівності (3) a враховано один раз, оскільки a ділиться на кожне з чисел $p_1, p_2, \ldots, p_s$, то воно враховується в другому рядку C_s^1 раз; оскільки a кратне p_ip_j ($1 \leqslant i, j \leqslant s, i \neq j$), то воно враховується в третьому рядку C_s^2 раз і т. д. Нарешті, через те що a кратне добутку $p_1p_2 \ldots p_s$, то воно враховується в s-му рядку C_s^s раз. У дальших рядках правої частини рівності (3) число a вже, очевидно, не враховується, бо воно ділиться тільки на $p_1, p_2, \ldots, p_s$. Отже, число a буде враховане у формулі (3) всього $1 - C_s^1 + C_s^2 - \ldots + (-1)^sC_s^s = (1-1)^s = 0$ раз, тобто цілком виключиться. З другого боку, числа, які не діляться на $p_1, p_2, \ldots, p_k$, враховуються по одному разу в першому доданку $[x]$, в решті доданків формули (3) їх не враховують. Отже, вся права частина рівності (3) визначає кількість натуральних чисел, менших або таких, що дорівнюють x які не діляться на прості числа $p_1, p_2, \ldots, p_k$, те саме визначає і ліва частина.

13. Очевидно, що $\varphi(n) = B(n; p_1, p_2, \ldots, p_k)$, бо всяке натуральне число тоді і тільки тоді взаємно просте з n, коли воно не ділиться на жодний простий множник числа n. Отже, до $\varphi(n)$ можна застосувати формулу (3) і, враховуючи, що всі числа n, $\frac{n}{p_i}$, $\frac{n}{p_ip_j}$, ..., $\frac{n}{p_1p_2\ldots p_k}$ — цілі, бо n ділиться на $p_1, p_2, \ldots, p_k$ за умовою, дістанемо:

$$\varphi(n) = n - \frac{n}{p_1} - \frac{n}{p_2} - \ldots \frac{n}{p_k} + \frac{n}{p_1p_2} + \ldots + \frac{n}{p_{k-1}p_k} - \ldots + (-1)^k\frac{n}{p_1p_2\ldots p_n},$$

або

$$\varphi(n) = n\left[1 - \frac{1}{p_1} - \frac{1}{p_2} - \ldots - \frac{1}{p_k} + \frac{1}{p_1p_2} + \ldots + \frac{1}{p_{k-1}p_k} - \ldots + (-1)^k\frac{1}{p_1p_2\ldots p_k}\right].$$

Неважко побачити, що вираз, який стоїть у квадратних дужках, дорівнює:

$$\left(1-\frac{1}{p_1}\right)\left(1-\frac{1}{p_2}\right)\ldots\left(1-\frac{1}{p_k}\right).$$

Отже, остаточно дістанемо

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

Це й треба було довести.

16. Відомо, що всі прості дільники числа $N = [x]$ не перевищують $\sqrt{N} = \sqrt{[x]}$; $B(x; p_1, p_2, \ldots, p_k)$ означатиме кількість чисел, які не перевищують x і які не діляться на $p_1, p_2, \ldots, p_k$, тобто це будуть (крім 1) прості числа, що не перевищують x і відмінні від $p_1, p_2, \ldots, p_k$. Приєднуючи до них ще k простих чисел $p_1, p_2, \ldots, p_k$ і виключаючи 1, дістанемо потрібний результат.

18. $$B(x; a_1, a_2, \ldots, a_k) = x - \left(\frac{x}{a_1} + \frac{x}{a_2} + \ldots + \frac{x}{a_k}\right) +$$
$$+\left(\frac{x}{a_1a_2} + \ldots + \frac{x}{a_{k-1}a_k}\right) - \ldots + (-1)^k\frac{x}{a_1a_2\ldots a_k} = x\left[1 - \frac{1}{a_1} -\right.$$
$$\left. - \frac{1}{a_2} - \ldots - \frac{1}{a_k} + \frac{1}{a_1a_2} + \ldots + \frac{1}{a_{k-1}a_k} - \ldots + (-1)^k\frac{1}{a_1a_2\ldots a_k}\right] =$$
$$= x\left(1-\frac{1}{a_1}\right)\left(1-\frac{1}{a_2}\right)\ldots\left(1-\frac{1}{a_k}\right).$$

23. У першому випадку всі натуральні числа, взаємно прості з m, будуть взаємно простими з n, і навпаки. Всякому $\alpha < m$ і взаємно простому з m відповідатиме p чисел:

$$\alpha, m+\alpha, 2m+\alpha, \ldots, (p-1)m+\alpha, \qquad (1)$$

менших від n і взаємно простих з m, а тому і з n. Отже, усіх чисел, менших від n і взаємно простих з n, буде:

$$\varphi(m)\cdot p = \varphi(mp) = \varphi(n).$$

А в другому випадку в системі чисел (1), що містить за довільним підрахунком q $\varphi(m)$ елементів, треба буде додатково закреслити усі числа, кратні q. Але в системі чисел, взаємно простих з m і менших від $n = mq$, містяться ті і тільки ті кратні числа q:

$$q, \alpha_1q, \alpha_2q, \ldots,$$

в яких множники $\alpha_1, \alpha_2, \ldots$, з одного боку, взаємно прості з m, а з другого — менші від m. Отже, в цьому випадку дістанемо:

$$\varphi(n) = \varphi(mq) = q \quad \varphi(m) - \varphi(m) = \varphi(m)(q-1).$$

24. $\varphi(mp^2) = \varphi(mp \quad p) = \varphi(mp)\,p = \varphi(m) \quad p\,(p-1)$;
$\varphi(mp^3) = \varphi(mp^2 \quad p) = \varphi(mp^2)\,p = \varphi(m)\,p^2\,(p-1)$; ...

25. Із задачі 24 випливає, що $\varphi(p^k) = p^{k-1}(p-1)$. Якщо тепер $n = p_1^{\alpha_1}p_2^{\alpha_2} \ldots p_k^{\alpha_k}$ — канонічний розклад числа n, то

$$\varphi(n) = p_1^{\alpha_1-1}(p_1-1)\,p_2^{\alpha_2-1}(p_2-1)\ \ldots\ p_k^{\alpha_k-1}(p_k-1) =$$
$$= n\left(1-\frac{1}{p_1}\right)\left(1-\frac{1}{p_2}\right)\ldots\left(1-\frac{1}{p_k}\right).$$

30. Необхідно, щоб x було парним, бо в противному разі матимемо: $\varphi(2)\varphi(x) = \varphi(3)\varphi(x)$ або $\varphi(2) = \varphi(3)$ (це якщо x не ділиться на 3); а коли $x \vdots 3$, тоді $x = 3^\beta \cdot x_1$ і $\varphi(2)\varphi(3^\beta)\varphi(x_1) = \varphi(3^{\beta+1})\varphi(x_1)$; $3^{\beta-1}\cdot 2 = 3^\beta$ 2, або $\beta = \beta - 1$ (абсурд!). Отже, $x = 2^\alpha y$, де $\alpha > 0$ і y — натуральне число, яке не ділиться на 2;

б) x не може бути кратним ні 7, ні 5, тобто $(x, 7) = 1$ і $(x, 5) = 1$, але тоді дістанемо неможливу рівність при будь-якому x:

$$\varphi(5)\varphi(x) = \varphi(7)\varphi(x), \text{ або } \varphi(5) = \varphi(7)!$$

34. Нехай k — ціле, таке, що $0 < k \leqslant \frac{n}{\delta}$ і $\left(k, \frac{n}{\delta}\right) = 1$. Для цього k складемо число $a = k\delta$ $(a = 1, 2, \ldots, n)$. Легко побачити, що $0 < a \leqslant n$

$$(a, n) = (k\delta, n) = \delta\left(k, \frac{n}{\delta}\right) = \delta.$$

Отже, число a належить до класу чисел, що мають з n один і той самий найбільший спільний дільник δ. Навпаки, нехай a — довільне число розглядуваного класу; тоді $(a, n) = \delta$, звідки $\left(\frac{a}{\delta}, \frac{n}{\delta}\right) = 1$. Отже, припускаючи, що $\frac{a}{\delta} = k$, можемо написати, що $\left(k, \frac{n}{\delta}\right) = 1$, причому $0 < k \leqslant \frac{n}{\delta}$, бо $0 < a \leqslant n$. Тому в розглядуваному класі є стільки чисел a, скільки буде чисел $k \leqslant \frac{n}{\delta}$ і взаємно простих з $\frac{n}{\delta}$, тобто $\varphi\left(\frac{n}{\delta}\right)$.

35. Усіх чисел $a = 1, 2, \ldots, n$ є n. До кожного класу, який характеризується умовою $(a, n) = \delta$, входить $\varphi\left(\frac{n}{\delta}\right)$ з цих чисел, тому $\sum_{\delta/n} \varphi\left(\frac{n}{\delta}\right) = n$.

Останню рівність можна переписати у вигляді: $\sum_{d/n} \varphi(d) = n$.

Розділ III

8. Припустимо, що x, y — будь-які цілі числа. Якщо вони обидва парні або непарні, то $x^2 + y^2$ буде парним. А коли, наприклад, x — парне, а y — непарне, то $x^2 \equiv 0 \pmod 4$, а $y^2 \equiv 1 \pmod 4$ і $x^2 + y^2 \equiv 1 \pmod 4$. Отже, ніколи не буває, щоб $x^2 + y^2 \equiv 3 \pmod 4$.

9. Усі непарні числа за модулем 8 можна подати у формі $8k \pm 1$ або $8k \pm 3$, але $(8k \pm 1)^2 \equiv 1 \pmod 8$ і $(8k \pm 3)^2 \equiv 1 \pmod 8$.

11. $(a+b)^p = a^p + pa^{p-1}b + \frac{p(p-1)}{2}a^{p-2}b + \ldots + b^p$; нехай p — просте, тоді всі коефіцієнти в другій частині, крім крайніх, діляться на p, тому можна написати: $(a+b)^p \equiv a^p + b^p \pmod p$ при будь-яких цілих a і b.

Замінивши тепер b через $b + c$, дістанемо:

$$(a+b+c)^p \equiv a^p + (b+c)^p \equiv a^p + b^p + c^p \pmod p.$$

Взагалі: $(a+b+\ldots+l)^p \equiv a^p + b^p + \ldots + l^p \pmod p$. Припускаючи тепер, що $a = b = \ldots = l = 1$, і припускаючи потім, що число таких одиниць дорівнює довільному натуральному числу a, дістанемо: $a^p \equiv a \pmod p$.

12. З $a \equiv b \pmod{p^n}$ випливає, що $a = b + lp^n$; піднісши обидві частини цієї рівності до p-го степеня, дістанемо:

$$a^p = b^p + pb^{p-1}lp^n + \frac{p(p-1)}{2}b^{p-2}l^2p^{2n} + \ldots$$

Кожний член у другій частині рівності, крім першого, ділиться на p^{n+1}. Тому справедлива конгруенція $a^p \equiv b^p \pmod{p^{n+1}}$. Беручи останню конгруенцію за вихідну і повторюючи попередній прийом, матимемо: $a^{p^2} \equiv b^{p^2} \pmod{p^{n+2}}$ і т. д., нарешті, дістанемо, що

$$a^{p^m} \equiv b^{p^m} \pmod{p^{n+m}}.$$

Припустивши тепер, що $m = p_1^{\alpha_1}p_2^{\alpha_2}\ldots p_k^{\alpha_k}$,

за теоремою Ферма маємо:

$$a^{p_1-1} \equiv 1 \pmod{p_1},\ a^{p_2-1} \equiv 1 \pmod{p_2},\ \ldots,\ a^{p_k-1} \equiv 1 \pmod{p_k}.$$

Застосовуючи до кожної з цих конгруенцій знайдений вище результат, дістанемо:

$$a^{p_1^{\alpha_1-1}(p_1-1)} \equiv 1 \pmod{p_1^{\alpha_1}},\ \ldots,\ a^{p_k^{\alpha_k-1}(p_k-1)} \equiv 1 \pmod{p_k^{\alpha_k}}$$

Підносячи обидві частини кожної з цих конгруенцій до відповідного степеня, дістанемо:

$$a^{\varphi(m)} \equiv 1 \pmod{p_1^{\alpha_1}},\ \ldots,\ a^{\varphi(m)} \equiv 1 \pmod{p_k^{\alpha_k}}.$$

звідки

$$a^{\varphi(m)} \equiv 1 \pmod{p_1^{\alpha_1}p_2^{\alpha_2}\ldots p_k^{\alpha_k}}, \text{ або } a^{\varphi(m)} \equiv 1 \pmod m.$$

13. Насамперед треба показати, що p є простим тоді і тільки тоді, коли C_p^k ділиться на p $(k = 1, 2, \ldots, p-1)$.

15. Скориставшись властивістю повної системи лишків, а саме: нехай x пробігає повну систему лишків за модулем m, тоді $ax + b$ також пробігатиме повну систему лишків за цим модулем; найменший невід'ємний лишок r чисел $ax + b$ пробігатиме значення $0, 1, 2, \ldots, m-1$. Тому

$$\sum_x \left\{\frac{ax+b}{m}\right\} \equiv \sum_{r=0}^{m-1} \frac{r}{m} = \frac{1}{2}(m-1) \pmod m.$$

16. Зазначеним способом дістанемо $m_1m_2\ldots m_k$ чисел, неконгруентних між собою за модулем $m_1m_2\ldots m_k$, бо з

$$x_1 + m_1x_2 + m_1m_2x_3 + \ldots + m_1m_2\ldots m_{k-1}x_k \equiv x_1' + m_1x_2' + m_1m_2x_3' + \ldots + m_1m_2\ldots m_{k-1}x_k' \pmod{m_1m_2\ldots m_k}$$

послідовно знаходимо

$$x_1 \equiv x_1' \pmod{m_1},\ x_1 = x_1';\ m_1x_2 \equiv m_1x_2' \pmod{m_2},\ x_2 = x_2';$$

і т. д.

17. а) Зазначеним способом дістанемо $m_1m_2\ldots m_k$ чисел, не конгруентних за модулем $m_1m_2\ldots m_k$, бо з

$$\mu_1x_1 + \ldots + \mu_kx_k \equiv \mu_1x_1' + \ldots + \mu_kx_k' \pmod{m_1m_2\ldots m_k}$$

випливало б (усяке μ_l, відмінне від μ_s кратне m_s)

$$\mu_sx_s \equiv \mu_sx_s' \pmod{m_s},\ x_s \equiv x_s' \pmod{m_s};$$

б) доведення аналогічне.

18. Доведемо спочатку першу частину. За умовою x набуває a значень, y — b значень; комбінуючи кожне значення x з кожним значенням y дістанемо ab значень для z. Покажемо тепер, що жодні два з цих значень z не конгруентні між собою за модулем ab.

Припустимо супротивне.

Нехай $z_1 = ay_1 + bx_1$, $z_2 = ay_2 + bx_2$ і нехай

$$ay_1 + bx_1 \equiv ay_2 + by_2 \pmod{ab}.$$

Тоді за властивістю конгруенцій: $ay_1 + bx_1 \equiv ay_2 + by_2 \pmod{a}$, $ay_1 + bx_1 \equiv ay_2 + by_2 \pmod{b}$. Звідси (на підставі висновку 3 з властивості 2, § 15) маємо

$$bx_1 \equiv bx_2 \pmod{a}, \quad ay_1 \equiv ay_2 \pmod{b}.$$

Але $(a, b) = 1$, тому $x_1 \equiv x_2 \pmod{a}$, $y_1 \equiv y_2 \pmod{b}$, що неможливо, бо x_1 і x_2 — числа повної системи лишків за модулем a і y_1, y_2 — числа повної системи лишків за модулем b. Цим першу частину теореми доведено.

Доведемо тепер другу частину твердження. Нехай $z = ay + bx$ взаємно просте з ab, а отже і з a, і з b окремо; тоді $z - ay = bx$ взаємно просте з a, тобто $(x, a) = 1$. Аналогічно, $z - bx = ay$ взаємно просте з b тобто $(y, b) = 1$.

Нехай тепер, навпаки, $(x, a) = 1$ і $(y, b) = 1$. Тоді, очевидно, $z = ax + by$ буде взаємно простим і з a, і з b, отже, і з ab. Цим доведено і другу частину твердження.

Розділ IV

8. Оскільки при простому p справедлива конгруенція $C_{p-1}^{a} \equiv (-1)^a \pmod{p}$ (див. задачу 14, розд. III), то

$$1 \cdot 2 \cdot \ldots \cdot (a-1)\, ab\, (-1)^{a-1} \frac{(p-1)(p-2)\ldots(p-a+1)}{1 \cdot 2 \cdot \ldots \cdot a} \equiv$$

$$\equiv b \cdot 1 \cdot 2 \cdot \ldots \cdot (a-1) \pmod{p}.$$

Ділячи цю тотожну конгруенцію почленно на $1 \cdot 2 \cdot \ldots \cdot (a-1)$, дістанемо, що

$$x \equiv b\, (-1)^{a-1} \frac{(p-1)(p-2)\ldots(p-a+1)}{1 \cdot 2 \ldots a} \pmod{p}$$

буде розв'язком конгруенції $ax \equiv b \pmod{p}$.

9. Твердження а) і б) випливають з означення символічного дробу; в) тут можна припустити, що $b_0 = b + mt$, де t визначається з умови $b + mt \equiv 0 \pmod{a}$; тоді конгруенцію $ax \equiv b \pmod{m}$ задовольняє ціле число, яким є звичайний дріб $\frac{b_0}{a}$; г) згідно з в) виберемо $b_{1,0}$, кратне a_1, і $b_{2,0}$, кратне a_2; тоді матимемо:

$$\frac{b_1}{a_1} \pm \frac{b_2}{a_2} \equiv \frac{b_{1,0}}{a_1} \pm \frac{b_{2,0}}{a_2} = \frac{b_{1,0}\, a_2 \pm b_{2,0}\, a_1}{a_1 a_2} \equiv \frac{b_1 a_2 \pm b_2 a_1}{a_1 a_2} \pmod{m}.$$

Аналогічно можна довести твердження д) і е).

15. Припустити, що $x = y + h$, де h задовольняє конгруенцію

$$nh + a_1 \equiv 0 \pmod{m}.$$

17. Кожний корінь конгруенції $f(x) \equiv 0 \pmod{p}$ є коренем однієї з конгруенцій $f_1(x) \equiv 0$, $f_2(x) \equiv 0 \pmod{p}$; коли б конгруенція $f_1(x) \equiv 0 \pmod{p}$ мала менше, ніж k розв'язків, то конгруенція $f_2(x) \equiv 0 \pmod{p}$ мала б більше, ніж l розв'язків, бо загальне число коренів дорівнює $n = k + l$. Але це

неможливо, бо конгруенція l-го степеня, за простим модулем p, має не більш як l розв'язків.

18. Припустимо, що $x^p - x \equiv f(x)\, q(x) + r(x) \pmod{p}$.

1) Нехай конгруенція $f(x) \equiv 0 \pmod{p}$ має n різних розв'язків: x_1, x_2, ..., x_n; ці розв'язки за теоремою Ферма задовольнятимуть і конгруенцію $x^p - x \equiv 0 \pmod{p}$, а значить, і конгруенцію $r(x) \equiv 0 \pmod{p}$. Але $r(x)$ має степінь менший від n, отже (див. наслідок з теореми 5, § 24), всі коефіцієнти її діляться на p.

2) Навпаки, якщо всі коефіцієнти в $r(x)$ діляться на p, тоді матимемо:

$$x^p - x \equiv f(x)\, q(x) \pmod{p}.$$

Тепер, на підставі результату попередньої задачі, робимо висновок, що $f(x) \equiv 0 \pmod{p}$ має n різних розв'язків.

23. $(2n+1)(2n+2) \ldots (4n-1)\, 4n \equiv (p-2n)[p-(2n-1)] \ldots (p-2) \times (p-1) \equiv (-1)^{2n} 2n\,(2n-1) \ldots 2 \cdot 1 \equiv (2n)! \pmod{p}$.
$\{(2n)!\}^2 \equiv (2n)!\, 2n\,(2n+1)(2n+2) \ldots (4n-1)\, 4n \equiv (4n)! \equiv (p-1)! \equiv -1 \pmod{p}$.

32. Твердження а) є прямим наслідком з теореми 2, § 16. б) В усякому разі, розв'язків буде не більш як m.

33. Таке поширення можливе завдяки тому, що сукупність класів чисел за простим модулем p утворює поле відносно операцій додавання і множення класів (див. теорему 3, § 21), а теорію детермінантів і теорію лінійних рівнянь можна без будь-яких змін поширити на випадок довільного поля, бо всі висновки, що є у цих розділах алгебри, грунтуються на загальних властивостях алгебраїчних операцій поля.

35. Замість системи конгруенцій розглянути систему лінійних рівнянь:

$$a_{i1}x_1 + \ldots + a_{in}x_n = b_i + mt_i \quad (i = 1, 2, \ldots, n)$$

і скористатись тим, що $D \neq 0$, бо $(D, m) = 1$.

36. Якщо $\alpha_1, \alpha_2, \ldots, \alpha_n$ — один з розв'язків системи конгруенцій за модулем p^{a-1}, то припускаємо, що $x_j = \alpha_j + p^{a-1} x_j'$; звідси:

$$a_{i1}x_1' + \ldots + a_{in}x_n' \equiv b_i' \pmod{p} \quad (i = 1, 2, \ldots, n),$$

де

$$b_i' = \frac{b_i - a_{i1}\alpha_1 - \ldots - a_{in}\alpha_n}{p^{a-1}}.$$

Розділ V

3. Припустимо, що δ — показник, до якого належить ab за модулем p; тоді $(ab)^{\alpha\beta} = (a^{\alpha})^{\beta} (b^{\beta})^{\alpha} \equiv 1 \pmod{p}$; звідси випливає, що $\delta / \alpha\beta$ (див. наслідок з властивості 2, § 29). З другого боку,

$$(ab)^{\alpha\delta} = a^{\alpha\delta} b^{\alpha\delta} \equiv 1 \pmod{p}, \text{ бо } (ab)^{\delta} \equiv 1 \pmod{p}.$$

Але $a^{\alpha\delta} \equiv 1 \pmod{p}$, бо a належить показнику δ за модулем p. Отже, $b^{\alpha\delta} \equiv 1 \pmod{p}$. Звідси $\beta / \alpha\delta$, бо b належить показнику β за модулем p.

Так само, виходячи з конгруенції $(ab)^{\beta\delta} \equiv 1 \pmod{p}$, дістанемо, що $\alpha / \beta\delta$. Але $(\alpha, \beta) = 1$, отже, β / δ і α / δ і тоді $\alpha\beta / \delta$. З $\delta / \alpha\beta$ і $\alpha\beta / \delta$ випливає, що $\alpha\beta = \delta$.

4. Припустимо, що $p - 1 = q_1^{\alpha_1} q_2^{\alpha_2} \ldots q_k^{\alpha_k}$. Розглянемо конгруенцію $x^{\frac{p-1}{q_i}} \equiv 1 \pmod{p}$. Ця конгруенція має не більш як $\frac{p-1}{q_i} < p - 1$ розв'язків. Тому серед наведених лишків за модулем p знайдеться принаймні один такий

a_i, що $a_l^{\frac{p-1}{q_l}} \not\equiv 1 \pmod p$. Візьмемо тепер число $b_l = a_l^{\frac{p-1}{\alpha_l}}$ і покажемо, що b_l належать до показника $q_l^{\alpha_l}$ за модулем p. Справді,

$$b_l^{q_l^{\alpha_l}} = \left(a_l^{\frac{p-1}{\alpha_l}}\right)^{q_l^{\alpha_l}} \equiv a_l^{p-1} \equiv 1 \pmod p$$

за малою теоремою Ферма. Отже, $b_l^{q_l^{\alpha_l}} \equiv 1 \pmod p$. Якщо тепер δ — показник числа b_l, то $\delta / q_l^{\alpha_l}$ і $\delta = q_l^{\beta}$, де $\beta \leqslant \alpha_l$. Припустимо, що $\beta < \alpha_l$. Тоді за означенням показника дістаємо, що $b_l^{q_l^{\beta}} \equiv 1 \pmod p$, або

$$\left(a_l^{\frac{p-1}{\alpha_l}}\right)^{q_l^{\beta}} \equiv 1 \pmod p,$$

або

$$a_l^{\frac{p-1}{\alpha_l} q_l^{\alpha_l - \beta}} \equiv 1 \pmod p.$$

Підносячи обидві частини останньої конгруенції до степеня $q_l^{\alpha_l - \beta - 1}$, дістанемо: $a_l^{\frac{p-1}{q_l}} \equiv 1 \pmod p$, що суперечить вибору числа a_l. Отже, залишається тільки, що $\beta = \alpha_l$, тобто b_l належить показнику $q_l^{\alpha_l}$ за модулем p.

Розглянемо тепер число $g = b_1 b_2 \ldots b_k$. Числа $q_l^{\alpha_l}$ попарно взаємно прості; отже, показник числа g за модулем p дорівнює добутку показників $q_l^{\alpha_l}$ чисел b_l за модулем p (див. попередню задачу), тобто дорівнює

$$q_1^{\alpha_1} q_2^{\alpha_2} \ldots q_k^{\alpha_k} = p - 1.$$

Звідси вже випливає, що g є первісним коренем за модулем p.

5. Маємо: $q^{p-1} = 1 + pT_0$;

$$(g + pt)^{p-1} = 1 + p(T_0 - g^{p-2}t + pT) = 1 + pu, \qquad (1)$$

де, одночасно з t, u пробігає повну систему лишків за модулем p. Тому можна вказати t з умовою, що u не ділиться на p. При вказаному t з (1) маємо також

$$\left.\begin{aligned} (g + pt)^{p(p-1)} &= (1 + pu)^p = 1 + p^2 u_2, \\ (g + pt)^{p^2(p-1)} &= (1 + p^2 u_2)^p = 1 + p^3 u_3, \ \ldots, \end{aligned}\right\} \qquad (2)$$

де u_2, u_3, ... не діляться на p.

Нехай тепер $g + pt$ за модулем p^α належить показнику δ. Тоді

$$(g + pt)^{\delta} \equiv 1 \pmod{p^\alpha}. \qquad (3)$$

Звідси $(g + pt)^{\delta} \equiv 1 \pmod p$; отже, δ кратне $p - 1$, а через те що δ ділить $\varphi(p^\alpha) = p^{\alpha-1}(p-1)$, то $\delta = p^{r-1}(p-1)$, де $r = 1, 2, \ldots, \alpha$.

Замінюючи ліву частину конгруенції (3) її виразом з відповідної з рівностей (1) і (2), дістанемо ($u = u_1$):

$$1 + p^r u_r \equiv 1 \pmod{p^\alpha}, \quad p^r \equiv 0 \pmod{p^\alpha}, \quad r = \alpha, \quad \delta = \varphi(p^\alpha),$$

тобто $g + pt$ — первісний корінь за модулем p^α.

6. Нехай g_1 — те з чисел g або $g + p^\alpha$, яке непарне. Оскільки $g_1 \equiv g \pmod{p^\alpha}$, то g_1 — первісний корінь за модулем p^α. З другого боку,

$(g, 2p^\alpha) = 1$, бо g_1 є непарне. Звідси g_1 повинно належати до деякого показника δ за модулем $2p^\alpha$: $g_1^{\delta} \equiv 1 \pmod{2p^\alpha}$, але в такому випадку і поготів $g_1^{\delta} \equiv 1 \pmod{p^\alpha}$. Через те що g_1 — первісний корінь за модулем p^α, звідси випливає, що $\varphi(p^\alpha) = \varphi(2p^\alpha)/\delta$. Водночас маємо, що $\delta \leqslant \varphi(2p^\alpha)$, отже, $\delta = \varphi(2p^\alpha)$ і g_1 є первісний корінь за модулем $2p^\alpha$.

7. Число 1 є, очевидно, первісним коренем за модулем 2, а 3 — первісним коренем за модулем 4. Покладемо тепер, що модуль дорівнює 2^α, де $\alpha \geqslant 3$. Позначимо через a довільне число, взаємно просте з 2^α, тоді можна записати, що $a = 4t \pm 1$, де t — ціле. Звідси

$$a^2 = 1 + 8t_1, \ a^4 = 1 + 16t_2, \ \ldots, \ a^{2\alpha-2} = 1 + 2^\alpha t_{\alpha-2} \equiv 1 \pmod{2^\alpha}.$$

тобто

$$a^{\frac{1}{2}\varphi(2^\alpha)} \equiv 1 \pmod{2^\alpha},$$

внаслідок чого a не може бути первісним коренем за модулем 2^α при $\alpha \geqslant 3$.

8 і 9. Треба показати, що при $(a, m) = 1$, $a^{\frac{1}{2}\varphi(m)} \equiv 1 \pmod m$.

10. Справді, якщо g — первісний корінь, то тим самим він належить показнику $c = \varphi(m)$ і, отже, жодну з конгруенцій

$$g^{\frac{c}{q_i}} \equiv 1 \pmod m \ (i = 1, 2, \ldots, k)$$

задовольнити не може. Навпаки, припустимо, що g не задовольняє жодну з цих конгруенцій. Коли б показник δ, до якого належить g, був менший від c, то, позначаючи буквою q один з простих дільників $\frac{c}{\delta}$, ми мали б:

$$\frac{c}{\delta} = qu, \quad \frac{c}{q} = \delta u, \quad g^{\frac{c}{q}} \equiv 1 \pmod p,$$

що суперечить умові.

11. Див. задачу 6.

17. Якщо $a^{\delta} \equiv 1 \pmod{p^\alpha}$, то не існує натурального $\delta_1 < \delta$, при якому $a^{\delta_1} \equiv 1 \pmod{p^\alpha}$, бо в противному разі ми мали б, що $a^{\delta_1} \equiv 1 \pmod{p^{\alpha-1}}$ і δ не було б показником a за модулем $p^{\alpha-1}$. Отже, коли $a^{\delta} \equiv 1 \pmod{p^\alpha}$, то a належить до показника δ за модулем p^α.

Якщо $a^{\delta} \not\equiv 1 \pmod{p^\alpha}$, то з конгруенції $a^{\delta} \equiv 1 \pmod{p^{\alpha-1}}$ виходить, що

$$a^{\delta} = 1 + p^{\alpha-1} T,$$

де T — ціле, яке не ділиться на p. Піднесемо обидві частини цієї рівності до степеня p:

$$a^{p\delta} = 1 + pT_1,$$

де T_1 — ціле, яке не ділиться на p. Отже, $a^{p\delta} \equiv 1 \pmod{p^\alpha}$.

Нехай a належить показнику δ_1 за модулем p^α; тоді з попередньої конгруенції виходить, що $\delta_1 / p\delta$. З другого боку, якщо $a^{\delta_1} \equiv 1 \pmod{p^\alpha}$, то й поготів $a^{\delta_1} \equiv 1 \pmod{p^{\alpha-1}}$, звідки δ / δ_1. Отже, $\delta_1 = \delta g_1$, $\delta p = \delta_1 q_2$, де q_1, q_2 — натуральні числа; $p\delta = \delta q_1 q_2$, або $p = q_1 q_2$. Оскільки p — просте, то або а) $q_1 = 1$, $q_2 = p$ або б) $q_1 = p$, $q_2 = 1$. Але випадок а) відпадає, бо тут буде

$\delta_1 = \delta$, що суперечить умові $a^{\delta} \not\equiv 1 \pmod{p^{\alpha}}$. Отже, залишається випадок б), тобто $\delta_1 = p\delta$.

27. При $p > 2$ маємо

$$1 \cdot 2 \ldots (p-1) = g^{1+2+\ldots+(p-1)} \equiv g^{\frac{p-1}{2}} \equiv -1 \pmod{p}.$$

Розділ VI

5. Треба знайти найменший невід'ємний лишок того класу чисел, якому належить 243^{402} за модулем 1000.

8. Задача зводиться до розв'язання конгруенції $x^{13} \equiv 17 \pmod{10}$.

16. Скористатись критерієм Ейлера: $10^{\frac{p-1}{2}} \equiv \pm 1 \pmod{p}$.

17. Справді, за умовою $g\mu \equiv -1 \pmod{d}$, звідки $a_0 g\mu \equiv a_0 \pmod{d}$. Оскільки $N = \left[\frac{N}{g}\right] g + a_0$, то $-a_0 = \left[\frac{N}{g}\right] g - N$ і остання конгруенція набуває вигляду: $a_0 g\mu \equiv \left[\frac{N}{g}\right] g - N \pmod{d}$, або $N \equiv g\left[\frac{N}{g}\right] - a_0 g\mu \pmod{d}$, або $N \equiv Mg \pmod{d}$. Ця конгруенція показує, що коли N ділиться на d, то й Mg ділиться на d, але оскільки $(d, g) = 1$, то M ділитиметься на d, і навпаки. Цим твердження доведено.

Примітка. Неважко побачити, що $\left[\frac{N}{g}\right]$ є число одиниць другого розряду, які містяться в N; μ залежить лише від d, а не від N і визначається однозначно за модулем d; за μ можна взяти абсолютно найменший лишок.

18. Справді, за умовою $g\mu \equiv 1 \pmod{d}$, звідси $-g\mu \equiv -1 \,(d)$, і μ є розв'язок конгруенції $gx \equiv 1 \pmod{d}$.

На підставі задачі 12 дістанемо, що $M = \left[\frac{N}{g}\right] + \mu a_0$ одночасно з N ділитиметься або не ділитиметься на d, що й доводить твердження.

28. Розглянемо один будь-який період що складається з цифр $z_1, z_2, \ldots, z_k$, який утворюється при перетворенні дробу $\frac{n}{m}$ у десятковий, і систему $r_0, r_1, \ldots, r_{k-1}$ всіх остач, що утворюються при цьому, нумеруючи їх по порядку, починаючи з $n = r_0$.

Через те що при діленні r_1 на m дістанемо в частці z_2 і остачу r_2 і т. д., то очевидно, що періоди дробів $\frac{r_0}{m}$, $\frac{r_1}{m}$, ..., $\frac{r_{k-1}}{m}$ 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_l вичерпують всю зведену систему лишків за модулем m. Періоди всіх нескоротнних дробів із знаменником m у цьому випадку складатимуться з кругових перестановок однієї й тієї самої системи з $k = \varphi(m)$ цифр $z_2, z_2, \ldots, z_k$.

29. Припускаючи, що $r_0 = 1$, прийдемо до таких конгруенцій за модулем m:

$$10^0 \equiv r_0 = 1,\ 10^1 \equiv r_1, \ldots,\ 10^q \equiv r_q,\ \ldots,\ 10^{k-1} \equiv r_{k-1}.$$

Тому, знаючи період $z_1, z_2, \ldots, z_k$ дробу $\frac{1}{m}$, можемо визначити число цифр q, на яке треба відступити праворуч для знаходження періоду $z_{q+1}, z_{q+2}, \ldots, z_q$ дробу $\frac{n}{m}$, розшукавши індекс n за основою 10 для модуля m:

$$q = \operatorname{ind}_{10} r_q = \operatorname{ind}_{10} n.$$

32. Якщо 10 — квадратний нелишок за модулем p, то $10^{\frac{p-1}{2}} \equiv -1 \pmod{p}$. Тому має бути найменше натуральне l, при якому $10^l \equiv -1 \pmod{p}$, звідки $10^{2l} \equiv 1 \pmod{p}$.

Позначимо буквою δ показник, до якого належить 10 за модулем p, тоді $\delta/2l$. Якщо δ — парне, то

$$10^{\delta} - 1 = \left(10^{\frac{\delta}{2}} - 1\right)\left(10^{\frac{\delta}{2}} + 1\right) \equiv 0 \pmod{p},$$

звідки $10^{\frac{\delta}{2}} \equiv -1 \pmod{p}$. Звідси внаслідок мінімальності l дістаємо, що $\frac{\delta}{2} = l$, $\delta = 2l$. Якщо δ — непарне, то δ/l. Звідси $l = \delta t$, де t — деяке натуральне число і

$$10^l = (10^{\delta})^t \equiv 1 \pmod{p},$$

що суперечить конгруенції $10^l \equiv -1 \pmod{p}$. Отже, δ повинно бути парним, тобто $\frac{1}{p}$ перетворюється у нескінченний десятковий періодичний дріб з парним числом цифр у періоді.

Нехай тепер $p = 4k + 3$ і дріб $\frac{1}{p}$ перетворюється у періодичний десятковий дріб з парним числом $\delta = 2l$ цифр у періоді. Тоді:

$$10^{2l} - 1 \equiv (10^l - 1)(10^l + 1) \equiv 0 \pmod{p},$$

звідки $10^l \equiv -1 \pmod{p}$. Очевидно, що $2l/p - 1$. Звідси $l \left| \frac{p-1}{2} \right.$. Але $\frac{p-1}{2} = 2k + 1$ — непарне число, отже, $\frac{p-1}{2l}$ — також непарне. Підносячи обидві частини конгруенції $10^l \equiv -1 \pmod{p}$ до непарного степеня $\frac{p-1}{2l}$, дістанемо:

$$10^{\frac{p-1}{2}} \equiv -1 \pmod{p},$$

тобто, згідно з критерієм Ейлера, число 10 є квадратичним нелишком за модулем p.

33. Нехай $\frac{1}{p} = 0, (\alpha_1 \alpha_2 \ldots \alpha_l \ldots \alpha_{2l})$, де $\alpha_1, \alpha_2, \ldots, \alpha_l, \ldots, \alpha_{2l}$ — цифри періоду. Тоді 10 належить до показника $2l$ за модулем p і $\frac{10^{2l} - 1}{p} = N$, де

$$N = 10^{2l-1}\alpha_1 = 10^{2l-2}\alpha_2 + \ldots + \alpha_{2l}.$$

Але

$$N = \frac{10^{2l} - 1}{p} = 10^l\left(\frac{10^l + 1}{p} - 1\right) + \left(10^l - \frac{10^l + 1}{p}\right).$$

Нехай

$$\frac{10^l + 1}{p} = 10^{l-1}\beta_1 + 10^{l-2}\beta_2 + \ldots + (\beta_l + 1),$$

де $0 \leqslant \beta_l \leqslant 9$, $0 \leqslant \beta_1 < 9$ $(i = 1, 2, \ldots, l-1)$. Тоді:

$$N = 10^l(10^{l-1}\beta_1 + 10^{l-2}\beta_2 + \ldots + \beta_l) + 10^{l-1}(9 - \beta_1) + \ldots + (9 - \beta_l),$$

звідки

$$\alpha_1 = \beta_1,\ \alpha_2 = \beta_2,\ \ldots,\ \alpha_l = \beta_l,\ \alpha_{l+1} = 9 - \beta_l,\ \ldots,\ \alpha_{2l} = 9 - \beta_l,$$

і твердження задачі очевидне.

Розділ VII

17. Доведення від супротивного. Припустимо, що

$$\left|\alpha - \frac{P_k}{Q_k}\right| \geqslant \frac{1}{2Q_k^2} \text{ і } \left|\alpha - \frac{P_{k-1}}{Q_{k-1}}\right| \geqslant \frac{1}{2Q_{k-1}^2}.$$

Підхідні дроби $\frac{P_k}{Q_k}$ і $\frac{P_{k-1}}{Q_{k-1}}$ знаходяться з різних боків від α, отже,

$$\left|\frac{P_k}{Q_k} - \frac{P_{k-1}}{Q_{k-1}}\right| = \left|\alpha - \frac{P_k}{Q_k}\right| + \left|\alpha - \frac{P_{k-1}}{Q_{k-1}}\right| > \frac{1}{2}\left(\frac{1}{Q_k^2} + \frac{1}{Q_{k-1}^2}\right).$$

З другого боку,

$$\left|\frac{P_k}{Q_k} - \frac{P_{k-1}}{Q_{k-1}}\right| = \frac{1}{Q_k Q_{k-1}}.$$

Отже,

$$\frac{1}{Q_k Q_{k-1}} > \frac{1}{2}\left(\frac{1}{Q_k^2} + \frac{1}{Q_{k-1}^2}\right),$$

звідки $(Q_k - Q_{k-1})^2 \leqslant 0$, що неможливо при $k > 1$.

18. Розкладемо $\frac{p}{q}$ у неперервний дріб з парним або непарним k неповних часток, не враховуючи q_0 залежно від того, чи буде різниця $\alpha = \frac{p}{q}$ додатною чи від'ємною: $\frac{p}{q} = [q_0;\ q_1,\ \ldots,\ q_k]$.

Отже,

$$\left|\alpha = \frac{p}{q}\right| = (-1)^k\left(\alpha - \frac{p}{q}\right),\ \frac{P_k}{Q_k} = \frac{p}{q}.$$

Звідси внаслідок нескоротності $\frac{p}{q}$ випливає, що $p = P_k$ і $q = Q_k$. Візьмемо далі $(k-1)$-й підхідний дріб $\frac{P_{k-1}}{Q_{k-1}}$ розкладу $\frac{p}{q}$. Оскільки

$$P_k Q_{k-1} - P_{k-1} Q_k = (-1)^{k-1},$$

то

$$pQ_{k-1} - qP_{k-1} = (-1)^{k-1}.$$

Підберемо далі таке число α_{k+1}, щоб виконувалась рівність

$$\alpha = \frac{p\alpha_{k+1} + P_{k-1}}{q\alpha_{k+1} + Q_{k-1}}. \tag{1}$$

Рівність (1) однозначно розв'язується відносно α_{k+1}:

$$\alpha_{k+1} = \frac{P_{k-1} - \alpha Q_{k-1}}{q\alpha - p} > 0,$$

$q\alpha - p \neq 0$ за умовою теореми. Отже, таке α_{k+1} завжди знайдеться і притому тільки одне.

Тепер дістанемо:

$$\alpha - \frac{p}{q} = \frac{p\alpha_{k+1} + P_{k-1}}{q\alpha_{k+1} + Q_{k-1}} - \frac{p}{q} = \frac{qP_{k-1} - pQ_{k-1}}{q(q\alpha_{k+1} + Q_{k-1})} = \frac{(-1)^k}{q(q\alpha_{k+1} + Q_{k-1})},$$

Отже,

$$\left|\alpha - \frac{p}{q}\right| = (-1)^k\left(\alpha - \frac{p}{q}\right) = \frac{1}{q(q\alpha_{k+1} + Q_{k-1})}.$$

Але за умовою теореми $\left|\alpha - \frac{p}{q}\right| < \frac{1}{2q^2}$, тому,

$$\frac{1}{2q^2} > \frac{1}{q(q\alpha_{k+1} + Q_{k-1})}.$$

Оскільки $q\alpha_{k+1} + Q_{k-1} > 0$ то $2q < q\alpha_{k+1} + Q_{k-1}$. Останню нерівність ми тільки підсилимо, якщо Q_{k-1} замінимо через $Q_k = q$. Отже, $2q < q\alpha_{k+1} + q$, звідки $\alpha_{k+1} > 1$. Розкладемо тепер α_{k+1} у неперервний дріб; нехай $\alpha_{k+1} = [q_{k+1};\ q_{k+2},\ \ldots]$. Оскільки $\alpha_{k+1} > 1$, то $q_{k+1} \geqslant 1$. Тому можна скласти такий неперервний дріб:

$$\omega = [q_0;\ q_1,\ \ldots,\ q_k,\ q_{k+1},\ q_{k+n},\ \ldots].$$

Легко побачити, що α_{k+1} є $k+1$ повною часткою цього неперервного дробу, а підхідним дробом k-го порядку буде $\frac{p}{q}$.

Отже,

$$\omega = \frac{p\alpha_{k+1} + P_{k-1}}{q\alpha_{k+1} + Q_{k-1}} \tag{2}$$

(див. теорему 2, § 38).

А тепер, порівнюючи рівності (1) і (2), бачимо, що $\omega = \alpha$ і $\frac{p}{q}$ є підхідним дробом порядку k розкладу α у неперервний дріб.

19. а) Розклавши $\frac{a}{c}$ у неперервний дріб, припустимо, що $\frac{a}{c} = \frac{P_n}{Q_n}$; виберемо n такої парності, щоб $P_n Q_{n-1} - P_{n-1} Q_n = ad - bc$, тоді з рівнянь $ad - bc = \pm 1$ знайдемо загальний розв'язок для b і d:

$$b = P_{n-1} + tP_n,\ d = Q_{n-1} + tQ_n,$$

де t — ціле. Оскільки, з другого боку, $(a, c) = 1$ і тому $c = Q_n \geqslant Q_{n-1}$, то з формули для d випливає, що умова $c \geqslant d$ задовольнятиметься тільки при $t = 0$, так що $b = P_{n-1}$, $d = Q_{n-1}$ і

$$\omega = \frac{P_n\omega' + P_{n-1}}{Q_n\omega' + Q_{n-1}}.$$

Звідси вже безпосередньо випливає, що ω' є $n+1$ повна частка у розкладі ω у неперервний дріб.

б) Необхідність легко довести безпосередньо. Доведемо достатність. Нехай справедливе співвідношення $\omega = \frac{a\omega' + b}{c\omega' + d}$ $(ad - bc = \pm 1)$ і припустимо, що $c\omega + d > 0$ (цього можна завжди досягти, змінюючи знаки в усіх чисел a, b, c і d).

Розклавши ω' у неперервний дріб

$$\omega' = [b_0;\ b_1,\ \ldots,\ b_{\nu-1},\ \omega_\nu] = \frac{P_{\nu-1}\,\omega_\nu + P_{\nu-2}}{Q_{\nu-1}\,\omega_\nu + Q_{\nu-2}}$$

і визначивши ω через ω_ν, дістанемо:

$$\omega = \frac{\alpha\omega_\nu + \beta}{\gamma\omega_\nu + \delta}, \qquad (3)$$

де $\alpha\delta - \beta\gamma = \pm 1$ і

$$\gamma = cP_{\nu-1} + dQ_{\nu-1} = \left(c\frac{P_{\nu-1}}{Q_{\nu-1}} + d\right)Q_{\nu-1},$$

$$\delta = cP_{\nu-2} + dQ_{\nu-2} = \left(c\frac{P_{\nu-2}}{Q_{\nu-2}} + d\right)Q_{\nu-2}.$$

Через те що

$$\lim_{\nu\to\infty}\frac{P_{\nu-1}}{Q_{\nu-1}} = \lim_{\nu\to\infty}\frac{P_{\nu-2}}{Q_{\nu-2}} = \omega',$$

а $c\omega' + d > 0$ і $Q_{\nu-1} > Q_{\nu-2} > 0$, то при досить великому ν буде $\gamma > \delta > 0$.

З рівності (3) за попередньою теоремою робимо висновок, що ω_ν є деяка повна частка для ω.

Звідси випливає, що послідовності неповних часток для ω і ω' збігатимуться, починаючи з деяких місць.

Розділ VIII

1. З рівності

$$Q_{k+1} = q_{k+1}Q_k + Q_{k-1}\ (k = 1, 2, \ldots)$$

випливає, що $Q_{k+1} < 2q_{k+1}Q_k$. Звідси: $Q_k < 2^k q_1 q_2 \ldots q_k$. Якщо тепер

$$q_{k+1} \geqslant 2^{k^2} q_1^k q_2^k \ldots q_k^k,$$

то й поготів $q_{k+1} > Q_k^k$ і тому ω трансцендентне.

2. Показати, що справджуються умови задачі 1.

ТАБЛИЦЯ ПРОСТИХ ЧИСЕЛ, ЯКІ НЕ ПЕРЕВИЩУЮТЬ 5000

2	127	283	467	661	877	1087	1297	1523
3	131	293	479	673	881	1091	1301	1531
5	137	307	487	677	883	1093	1303	1543
7	139	311	491	683	887	1097	1307	1549
11	149	313	499	691	907	1103	1319	1553
13	151	317	503	701	911	1109	1321	1559
17	157	331	509	709	919	1117	1327	1567
19	163	337	521	719	929	1123	1361	1571
23	167	347	523	727	937	1129	1367	1579
29	173	349	541	733	941	1151	1373	1583
31	179	353	547	739	947	1153	1381	1597
37	181	359	557	743	953	1163	1399	1601
41	191	367	563	751	967	1171	1409	1607
43	193	373	569	757	971	1181	1423	1609
47	197	379	571	761	977	1187	1427	1613
53	199	383	577	769	983	1193	1429	1619
59	211	389	587	773	991	1201	1433	1621
61	223	397	593	787	997	1213	1439	1627
67	227	401	599	797	1009	1217	1447	1637
71	229	409	601	809	1013	1223	1451	1657
73	233	419	607	811	1019	1229	1453	1663
79	239	421	613	821	1021	1231	1459	1667
83	241	431	617	823	1031	1237	1471	1669
89	251	433	619	827	1033	1249	1481	1693
97	257	439	631	829	1039	1259	1483	1697
101	263	443	641	839	1049	1277	1487	1699
103	269	449	643	853	1051	1279	1489	1709
107	271	457	647	857	1061	1283	1493	1721
109	277	461	653	859	1063	1289	1499	1723
113	281	463	659	863	1069	1291	1511	1733

1741	1993	2221	2437	2689	2909	3187	3433	3659
1747	1997	2237	2441	2693	2917	3191	3449	3671
1753	1999	2239	2447	2699	2927	3203	3457	3673
1759	2003	2243	2459	2707	2939	3209	3461	3677
1777	2011	2251	2467	2711	2953	3217	3463	3691
1783	2017	2267	2473	2713	2957	3221	3467	3697
1787	2027	2269	2477	2719	2963	3229	3469	3701
1789	2029	2273	2503	2729	2969	3251	3491	3709
1801	2039	2281	2521	2731	2971	3253	3499	3719
1811	2053	2287	2531	2741	2999	3257	3511	3727
1823	2063	2293	2539	2749	3001	3259	3517	3733
1831	2069	2297	2543	2753	3011	3271	3527	3739
1847	2081	2309	2549	2767	3019	3299	3529	3761
1861	2083	2311	2551	2777	3023	3301	3533	3767
1867	2087	2333	2557	2789	3037	3307	3539	3769
1871	2089	2339	2579	2791	3041	3313	3541	3779
1873	2099	2341	2591	2797	3049	3319	3547	3793
1877	2111	2347	2593	2801	3061	3323	3557	3797
1879	2113	2351	2609	2803	3067	3329	3559	3803
1889	2129	2357	2617	2819	3079	3331	3571	3821
1901	2131	2371	2621	2833	3083	3343	3581	3823
1907	2137	2377	2633	2837	3089	3347	3583	3833
1913	2141	2381	2647	2843	3109	3359	3593	3847
1931	2143	2383	2657	2851	3119	3361	3607	3851
1933	2153	2389	2659	2857	3121	3371	3613	3853
1949	2161	2393	2663	2861	3137	3373	3617	3863
1951	2179	2399	2671	2879	3163	3389	3623	3877
1973	2203	2411	2677	2887	3167	3391	3631	3881
1979	2207	2417	2683	2897	3169	3407	3637	3889
1987	2213	2423	2687	2903	3181	3413	3643	3907

3911	4153	4421	4663	4943
3917	4157	4423	4673	4951
3919	4159	4441	4679	4957
3923	4177	4447	4691	4967
3929	4201	4451	4703	4969
3931	4211	4457	4721	4973
3943	4217	4463	4723	4987
3947	4219	4481	4729	4993
3967	4229	4483	4733	4999
3989	4231	4493	4751	
4001	4241	4507	4759	
4003	4243	4513	4783	
4007	4253	4517	4787	
4013	4259	4519	4789	
4019	4261	4523	4793	
4021	4271	4547	4799	
4027	4273	4549	4801	
4049	4283	4561	4813	
4051	4289	4567	4817	
4057	4297	4583	4831	
4073	4327	4591	4861	
4079	4337	4597	4871	
4091	4339	4603	4877	
4093	4349	4621	4889	
4099	4357	4637	4903	
4111	4363	4639	4909	
4127	4373	4643	4919	
4129	4391	4649	4931	
4133	4397	4651	4933	
4139	4409	4657	4937	

ТАБЛИЦІ ПЕРВІСНИХ КОРЕНІВ ТА ІНДЕКСІВ[1]

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				10	10	10	10

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					10	10	10	10

[1] Скрізь за основу таблиці індексів береться найменший первісний корінь.

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				

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, 11.

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, 37.

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	11	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	32	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	454	4	12
1	36	29	8	24	72	58	16	8	65	37
2	32	17	51	74	64	34	23	9	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	55	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	50	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	64	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				

ЛІТЕРАТУРА

Монографії

Башмакова И. Г. Обоснование теории делимости в трудах Е. И. Золотарева. В кн.: «Историко-математические исследования», Вып. 2. М — Л., 1949, стор. 233—351.

Боревич З. И., Шафаревич И. Р. Теория чисел. М., «Наука», 1964.

Вельмин В. П. Введение в теорию алгебраических чисел. Варшава, 1913.

Венков Б. А. Элементарная теория чисел. М. — Л., ГТТИ, 1937.

Вейль Г. Алгебраическая теория чисел. М., ГИИЛ, 1947.

Виноградов И. М. Избранные труды. М., Изд-во АН СССР, 1952.

Виноградов И. М. Новый метод в аналитической теории чисел. М., Изд-во АН СССР, 1937.

Гаусс К. Ф. Труды по теории чисел. Под ред. акад. И. М. Виноградова. М., Изд-во АН СССР, 1959.

Гельфонд А. О. Трансцендентные и алгебраические числа, М., Гостехиздат, 1952.

Гельфонд А. О., Линник Ю. В. Элементарные методы в аналитической теории чисел. М., Физматгиз, 1962.

Граве Д. А. Трактат по алгебраическому анализу, т. II. К., Изд-во АН УССР, 1939.

Граве Д. А. Арифметическая теория алгебраических величин, т. I, Квадратическая область, 1909—191, 1910 літогр.

Делоне Б. Н. Петербургская школа теории чисел. М., Изд-во АН СССР, 1947.

Ингам А. Е. Распределение простых чисел. ОНТИ, 1936.

Касселс Д. Введение в теорию диофантовых приближений. М., ИЛ, 1961.

Коробов Н. М. Теоретико-числовые методы в приближенном анализе. М., Физматгиз, 1963.

Кубилюс И. П. Вероятностные методы в теории чисел. Изд. 2 Вильнюс, 1962.

Ленг С. Алгебраические числа. М., «Мир», 1966.

Прахар К. Распределение простых чисел. М., «Мир», 1967.

Титчмарш Е. К. Теория дзета-функции Римана. М., ИЛ, 1953

Трост Э. Простые числа. М., Физматгиз, 1959.

Хуа Ло-ген. Аддитивная теория простых чисел. Труды математического института им. В. А. Стеклова АН СССР, 22, 1947.

Хуа Ло-ген. Метод тригонометрических сумм и его применение в теории чисел. М., «Мир», 1964.

Хинчин А. Я. Цепные дроби. Изд. 3. М., Физматгиз, 1961.

Хованский А. Н. Приложение цепных дробей и их обобщений к вопросам приближенного анализа. М., Гостехиздат, 1956.

Чебышев П. Л. Теория сравнений Изд. 3. СПб, 1901.

Чебышев П. Л. Полное собрание сочинений, т. I. М. — Л., Изд-во АН СССР, 1946.

Чудаков Н. Г. Введение в теорию *L*-функций Дирихле. М. — Л., Гостехиздат, 1947.
Чеботарев Н. Г. Основы теории Галуа, ч. II, ОНТИ, ГТТИ, М. — Л., 1937.

Підручники і навчальні посібники

Александров В. А. Задачник-практикум по теории чисел. Для студентов-заочников физ.-мат. фак. пед. инст. М., Учпедгиз, 1960.
Арнольд И. В. Теория чисел. М., Учпедгиз, 1939.
Архангельская В. М. Элементарная теория чисел. Изд-во Саратовского ун-та, 1963.
Архангельская В. М. *L*-функции Дирихле. Изд-во Саратовского ун-та, 1963.
Бевз Г. П. Теорія чисел і теоретична арифметика. К., «Радянська школа», 1963.
Бородін О. І. Теорія чисел. Вид. 2. К., «Радянська школа», 1965.
Бухштаб А. А. Теория чисел. Изд. 2. М., «Просвещение», 1966.
Виноградов И. М. Основы теории чисел. Изд. 7. М., «Наука», 1965.
Гекке Э. Лекции по теории алгебраических чисел. М., ГТТИ, 1940.
Граве Д. А. Элементарный курс теории чисел. К., 1913.
Гребенча М. К. Теория чисел. М., Изд-во Учпедгиз, 1949.
Грибанов В. У., Титов П. И. Сборник упражнений по теории чисел. М., «Просвещение», 1964.
Іваненко В. В. Задачник з теорії чисел К., «Радянська школа», 1958.
Иванов И. И. Теория чисел. (Литогр.). СПб, 1910.
Литвер Е. Л. Теория чисел (Методические указания). Изд-во МГУ, 1963.
Лежен — Дирихле П. Г. Лекции по теории чисел. ОНТИ, 1936.
Диксон Л. Е. Введение в теорию чисел. Тбилиси, Изд-во АН Груз. ССР, 1941.
Егоров Д. Ф. Элементы теории чисел. Москва — Петроград, 1923.
Марчевский М. Н. Теория чисел. Изд-во Харьковского ун-та, 1958.
Михелович Ш. Х. Теория чисел. Изд. 2. М., «Высшая школа», 1967.
Окунев Л. Я. Краткий курс теории чисел. М., Учпедгиз, 1956.
Слугинов С. П. Основы теории чисел. Казань, 1913.
Сушкевич А. К. Теория чисел. Изд. 2. Изд-во Харьковского ун-та, 1956.
Сохоцкий В. В. Высшая алгебра. Часть II. Начало теории чисел. СПб, 1888.
Хассе Г. Лекции по теории чисел. М., ИЛ., 1953.
Хинчин А. Я. Элементы теории чисел. В кн.: «Энциклопедия элементарной математики», т. I. М., Гостехиздат, 1951.

Оглядові статті і популярна література

Вальфиш А. З. Уравнения Пелля. Тбилиси, Изд-во АН Груз. ССР, 1952.
Васильев А. В. Целое число. Пг., 1922.
Виноградов И. М. Некоторые проблемы аналитической теории чисел. В сб.: «Труды третьего Всесоюзного математического съезда», т. III. М., Изд-во АН СССР, 1958.
Воробьев Н. Н. Признаки делимости. М., Физматгиз, 1963.
Воробьев Н. Н. Числа Фибоначчи. М., «Наука», 1964.

Гельфонд А. О. О проблеме приближения алгебраических чисел рациональными. В сб.: «Математическое просвещение». Вып. 2. М., ГТТИ, 1957.
Гельфонд А. О. Решение уравнений в целых числах. Серия «Популярные лекции по математике», вып. 8. М. — Л. ГТТИ, 1952.
Гельфонд А. О. Теория чисел. В сб.: «Математика в СССР за 30 лет». М., Гостехиздат, 1947.
Гельфонд А. О., Линник В. Ю. Чисел теория. «БСЭ». Изд. 2, т. 47. М., 1957.
Голубев В. А. Реферативный обзор современных работ по элементарной теории чисел. «Математика в школе», 1958, № 6; 1960, № 5.
Дринфельд Г. И. Трансцендентичность чисел e и π. Изд-во Харьковского ун-та, 1952.
Дэвенпорт Г. Высшая арифметика, введение в теорию чисел. М., «Наука», 1965.
Линник Ю. В. Теория чисел. В сб.: «Математика в СССР за 40 лет» (1917—1957), т. I. М., Физматгиз, 1959.
Линник Ю. В. О наименьшем числе в арифм. прогрессии. В кн.: «Математический сборник», т. 15. М., Изд. АН СССР, 1944, стор. 135—178; 347—368.
Марджанишвили К. К. Простые числа. В сб.: «Математика, ее содержание, методы и значение», т. II. М., Изд-во АН СССР, 1956.
Нивен А. Числа рациональные и иррациональные. М., «Мир», 1966.
Постников А. Г., Романов К. П. Упрощение элементарного доказательства А. Сельберга асимптотического закона распределения простых чисел. В журнале «Успехи математических наук», т. X, М., 1955.
Радимахер Г. и Теплиц О. Числа и фигуры. Изд. 4. М., «Наука», 1966.
Райк А. Е. Уральский математик Иван Михеевич Первушин. В кн.: «Истор. мат. иссл.», т. VI. М., Гостехиздат, 1953, стор. 535—572.
Сегал Б. И. Теория чисел. В кн.: «Математика и естествознание в СССР», М., Изд-во АН СССР, 1938.
Серпинский В. Пифагоровы треугольники. М., Учпедгиз, 1959.
Серпинский В. О решении уравнений в целых числах. М., Физматгиз. 1961.
Серпинский В. Сто простых, но одновременно и трудных вопросов арифметики. М., Учпедгиз, 1961.
Серпинский В. Что мы знаем и чего мы не знаем о простых числах. М. — Л., Физматгиз. 1963.
Соколов И. Г. Памяти Л. З. Шнирельмана. В кн.: «Вопросы элементарной и высшей математики». Вып. I. Изд-во Харьковского ун-та, 1952.
Хинчин А. Я. Три жемчужины теории чисел. М., Гостехиздат, 1947.
Хинчин А. Я. Теория чисел. Очерк развития за время 1917—1927. В кн.: «Математический сборник», т. 15, М., Изд. АН СССР, 1928, доп.вып. 1—4.
Хинчин А. Я. Великая теорема Ферма. Изд. 2. М., ГТТИ, 1932.
Шнирельман Л. Г. Простые числа. М., Гостехиздат, 1940.

Предметний покажчик

ЗМІСТ

Розділ VIII

Алгебраїчні і трансцендентні числа

Розділ IX

Розподіл простих чисел у натуральному ряді

БОРОДИН АЛЕКСЕЙ ИВАНОВИЧ

ТЕОРИЯ ЧИСЕЛ

(на украинском языке)

Издательство «Вища школа»

Редактор Г. П. Трофімчук
Літредактор Н. Г. Кирилова
Обкладинка художника Р. К. Похолюка
Художній редактор С. П. Духленко.
Технічний редактор Г. Д. Новік
Коректор Н. В. Волкова

Здано до набору 22.I.70 р. Підписано до друку 17.VII. 70 р. Формат паперу 60×90¹/₁₆. Папір друк. № 2. Фіз.-друк. арк. 17,25. Умовн. арк. 17,25. Видавн. арк. 15,23. Тираж 4000. Видавн. № 216. БФ 08861. Ціна 63 коп. Зам. № 46.

Видавництво «Вища школа», Київ, Гоголівська, 7.
ТП вид-ва «Вища школа» — 1970, поз. 26

Книжкова ф-ка ім. М. В. Фрунзе Комітету по пресі при Раді Міністрів УРСР. Харків, Донець-Захаржевська, 6/8.