МІНІСТЕРСТВО ОСВІТИ І НАУКИ УКРАЇНИ
Державний заклад:
ПІВДЕННОУКРАЇНСЬКИЙ НАЦІОНАЛЬНИЙ ПЕДАГОГІЧНИЙ
УНІВЕРСИТЕТ ІМЕНІ К. Д. УШИНСЬКОГО
Кафедра вищої математики і статистики

О. М. Болдарєва, О. М. Яковлєва

Методичні рекомендації до самостійної роботи з дисципліни «Алгебра і теорія чисел» (курс лекцій)

Одеса – 2021

УДК 511.1

Укладачі:

к.ф.-м.н., доцент кафедри вищої математики і статистики ДЗ «Південноукраїнський національний педагогічний університет імені К. Д. Ушинського» Яковлєва Ольга Миколаївна

к.ф.-м.н., доцент кафедри вищої математики і статистики ДЗ «Південноукраїнський національний педагогічний університет імені К. Д. Ушинського» Болдарєва Ольга Миколаївна

Рецензенти:

к.ф.-м.н., доц. кафедри комп'ютерної алгебри та дискретної математики ОНУ імені І. І. Мечникова Савастру Ольга Володимирівна

к.ф.-м.н., старший викладач кафедри вищої математики і статистики ДЗ «Південноукраїнський національний педагогічний університет імені К. Д. Ушинського» Драганюк Сергій Володимирович

Методичні рекомендації до самостійної роботи з дисципліни «Алгебра і теорія чисел» (курс лекцій) розроблено для здобувачів першого (бакалаврського) рівня вищої освіти галузі знань 01 Освіта / Педагогіка спеціальностей 014. 04 Середня освіта (Математика), 014.08 Середня освіта (Фізика) денної та заочної форм навчання, які вивчають теорію чисел, а також може бути запропонований викладачам закладів середньої освіти. Методичні рекомендації містять теоретичний матеріал з теорії подільності, теоретичні завдання для самостійної роботи. Матеріал методичних рекомендацій може бути використаний на лекціях, а також під час самостійної роботи студентів для опрацювання питань навчальної дисципліни «Алгебра і теорія чисел».

Зміст

Вступ

Теорія чисел, або вища арифметика, – галузь математики, яка розпочалась з вивчення властивостей натуральних чисел, пов'язаних з питаннями подільності, і розв'язання алгебраїчних рівнянь у натуральних, а згодом у цілих числах. Вже піфагорійці, Евклід і Діофант Олександрійський зробили вагомий внесок до становлення теорії чисел, але вона дістала величезного розвитку, починаючи з кінця 18 ст. Надзвичайно плідними для розвитку теорії чисел виявилися спроби довести велику теорему Ферма, які призвели до виникнення алгебраїчної теорії чисел, і, певною мірою, абстрактної алгебри. Роботи Л. Ейлера, Б. Рімана та багатьох інших ясно продемонстрували продуктивність аналітичного напрямку в розв'язанні теоретико-числових питань.

У елементарній теорії чисел натуральні і цілі числа вивчаються без використання методів інших розділів математики. Такі питання, як подільність цілих чисел, прості числа і їх властивості, алгоритм Евкліда для обчислення найбільшого спільного дільника і найменшого спільного кратного, розкладання числа на прості множники, ланцюгові дроби (теорія подільності), теорія порівнянь, діофантові рівняння, досконалі числа, мала теорема Ферма, теорема Ейлера та інші (теорія порівнянь), відносяться до цього розділу.

У теорії чисел у широкому розумінні розглядаються як алгебраїчні, так і трансцендентні числа, а також функції, пов'язані з арифметикою натуральних чисел, та їх узагальненнями. У дослідженнях з теорії чисел, поряд з елементарними і алгебраїчними методами застосовуються також геометричні і аналітичні. Одну із провідних тем в теорії чисел від часів Евкліда складають питання про властивості простих чисел.

Зміст методичних рекомендацій «Алгебра і теорія чисел» відповідає програмам навчальної дисципліни «Алгебра і теорія чисел» для здобувачів першого (бакалаврського) рівня вищої освіти галузі знань 01 Освіта / Педагогіка спеціальностей 014.04 Середня освіта (Математика) і

014.08 Середня освіта (Фізика) фізико-математичного факультету ДЗ «Південноукраїнський національний педагогічний університет імені К. Д. Ушинського» і охоплює теоретичний матеріал теорії подільності, яка є незмінною складовою навчальної дисципліни «Алгебра і теорія чисел». Методичні рекомендації містять теоретичний матеріал з теорії подільності, приклади розв’язання типових завдань, теоретичні завдання для самостійної роботи студентів.

Методичні рекомендації призначені для самостійної роботи студентів фізико-математичного факультету, а також можуть бути використані на лекційних і практичних заняттях з навчальної дисципліни «Алгебра і теорія чисел».

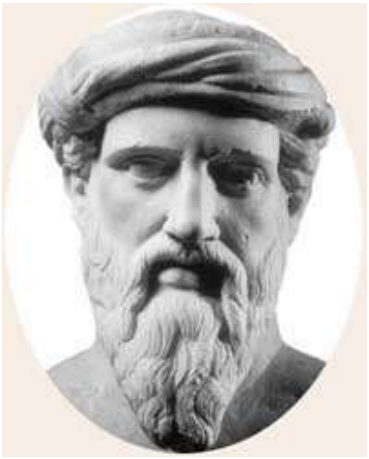
Короткий історичний огляд розвитку теорії чисел

Історія розвитку теорії чисел нерозривно пов'язана з розвитком поняття числа та дослідження властивостей натуральних і цілих чисел.

Як відомо, число дозволяє виразити результати розрахунків або вимірювань. З'явились особливі назви для чисел, спочатку невеликих, а потім й більших. З часом люди навчилися не лише називати числа, а й позначати їх. Першими записами чисел можна вважати зарубки на дерев'яних дощечках або кістках, а пізніше – риски. Великі числа зображати таким чином було нелегко, тому стали застосовувати особливі знаки (цифри) для деякої сукупності рисок. У III ст. до н.е. Архімед розробив систему позначень чисел аж до такого величезного числа як $10^{8 \cdot 10^{16}}$.

Вже вавилоняни користувалися, по суті, позиційним принципом позначення чисел – один і той же знак означав у них і 1, і 60, і 360 (їх система числення була 60-річною). Не знали вони лише знак для нуля, – цей винахід зробили індійські математики у VI ст. Арифметичні дії над числами вавилоняни виконували за допомогою таблиць добутків, квадратів, кубів тощо, що значно спрощувало їх непрості обчислення. Математичні папіруси Древнього Єгипту (II тисячоліття до н.е.) містили навіть описи розв'язків задач, які призводять до рівняння першого степеня з одним невідомим або рівняння виду $ax^2=b$ (без використання буквених позначень, описовий характер розв'язку).

Властивості натуральних чисел вперше почали вивчати математики Стародавньої Греції. Математики піфагорійської школи (VII – IV ст до н.е.) у першу чергу цікавилися містичними і нумерологічними властивостями чисел. Вони ввели поняття досконалих і дружніх чисел. У досконалого числа сума його дільників, відмінних від самого числа, дорівнює самому числу. Наприклад, власні дільники числа 6: 1, 2 і 3, 1 + 2 + 3 = 6. Числа називаються дружніми, якщо сума власних дільників одного числа дорівнює іншому, і навпаки. Дружніми числами, наприклад, є числа 220 і 284.



Давньогрецький філософ і математик Піфагор (V ст. до н.е.) вважав, що «…елементи чисел (натуральних) є елементами усіх речей і весь світ у цілому є гармонією і числом». Піфагорійці вперше розділили числа на парні і непарні, прості і складені числа, вони вірили, що числові закони містять у собі таємниці світу.

На час появи роботи Евкліда (IV ст. до н.е.) «Начала», вже були доведені деякі факти щодо простих чисел. Евклід довів, що простих чисел нескінченно багато. Це, до речі, один з перших прикладів використання доведення від протилежного. Також він довів основну арифметики – кожне натуральне число, відмінне від 1, можна представити єдиним чином у вигляді добутку простих чисел – і дав систематичний виклад теорії подільності, в основу якої було покладено алгоритм знаходження найбільшого спільного дільника двох чисел, який ми називаємо алгоритмом Евкліда.

Систематизація проблем теорії чисел і методів їх розв’язання була проведена іншим видатним вченим Стародавньої Греції Діофантом Олександрійським (III ст. до н.е.) у його роботі «Арифметика», котра, в основному, присвячена розв’язуванню рівнянь в натуральних і додатних раціональних числах. Діофант був першим грецьким математиком, який розглядав дроби на рівні з натуральними числами. Він також першим серед античних вчених запропонував математичну символіку, яка дозволяла формулювати отримані ним результати в досить компактному вигляді.

Особливо у його роботі потрібно виділити задачі, розв’язок яких зводився до розв’язування алгебраїчних рівнянь з числом невідомих не менш двох (так званих, невизначених рівнянь або діофантових рівнянь). Наприклад, такими рівняннями є рівняння виду $3x+5y=7$, $x^2+y^2=z^2$. Діофант

розробляв методи пошуку натуральних розв’язків невизначених рівнянь. Методи Діофанта справили величезний вплив на роботи Ф. Вієта і П. Ферма. Розв’язуванням діофантових рівнянь цікавилася більшість великих математиків минулого: Л. Ейлер, А.-М. Лежандр, К. Гаус тощо. Лише у 1970 році радянський математик Ю. В. Матіясевич довів, що загального методу розв’язку таких рівнянь бути не може.

З VI століття н.е. центр математичних досліджень зміщується в Індію і Китай, держави Ближнього Сходу та Середньої Азії. Китайські та індійські математики широко використовували від’ємні числа. Китайські математики відомі своєю теоремою про залишки, для доведення якої потрібен алгоритм Евкліда. Індійські математики ввели позначення нуля і знаку для нього. Це дозволило їм створити десяткову систему запису натуральних чисел і розробити правила операцій над ними. Серед індійських математиків можемо виділити Аріабхату, Брамагупту. У працях Аріабхати зустрічається аналог алгоритму Евкліда. Брамагупта вивчав діофантові рівняння другого степеня, зокрема рівняння, яке пізніше назвали рівняння Пелля.

У Європі роботи з теорії чисел почали з'являтися тільки в пізньому Середньовіччі. Італійський математик Л. Фібоначчі (близько 1170 – 1250 рр.) систематично вводить в використання арабські цифри замість римських і 10-річну систему числення, які араби привезли в Європу. Добре відома робота Л. Фібоначчі – «Книга про абак», яку можна вважати математичною енциклопедією того часу. У книзі викладені майже всі арифметичні і алгебраїчні відомості, відомі на той момент. У ній Л. Фібоначчі вперше в Європі навів від’ємні числа, які розглядав, як «борг», дав прийоми добування кубічних коренів, застосовував 10-тирічну систему числення тощо.

Добре відомою є так звана послідовність Фібоначчі 1, 1, 2, 3, 5, 8, ... яка володіє цікавими і несподіваними властивостями. Ця послідовність вперше з'явилася в задачі «Про кроликів» Л. Фібоначчі. Після робіт Л. Фібоначчі роботи по теорії чисел стали з'являтись тільки в період пізнього Ренесансу.

Подальший розвиток теорія чисел отримала в роботах французького математика П. Ферма (1601 – 1665 рр.). Знамените рівняння П. Ферма, яке він більше трьохсот років назад написав на полях «Арифметики» Діофанта, і сьогодні відоме більш як велика теорема Ферма (рівняння $x^n+y^n=z^n$, $n>2$ не має розв'язків у цілих числах $x, y, z \neq 0$). Цю теорему довести лише у 1994 році британський математики Е. Вайлс. Відмітимо, що і досі не всі математики приймають достовірність його доведення. Сам П. Ферма навів доведення теореми лише для $n=4$. Окрім цього, відомою є мала теорема Ферма: будь-якого простого p і цілого a, вираз $a^p - a$ ділиться на p.

П. Ферма довів гіпотезу Альбера Жирара, що будь-яке просте число виду $4n + 1$ можна записати єдиним чином у вигляді суми двох квадратів, і також сформулював теорему про те, що будь-яке число можна представити у вигляді суми чотирьох квадратів. Він розробив новий метод факторизації великих чисел, і продемонстрував його на числі $2027651281 = 44021 \times 46061$.

Узагальненням малої теореми і доведенням великої теореми Ферма для окремих випадків займався на початку XVIII століття видатний німецький математик Л. Ейлер (1707 – 1783 рр.).

Він є автором 866 наукових публікацій, зокрема у галузях математичного аналізу, диференціальної геометрії, теорії чисел, теорії графів, наближених обчислень, небесної механіки, математичної фізики, оптики, балістики, кораблебудуванні, теорії музики, що мали значний вплив на розвиток науки. Саме він ввів більшість математичних понять та символів у сучасну математику, наприклад: $f(x)$, e, π, уявна одиниця i, символ суми $\sum$

тощо. Багато ранніх робіт Л. Ейлера з теорії чисел базувалось на роботах П. Ферма. Математик опрацював деякі його ідеї і спростував деякі з його припущень. Він пов'язав характер розподілу простих чисел з ідеями з математичного аналізу. Довів, що сума обернених до простих чисел розходиться. У цей спосіб він виявив зв'язок між дзета-функцією Рімана і простими числами, результат відомий як тотожність Ейлера у теорії чисел.

Л. Ейлер довів малу теорему Ферма, ввів в теорію чисел функцію Ейлера. Використовуючи властивості цієї функції, він узагальнив малу теорему Ферма до теоремою, що стала носити назву теорема Ейлера. Він зробив значний внесок у теорію досконалих чисел, якою математики були зачаровані з часів Евкліда. Ідеї Л. Ейлера підготували ґрунт для робіт К. Гауса.

Великий вплив на розвиток теорії чисел належить роботам видатного німецького математика К. Гауса (1777 – 1855 рр.).

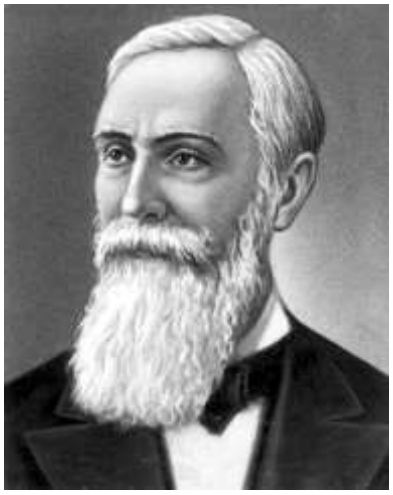
Його праці мали величезний вплив на весь подальший розвиток вищої алгебри, диференціальної геометрії, класичної теорії електрики і магнетизму, геодезії, теоретичної астрономії тощо.

У своїй першій великій роботі «Арифметичні дослідження» К. Гаус розвинув теорію квадратичних лишків, уперше довів квадратичний закон взаємності – одну з центральних теорем теорії чисел. У вказаній роботі він по-новому докладно розробив теорію квадратичних форм, яку раніше побудував Ж.-Л. Лагранж, виклав теорію поділу кола, яка багато в чому була прообразом теорії Е. Галуа. К. Гаус розробив загальні методи

розв'язання рівнянь виду $x^n-1=0$, а також встановив зв'язок між цими рівняннями і побудовою правильних многокутників, а саме: знайшов усі такі значення n, для яких правильний n-кутник можна побудувати циркулем і лінійкою. Це було першим, після древньогрецьких геометрів, значним кроком уперед у цьому питанні.

Дослідження та роботи Гауса мали таку глибину, різносторонність, розкриття нових, невідомих до того законів природи в галузі фізики, геодезії, що математики-сучасники вважали К. Гауса найкращим математиком світу, «королем» математики.

Серед значних робіт відомих математиків, які вплинули на розвиток теорії чисел як науки, можна відмітити, зокрема, роботи Й. Дирихле. Й. Дирихле разом з К. Гаусом, своїм вчителем, створили теорію квадратичних форм. Крім того, вони сформулювали ряд завдань щодо кількості цілих точок в областях на площині.



Відмітимо роботи російського математика XIX ст. П. Чебишева, який займався вивченням розподілу простих чисел і показав закон прямування до нескінченності числа простих чисел, довів гіпотезу Бертрана про існування простого числа в інтервалі $(x, 2x)$, $x \geq 2$.

У другій половині XIX ст. та на початку XX ст. над розвитком теорії чисел працювали О. М. Коркін, Є. І. Золотарьов і А. А. Марков, Д. Гільберт і Е. Куммер, Ш. Ерміт, Ф. Лінденман, Ш. ла Валле Пуссен і Ж. Адамар, Б. Ріман, Г. Вейль, Г. Вороний та інші. Великий внесок у розвиток теорії чисел як науки належить радянському математику І. М. Виноградову.

У XX ст. в роботах Д. Гілберта, Т. Такагі, Ф. Фуртвенглера, Г. Хассе, Е. Артіна була побудована теорія полів класів, що знаходить застосування в алгебраїчній теорії чисел. Радянський математик А. О. Гельфонд в 1934 році вирішив 7-му проблему Гілберта про трансцендентність чисел спеціального

виду. Питання наближення алгебраїчних чисел раціональними були розвинені в роботах А. Тує, К. Зігеля і Ф. Рота.

Чим особливою є теорія чисел? Пошук розв'язку проблем теорії чисел часто виходив за її рамки і був поштовхом розвитку нових розділів теорії чисел, математики або суміжних наук, наприклад, фізики, інформатики, криптографії тощо. Поняття «кільця» і «ідеалу», які виникли в теорії чисел, стали одними з основних понять сучасної теоретичної математики.

Теорія чисел знайшла своє застосування в теорії телефонних мереж (кабелів), в кристалографії, при розв'язанні деяких завдань теорії наближених обчислень, теорії динамічних систем тощо. З другої половини XX ст. результати теорії чисел почали широко застосовувати в теорії кодування і захисту інформації. Широко використовують теорію чисел і у криптографії – науці про математичні методи забезпечення конфіденційності, цілісності і автентичності інформації. У традиційній криптографії з неважкими перетвореннями (проста заміна, перестановка, гамування) не було необхідності застосовувати глибокі результати теорії чисел. Ситуація змінилася з появою криптосистем з відкритим ключем, в основі яких лежать односторонні перетворення, наприклад операція піднесення до степеня за великим модулем. Авторами криптосистем з відкритим ключем були американські вчені У. Діффі і М. Хеллман. Вперше вона була реалізована в вигляді системи RSA, назва якої утворено початковими буквами прізвищ авторів: Р. Ривест, А. Шамір, Л. Адлеман. В криптосистемі RSA використовується степенева функція $y=x^e \pmod N$. При цьому виникає задача вибору модуля N і степеня e,таких, що існує степінь d, що задовольняє умові $y^d=x \bmod N$ для будь-якого $0 \le x \le N-1$.

Чимало питань теорії чисел залишаються відкритими і сьогодні. До таких задач, наприклад, можна віднести гіпотезу Гольдбаха (будь-яке парне натуральне число є сумою двох простих); знаходження формули, яка задаватиме прості числа; гіпотезу про нескінченність множини чисел-близнюків (простих чисел, що відрізняються одне від одного на 2); гіпотезу

Рімана (доведення або спростування якої буде мати далекосяжні наслідки для теорії чисел, особливо в частині розподілу простих чисел) тощо.

Відомий англійський математик Г. Х. Харді стверджував, що елементарну теорію чисел слід вважати одним з кращих предметів для початкового математичної освіти. Вона вимагає дуже мало попередніх знань, а предмет її зрозумілий і близький; методи міркувань, прийняті нею, прості, загальні і нечисленні; серед математичних наук немає рівної їй у зверненні до природної людської допитливості. Дійсно, багато питань ставляться настільки конкретно, що зазвичай допускають «експериментальну» числову перевірку; велика кількість досить глибоких проблем допускає наочну інтерпретацію (наприклад, знаходження «піфагорових трійок»).

До того ж елементарна теорія чисел найкращим чином поєднує дедуктивне і інтуїтивне, що вельми важливо при викладанні математики. Теорія чисел дає ясні і точні доведення та теореми бездоганної строгості, формує математичне мислення і сприяє набуттю навичок, корисних в будь-якій галузі математики. Найчастіше розв’язання її завдань вимагає подолання значних труднощів, математичної винахідливості, пошуку нових методів і ідей, що знаходять продовження в сучасній математиці.

§ 1. Відношення подільності на множині натуральних чисел та його властивості

Поняття подільності – одне з основних понять арифметики і теорії чисел. Античні математики вважали важливим розглядати разом з кожним числом всі його дільники. Числа, що мають багато дільників, називалися «abundant» (надлишковими), а які мають мало дільників, – «defizient» (недостатніми), при цьому в якості запобіжного заходу використовувалася не кількість, а сума дільників, яку порівнювали з самим числом. На жаль, зустрічаються переконання, що пошук дільників чисел і розв'язання задач, які пов'язані з ними, є заняттям тільки для тих, хто обчислює, але не для математиків. Тому ми процитуємо Карла Гауса: *«…задача различать простые и составные числа, а последние разлагать на простые множители, принадлежит к важнейшим и полезнейшим задачам во всей арифметике… она занимала ум как древних, так и современных математиков…».* Завдяки праці математиків на протязі декількох тисяч років над проблемами подільності чисел було вирішено чимало задач теорії подільності, але і зараз в цьому розділі математики існують питання, на які доки не має відповіді.

Будемо розглядати множину натуральних чисел.

Означення. *Число a ділиться на число b, якщо існує таке число c, що*

$$a = b \cdot c.$$

Число a називається діленим, b – дільником і c – часткою.

Якщо a ділиться на b, то пишуть $a \vdots b$ (a кратне b або a ділиться на b).

Оберненим до відношення «$a \vdots b$» є відношення «b ділить a», яке позначають так: $b|a$.

Відношення подільності чисел має наступні властивості:

Властивість 1. *Відношення подільності рефлексивно, тобто для будь-якого $a \in N, a \vdots a$.*

Це випливає з того, що $a = a \cdot 1$ і $1 \in N$.

Властивість 2. *Відношення подільності транзитивно, тобто з* $a \vdots b$ *і* $b \vdots c$ *випливає, що* $a \vdots c$.

Дійсно, так як $a \vdots b$ і $b \vdots c$, то існують такі числа q і t, що $a = b \cdot q$ і $b = c \cdot t$. Але тоді $a = b \cdot q = (c \cdot t) \cdot q = c \cdot (t \cdot q)$ і тому $a \vdots c$.

Властивість 3. *Якщо* $a \vdots c$ *і* $b \vdots c$, *то* $(a + b) \vdots c$.

Справді, так як $a \vdots c$ і $b \vdots c$, то то існують такі числа q і t, що $a = cq$ і $b = ct$. Але тоді $a + b = cq + ct = c \cdot (q + t)$.

Так як $q + t -$ число, то $(a + b) \vdots c$.

Так само доводиться, що з $a \vdots c$ і $b \vdots c$, випливає $(a - b) \vdots c$.

Обернена властивість не виконується, тобто $(a \pm b) \vdots c$, то це не означає, що $a \vdots c$ і $b \vdots c$.

Наприклад, $10 = (2 + 8) \vdots 5$, проте 2 не ділиться на 5 і 8 не ділиться на 5.

Властивість 4. *Якщо* $a \vdots c$ *і* $b \in N$, *то* $(ab) \vdots c$.

Справді, так як $a \vdots c$, то існує $q \in N$ таке, що $a = cq$. Але тоді добуток $ab = (cq) \cdot b = c \cdot (qb)$. Так як $qb \in N$, то $(ab) \vdots c$.

Властивість 5. *Якщо* $a \vdots c$, b *не ділиться на* c, *то* $a \pm b$ *не ділиться на* c.

Справді, якби $(a + b) \vdots c$, то із $a \vdots c$ всупереч умові випливало би, що і $b \vdots c$.

Властивість 6. *Будь-яке число* $a \in N$ *ділиться на* 1.

Це випливає з того, що $a = a \cdot 1$ і $1 \in N$.

Властивість 7. *Якщо* $a \vdots b$, *то* $| a | \geq | b |$.

Справді, $a = b \cdot c$, і тому $|a| = |b| \cdot |c| \geq |b|$.

Зараз ми сформулюємо властивість, яка буде відноситися до цілих чисел.

Властивість 8. *Якщо* $a \vdots b$ *і* $| a | < | b |$, *то* $a = 0$.

Справді, якщо $a \vdots b$ і $|a| < |b|$, то виходить, що $a = b \cdot c$ і $|a| = |b| \cdot |c| < |b|$. А це виконується тоді і тільки тоді, коли $|a| = 0$ і $|c| = 0$, отже $a = 0$ і $0 = |b| \cdot 0 < |b|$.

Теорема. *Відношення подільності на множині натуральних чисел рефлексивне, антисиметричне, транзитивне, незв'язне, тобто утворює на множині натуральних чисел частковий порядок.*

1) $\forall a \in N \ a \vdots a$ – рефлексивність відношення.

2) З умов $a \vdots b$ і $b \vdots a$ слідує, що $a=b$ – антисиметричність відношення.

3) Якщо $a \vdots b$ і $b \vdots c$, то $a \vdots c$ – транзитивність відношення.

Виконання умов (1) – (3) показує, що відношення « ⋮ » встановлює на N нестрогий порядок.

Цей порядок буде частковим, бо відношення подільності не є зв’язним, тобто умова $\forall a, b \in N$: або $a \vdots b$, або $b \vdots a$, або $a=b$ не виконується. Наприклад, 5 не ділиться на 2 і 2 не ділиться на 5 і $5 \neq 2$.

Завдання. Доведіть, що на множині цілих чисел, відмінних від нуля, відношення подільності не утворює часткового порядку.

Відношення подільності на множині натуральних чисел пов'язане з операціями над ними. На цей зв'язок вказують такі теореми.

Теорема про подільність суми. *Якщо кожний із доданків ділиться на задане число, то й сума ділиться на це число.*

Обернене твердження невірне (наведіть приклад).

Теорема про подільність різниці. *Якщо зменшуване і від'ємник діляться на дане число, то й різниця ділиться на це число.*

Обернене твердження невірне (наведіть приклад).

Теорема про подільність добутку. *Якщо у добутку кількох чисел хоч один із множників ділиться на задане число, то й добуток ділиться на це*

число.

Завдання. Доведіть теореми самостійно.

Приклад 1. Довести, що $(10^{n+1} - 9n - 10) \vdots 81 \ \ \forall n \in \mathbf{N}$.

Застосуємо для доведення метод математичної індукції.

1. Перевіримо справедливість даного твердження для $n = 1$:

$10^{1+1} - 9 \cdot 1 - 10 = 81 \vdots 81$ – вірно.

2. Припустимо, що для $n=k$ твердження $(10^{k+1} - 9k - 10) \vdots 81$ вірне.

3. Доведемо, що для $n = k+1$ дане твердження вірне, тобто $(10^{(k+1)+1} - 9(k+1) - 10) \vdots 81$.

$10^{(k+1)+1} - 9(k+1) - 10 = 10^{k+1} \cdot 10 - 9k - 9 - 10 = 10(10^{k+1} - 9k - 10) + 90k + 100 - 9k - 19 = 10(10^{k+1} - 9k - 10) + 81k + 81.$

Оскільки перший доданок суми ділиться на 81 за припущенням, другий та третій – за властивостями відношення подільності, то і вся сума ділиться на 81, що і треба було довести. Таким чином доведено, що твердження вірне для всіх $n \in \mathbf{N}$.

Для того, щоб зрозуміти, чи ділиться число a на число b, виконують операцію ділення, проте, для деяких дільників не обов'язково виконувати ділення, досить застосувати ознаки подільності.

Означення. *Ознака подільності на натуральне число n – це умова, якій відповідає число a тоді й тільки тоді, коли,* $a \vdots n$.

Сформулюємо деякі найпоширеніші ознаки подільності:

Число a ділиться **на 2** тоді і тільки тоді, коли воно закінчується цифрою 0, 2, 4, 6 або 8.

Число a ділиться **на 3 (9)** тоді і тільки тоді, коли сума його цифр ділиться на 3 (9).

Число a ділиться **на 4 (25, 50)** тоді і тільки тоді, коли число, утворене його двома останніми цифрами, ділиться на 4.

Число a ділиться **на 5** тоді і тільки тоді, коли воно закінчується цифрою 5 або цифрою 0.

Число a ділиться **на 11** тоді і тільки тоді, коли сума цифр цього числа, взятих позмінно із знаками «+» та «–», ділиться на 11.

Ознаки подільності можна доводити декількома методами, ми доведемо обрані ознаки за допомогою порозрядного розкладання числа.

Ознака подільності на 3(9)

Нехай розглядається трицифрове число $\overline{abc}$.

$\overline{abc} = 100a + 10b + c = (99a + a) + (9b + b) + c = (a + b + c) + 9(11a + b)$.

Якщо число $\overline{abc}$ ділиться на 3 (9) і другий доданок суми ділиться на 3 (9), то і доданок $(a + b + c)$ ділиться на 3 (9). Отже, число ділиться на 3 (9) тоді і тільки тоді, коли сума цифр цього числа ділиться на 3 (9).

Ознака подільності на 11

Для виводу ознаки подільності на 11 розглянемо, наприклад, чотирьох цифрове число $\overline{abcd}$ і розкладемо його по розрядах:

$\overline{abcd} = 1000a + 100b + 10c + d = (1001a - a) + (99b + b) + (11c - c) + d =$

$= (1001a + 99b + 11c) + (d - c + b - a)$.

Якщо число $\overline{abcd}$ ділиться на 11 і перший доданок ділиться на 11, то і доданок $(d - c + b - a)$ ділиться на 11. Тому число ділиться на 11 тоді і тільки тоді, коли сума цифр цього числа, взятих позмінно із знаками + і –, ділиться на 11.

Завдання. Самостійно доведіть ознаки подільності на 2, 4, 5, 8, 25, 50.

§ 2. Теорема про ділення з остачею

У цьому пункті будемо розглядати множину цілих чисел. Оскільки ділення цілих чисел націло виконується не завжди, тому введемо ***операцію***

ділення з остачею.

Означення. *Поділити з остачею ціле число a на ціле число $b\neq 0$ означає знайти таке ціле число q і таке ціле число r, $0\leq r < |b|$, що $a=bq+r$.*

При цьому число a називається діленим, b – дільником, q – неповною часткою, а r – остачею від ділення a на b.

Теорема про ділення з остачею. *Для будь-яких цілих чисел a і b, $b \neq 0$, існує єдина пара цілих чисел q і r таких, що $a = bq + r$, $0 \leq r < |b|$.*

Доведемо єдиність існування таких чисел.

Припустимо, що

$a=bq_1 + r_1 = bq_2 + r_2$, де $0 \leq r_1 < b_1$, $0 \leq r_2 < b_2$.

$bq_1 + r_1= bq_2 + r_2$

$b(q_1 – q_2) = r_2 - r_1$, звідки слідує, що $r_2 – r_1 \vdots b$ і $|r_2 – r_1| < b$,

тобто $r_2 – r_1=0$, $r_1 = r_2$, звідки $q_1 = q_2$.

З теореми слідує, що ціле число a тоді і тільки тоді кратне цілому числу $b\neq 0$, коли остача від ділення a на b дорівнює нулю. При $r=0$ ділення з остачею є діленням націло.

Приклад 2. Поділити з остачею число a на число b:

1) a=43, b=12; 2) a=12, b= 43; 3) $a = – 43$, $b = 16$.

1) За теоремою про ділення з остачею нам потрібно знайти пару цілих чисел q і r таких, що

$43= 12q + r$, де $0 \leq r < 12$.

$43 = 12 \cdot 3 + 7$, де $0 \leq 7 < 12$, $r = 7$.

Аналогічно:

2) $12 = 43 \cdot 0 + 12$, де $0 \leq 12 < 43$, $r = 12$.

3) $a = – 43$, $b = 16$. Часто в цьому випадку теорему про ділення з остачею записують так: $–43=16\cdot(–2) – 11$. Хоча це вірна рівність, але $r = –11<0$, що неможливо, оскільки остача не може бути від'ємним числом.

У цьому випадку:

$– 43 = 16 \cdot (–3) + 5$, $0 \leq 5 < 16$, $r = 5$.

§ 3. Прості та складені числа. Основна теорема арифметики

Розглядається множина натуральних чисел.

В теорії подільності загально прийнято ділення множини натуральних чисел на класи в залежності від кількості дільників у числа. Кожне натуральне число $a \neq 1$ має, принаймні, два дільника $-$ 1 і саме число a. Якщо у числа a є дільник, відмінний від 1 і a, то він називається власним.

Існують натуральні числа що не мають власних дільників і натуральні числа, які мають власні дільники. Перші числа ми назвемо простими, а другі $-$ складеними. Тому визначення простого і складеного числа можна дати через кількість дільників числа.

Означення. *Натуральне число p, відмінне від 1, називається простим, якщо воно має тільки два дільники: 1 і p.*

Означення. *Натуральне число a називають складеним, якщо воно має більше двох дільників.*

Першими простими числами в натуральному ряду чисел є числа $2, 3, 5, 7, 11, 13, 17, 19, 23, 29, 31, 37, 41, \ldots$. Серед простих чисел є лише одне парне число $-$ це число 2. Всі інші парні числа, крім 2, складені. Число 1 не належить ні до простих, ні до складених чисел. Таким чином множина натуральних чисел розбивається на три класи: перший клас містить тільки одне число $-$ 1, другий клас містить прості числа, третій клас $-$ складені числа.

Теорема Евкліда. *Множина простих чисел нескінченна.*

Припустимо, що множина простих чисел скінченна і складається з чисел 2, 3, 5,…, p, де p – найбільше просте число.

Розглянемо натуральне число $A= 2\cdot3\cdot5\cdot\ldots\cdot p + 1$, $A>1$.

При діленні числа A на 2 отримаємо остачу $r = 1$, при діленні числа A на 3 отримаємо остачу $r = 1$ і т.д. Отже, число A не ділиться на жодне з відомих простих чисел 2, 3, …, p.

Таким чином, А або нове просте число, або складене число, що не ділиться ні на одне з відомих простих чисел, тобто існує нове просте число, яке є дільником числа А. Припущення, що множина простих чисел скінченна, привела нас до суперечки, тому прості числа утворюють нескінченну множину. Теорему доведено.

Дійсно, наприклад, число А = 2·3·5 + 1 = 31 – просте, але воно не входить до множини простих чисел {2, 3, 5}.

А, наприклад, число А = 2·3·5·7·11·13 + 1 = 30031 = 59·509 – складене, але ми одержали два простих числа 59 і 509, що не входять до множини простих чисел {2, 3, 5, 7, 11, 13}.

Наслідок. *Множина складених чисел нескінченна.*

Формулювати означення простого та складеного числа можна дати не тільки з точки зору кількості дільників числа. Згідно з означенням, якщо $n -$ складене, то існує такий дільник δ, що $n = n_1\delta$, де $1 < n_1 < n, 1 < \delta < n$.

З цих міркувань випливає наступне означення простого і складеного числа.

Означення. *Якщо натуральне число a можна подати у вигляді добутку $a = b \cdot c$ тоді і тільки тоді, коли або $b = 1$ або $c = 1$, то число $a -$ просте. Якщо ж існують числа b і c такі, що $1 < b < a$ і $1 < c < a$, то число $a -$ складене.*

Приклад 3. Довести, що число $n^4 + 4$ є складеним, якщо $n \neq \pm 1$, $n \in \mathbf{Z}$.

$n^4+4 = n^4 + 4n^2 + 4 – 4n^2 = (n^2+2)^2 – (2n)^2 = (n^2+2n+2)\cdot(n^2–2n+2)$. Оскільки кожен множник більше 1 при $n \neq \pm 1$ *(доведіть самостійно)*, то число $n^4 + 4$ – складене.

Властивості простих чисел:

Розглянемо деякі властивості простих чисел.

Властивість 1. *Якщо просте число p ділиться на деяке натуральне число $n \neq 1$, то $p = n$.*

Справді, якби $p \neq n$, то p мало б три дільника: $1, p$ і n, то не було б простим.

Властивість 2. *Будь-яке натуральне число* $n > 1$ *ділиться хоча б на одне просте число.*

Застосуємо метод математичної індукції.

1) Для натурального числа $n = 2$ теорема справедлива, тобто 2 ділиться на просте число 2.

2) Припустимо, що твердження теореми справедливо для всіх натуральних чисел, більших за 1 і менших n, і доведемо справедливість теореми для числа n.

Якщо $n -$ просте, то n ділиться на просте число $p = n$, і теорема доведена.

Якщо ж n $-$ складене, то $n = n_1 c$ $(1 < n_1 < n, 1 < c < n)$.

Так як $n_1 < n$, то по індуктивному припущенню для n_1 теорема є вірною, тобто n_1 ділиться хоча б на одне просте число p. Але тоді і $n \vdots p$. Теорема доведена.

Властивість 3. *Якщо добуток двох або декількох натуральних чисел ділиться на просте число* p*, то хоча б один із співмножників ділиться на* p.

Скористаємося методом математичної індукції. Розглянемо спочатку добуток двох співмножників. Нехай $a_1 a_2 \vdots p$. Тут можливі два випадки: $a_1 \vdots p$ або a_1 не ділиться на p. Якщо $a_1 \vdots p$, то твердження доведено. Якщо a_1 не ділиться на p, то a_1 і p взаємно прості; то $a_2 \vdots p$.

Припустимо далі, що теорема справедлива для випадку, коли добуток містить менше $k + 1$ співмножників, і доведемо справедливість її для випадку $k + 1$ співмножників.

Розглянемо добуток $k + 1$ співмножників:

$$n = a_1 a_2 \dots a_k a_{k+1}.$$

Представимо цей вираз у вигляді двох співмножників, використовуючи сполучний закон:

$$n = (a_1 \dots a_k) \cdot a_{k+1} = m \cdot a_{k+1}.$$

Але для двох співмножників теорема доведена; отже, одне з чисел m або a_{k+1} має ділитися на p.

Якщо $a_{k+1} \vdots p$, то теорема доведена.

Якщо $m \vdots p$, то в силу індуктивного припущення (m містить k співмножників) хоча б одне з чисел $a_1,\ a_2, \dots, a_k$ має ділитися на p. Теорема доведена.

Для складених чисел ця властивість не виконується.

Дійсно, 48 ⋮ 4, 48 = 4·12, але 4 ⋮ 4 і 12 ⋮ 4.

Властивість 4. *Для будь-якого натурального числа $n > 1$ найменший, відмінний від 1 додатній дільник завжди є просте число.*

Розглянемо множину M додатних, відмінних від 1 дільників числа n. Множина M не порожня, так як $n \in M (n \vdots n \text{ і } n > 1)$. В множині M має бути найменше число $q > 1$. Якби q не було простим числом, то існувало б a таке, що $1 < a < q$ і $a \vdots q$; але так як $q \vdots n$, то тоді було б $a \vdots n$, що суперечить тому, що q – найменший, відмінний від одиниці додатній дільник n. Припущення, що q не є простим числом, привело нас до протиріччя, отже, q – просте число.

Властивість 5. *Найменший простий дільник складеного числа n не більше за* $\sqrt{n}$.

Дійсно, якщо $n = ab$ і a – найменший дільник, то

$$a \le b,$$

помножимо обидві частини нерівності на число a:

$$a^2 \le ab = n,$$

звідки $a \le \sqrt{n}$.

Наступна теорема грає найважливішу роль в теорії подільності і в теорії чисел. Вона називається *основною теоремою арифметики* і має досить цікаву історію. В «Началах» Евкліда вона ще не зустрічається, але деякі арифметичні пропозиції в книзі VII вже еквівалентні їй. Точно вона не

формулюється навіть у «Введении в теорию чисел», написаному в 1798 році А.-М. Лежандром. Перше точне формулювання теореми і її доведення дав К. Гаус в 1801 році в своїх відомих «Арифметических исследованиях».

Теорема (Основна теорема арифметики). *Кожне, відмінне від 1, натуральне число n можна записати у вигляді добутку простих чисел єдиним способом, якщо не брати до уваги порядку розміщення співмножників.*

Нехай a – натуральне число, більше 1.

Спочатку доведемо можливість розкладання числа a на прості множники.

Нехай p_1 – найменший додатній і відмінний від 1 дільник числа a. Це означає, що число p_1 – просте. Тоді за означенням подільності існує таке ціле число a_1, що $a = p_1 a_1$. Якщо $a_1 > 1$, то існує його найменший простий дільник p_2, звідки $a_1 = p_2 a_2$ і $a = p_1 p_2 a_2$. Якщо $a_2 > 1$, то існує його найменший простий дільник p_3, тому $a_2 = p_3 a_3$, звідки $a = p_1 p_2 p_3 a_3$. І так продовжуємо цей процес, поки не отримаємо $a_n = 1$, що неминуче, так як $a, a_1, a_2, \ldots$ – послідовність спадаючих цілих додатних чисел. Отже, ми завжди можемо отримати розкладання числа a на прості множники виду $a = p_1 p_2 \ldots p_n$ (при $n = 1$ маємо $a = p_1$, це розкладання відповідає випадку, коли число a просте).

Залишилося довести єдиність отриманого розкладу.

Припустимо, що крім розкладу $a = p_1 p_2 \ldots p_n$ існує ще один розклад числа a на прості множники $q_1, q_2, \ldots, q_m$ вида $a = q_1 q_2 \ldots q_m$. Тоді має бути справедливою рівність $p_1 p_2 \ldots p_n = q_1 q_2 \ldots q_m$.

Покажемо, що при $n \neq m$ це рівність неможливо, а при $n = m$ добутки $p_1 p_2 \ldots p_n$ і $q_1 q_2 \ldots q_m$ тотожно рівні.

Права частина останньої рівності ділиться на q_1, тоді хоча б один із множників $p_1 p_2 \ldots p_n$ повинен ділитися на q_1. Припустимо, що $q_1 \vdots p_1$, але так

як числа p_1 і q_1 прості, то $p_1 \vdots q_1$ тільки тоді, коли $q_1 = p_1$. Це дозволяє нам скоротити обидві частини рівності $p_1 p_2 \dots p_n = q_1 q_2 \dots q_m$ на $q_1 = p_1$, отримуємо $p_2 \dots p_n = q_2 \dots q_m$. Міркуючи аналогічно про p_2 і q_2, прийдемо до рівності $p_3 \dots p_n = q_3 \dots q_m$. І так діємо далі, поки в будь-якої частині рівності не скоротяться всі множники.

При $n \neq m$ ми отримаємо або рівність

$$1 = q_{n+1} \dots q_m,$$

бо рівність

$$p_{m+1} \dots p_n = 1,$$

які неможливі для простих чисел $q_{n+1} \dots q_m$ і $p_{m+1} \dots p_n$. Якщо ж $n = m$, то ми отримаємо тотожність $1 = 1$, яке вказує на тотожну рівність розкладів $a = p_1 p_2 \dots p_n$ і $a = q_1 q_2 \dots q_m$. Цим доведено єдиність розкладу числа на прості множники.

Ця теорема показує, що всі натуральні числа, відмінні від 1, дістають з простих чисел за допомогою операції множення. Кожне складене натуральне число є деяким добутком простих чисел, причому різні добутки визначають різні числа. Процес розкладу числа на прості множники називають *факторизацією*.

Задача факторизації для неспеціаліста може здаватися нескладною, проте універсального і ефективного методу факторизації чисел доки не знайдено.

Проблема визначення того, чи є вказане велике ціле число простим, завжди привертала увагу математиків. Довгий час вважалося, що вона має лише теоретичний інтерес. Однак кілька десятків років тому стало ясно, що побудова великих простих чисел є важливою для захисту інформації. Прості числа стали основою для генерації криптографічних ключів, які використовуються в найпопулярнішій криптографічній системі RSA, в системі електронних платежів WebMoney. Остання до сих пір вважається найбільш захищеною з криптографічної точки зору.

Задача факторизації чисел, або розкладання їх на множники, має тривалу історію, ще з античних часів Ератосфена (284 – 202 рр. до н.е.). У

подальшому питання розкладу на множники є пов'язаним з іменами таких великих математиків, як Л. Фібоначчі (1180 – 1250 рр.), П. Ферма (1601 – 1665 рр.), Л. Ейлер (1707 – 1783 рр.), Ж. Лежандр (1752 – 1833 рр.), К. Гаус (1777 – 1855 рр.). Фундаментальність проблеми вперше була відзначена К. Гаусом.

У розкладі $n = p_1 \cdot p_2 \cdot \ldots \cdot p_s$ (*) натурального числа n на прості множники деякі з цих множників можуть повторюватись. Якщо простий множник p_i повторюється у розкладі k раз, то його називають k-кратним множником числа n, або кажуть, що множник p_i має *кратність* k.

Позначимо символами $p_1, p_2, \ldots, p_m$ ($m \in \mathbf{N}$) попарно різні множники у розкладі (*). Нехай множник p_i ($i = 1,\ldots, m$) має відповідну кратність k_i. Тоді розклад числа n у добуток простих множників можна записати так:

$$n = p_1^{k1} \cdot p_2^{k2} \cdot \ldots \cdot p_m^{km}, \text{ де } k_i > 0,\ i = 1,\ldots, m.$$

Цей запис називають *канонічним розкладом числа n на прості множники*. Канонічний запис натурального числа єдиний.

Приклад 4. Знайти канонічний розклад числа 990, 2873.

а) Застосуємо ознаки подільності:

$$990 = 99 \cdot 10 = 3^2 \cdot 11 \cdot 2 \cdot 5 = 2 \cdot 3^2 \cdot 5 \cdot 11.$$

б) Дане число не має малих дільників (2,3,5,7), тому використаємо метод пробних ділень:

$$\sqrt{2873} \approx 53$$

Випишемо усі прості числа до числа 53 включно: 2, 3, 5, 7, 11, 13, 17, 19, 23, 29, 31, 37, 41, 43, 49, 53.

$2873 = 13 \cdot 221$

$\sqrt{221} \approx 14$

2, 3, 5, 7, 11, 13

$221 = 13 \cdot 17$

$2873 = 13 \cdot 13 \cdot 17 = 13^2 \cdot 17.$

Наслідок. *Якщо натуральні числа a і b, відмінні від 1, записано в формі*

$$a = p_1^{k1} \cdot p_2^{k2} \cdot \ldots \cdot p_m^{km},\ k_i \geq 0,$$

$$b = p_1^{t1} \cdot p_2^{t2} \cdot \ldots \cdot p_m^{tm},\ t_i \geq 0,$$

то $a \vdots b$ *тоді і тільки тоді, коли* $k_i \geq t_i$, $i = 1, \ldots, m$.

Цей наслідок іноді називають *загальною ознакою подільності* натуральних чисел. Доведемо його для загального випадку.

Теорема (загальна ознака подільності). *Якщо канонічний розклад числа* $n = p_1^{k_1} p_2^{k_2} \ldots p_m^{k_m}$, *то всі дільники цього числа збігаються з числами вигляду*

$$d = p_1^{s_1} p_2^{s_2} \ldots p_m^{s_m}, \qquad (*)$$

де $0 \leq s_i \leq k_i$, $i = 1, 2, \ldots, m$.

Справді, очевидно, що всяке число d виду (*) є дільником числа n. Навпаки, якщо d є дільником числа n, то $n = dq$, де q – деяке натуральне число. Через те, що для n існує тільки один канонічний розклад, то з рівності $n = dq$ випливає, що в канонічний розклад числа d можуть входити тільки прості числа $p_1, p_2, \ldots, p_m$, причому їх степені відповідно не вищі від $k_1, k_2, \ldots, k_m$. Тому канонічне зображення d має вигляд (*).

Візьмемо тепер довільні два натуральних числа a і b. Припустимо, що вони мають такі канонічні розклади:

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

Позначимо символами $p_1 p_2 \ldots p_s$ всі різні множники, кожен з яких входить до розкладу принаймні одного з чисел a і b, то вважатимемо, що він входить до цього розкладу в нульовому степені. За цієї умови канонічні розклади чисел a і b можна записати так:

$$a = p_1^{k_1} p_2^{k_2} \ldots p_s^{k_s}, \qquad b = p_1^{m_1} p_2^{m_2} \ldots p_s^{m_s},$$

де кожен з показників k_i і m_i, $i = 1, 2, \ldots, s$, є ціле невід'ємне число. Для чисел a і b правильні такі твердження.

Приклад 5. Числа $a = p_1^{n+5} p_2^{21-3n}$ і $b = p_1^{7} p_2^{2n-1}$ записано у канонічній формі, p_1, p_2 – різні прості числа. При яких натуральних значеннях n число a ділиться на число b?

Маємо систему лінійних нерівностей:

$\begin{cases} n+5 \geq 7 \\ 21-3n \geq 2n-1 \end{cases} \quad \begin{cases} n \geq 2 \\ n \leq 4{,}4 \end{cases}$, звідки n=2, 3, 4.

§ 4. Число та сума натуральних дільників натурального числа *n*

Число натуральних дільників числа $n \in N$

Функція $\tau(n)$ визначена для всіх $n \in \mathbf{N}$, і її значення дорівнює числу всіх натуральних дільників числа *n*.

Теорема. *Якщо число n має канонічний розклад* $n = {p_1}^{k_1}{p_2}^{k_2} \dots {p_n}^{k_m}$, *то* $\tau(n) = (k_1 + 1)(k_2 + 1)\dots(k_m + 1)$.

Всі дільники числа n збігаються з числами вигляду $d = {p_1}^{s_1}{p_2}^{s_2} \dots {p_m}^{s_m}$, де $0 \leq s_i \leq k_i,\ i = 1, 2, \dots, m$. Оскільки показник s_1 може набувати $k_1 + 1$ значень від 0 до k_1, s_2 може набувати $k_2 + 1$ значень від 0 до $k_2, \dots, s_m$ може набувати $k_m + 1$ значень від 0 до k_m, то ${p_1}^{s_1}$ може набувати $k_1 + 1$ різних значень, ${p_2}^{s_2}$ може набувати $k_2 + 1$ різних значень, …, ${p_m}^{m}$ може набувати $k_m + 1$ різних значень. Тому за узагальненим правилом добутку d може набувати $(k_1 + 1)(k_2 + 1) \dots (k_m + 1)$ різних значень.

Отже, число n має $(k_1 + 1) \cdot (k_2 + 1) \dots (k_m + 1)$ додатних дільників, тобто $\tau({p_1}^{k_1}{p_2}^{k_2} \dots {p_m}^{k_m}) = (k_1 + 1)(k_2 + 1) \dots (k_m + 1)$.

Теорему доведено.

Наслідок. *Якщо p – просте, то τ(p)=2.*

Дійсно, так як *p* – просте, то воно має лише два дільники.

Сума натуральних дільників числа $n \in N$

Функція $\sigma(n)$ визначена для всіх $n \in \mathbf{N}$, і її значення дорівнює сумі всіх натуральних дільників числа *n***.**

Теорема. *Якщо число n має канонічний розклад* $n = {p_1}^{k_1}{p_2}^{k_2} \dots {p_n}^{k_m}$, *то* $\sigma(n) = \frac{p_1^{\alpha_1+1}-1}{p_1-1} \cdot \frac{p_2^{\alpha_2+1}-1}{p_2-1} \cdot \dots \cdot \frac{p_m^{\alpha_m+1}-1}{p_m-1}$.

Множина дільників числа n збігається з множиною чисел виду ${p_1}^{s_1}{p_2}^{s_2} \dots {p_m}^{s_m}$, де $s_i = 0, 1, 2, \dots, k_i, i = 1, 2, \dots, m$.

Тому

$$\sigma({p_1}^{k_1}{p_2}^{k_2} \dots {p_m}^{k_m}) = \sum {p_1}^{s_1}{p_2}^{s_1} \dots {p_m}^{s_m}$$

$(s_i = 0, 1, 2, \dots, k_i, i = 1, 2, \dots, m)$.

Але $\sum {p_1}^{s_1}{p_2}^{s_1} \dots {p_m}^{s_m} = (1 + p_1 + {p_1}^2 + \dots + {p_1}^{k_1})(1 + p_2 + {p_2}^2 + \dots + {p_2}^{k_2}) \dots (1 + p_m + {p_m}^2 + \dots + {p_m}^{k_m})$

$(s_i = 0, 1, 2, \dots, k_i, \ \ i = 1, 2, \dots, m)$.

Справді, виконавши множення у правій частині рівності, дістанемо доданки вигляду ${p_1}^{s_1}{p_2}^{s_1} \dots {p_m}^{s_m}$, де s_i набуває значень від 0 до $k_i (i = 1, 2, \dots, m)$, тобто всі доданки лівої частини рівності, причому кожен з цих доданків ми отримуємо лише раз.

Оскільки $(1 + p_i + {p_i}^2 + \dots + {p_i}^{k_i}) = \frac{{p_i}^{k_i+1}-1}{p_i-1} (i = 1, 2, \dots, m)$, то

$$\sum {p_1}^{s_1}{p_2}^{s_1} \dots {p_m}^{s_m} = \frac{{p_1}^{k_1+1}-1}{p_1-1} \cdot \frac{{p_2}^{k_2+1}-1}{p_2-1} \dots \frac{{p_m}^{k_m+1}-1}{p_m-1}$$

$(s_i = 1, 2, \dots, k_i, \quad i = 1, 2, \dots, m)$.

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

Теорему доведено.

Наслідок. *Якщо p – просте, то σ(p) = p + 1.*

Дійсно, дільниками простого числа *p* є тільки 1 і *p*.

Приклад 6. Знайти число і суму всіх натуральних дільників числа 360.

Знаходимо канонічний розклад числа $360 = 2^3 \cdot 3^2 \cdot 5^1$, тоді:

$\tau(360) = (3 + 1)(2 + 1)(1 + 1) = 24$,

$$\sigma(360)=\frac{2^{3+1}-1}{2-1}\cdot\frac{3^{2+1}-1}{3-1}\cdot\frac{5^{1+1}-1}{5-1}=1170.$$

Означення. *Натуральне число* n *називається досконалим, якщо виконується* $\sigma(n)=2n$*, тобто сума дільників числа дорівнює подвоєному цьому числу.*

Якщо $\sigma(n)<2n$, то число n называється *недостатнім*, а якщо $\sigma(n)>2n$, то число n называється *надлишковим*.

Всі степені простих чисел є недостатніми (*доведіть самостійно*).

Кожне досконале число повинно містити, щонайменше, два різних простих дільника.

Піфагорійці знали тільки три таких числа: $6, 28, 496$.

$28=1+2+4+7+14;$

$496=1+2+4+8+16+31+62+124+248.$

У «Арифметиці» Нікомаха із Герази (I ст. н. е.) зустрічається четверте досконале число: 8128. Нікомах писав*: «Совершенные числа красивы. Однако красивые вещи редки и малочисленны. Большинство чисел являются избыточными или недостаточными, в то время как совершенных чисел немного. Среди единиц их всего лишь одно, так же среди десятков, сотен и тысяч».* Зі сказаного видно, що в міру просування від початку в натуральному ряду досконалі числа зустрічаються все рідше. У перших $10\,000$ натуральних чисел є всього чотири досконалих числа. На сьогодні відомо сорок дев'ять парних досконалих чисел. Ніхто доки не зміг довести, непарні досконалі числа існують.

§ 5. НСД та НСК натуральних чисел

У цьому пункті будемо розглядати лише натуральні числа.

Означення. *Якщо кожне з натуральних чисел* $a_1, a_2, \ldots, a_n$ *ділиться на натуральне число* d*, то число* d *називається спільним дільником чисел* $a_1, a_2, \ldots, a_n$*. Найбільший спільний дільник чисел* $a_1, a_2, \ldots, a_n$ *називається найбільшим спільним дільником (НСД) цих чисел і позначається символом*

$(a_1, a_2, \ldots, a_n)$.

Якщо НСД чисел $a_1, a_2, \ldots, a_n$ дорівнює 1, то ці числа називають *взаємно простими*. Наприклад, числа 12 і 25; 12, 77 і 50 – взаємно прості.

Розглянемо основні властивості НСД чисел:

Властивість 1. *Якщо $a \vdots b$, то $(a, b) = b$, де $a, b \in \boldsymbol{N}$.*

Зрозуміло, що кожний дільник числа b є дільником числа a. Множина спільних дільників чисел a і b співпадає с множиною дільників числа b, тому НСД чисел a і b є само число b.

Властивість 2. *Якщо натуральні числа a, b, q, r зв'язані умовою $a=bq+r$, то $(a, b) = (b, r)$.*

Завдання. Доведіть властивість 2 самостійно.

Властивість 3. *Алгоритм Евкліда.*

Для знаходження НСД двох натуральних чисел користуються *алгоритмом Евкліда*. Будемо вважати, що $a \geq b$.

Розділимо число a на b, за теоремою про ділення з с остачею дістанемо:

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

Тепер розділимо b на r_1 і т. д.:

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

$$r_1 = r_2q_3 + r_3, \qquad \text{де } 0 \leq r_3 < r_2 \text{ і т.д.}$$

Отримаємо монотонно спадаючу, обмежену знизу послідовність невід'ємних цілих чисел: $b > r_1 > r_2 > \ldots \geq 0$. Тому на деякому кроці дістанемо, що $r_{n-1} = r_nq_{n+1} + 0$, де $r_{n+1} = 0$. За властивістю 2:

$$(a, b) = (b, r_1) = (r_1, r_2) = \ldots = (r_{n-1}, r_n) = (r_n, r_{n+1}) = (r_n, 0) = r_n.$$

Остання, відмінна від нуля остача в алгоритмі Евкліда, що застосовано до чисел a і b, є найбільшим спільним дільником чисел a і b.

Приклад 7. Знайти НСД чисел 1066 і 1970 за алгоритмом Евкліда.

Виконуємо послідовне ділення за алгоритмом Евкліда:

$1970 = 1066 \cdot 1 + 904, \quad b_1 = 1066, r_1 = 904,$

$1066 = 904 \cdot 1 + 162, \quad b_2 = 904, \quad r_2 = 162,$

$904 = 162 \cdot 5 + 74, \quad b_3 = 162, \quad r_3 = 74,$

$162 = 74 \cdot 2 + 14, \quad b_4 = 74, \quad r_4 = 14,$

$74 = 14 \cdot 5 + 4, \quad b_5 = 14, \quad r_5 = 4,$

$14 = 4 \cdot 3 + 2, \quad b_6 = 4, \quad r_6 = 2,$

$4 = 2 \cdot 2 + 0, \quad b_7 = 2, \quad r_7 = 0.$

Таке послідовне ділення можна записати в скороченій формі:

		106	
	1970	6	
	1066	1	
1066	904		$=r_1$
904	1		
904	162		$=r_2$
830	5		
162	74		$=r_3$
148	2		
74	14		$=r_4$
70	5		
14	4		$=r_5$
12	3		
4	2		$=r_6$
4	2		
0			$=r_7$

У нашому випадку $r_6 = 2$, $r_7 = 0$, тоді (1066, 1970) = 2.

Давньогрецькі математики називали цей алгоритм «взаємне віднімання». Алгоритм не було відкрито Евклідом, так як згадка про нього є вже в *Топіці* Аристотеля. Але Евклід описав його в своїх «Началах»: в VII книзі для знаходження найбільшого спільного дільника двох натуральних чисел і в X

книзі для знаходження найбільшої спільної міри двох однорідних величин. В обох випадках Евклід дав геометричний опис алгоритму як алгоритму для знаходження найбільшої спільної міри двох відрізків.

Властивість 4. $(am, bm) = m(a, b)\ \forall m \in \mathbf{N}$.

Для доведення цієї властивості достатньо помножити усі рівності в алгоритмі Евкліда на *m*.

Приклад 8. Знайти НСД чисел 432 і 240.

За властивістю 4:

$(432, 240) = 4\cdot(108, 60) = 16\cdot(27,15) = 48\cdot(9,5) = 48\cdot 1 = 48.$

Властивість 5. *Якщо (a, b) = d, то* $\left(\frac{a}{d}, \frac{b}{d}\right) = 1$.

Дійсно, якщо $\left(\frac{a}{d}, \frac{b}{d}\right) \neq 1$, то позначимо $\left(\frac{a}{d}, \frac{b}{d}\right) = c$, де $c>1$.

Маємо $\left(c\cdot\frac{a_1}{c}, c\cdot\frac{b_1}{c}\right) = c\cdot\left(\frac{a_1}{c}, \frac{b_1}{c}\right)$ за властивістю 4. Але тоді $(a, b)=dc$. Дістали протиріччя, наше припущення невірне.

Властивість 6. $(a_1, a_2, a_3) = ((a_1, a_2), a_3)$.

Властивість 7 ***(****Співвідношення Безу). Якщо (a, b) = d, то існує пара цілих чисел x і y таких, що d = ax + by.*

Таке представлення називають *лінійним зобрознакаженням НСД чисел a і b*. Числа *x* та *y* називають *коефіцієнтами Безу*. Коефіцієнти Безу визначені неоднозначно.

Приклад 9. Знайти лінійне зображення НСД чисел 899 і 493.

Знайдемо $d = (899,493)$ та цілі числа x і y, такі, що $d = 899x + 493y$. Використаємо алгоритм Евкліда:

$899 = 493 \cdot 1 + 406,$

$493 = 406 \cdot 1 + 87,$

$406 = 87 \cdot 4 + 58,$

$87 = 58 \cdot 1 + 29,$

$58 = 29 \cdot 2 + 0$, звідки $d = 29$.

Починаючи з передостанньої рівності, виражаємо остачі:

$d = 29 = 87 - 58 \cdot 1,$

$58 = 406 - 87 \cdot 4,$

$87 = 493 - 406 \cdot 1,$

$406 = 899 - 493 \cdot 1.$

Замінюватимемо послідовно остачі в цих рівностях:

$d = 29 = 87 - 58 \cdot 1 = 87 - (406 - 87 \cdot 4) = 5 \cdot 87 - 406 =$

$=5 \cdot (493 - 406 \cdot 1) - 406 = 5 \cdot 493 - 6 \cdot 406 =$

$= 5 \cdot 493 - 6 \cdot (899 - 493) = 11 \cdot 493 - 6 \cdot 899.$

Отже, $29 = 11 \cdot 493 - 6 \cdot 899$, звідки $x = -6$, $y = 11$.

Означення. *Нехай $a_1, a_2, \ldots, a_n$ – натуральні числа. Натуральне число M, яке ділиться на всі числа $a_1, a_2, \ldots, a_n$, називають спільним кратним цих чисел. Найменше з спільних кратних чисел $a_1, a_2, \ldots, a_n$ називають найменшим спільним кратним (НСК) цих чисел і позначають символом $[a_1, a_2, \ldots, a_n]$.*

Властивість 1. Одним із способів знаходження НСД і НСК натуральних чисел ґрунтується на розкладі чисел на прості множники.

Нехай числа a і b записано у виді наступного розкладу:

$a = p_1^{k1} \cdot p_2^{k2} \cdot \ldots \cdot p_m^{km}$, $k_i \geq 0$,

$b = p_1^{t1} \cdot p_2^{t2} \cdot \ldots \cdot p_m^{tm}$, $t_i \geq 0$,

де $p_1, p_2, \ldots, p_m$ – різні прості множники, кожен з яких входить до розкладу хоча б одного з чисел a і b. Якщо простий множник p_i не міститься в

канонічному розкладі якого-небудь з чисел a і b, то вважатимемо, що він входить до цього розкладу в нульовій степені. Тоді:

$$(a,b)=p_1^{\min(k1,t1)}\cdot p_2^{\min(k2,t2)}\cdot\ldots\cdot p_m^{\min(km,tm)},$$

$$[a,b]=p_1^{\max(k1,t1)}\cdot p_2^{\max(k2,t2)}\cdot\ldots\cdot p_m^{\max(km,tm)}.$$

Приклад 10. Знайти НСД і НСК чисел 1066 і 1970 «шкільним» способом. Знайдемо канонічні розклади чисел 680 і 5202:

$680 = 2^3 \cdot 5 \cdot 17$, $5202 = 2 \cdot 3^2 \cdot 17^2$.

$(680, 5202) = 2^1 \cdot 17^1 = 34$,

$[680, 5202] = 2^3 \cdot 3^2 \cdot 5^1 \cdot 17^2 = 104040$.

Наступний спосіб знаходження НСК не потребує розкладу числа на прості множники.

Властивість 2. $[a,b]=\frac{ab}{(a,b)}$, *де a, b – довільні натуральні числа.*

Обчислимо $a\cdot b = p_1^{k1}\cdot p_2^{k2}\cdot\ldots\cdot p_m^{km}\cdot p_1^{t1}\cdot p_2^{t2}\cdot\ldots\cdot p_m^{tm}=(a,b)\cdot[a,b]$. Дійсно, якщо розглянути множники p_1^{k1} і p_1^{t1}, то з чисел k_1 і t_1 одне буде більшим, друге меншим, тобто один з множників ввійде у НСД, а другий – у НСК. Якщо ці числа рівні, то множник ввійде і у НСД, і у НСК.

Отримуємо, що $[a,b]=\frac{ab}{(a,b)}$.

Наслідок. *НСК взаємно простих чисел дорівнює їхньому добутку.*

Дійсно, так як $(a,b)=1$, то $a\cdot b = [a,b]$.

Приклад 11. Знайти НСК чисел 1066 і 1970.

За алгоритмом Евкліда знаходимо, що (345, 735)= 15.

$$[345,735]=\frac{345\cdot 735}{(345,375)}=\frac{345\cdot 735}{15}=16905.$$

§ 6. Функція Ейлера

Означення. *Функція Ейлера $\varphi(n)$ визначена для всіх $n \in \mathbf{N}$, і її значення*

дорівнює кількості натуральних чисел взаємно простих з числом n, які не перевищують числа n.

Розглянемо основні властивості цієї функції:

Властивість 1. *φ(1) = 1.*

Властивість 2. *φ(p) = p – 1, якщо p – просте.*

Якщо p – просте, то всі натуральні числа до p не мають з ним спільних дільників, відмінних від 1, тому $\varphi(p) = p - 1$.

Властивість 3. *$\varphi(p^k) = p^{k-1}(p - 1)$, якщо p – просте.*

Згрупуємо всі числа від 1 до p^k наступним способом:

1	2	3	...	p
$p+1$	$p+2$	$p+3$	...	$2p$
...	...	...	...	...
...	...	...	...	p^k

Кожна група містить p чисел, з них $(p-1)$ число взаємно-просте числом p. Числа розбиті на p^{k-1} групп. Тоді $\varphi(p^k) = p^{k-1} \cdot (p-1)$.

Властивість 4. *φ(ab) = φ(a)·φ(b), де a і b взаємно прості числа.*

Цю властивість називають властивістю мультипликативності.

Теорема. $\varphi(n) = n\left(1 - \frac{1}{p_1}\right)\left(1 - \frac{1}{p_2}\right) \dots \left(1 - \frac{1}{p_m}\right)$, *де* $n = {p_1}^{k_1} {p_2}^{k_2} \dots {p_n}^{k_m}$ *– канонічний розклад числа.*

Доведемо формулу, використовуючи властивості 2 і 3.

$$\varphi(n) = \varphi({p_1}^{k_1} {p_2}^{k_2} \dots {p_m}^{k_m}) = \varphi({p_1}^{k_1})\varphi({p_2}^{k_2}) \dots \varphi({p_m}^{k_m}) =$$

$$= {p_1}^{k_1 - 1} \cdot (p_1 - 1) {p_2}^{k_2 - 1}(p_2 - 1) \dots {p_m}^{k_m - 1}(p_m - 1) =$$

$$= {p_1}^{k_1}\left(1 - \frac{1}{p_1}\right) {p_2}^{k_2}\left(1 - \frac{1}{p_2}\right) \dots {p_m}^{k_m}\left(1 - \frac{1}{p_m}\right) =$$

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

Приклад 12. Обчислити функцію Ейлера для чисел 50; 383.

1) $n = 50 = 2 \cdot 25 = 2 \cdot 5^2$: $\varphi(50) = \varphi(2) \cdot \varphi(5^2) = (2 - 1) \cdot 5^{2-1} \cdot (5 - 1) = 5 \cdot 4 = 20$.

2) $n = 383$

$\sqrt{383} \approx 19$ 2, 3, 5, 7, 11, 13, 17, 19

Переконуємось, що число 383 – просте, тому φ(383) = 383 – 1 = 382.

§ 7. Скінченні ланцюгові дроби

У теорії чисел, математичному аналізі, теорії ймовірностей, в обчислювальній математиці широко використовуються так звані ланцюгові дроби.

Нехай $\alpha = \frac{a}{b}$ – раціональне число, вважаємо, що дріб нескоротний. Розділимо a на b:

$a = bq_0 + r_0$, $0 \le r_0 < b$, $q_0 = \left[\frac{a}{b}\right] \in$ Z.

$$\frac{a}{b} = \frac{bq_0 + r_0}{b} = q_0 + \frac{r_0}{b} = q_0 + \frac{1}{\frac{b}{r_0}}.$$

Числа b, $r_0 \in \mathbf{N}$ і $b > r_0$, застосуємо для цих чисел алгоритм Евкліда. Число α – раціональне, тобто зазначений процес скінченний, існує натуральне n, для якого $r_{n+1} = 0$. Тоді число $\alpha = \frac{a}{b}$ можна подати так:

$$\alpha = \frac{a}{b} = q_0 + \cfrac{1}{q_1 + \cfrac{1}{q_2 + \ldots + \cfrac{1}{q_{n-1} + \cfrac{1}{q_n}}}}.$$

Означення. *Запис раціонального числа* $\frac{a}{b} = [q_0; q_1, q_2, \ldots, q_n]$, *де* $q_0 = \left[\frac{a}{b}\right] \in \mathbf{Z}$, $q_1, q_2, \ldots, q_n \in \mathbf{N}$, *називають скінченним ланцюговим дробом.*

Тим самим було доведено теорему:

Теорема. *Кожне раціональне число можна представити у виді скінченного ланцюгового дробу єдиним способом.*

Приклад 13. Знайти раціональне число α, яке відповідає ланцюговому дробу [2; 1, 3].

$$\alpha = 2 + \frac{1}{1+\frac{1}{3}} = 2 + \frac{1}{4/3} = 2 + \frac{3}{4} = \frac{11}{4}.$$

Приклад 14. Розкласти у ланцюговий дріб звичайний дріб $-\frac{23}{36}$.

Спочатку виділимо цілу частину, для чого застосуємо теорему про ділення з остачею.

$$-\frac{23}{36} = \frac{36 \cdot (-1) + 13}{36} = -1 + \frac{13}{36} = -1 + \frac{1}{\frac{36}{13}}, q_0 = -1$$

Застосуємо алгоритм Евкліда:

36	13
26	$2 = q_1$
13	10
10	$1 = q_2$
13	3
9	$3 = q_3$
3	1
3	$3 = q_4$
0	

$$-\frac{23}{36} = [-1; 2, 1, 3, 3]$$

§ 8. Підхідні дроби

Означення. *k-тим підхідним дробом для ланцюгового дробу* $\frac{a}{b} = [q_0;q_1,q_2,\ldots,q_n]$ *називається дріб виду* $\frac{P_k}{Q_k} = [q_0; q_1, q_2, ..., q_k]$, *де* P_k *– чисельник,* Q_k *– знаменник підхідного дробу,* $0 \le k \le n$.

Очевидно, що $\frac{P_0}{Q_0} = q_0 = \left[\frac{a}{b}\right], \frac{P_n}{Q_n} = \frac{a}{b}.$

Теорема. *Чисельники і знаменники підхідних дробів можна обчислити за рекурентними формулами:*

$$\begin{cases} P_k = q_k \cdot P_{k-1} + P_{k-2} \\ Q_k = q_k \cdot Q_{k-1} + Q_{k-2} \end{cases},$$

де $P_0 = q_0$, $Q_0 = 1$.

Щоб формули виконувалися при $k = 1$, вважаємо, що $P_{-1}=1$, $Q_{-1}=0$.

Завдання. Доведіть рекурентні формули самостійно, використовуючи ММІ.

Обчислення підхідних дробів зручно проводити за допомогою таблиці:

k	–	0	1	2	- - -	n
q_k	–	q_0	q_1	q_2	- - -	q_n
P_k	1	q_0	$P_1 = q_1 \cdot q_0 + 1$	$P_2 = q_2 \cdot P_1 + q_0$	- - -	P_n
Q_k	0	1	$Q_1 = q_1 \cdot 1 + 0$	$Q_2 = q_2 \cdot Q_1 + 1$	- - -	Q_n

Приклад 15. Знайти підхідні дроби ланцюгового дробу [2; 3, 1, 1, 5].

Складемо таблицю підхідних дробів:

k	–	0	1	2	3	4
q_k	–	2	3	1	1	5
P_k	1	2	7	9	16	89
Q_k	0	1	3	4	7	39

$[2; 3, 1, 1, 5] = \frac{89}{39}$.

$$\frac{P_0}{Q_0} = 2; \frac{P_1}{Q_1} = \frac{7}{3}; \frac{P_2}{Q_2} = \frac{9}{4}; \frac{P_3}{Q_3} = \frac{16}{7}; \frac{P_4}{Q_4} = \frac{89}{39}$$

§ 9. Властивості підхідних дробів

Властивість 1. $P_k Q_{k-1} - Q_k P_{k-1} = (-1)^{k-1}$, $k \in N$, $P_0 = q_0$, $Q_0 = 1$.

Доведемо властивість математичною індукцією по k.

При $k=1$: $P_1Q_0 - Q_1P_0 = 1$

$(q_1q_0 + 1) \cdot 1 - q_1 \cdot 1 \cdot q_0 = q_1q_0 + 1 - q_1q_0 = 1$, твердження вірне.

Нехай твердження вірне для $k=n$: $P_nQ_{n-1} - Q_nP_{n-1} = (-1)^{n-1}$

Доведемо твердження для $k= n+1$:

$P_{n+1}Q_n - Q_{n+1}P_n =$

(використаємо рекурентні формули для обчислення P_k і Q_k)

$= (q_{n+1} P_n + P_{n-1}) Q_n - (q_{n+1} Q_n + Q_{n-1}) P_n =$

$= q_{n+1} P_n Q_n + P_{n-1}Q_n - q_{n+1} Q_n P_n - Q_{n-1}P_n = P_{n-1} Q_n - Q_{n-1}P_n =$

$= -(P_n Q_{n-1} - Q_nP_{n-1}) = -(-1)^{n-1} = (-1)^n$, тобто твердження вірне для $k= n+1$.

Це означає, що рівність вірна для $\forall\ n \in N$.

Властивість 2. *Знаменники підхідних дробів утворюють монотонно зростаючу послідовність, починаючи з другого номеру.*

Ця властивість випливає з виду рекурентної формули для значень Q_k.

Властивість 3. *Кожен підхідний дріб непарного порядку більше за кожен підхідний дріб парного порядку.*

Оцінимо різницю:

$$\frac{P_k}{Q_k} - \frac{P_{k-1}}{Q_{k-1}} = \frac{P_kQ_{k-1} - Q_kP_{k-1}}{Q_kQ_{k-1}} = \frac{(-1)^{k-1}}{Q_kQ_{k-1}}$$

Так як $Q_kQ_{k-1} > 0$ для $k > 1$, то знак різниці визначає множник $(-1)^{k-1}$. Якщо $k-$ парне, то $(-1)^{k-1} = -1$, а при $k-$ непарному $(-1)^{k-1} = 1$, тобто

$$\frac{P_k}{Q_k} - \frac{P_{k-1}}{Q_{k-1}} = \begin{cases} > 0 \text{ при } k \text{ непарному} \\ < 0 \text{ при } k \text{ парному.} \end{cases}$$

Властивість 4. *Чисельник і знаменник підхідного дробу є взаємно-простими числами.*

Позначимо $(P_k, Q_k) = d \geq 1$, звідки $P_k \vdots d$ і $Q_k \vdots d$.

З умови $P_kQ_{k-1}- Q_kP_{k-1}=(-1)^{k-1}$ отримуємо, що $(-1)^{k-1} \vdots d$, бо $P_kQ_{k-1}- Q_kP_{k-1} \vdots d, d \in N$. Це можливо тоді і тільки тоді, коли $d=1$, що і потрібно було довести.

Властивість 5. *Підхідні дроби парного порядку утворюють монотонно зростаючу послідовність, а підхідні дроби непарного порядку – монотонно спадаючу послідовність.*

Оцінимо різницю сусідніх підхідних дробів однакової парності:

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

Замінимо значення P_k і Q_k за рекурентними формулами:

$$\begin{cases} P_k = q_k \cdot P_{k-1} + P_{k-2} \\ Q_k = q_k \cdot Q_{k-1} + Q_{k-2} \end{cases},$$

Тоді $P_kQ_{k-2} - Q_kP_{k-2} = (q_kP_{k-1} + P_{k-2})Q_{k-2} - P_{k-2}(q_kQ_{k-1} + Q_{k-2}) =$ $=q_kP_{k-1}Q_{k-2} + P_{k-2}Q_{k-2} - P_{k-2}q_kQ_{k-1} - P_{k-2}Q_{k-2} = q_k(P_{k-1}Q_{k-2} - P_{k-2}Q_{k-1})$ = (за властивістю 1) = $q_k(-1)^{k-2}$.

Так як $q_k > 0$ і $Q_k > 0$ для $k \in \mathbb{N}$ то:

$$\frac{P_k}{Q_k} - \frac{P_{k-2}}{Q_{k-2}} = \frac{q_k(-1)^{k-2}}{Q_kQ_{k-2}} = \begin{cases} > 0, \text{якщо k} - \text{парне} \\ < 0, \text{якщо k} - \text{непарне'} \end{cases}$$

що і потрібно було довести.

Властивість 6. *Відстань між сусідніми підхідними дробами зменшується зі збільшенням їх номера. Похибка наближення* $\frac{a}{b}$ *k-им підхідним дробом* $\frac{P_k}{Q_k}$ *не перевищує* $\frac{1}{Q_k^2}$.

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

Наближення дробу підхідними дробами парного порядку є наближенням з недоліком, а парного порядку – зі збільшенням.

Вчення про неперервні (ланцюгові) дроби бере свій початок ще у Стародавній Греції. Застосування ланцюгових дробів при розв'язанні класичної задачі про квадратуру круга зіграло свою роль при знаходженні наближеного значення числа π.

Вперше ланцюгові дроби як такі з'являються в труді «Алгебра» італійського математика Рафаеля Бомбеллі (1526-1572 рр.). Р. Бомбеллі прийшов до ланцюгових дробів у процесі операції добування квадратного кореня. Скінченні ланцюгові дроби розглядав і німецький математик Даніель Швентер (1585-1636 рр.). Д. Швентер прийшов до ланцюгових дробів у процесі розв'язання проблеми наближеного представлення звичайних дробів з великими чисельниками і знаменниками. Він розкладав звичайний дріб у ланцюговий за допомогою оригінального способу. У результаті Д. Швентер знайшов рекурентні співвідношення для обчислення чисельників і знаменників підхідних дробів. Але при цьому він сам розглядав тільки звичайні дроби, чисельники яких дорівнювали 1.

Широке використання ланцюгові дроби отримали, починаючи з робіт відомого голландського фізика, астронома і математика Хрістіана Гюйгенса (1629 – 1695 рр.). У 1680 р. він працював над «планетною машиною», за допомогою якої намагався відтворити рух планет навколо Сонця. Х. Гюйгенс розглядав задачу підбору зубчатих коліс для побудови моделі, число зубців не можна було брати дуже великим, бо зробити такі зубчаті колеса у той час було неможливо, тому доводилось відшукувати наближення меншими числами. Розв`язок цієї задачі привів до розвитку теорії ланцюгових дробів.

Повну систематичну теорію ланцюгових дробів виклали Л. Ейлер та Ж. Лагранж. Термін «неперервні дроби» ввів Л. Ейлер у 1737 році. Слід зауважити, що термін «ланцюговий дріб» з'явився лише в XVIII столітті, а до цього часу використовувалося поняття «неперервний дріб». Роботи Л. Ейлера з теорії ланцюгових дробів були продовженні М. Софроновим (1729 – 1760 рр.), Д. Бернуллі (1700 – 1782 рр.) та ін.

Ланцюгові дроби мають ряд унікальних властивостей, що забезпечують їм широке використання в теоретичній та прикладній математиці. Проблема складання календаря тісно пов'язана з ланцюговими дробами. Ланцюгові дроби широко застосовуються в теорії чисел: узагальнено деякі основні алгоритми (алгоритм Евкліда, Остроградського, Ейлера), побудовано

ефективні методи розв'язання алгебраїчних і трансцендентних рівнянь, невизначених рівнянь, рівнянь рекурентного типу тощо. Ланцюгові дроби дають велику перевагу в точності при наближеному знаходженні коренів квадратних рівнянь, обчисленні логарифмів чисел. Ланцюгові дроби використовуються для знаходження наближених значень функцій. У даний час ланцюгові дроби знаходять все більше застосування в обчислювальній техніці.

§ 10. Відношення порівнянності цілих чисел за модулем

Нехай m – деяке натуральне число, $m \neq 1$.

Означення. *Цілі числа a і b називають порівнянними (конгруентними) за модулем m, якщо $(a - b) \vdots m$.*

Символічно це відношення записується $a \equiv b \pmod{m}$ і читається «a порівняно з b за модулем m».

Приклад 16. Які з чисел a, b, c порівнянні з числом $d = 15$ за модулем $m = 27$, якщо $a = 217$, $b = 150$, $c = -363$?

Складемо відповідні порівняння і перевіримо, чи є вони вірними:

1) $217 \equiv 15 \pmod{27}$.

За означенням, знаходимо:

$(217 - 15) = 202 \not\vdots 27$, тому $217 \not\equiv 15 \pmod{27}$

2) $150 \equiv 15 \pmod{27}$.

$(150 - 15) = 135 \vdots 27$, тому $150 \equiv 15 \pmod{27}$

3) $-363 \equiv 15 \pmod{19}$.

$(-363 - 15) = -378 \vdots 27$, тому $-363 \equiv 15 \pmod{27}$

Теорема. *Число a порівняно з остачею, яка утворюються при діленні даного числа на модуль m, тобто $a \equiv r \pmod{m}$, де $a = mq + r$, $0 \leq r < m$.*

За теоремою про ділення з остачею $\forall a \in \mathbf{Z}$ можна розділити на m:

$$a = mq + r, \text{ де } 0 \leq r < m.$$

Тоді $a - r = mq \vdots m$ і $a \equiv r \pmod m$.

Наслідок. *Якщо* $a \vdots m$, *то* $a \equiv 0 \pmod m$.

Теорема (Критерій порівнянності чисел за модулем). *Цілі числа порівнянні за модулем m тоді і тільки тоді, коли вони дають однакові остачі при діленні на m.*

Необхідність: нехай $a \equiv b \pmod m$. Розділимо числа a і b на модуль m.

$a = mq + r$, де $0 \le r < m$

$b = m_1q + r_1$, де $0 \le r_1 < m$

$(a - b) = m(q - q_1) + (r - r_1) \vdots m$ за умовою, тому $(r - r_1) \vdots m$ і $0 \le r - r_1 < m$, звідки $r - r_1 = 0$, тобто $r = r_1$, що і потрібно будо довести.

Достатність: доведіть самостійно.

Приклад 17. Записати у вигляді порівнянь умови:

1) при діленні на 5 число a дає остачу 3; 2) числа 19 і 9 дають неоднакові остачі при діленні на 7; 3) $n = 8k + 5$, $k \in \mathbf{Z}$; 4) n – непарне**.**

1) $a = 5t + 3$, звідки $a \equiv 3 \pmod 5$

2) $19 \not\equiv 9 \pmod 7$

3) $n \equiv 5 \pmod 8$

4) $n = 2k+1$, $k \in \mathbf{Z}$, тому $n \equiv 1 \pmod 2$.

§ 11. Основні властивості порівнянь

Властивість 1. *Порівняння за одним й тим же модулем можна почлено додавати, віднімати, множити, тобто*

якщо $a \equiv b \pmod m$, $c \equiv d \pmod m$, то $a \pm c \equiv b \pm d \pmod m$, $ac \equiv bd \pmod m$.

Доведемо цю властивість, використовуючи означення порівнянності чисел за модулем. Якщо $a \equiv b \pmod m$ і $c \equiv d \pmod m$, то $a - b = mq$ і $c - d = mk$.

Тоді $(a + c) - (b + d) = (a - b) + (c - d) \vdots m$.

Тоді $ac - bd = ac - bc + bc - bd = (a - b)c + b(c - b) \vdots m$.

Властивість 2. *Члени порівняння можна переносити із однієї частини в другу з протилежним знаком, тобто*

якщо $a+c \equiv b(mod\ m)$, то $a \equiv b-c\ (mod\ m)$.

Властивість 3. *До однієї частини порівняння можна додавати або віднімати від неї любе число, кратне модулю, тобто*

якщо $a \equiv b\ (\mathrm{mod}\ m)$, то $a \equiv b \pm mk\ (\mathrm{mod}\ m)\ \forall k \in \mathrm{Z}$.

Властивість 4. *Обидві частини порівняння можна підносити до ступеню з натуральним показником.*

Ця властивість є наслідком властивості 1.

Властивість 5. *Обидві частини порівняння можна поділити на їхній спільний дільник, якщо він взаємно простий з модулем.*

Завдання. Доведіть властивості 2-5 порівнянь самостійно.

§ 12. Кільце класів лишків Z_m

Теорема. *Відношення порівнянності цілих чисел за модулем m є відношенням еквівалентності на множині цілих чисел.*

1) рефлективність: $a \equiv a\ (\mathrm{mod}\ m)$, тому що $a - a = 0 \vdots m$.

2) симетричність: якщо $a \equiv b\ (\mathrm{mod}\ m)$, то $b \equiv a\ (\mathrm{mod}\ m)$.

$b - a = -(a - b) \vdots m$, тому $b \equiv a\ (mod\ m)$.

3) транзитивність: якщо $a \equiv b\ (\mathrm{mod}\ m)$ та $b \equiv c\ (\mathrm{mod}\ m)$, то $a \equiv c\ (\mathrm{mod}\ m)$.

(доведіть самостійно)

Тому множина цілих чисел розбивається на класи еквівалентності. В один і той же клас попадають числа, які дають одну і ту ж остачу при діленні на m, звідки випливає, що класів еквівалентності рівно m.

Класи еквівалентності називають *класами лишків* за даним модулем. *Лишком* (або представником цього класу) за модулем m називають будь-яке число цього класу. Таким чином, до класу лишків, який містить число a, належать усі цілі числа виду

$$x = a + mt, \text{ де } t \in \mathbf{Z}.$$

Цей клас позначають символом $\bar{a} = \{ x \in \mathbf{Z} | \ x \equiv a \pmod{m}\}$. Представником класу лишків $\bar{a}$ може бути будь-який елемент цього класу.

На множині класів лишків Z_m введемо операції додавання і множення наступним чином: якщо $a \in \bar{a}$, $b \in \bar{b}$, то $a+b \in \overline{a+b}$ і $a \cdot b \in \overline{ab}$. Наприклад, якщо $m = 10$, то $\bar{4} + \bar{9} = \overline{4+9} = \overline{13} = \bar{3}$, а $\bar{4} \cdot \bar{9} = \overline{4 \cdot 9} = \overline{36} = \bar{6}$.

Теорема. *Множина класів лишків відносно операцій додавання та множення класів утворює комутативне кільце з одиницею Z_m.*

Зрозуміло, що нулем кільця є клас лишків $\bar{0}$ (клас цілих чисел, які діляться на m), а одиницею кільця є клас $\bar{1}$ (клас цілих чисел, які при діленні на m дають остачу 1).

Теорема. *В кільці Z_m немає дільників нуля, якщо m – просте число.*

Теорема. *Z_m є полем, якщо m – просте число.*

Завдання. Доведіть теореми самостійно.

Завдання. Покажіть, що поле Z_m є полем скінченної характеристики m.

За модулем m виділяють *повну* та *зведену* системи лишків.

Означення. *Повною системою лишків (ПСЛ) за модулем m називають будь-яку систему лишків, утворену з m чисел, взятих по одному з кожного класу лишків.*

Повна система найменших невід'ємних лишків за модулем m – система остач від ділення на m. Ця система містить лишки 0, 1, 2, 3,…, m–1.

Теорема. *Якщо $(a, m) = 1$, b – довільне ціле число, x пробігає ПСЛ за модулем m, то лінійна форма $ax+b$ також пробігає ПСЛ за модулем m.*

Нехай $x_1, x_2, \ldots, x_{m-1}$ є ПСЛ за модулем m. Усі ці числа попарно не порівняні між собою (за означенням ПСЛ). Тоді і числа ax_i+b і ax_k+b, де x_i і x_k різні числа з ПСЛ, також непорівняні між собою за модулем m. Дійсно, якщо

$$ax_i+b \equiv ax_k+b \pmod{m}, \text{ то } ax_i \equiv ax_k \pmod{m} \text{ і } x_i \equiv x_k \pmod{m}$$

(за властивостями порівнянь), що є протиріччям.

Означення. *Якщо $(a, m) = 1$, то клас $\bar{a}$ називають взаємно простим з модулем m.*

Означення. *Зведеною системою лишків (ЗСЛ) за модулем m називають будь-яку систему лишків, утворену з φ(m) чисел, взятих по одному з кожного класу, взаємно простого з модулем m.*

Нагадаємо, що $\varphi(m)$ – значення функції Ейлера від числа m.

Теорема. *Якщо (a, m) = 1, x пробігає ЗСЛ за модулем m, то лінійна форма ax також пробігає ЗСЛ за модулем m.*

Завдання. Доведіть теорему самостійно.

Приклад 19. Виписати ПСЛ та ЗСЛ за модулем m=20.

1) Повна система найменших невід'ємних лишків:

0, 1, 2, 3, 4, 5, 6, 7, 8, 9, 10, 11, 12, 13, 14, 15, 16, 17, 18, 19.

2) Зведена система лишків.

Обчислимо $\varphi(20) = \varphi(2^2) \cdot \varphi(5) = 8$. У системі 8 елементів.

В повній системі найменших невід'ємних лишків знайдемо лишки, взаємно прості з числом 20:

(0, 20)≠1, (1, 20)=1, (2, 20)≠1, (3, 20)=1, (4, 12)≠1 і так далі.

Зведена система лишків: 1, 3, 7, 9, 11, 13, 17, 19.

§ 13. Теорема Ейлера. Теорема Ферма.

Велике значення в теорії чисел відіграють теореми Ейлера і Ферма.

Теорема Ейлера. *Якщо $a \in Z$, $m \in N$, $m > 1$ і $(a, m) = 1$, то*

$$a^{\varphi(m)} \equiv 1 (\mathrm{mod}\ m).$$

Розглянемо ЗСЛ за модулем m: $x_1, x_2, \ldots, x_{\varphi(m)}$. Якщо ми помножимо цю систему на число a, де $(a, m) = 1$: $ax_1, ax_2, \ldots, ax_{\varphi(m)}$, то вона також буде утворювати ЗСЛ за модулем m. Кожен лишок з цієї системи можна замінити найменшим невід'ємним лишком за модулем m: $r_1, r_2, \ldots, r_{\varphi(m)}$. Маємо порівняння:

$ax_1 \equiv r_1 (\mathrm{mod}\ m)$

$ax_2 \equiv r_2 (\mathrm{mod}\ m)$

……..

$ax_{\varphi(m)} \equiv r_{\varphi(m)} (mod\ m)$

Перемножимо порівняння (це можна зробити згідно з властивостями порівнянь):

$a^{\varphi(m)} x_1 x_2 \ldots x_{\varphi(m)} \equiv r_1 r_2 \ldots r_{\varphi(m)} (mod\ m).$

Оскільки $\{x_1, x_2, \ldots, x_{\varphi(m)}\} = \{ r_1, r_2, \ldots, r_{\varphi(m)} \}$, то обидві частини порівняння можна скоротити, так як усі ці числа взаємно-прості з модулем m.

Маємо: $a^{\varphi(m)} \equiv 1 (\text{mod } m)$, що і потрібно було довести.

Наступна теорема є наслідком теореми Ейлера.

Теорема Ферма. *Якщо p – просте, $(a, p) = 1$, то*

$$a^p \equiv a\ (mod\ p).$$

Дійсно, оскільки p – просте, то $\varphi(p) = p - 1$. Тоді за теоремою Ейлера матимемо $a^{p-1} \equiv 1 (\text{mod } p)$. Помножимо обидві частини порівняння на a:

$$a^p \equiv a (\text{mod } p),$$

що потрібно було довести.

Приклад 20. Чи виконується теорема Ейлера для чисел:

1) $a = 10$, $m = 51$; 2) $a = 3$, $m = 18$?

1) Оскільки $(10, 51) = 1$, то теорема Ейлера виконується.

2) Оскільки $(3, 18) = 3$, то теорема Ейлера не виконується.

Дійсно, $\varphi(18) = \varphi(3^2) \cdot \varphi(2) = 3 \cdot 2 = 6$.

$3^6 = 3^4 \cdot 3^2 = 81 \cdot 9 \equiv 9 \cdot 9 = 81 \equiv 9 \not\equiv 1 (\text{mod } 18)$.

§ 14. Порівняння 1-го степеня з одним невідомим

Порівнянням степеня n з одним невідомим за модулем m називають порівняння виду:

$$a_n x^n + a_{n-1} x^{n-1} + \ldots + a_1 x + a_0 \equiv 0 (\text{mod } m), \qquad (1)$$

де ліва частина – многочлен степеня n з цілими коефіцієнтами, $a_n \not\vdots m$.

Означення. *Розв'язком порівняння (1) називають клас лишків за модулем m, кожне число якого задовольняє це порівняння.*

Якщо a – число, яке задовольняє (1), то розв'язок порівняння записують у виді $x \equiv a \pmod m$.

Ми будемо розглядати порівняння 1-го степеню з одним невідомим, тобто порівняння виду:

$$ax \equiv b \pmod m. \qquad (2)$$

Теорема про кількість розв'язків. *Якщо у порівнянні* $ax \equiv b \pmod m$*:*

1) $(a, m) = 1$*, то порівняння має єдиний розв'язок;*

2) $(a, m) = d$, $d > 1$ *і* $b \vdots d$*, то порівняння має* d *розв'язків;*

3) $(a, m) = d$, $d > 1$ *і* $b \not\vdots d$*, то порівняння не має розв'язків.*

Зауваження. Опишемо загальну схему розв'язання порівняння (2), що має декілька розв'язків. Нехай $(a, m) = d$ і $b \vdots d$. Ділимо обидві частини порівняння та модуль на d: $a_1x \equiv b_1 \pmod{m_1}$, де $(a_1, m_1) = 1$; дане порівняння має єдиний розв'язок. Знаходимо його: $x \equiv x_0 \pmod{m_1}$. Розв'язки порівняння(2) знаходять за формулою:

$$\boldsymbol{x \equiv x_0 + m_1k \pmod m}\textbf{, де } \boldsymbol{k = 0, 1, 2, \ldots, d-1.}$$

Порівнянням 1-го степеня (лінійним порівнянням) з одним невідомим називають порівняння виду

$$ax \equiv b \pmod m. \qquad (1)$$

Означення. Розв'язком порівняння $ax \equiv b \pmod m$ називають клас лишків за модулем m, кожне число якого перетворює це порівняння в тотожність.

Якщо c – число, яке задовольняє порівняння (1), то розв'язок порівняння записують у вигляді $x \equiv c \pmod m$. Очевидно, що всі числа з класу лишків, які породжені числом c, також задовольняють це порівняння.

Насправді, $\bar{c} = \{c + mt, t \in Z\}$, тоді

$$a(c+mt) \equiv b \pmod m$$

$$a(c+mt) - b = (ac - b) + mt \vdots m$$ – істино.

Оскільки класів лишків за модулем m рівно m, то порівняння може мати максимум m розв'язків.

Теорема про кількість розв'язків порівняння.

Якщо у порівняння $ax \equiv b \pmod m$:

1) $(a, m) = 1$, то порівняння має єдиний розв'язок;

2) $(a, m) = d$, $d > 1$ и $b \vdots d$, то має d розв'язків;

3) $(a, m) = d$, $d > 1$ и $b \not\vdots d$, порівняння розв'язків не має.

Доведення:

Доведемо випадки 1) та 3), випадок 2) залишаємо для самостійної роботи.

1) Розглянемо лінійну форму $ax–b$, де x пробігає повну систему лишків (ПСЛ) за модулем m. Очевидно, що існує тільки один лишок x_0 такий, що вираз $ax_0–b$ буде ділитися на m. Якщо б знайшовся інший лишок x_1 з ПСЛ, що задовольняє цю умову, то ми б отримали, що

$$ax_0–b \equiv ax_1–b \pmod m$$

$$ax_0 \equiv ax_1 \pmod m$$

за умовою $(a, m) = 1$, тобто обидві частини порівняння можна поділити на a, отримаємо, що $x_0 \equiv x_1 \pmod m$, це означає, що ці лишки взято з одного класу, що неможливо, оскільки ми розглядаємо ПСЛ. Отже, отримали, що порівняння (1) має єдиний розв'язок.

3) якщо $(a, m) = d$, $d > 1$ та $b \not\vdots d$. Коли б у порівняння існував би розв'язок $x \equiv c \pmod m$, то порівняння $ac \equiv b \pmod m$ було б тотожністю, тобто вираз $ac–b \vdots m$ за означенням, звідки маємо, що $ac–b = mt$, та $b = ac+mt$, при чому права частина рівності ділиться на d, а ліва не ділиться на d за умовою. Отримали протиріччя, отже, наше припущення, що порівняння має розв'язок, не вірно, порівняння (1) розв'язків не має.

Приклад. Визначити кількість розв'язків порівняння:

а) $27x \equiv 44 \pmod{52}$; б) $16x \equiv 40 \pmod{56}$.

а) $27x \equiv 44 \pmod{52}$

$a = 27$, $m = 52$, $b = 44$

Встановляємо, що $(a, m)=(27, 52)=3$ та $44 \not\vdots 3$. Порівняння розв'язків немає.

б) $16x \equiv 40 \pmod{56}$

a=16, m=56, b=40

Знайдемо, що (a, m)=(16, 56)=8 і 40⋮8. Порівняння має 8 розв'язків.

Зауваження. Перед розв'язуванням порівняння необхідно визначити, скільки розв'язків має порівняння, а потім переходити до його розв'язування. Після розв'язування порівняння корисно зробити перевірку.

§ 15. Вивід ознак подільності методом Паскаля

Одним з найбільших загальних методом одержування ознак подільності є *ознака Паскаля*.

Теорема. *Для того щоб натуральне число* $a = a_n a_{n-1} \dots a_1 a_0$ *ділилось на натуральне число* m, *необхідно і достатньо, щоб на* m *ділилась сума виду* $f(a) = a_n r_n + a_{n-1} r_{n-1} + \dots + a_1 r_1 + a_0 r_0$, *де* $r_i \equiv 10^i \pmod m$, $i = \overline{0,n}$, $r_0 = 1$.

Розглянемо різницю:

$a - f(a) = (a_n 10^n + a_{n-1} 10^{n-1} + \dots + a_1 10 + a_0) - (a_n r_n + a_{n-1} r_{n-1} + \dots + a_1 r_1 + a_0 r_0) = a_n(10^n - r_n) + \dots + a_1(10 - r_1)$. Так як кожний доданок ділиться на m, то і різниця $a - f(a) \vdots m$. Звідки одразу слідує, що якщо a ділиться на m, то і $f(a)$ ділиться на m, і навпаки.

Виведемо ознаку подільності на 3, на 9 методом Паскаля.

Розкладемо число по розрядах $a = a_n 10^n + a_{n-1} 10^{n-1} + \dots + a_1 10 + a_0$. Так як $10^k \equiv 1 \pmod 3$ і $10^k \equiv 1 \pmod 9$, $k \in \mathbf{N}$, то $f(a) = a_n + a_{n-1} + \dots + a_1 + a_0$.

За ознакою Паскаля, число $a \vdots 3$ (9) $\Leftrightarrow$ $f(a) \vdots 3$(9), тобто число ділиться на 3(9) тоді і тільки тоді, коли на 3 (9) ділиться сума цифр цього числа.

Виведемо ознаку подільності на 11.

Нехай $a = a_n 10^n + a_{n-1} 10^{n-1} + \dots + a_1 10 + a_0$.

$10^k \equiv 1 \pmod{11}$, якщо k – парне, і $10^k \equiv -1 \pmod{11}$, якщо k – непарне. Тому

$$f(a) = a_0 - a_1 + a_2 - a_3 + \dots = (a_0 + a_2 + \dots) - (a_1 + a_3 + \dots).$$

За ознакою Паскаля, число $a \vdots 11 \Leftrightarrow f(a) \vdots 11$, тобто число ділиться на 11

тоді і тільки тоді, коли різниця між сумами цифр, що стоять на парних і непарних місцях, ділиться на 11.

Завдання. Виведіть самостійно ознаку подільності на 4, 5, 8 методом Паскаля.

Список використаної літератури

1. Бухштаб А. А. Теория чисел / А. А. Бухштаб. – М: Просвещение, 1966. – 386 с.
2. Воробьев Н. Н. Признаки делимости / Н. Н. Воробьев. – М: Наука, 1980. – 96 с. – (3).
3. Даан-Дальмедико А. Пути и лабиринты / А. З. Даан-Дальмедико, Ж. Пейффер. – М: Мир, 196. – 433 с.
4. Дэвенпорт Г. Высшая арифметика. Введение в теорию чисел / Г. Дэвенпорт. – М: Наука, 1965. – 176 с.
5. Завало С. Т. Алгебра і теорія чисел / С. Т. Завало, В. Н. Костарчук, В. І. Хацет. – Київ: Вища школа, Ч.2., 1980. – 400 с.
6. Куликов Л. Я. Алгебра и теория чисел / Л. Я Куликов. – Москва: Высшая школа, 1979. – 559 с.
7. Оре О. Приглашение в теорию чисел / О. Оре. – Москва: Наука, 1980. – 128 с.
8. Практикум. Алгебра і теорія чисел / С. Т. Завало, С. С. Левіщенко, В. В. Пилаєв, І. О. Рокицький. – Київ: Вища школа, 1986. – 264 с.
9. Хинчин А. Я. Цепные дроби. / А. Я. Хинчин. – М: Наука, 1980. – 112 с.
10. Хассе Г. Лекции по теории чисел / Г. Хассе. – М: Наука, 1953. – 533 с.
11. Шень А. Простые и составные числа / А. Шень. – М.: МЦНМО, 2016. – 16 с. – (3).
12. Юшкевич А. П. История математики / А. П. Юшкевич. – М: Наука, 1970.

Предметний покажчик