МІНІСТЕРСТВО ОСВІТИ І НАУКИ УКРАЇНИ
ХЕРСОНСЬКИЙ ДЕРЖАВНИЙ УНІВЕРСИТЕТ
Факультет комп'ютерних наук, фізики та математики
Кафедра алгебри, геометрії та математичного аналізу

ЧИСЛА МЕРСЕННА ТА ЧИСЛА ФЕРМА

Кваліфікаційна робота (проєкт)
на здобуття ступеня вищої освіти "магістр"

Виконала: студентка 2 курсу, 221М групи
Спеціальності 014 Середня освіта
Спеціалізації 014.04 Математика
Освітньо-професійної програми «Середня освіта (математика)»
Гринишак Світлана Володимирівна
Керівник доктор фізико-математичних наук,
професор Савченко Олександр Григорович
Рецензент професорка кафедри інформаційних технологій та фіз.-мат. дисциплін Херсонської філії Національного університету кораблебудування ім. адмірала Макарова,
докторка педагогічних наук
Літвінова Марина Борисівна

Івано-Франківськ – 2022

ЗМІСТ

ВСТУП

Теорія чисел – це розділ математики, в якому вивчаються властивості чисел. Багато тверджень в області теорії чисел, як і в математиці взагалі, відносяться не до окремих об‘єктів, а до цілого класу об‘єктів, які мають якусь спільну властивість. Особливо важливу роль в теорії чисел відіграє клас простих чисел, які виступають «цеглинками» в розкладі чисел на множники. Дивовижна теорема, названа основною теоремою арифметики [6], стверджує: будь-яке натуральне число розкладається на прості множники, причому єдиним способом (з точністю до порядку їх розміщення). Розклавши два числа на прості множники, неважко визначити, ділиться одне з них на інше чи ні. Але до сих пір буває важко визначити, чи є дане велике число простим.

Серед математиків інтерес до чисел не послаблювався ніколи. Свій внесок до розвитку загальної теорії чисел внесли такі видатні вчені свого часу, як Евклід [19], Діофант, Ферма [6], Ейлер, Діріхле [3] та інші. Першу спробу розв‘язати питання про виділення простих чисел з множини натуральних здійснив видатний старогрецький математик, астроном, географ, поет і філософ Ератосфен (276-194 рр. до н.е.) [8]. Після Ератосфена аж до XIX ст. не було знайдено досконалішого способу складання таблиці простих чисел.

Вдосконалення методу Ератосфена мало-помалу привели до того, що на сьогодні складені досить надійні таблиці простих чисел приблизно до 10000000. Вони надають у наше розпорядження широкий емпіричний матеріал, який дозволяє судити про розподіл та властивості простих чисел. Спираючись на ці таблиці, можна висловити ряд гіпотез, що стосуються простих чисел. Питанням знаходження формули простого числа займалися в свій час такі видатні математики, як П. Ферма, Л. Ейлер, Лежандр [12], проте їх пошуки елементарних формул, що давали б тільки прості числа, виявилися марними.

Серед простих чисел інтерес викликають ті, які можна знайти за рекурентними співвідношеннями. Такими є числа Мерсенна та числа Ферма. Знаходження таких чисел є важливим для задач криптографії, а простий, але повільний метод перевірки простоти заданого числа відомий як перебір дільників. Проте більш швидкі методи перевірки доступні для чисел, які мають особливі форми, такі, які числа Мерсенна та Ферма, а завдяки зручності перевірки простоти ці числа використовуються для знаходження надвеликих простих чисел.

На сьогоднішній день знайдено найбільше просте число в рамках проекту GIMPS (Great Internet Mersenne Prime Search) – це широкомасштабний проект добровільних обчислень по пошуку простих чисел Мерсенна. Цей проект вважається найбільш довготривалим, він продовжується вже більше 20 років. Таким чином, інтерес до простих чисел серед математиків та науковців не послаблюється і у наш час, а тому питання, пов’язані з цими числами, залишаються актуальними і зараз.

Основна *мета* роботи полягає у систематизації теоретичних відомостей про прості числа та шляхів і засобів розв’язування основних задач, пов’язаних з простими числами.

Предмет дослідження – загальна теорія чисел. *Об‘єкт* дослідження – клас простих чисел.

Виходячи з мети, визначені такі основні *завдання* роботи:

- розгляд основних теоретичних відомостей з теорії простих чисел;
- розкриття питання про прості числа, що задовольняють певним співвідношенням, зокрема, про числа Ферма та Мерсенна;
- розгляд можливості застосування простих чисел до розв’язування різноманітних задач теорії чисел.

Для досягнення мети дослідження і розв’язання основних завдань застосовані *методи*: теоретичний аналіз літератури з теорії простих

чисел, вивчення та узагальнення досвіду розв’язування задач, пов’язаних з простими числами, метод математичної індукції, метод доведення від супротивного.

Теоретичне значення дослідження: в найбільш доступній формі донесена інформація про прості числа, показана їх роль в теорії чисел та алгебрі. *Практичне значення* полягає у розробці практичних завдань з теми дослідження, які можуть бути запропоновані здобувачам на факультативних заняттях з математики в школі.

Дослідження було виконано в межах теми науково-дослідної роботи «Формування професійної компетентності майбутніх вчителів математики на сучасному етапі соціально-економічного розвитку України» (державний реєстраційний номер 0117U001734) кафедри алгебри, геометрії та математичного аналізу Херсонського державного університету.

Апробація результатів дослідження. За результатами виконаного дослідження було опубліковано тези в альманаху «Магістерські студії» (Херсонський державний університет).

В структурі роботи виділено три основні розділи. Перший розділ містить теоретичний матеріал, пов‘язаний з поняттям простого числа та з основними властивостями простих чисел, зокрема, розкладу числа на прості множники, питанню про кількість простих чисел в множині всіх дійсних чисел та ін.

У другому розділі розглядаються властивості простих чисел, що задовольняють певним співвідношенням, зокрема, простих чисел Ферма та Мерсенна. В ньому також розглянуто історичний аспект питання дослідження таких чисел та спроби вчених-математиків розв‘язати проблему знаходження загальної формули для простих чисел. Крім того, в розділі розглянуто алгоритм тесту Люка-Лемера, який дозволяє здійснювати пошук простих чисел Мерсенна та Ферма.

Третій розділ розкриває питання про можливість застосування

властивостей простих чисел при розв’язуванні задач теорії чисел. Цей розділ являє собою практичну частину роботи та містить приклади розв’язування задач, пов’язаних із властивостями простих чисел, натуральних чисел, ознак подільності та ін. Зміст цього розділу обумовлює практичну значимість виконаного дослідження. Матеріал роботи може бути використаний здобувачами та викладачами вищих навчальних закладів, а також вчителями загальноосвітніх шкіл.

РОЗДІЛ 1
ОСНОВНІ ПОЛОЖЕННЯ ТЕОРІЇ ПРОСТИХ ЧИСЕЛ

1.1. Загальні положення

Елементарна теорія чисел займається в першу чергу натуральними числами 1, 2, 3, … Приєднавши нуль та цілі числа, отримаємо область усіх цілих чисел, в якій необмежено виконуються операції додавання, віднімання та множення [16]. Для ділення це не так, тому поняття подільності відіграє важливу роль. Якщо натуральне число a представлено у вигляді добутку $a = dd'$, де d і d' – натуральні числа, то d називається *дільником* a. В таких випадках використовують позначення $d \mid a$. d' називають додатковим до d дільником a. Кожне a має тривіальні дільники 1, a [14].

Натуральне число $p \neq 1$ називається *простим*, якщо воно не має жодних тривіальних дільників. Число 1 не вважається простим, так як кожне ціле число ділиться на 1.

Таким чином, послідовність простих чисел починається числами

2, 3, 5, 7, 11, 13, 17, 19, 23, 29,…;

2 – єдине парне просте.

Постає питання, чи маємо ми можливість відносно кожного натурального числа $n > 1$ встановити, просте воно чи ні. Виявляється, саме визначення простих чисел дозволяє відповісти на це питання.

Дійсно, якщо натуральне число $n > 1$ не є простим, то воно представляє собою добуток двох натуральних чисел a і b, більших одиниці, тобто

$$n = ab, \text{ де } a > 1 \text{ і } b > 1,$$

звідки випливає, що $n > a$ і $n > b$. Натуральне число $n > 1$, яке не є простим, є, таким чином, добутком двох натуральних чисел, менших n. Таке число ми називаємо *складеним*. Якщо число n складене, то $n = ab$,

де a і b – натуральні > 1 і < n.

Теорема 1.1. Кожне натуральне число $n > 1$ має хоча б один простий дільник.

Доведення.

Нехай n – натуральне число > 1. Це число має дільники, більші одиниці, наприклад саме n. Серед дільників числа n, більших одиниці, існує найменший. Позначимо його через p. Якщо би число p не було простим, то, згідно з визначенням простих чисел, p було б добутком двох натуральних чисел, більших одиниці: $p = ab > a$. В цьому випадку a було б дільником числа p, а значить, і числа n, більшим одиниці і причому меншим p, що суперечить визначенню числа p.

Теорему доведено.

Теорема 1.2. Кожне складене число має принаймні один простий дільник.

Твердження 1.1. Серед кожних трьох послідовних натуральних чисел > 1 принаймні одне має хоча б два різні прості дільники.

Проте можна відмітити [17], що для $n = 7$ маємо

$$n + 1 = 2^3,\ n + 2 = 3^2,$$

і, отже, кожне з чисел n, $n + 1$, $n + 2$ має лише по одному простому дільнику.

Теорема 1.3. Множина простих чисел нескінченна.

Доведення.

Припустимо, що існує найбільше просте число p і

$$P = 2 \cdot 3 \cdot 5 \cdot 7 \cdot \ldots \cdot p$$

– добуток усіх простих чисел. Число $P + 1$ не ділиться на жодне із цих простих чисел, так як в остачі кожен раз одержуємо 1. Тому $P + 1$ або саме є простим числом > p або добутком простих чисел > p. Ми прийшли до протиріччя.

Теорему доведено.

Визначний давньогрецький математик і астроном, історик та

географ (вперше досить точно знайшов величину земного меридіану) Ератосфен (276-196 рр. до н.е.) [6] запропонував цікавий спосіб знаходження простих чисел, які не перевищують N. Треба записати всі числа від 2 до N. Число 2, яке є просте, залишити, а всі інші парні числа викреслити. Перше не закреслене число 3 залишити, а всі інші числа, які діляться на 3, викреслити. Продовжуючи цю процедуру, рано чи пізно викреслимо всі числа, які не перевищують число N і не є простими. Числа, які залишились не закресленими, будуть простими.

Цю процедуру називають *решетом Ератосфена*.

Існують таблиці простих чисел до 100000000, причому прості числа з‘являються серед натуральних за якимось дуже загадковим законом. Спробуємо оцінити зверху величину n-го простого числа, скориставшись міркуваннями Евкліда і методом математичної індукції. Припустимо, що

$$p_1 \le 2,\ p_2 \le 2^2,\ \ldots,\ p_n \le 2^{2^{n-1}}.$$

Оскільки p_{n+1} не перевищує найбільшого простого дільника числа $p_1 \ldots p_n + 1$, то, використовуючи припущення індукції, маємо:

$$p_{n+1} \le p_1 \ldots p_n + 1 \le 2^{1+2+\ldots+2^{n-1}+1} = 2^{2^n}.$$

Ця оцінка дуже завищує реальну величину p_n.

Вивчення розподілу простих чисел концентрується в першу чергу на пошуках функції $\pi(x)$, яка дає кількість простих чисел $\le x$. Розглядаючи таблицю простих чисел, можна помітити, що функція $\pi(x)$ дуже нерегулярна. Так, серед m послідовних чисел

$$(m+1)! + 2,\ (m+1)! + 3,\ \ldots,\ (m+1)! + m + 1$$

простих зовсім немає, бо перше число ділиться на 2, друге – на 3, останнє – на $m + 1$.

Взагалі в послідовності простих чисел можуть бути як завгодно великі пропуски, причому пропуски певної довжини ще й

повторюються. Так, пропуск довжини 34 лежить від 1327 і 1361, а також між 8467 і 8501. Між 370261 та 370373 лежить пропуск довжини 112.

Проте існують прості числа p, $p + 2$ з мінімальним пропуском 2. Їх називають *числами-близнюками*. Такими є числа

11 і 13, 41 і 43, 2309 і 2311, 10016957 і 10016959.

Неважко побудувати графік функції $\pi(x)$ при $x \leq 100$, важче при $x \leq 40000$.

Помітимо, що кожного разу, коли переходимо від одного степеня 10 до іншого, відношення $\frac{x}{\pi(x)}$ збільшується приблизно на $2{,}3 = ln10$.

Тому К.Ф. Гаусс [32] висловив припущення:

$$\pi(x) \approx \frac{x}{\pi(x)}, \text{ якщо } x \to \infty. \qquad (1.1)$$

Формулу (1.1) називають *асимптотичним законом розподілу простих чисел*. Наведемо таблицю, на складання якої витрачено тисячі годин підрахунків:

x	$\pi(x)$	$\frac{x}{\pi(x)}$
10	4	2,5
100	25	4,0
1000	168	6,0
10000	1229	8,0
100000	79592	10,4
1000000	78498	12,7
10000000	664579	15,0
100000000	5761455	17,4
1000000000	50847534	19,7
10000000000	455052512	22,0

Якщо порівняємо графіки функцій $\pi(x)$ та $\frac{x}{\pi(x)}$, то помітимо, що вони не зовсім збігаються. Виявляється, функція $\pi(x)$ більш схожа на функцію $\frac{x}{\ln x - 1}$. Точніше [11], у 1808 р. французький математик Лежандр (1752-1833) помітив, що $\pi(x) \approx \frac{x}{\ln x - 1{,}08366}$. Пізніше Гаусс [16] встановив, що краще функцію $\pi(x)$ наближувати логарифмічною сумою:

$$Ls(x) = \frac{1}{\ln 2} + \ldots + \frac{1}{\ln x},$$

або, що майже те саме, логарифмічним інтегралом

$$\pi(x) \approx Li(x) \approx \int_2^x \frac{dt}{\ln t}.$$

Якщо порівняти графіки функцій $\pi(x)$ та $Li(x)$, то можна побачити, що вони майже збігаються.

Строге доведення цих наближень у 1896 р. знайдено французькими математиками Ж. Адамаром (1865-1963) та Ш. Валле Пуссеном (1866-1962) [28]. Вони відмітили той факт, що хоча для функції $\pi(x)$ невідома «проста» формула, можна, однак, сформулювати твердження про її порядок. Найбільш виразним є закон розподілу простих чисел, запропонований ними, який стверджує, що відношення $\pi(x)$ і функція $f(x) = \frac{x}{\log x^2}$ прямує до 1 із ростом x.

Відносна похибка $[\pi(x) - f(x)] / \pi(x)$, яка виникає при заміні $\pi(x)$ на $f(x)$, стає таким чином з ростом x якомога меншою. Цей центральний результат відзначається як

Теорема 1.4. $\lim_{x\to\infty} \frac{\pi(x)\log x}{x} = 1$ або $\pi(x) \sim \frac{x}{\log x}$.

Крім того, справедлива наступна теорема Діріхле про арифметичну прогресію.

Теорема 1.5. Кожна арифметична прогресія $a + kd$ ($k = 0, 1, 2, \ldots$), де k і a не мають спільних дільників, містить нескінченно багато простих чисел.

Доведено, що існує нескінченно багато арифметичних прогресій, утворених із різних простих чисел. Ми знаємо багато прогресій, утворених із трьох різних простих чисел, першими членами яких є число 3, наприклад:

3, 7, 11, …; 3, 11, 19, …; 3, 13, 23, …; 3, 17, 31, …;

3, 23, 43, …; 3, 31, 59, …; 3, 37, 71, …; 3, 41, 79, …

Однак невідомо, чи існує їх нескінченно багато.

Існує тільки одна арифметична прогресія з різницею 2, складена із трьох простих чисел, а саме 3, 5, 7 (так як із трьох послідовних непарних чисел одне завжди ділиться на 3), а також тільки одна арифметична прогресія з різницею 4, а саме: 3, 7, 11. Очевидно, не може бути арифметичних прогресій, складених із трьох простих чисел, з непарною різницею.

Ми не знаємо, чи існує арифметична прогресія, утворена із ста різних простих чисел. М. Кантор довів [18], що в арифметичній прогресії, складеній із $n > 1$ простих чисел, різниця прогресій повинна ділитися на кожне просте число $\leq n$. Звідси випливає, що якщо існує арифметична прогресія, утворена із ста різних простих чисел, то різниця її повинна бути величезним числом, яке має принаймні декілька десятків цифр.

Твердження 1.2. Числа p, q і r, для яких

$$p(p + 1),\ q(q + 1) \text{ і } r(r + 1)$$

утворюють зростаючу арифметичну прогресію

Такі, наприклад, прості числа $p = 127$, $q = 3697$ і $r = 5527$.

А ось спосіб, за допомогою якого можна шукати такі прості числа.

З рівності

$$n(n + 1) + (41n + 21) = 2(29n + 14)(29n + 15)$$

випливає, що при $n \in N$ числа

$$n(n + 1),\ (29n + 14)(29n + 15) \text{ і } (41n + 20)(41n + 21)$$

складають арифметичну прогресію. Якщо б при деякому $n \in N$ числа

$$n,\ 29n + 14 \text{ і } 41n + 20$$

усі три були простими, то ми б мали три шуканих числа.

Таким чином, потрібно замість n підставляти послідовні непарні прості числа і перевіряти, чи будуть обидва числа $29n + 4$ і $41n + 20$ простими. Найменшим таким числом n є $n = 127$, яке і призводить до розв'язку, що наведено вище. Однак не можна стверджувати, що вказаним способом можуть бути знайдені усі трійки простих чисел, які задовольняють умові нашого твердження [25].

Відомо [31], що будь-яке натуральне число n можна розкласти в добуток простих чисел: $n = p_1 \cdot p_2 \cdot \ldots \cdot p_r$, $r \geq 1$, причому такий розклад з точністю до порядку множників єдиний. У ньому серед простих чисел $p_1, p_2, \ldots, p_r$ можуть бути однакові, причому, якщо серед них, наприклад, $k \leq r$ чисел різні, то n можна подати ще й в такому вигляді:

$$n = p_1^{\alpha_1} \ldots p_k^{\alpha_k},\ 1 \leq k \leq r,\ \alpha_i \geq 1,\ \alpha_1 + .. + \alpha_k = r, \qquad (1.2)$$

де α_i – кратність числа p_i у розкладі (1.2).

Розклад (1.2) називають *канонічним розкладом числа на прості множники*. Зауважимо, що єдиність розкладу натурального числа на прості множники не є очевидним фактом. Є "арифметики" [15], де аналогічна властивість не виконується.

Канонічний розклад натурального числа можна записати також у формі нескінченого добутку, розповсюдженого на всі прості числа p_i ($i = 1, 2, 3,\ldots$). При цьому показник α_t простого числа p_t, яке не входить в a, рівний нулю:

$$a = \prod_{i=1}^{\infty} p_i^{\alpha_i}\ ,\ \alpha_i \geq 0$$

для $i \geq 1,\ \alpha_i \geq 0$ лише для скінченного числа i.

Ймовірно, твердження $d \mid a$ рівнозначне нерівності $\delta_i \leq a_i$ для всіх i, якщо δ_i відіграє для d ту ж саму роль, що α_i для a. Якщо a і b представлені в такій формі, а $\tau_i = \min(\alpha_i, \beta_i)$ позначає найменше з чисел α_i і β_i для $\alpha_i \neq \beta_i$ і $\tau_i = \alpha_i$ для $\alpha_i = \beta_i$, то число

$$t = \prod_{i=1}^{\infty} p_i^{\tau_i}$$

є дільником як для a, так і для b, тобто *спільним дільником* a і b.

Так як τ_i для спільного дільника збільшити не можна, то t – найбільший спільний дільник чисел a і b. Пишуть $t = (a, b)$. Кожен інший спільний дільник a і b є дільником t. Якщо $(a, b) = 1$, то a і b називаються *взаємно простими*. Якщо під $\mu_i = Max(\alpha_i, \beta_i)$ розуміти найбільше з чисел α_i і β_i, то число $m = \coprod_{i=1}^{\infty} p_i^{\mu_i}$ буде кратним як числу a, так і числу b. Так як μ_i для загального кратного зменшити не можна, то m – *найменше кратне* чисел a і b. Пишуть $m = [a, b]$.

З рівності $ab = \prod p_i^{\alpha_i + \beta_i}$ випливає корисна формула:

$$[a,b] = \frac{ab}{(a,b)}. \qquad (1.3)$$

Діленням на $m > 0$ можна усі $n > 0$ розбити на m класів, помістивши в один клас усі числа, які мають одну і ту ж остачу. Кожен клас характеризується однією з остач 0, 1, 2, …, m – 1. Два класи a і b одного і того ж класу називають *конгруентними по модулю* m. Пишуть

$$a \equiv b (\mathrm{mod}\, m).$$

Така конгруенція рівносильна твердженню: a – b ділиться на m [21].

Розрізняють повну систему лишків по модулю m та зведену систему лишків по модулю m в залежності від того, чи розглядаються усі лишки 0, 1, 2,…, або ті з них, які взаємно прості з модулем [19].

З конгруенцій

$$a \equiv a_1 (\mathrm{mod}\, m),\ b \equiv b_1 (\mathrm{mod}\, m)$$

випливає, що

$$a \pm b \equiv a_1 + b_1 (\mathrm{mod}\, m) \text{ і } ab \equiv a_1 b_1 (\mathrm{mod}\, m).$$

Теорема 1.6 (*Ейлера*). Якщо $(a, m) = 1$, то

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

де $\varphi(m)$ – функція Ейлера.

$\varphi(m)$ позначає кількість чисел $< m$ і взаємно простих з m, зокрема

$$\varphi(p) = p - 1. \qquad (1.4)$$

Якщо d – найменший цілий додатний показник, для якого

$$a^d \equiv 1 (\mathrm{mod}\, m),$$

то кажуть, що a по *mod* m належить показнику d. Так, 2 по *mod* 7 належить показнику 3 ($2^3 \equiv 1 (\mathrm{mod}\, 7)$). Ймовірно, для $(a, m) = 1$

$$a^n \equiv 1 (\mathrm{mod}\, m)$$

тоді і тільки тоді, коли $d \mid n$; зокрема, d є дільником $\varphi(m)$.

d степенів $a, a^2, \ldots, a^d$ різні по *mod* m, так як із

$$a^r \equiv a^s \text{ і } d \geq r > s$$

випливає

$$a^{r-s} \equiv 1 \text{ при } r - s < d,$$

що суперечить вибору d. Якщо a належить по *mod* m показнику $\varphi(m)$, то a називається *первісним коренем* по *mod* m. Тоді $\varphi(m)$ степенів a, $a^2, \ldots, a^{\varphi(m)}$ являє собою в точності $\varphi(m)$ лишків, взаємно простих з m. Не для будь-якого модуля існують первісні корені, а лише для

$$m = 2, 4, p^e, 2p^e$$

(p – непарне просте число) [22].

Числа a, взаємно прості з $p > 2$, розкладаються на два класи, в залежності від того, чи має розв'язок конгруенція

$$x^2 \equiv a(\mathrm{mod}\, p),$$

чи ні. Числа першого класу називаються *квадратичними лишками* по *mod p*, другого класу – *квадратичними нелишками* по *mod p*. Ця властивість виражається символом Лежандра:

$$\left(\frac{a}{p}\right) = \begin{cases} 1, \textit{якщо } a - \textit{квадратичний лишок по} \bmod p, \\ -1, \textit{якщо } a - \textit{квадратичний нелишок по} \bmod p. \end{cases} \qquad (1.5)$$

Якщо ρ – первісний корінь по *modp*, то очевидно кожне ρ^{2k} – квадратичний лишок, а кожне ρ^{2k+1} – квадратичний нелишок.

Легко встановити справедливість важливої формули:

$$\left(\frac{a}{p}\right)\left(\frac{b}{p}\right) = \left(\frac{ab}{p}\right),\ (a, p) = (b, p) = 1. \qquad (1.6)$$

За теоремою 1.6 для $(a, p) = 1$

$$a^{p-1} - 1 = \left(a^{\frac{p-1}{2}} - 1\right)\left(a^{\frac{p-1}{2}} + 1\right) \equiv 0(\mathrm{mod}\ p)$$

Так як $-1 \not\equiv +1$ (*mod p*), то для $\forall a$ або тільки перший, або тільки другий множник ділиться на p. Для $a = \rho^{2k}$ це буде перший, а для $a = \rho^{2k+1}$ – другий множник. Звідси випливає критерій Ейлера:

$$\left(\frac{a}{p}\right) \equiv a^{\frac{p-1}{2}} (\mathrm{mod}\, p).$$

Важливе твердження про квадратичні лишки має *закон взаємності*. Цей закон виражає

Теорема 1.7. $\left(\frac{p}{q}\right)\left(\frac{q}{p}\right) = (-1)^{\frac{p-1}{2}\cdot\frac{q-1}{2}}$, ($p$, q – непарні прості числа).

1.2. Спільні критерії простих чисел

Розглянемо деякі важливі спільні критерії простих чисел.

Теорема Вільсона. Число n буде простим тоді і тільки тоді, коли

$$(n-1)! + 1 \equiv x \,(mod\ n).$$

Доведення.

За теоремою Ейлера

$$x^{p-1} - 1 \equiv 0 (mod\ p)$$

має розв'язків $1, \ldots p - 1$, тоді

$$x^{p-1} = (x-1)(x-2)\ldots(x-p+1) + pF(x).$$

Покладемо $x = 0$, тоді

$$(p-1)! \equiv -1 (mod\ p).$$

Якщо ж n складене, то воно містить простий множник $q < n$. q є дільником $(n-1)!$, так що $(n-1)! + 1$ не ділиться на q, а значить, і на n.

Теорему доведено.

Теорема Ферма. Якщо $p -$ просте число і $(a, p) = 1$, то

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

Доведення.

Дійсно, за теоремою Ейлера, якщо $(a, p) = 1$, то

$$a^{\varphi(p)} \equiv 1(p), \text{ звідки } a^{p-1} \equiv 1(p),$$

а тоді з останнього співвідношення випливає. що $a^p \equiv a(p)$.

Теорему доведено.

Теорема Лейбніца. Для того, щоб натуральне число $p > 2$ було простим, необхідно і достатньо, щоб число

$$(p-1)! - 1$$

ділилося на p.

Внаслідок тотожності

$$2n + 1 = (n+1)^2 - n^2$$

кожне непарне число можна представити у вигляді різниці двох квадратів. Для будь якого непарного простого числа таке представлення очевидно, однозначне, так як із

$$p = 2m + 1 = x^2 - y^2 = (x-y)(x+y)$$

випливає

$$x - y = 1,\ x + y = 2m + 1,$$

тобто $x = m + 1$, $y = m$. Покажемо тепер, що і загальна форма $ax^2 + by^2$, де a, b – натуральні числа, представляє просте число найбільше одним способом. Із

$$p = ax^2 + by^2 = au^2 + bv^2,$$

де x, y, u, v – натуральні числа, $(x, y) = (u, v) = 1$ випливає

$$p(v^2 - y^2) = a(x^2 v^2 - y^2 u^2)$$

і так як $a < p$, то

$$yu \equiv \pm xv \ (mod\ p). \qquad (1.7)$$

Перемноживши обидва представлення, отримаємо

$$p^2 = (axu \pm byv)^2 + ab(uy \mp vx)^2, \qquad (1.8)$$

де можна взяти або верхні, або нижні знаки.

Якщо $uy = vx$, то внаслідок

$$(u, v) = (x, y) = 1$$

буде $u \mid x$ і $x \mid u$, тобто $u = x$ і $v = y$.

Якщо $uy \neq vx$, то із (1.7) і (1.8)

$$|uy \mp vx| = p,\ a = b = 1,\ axu \pm byv = 0,$$

так як інакше (1.8) не виконується. Таким чином,

$$xu = \pm yv \text{ і } x = \pm v,\ y = \pm u$$

і представлення

$$p = x^2 + y^2 \ (a = b = 1)$$

однозначне.

Якби ми показали, що складені числа, які мають власне представлення $ax^2 + by^2$, допускають більше одного представлення, то ми отримали б критерій простих чисел, так як в цьому випадку прості числа характеризувалися би однозначним представленням. Представлення $2x^2 + 3y^2 = 14$, яке має єдиний розв'язок $x = 1$, $y = 2$, показує, що це не виконується для всіх a, b.

Ейлер помітив [26], що $x^2 + dy^2$ $(d \geq 1)$ для спеціальних значень d однозначно і власним чином представляє лише прості числа.

Коефіцієнти d він назвав *підходящими числами* (Numeri idonei). Висновок критерію, за допомогою якого Ейлер отримав Numeri idonei, не є достатньо обґрунтованим, однак Гаусс [16] за допомогою своєї теорії квадратичних форм знайшов ці ж самі числа, тим самим їх існування обґрунтовано.

Розглянемо важливу теорему.

Теорема 1.8. Конгруенція

$$x^2 + dy^2 \equiv 0 \ (p), \qquad (1.9)$$

де $p \neq 2$ – просте, $d \in N$, $(x, p) = 1$, $(y, p) = 1$ розв'язна в Z, якщо символ Лежандра $\left(\frac{-d}{p}\right) = 1$. Зокрема,

1. Якщо $d = 1$, $p = 4k + 1$, то рівняння $x^2 + y^2 = p$ має розв'язки в Z.

2. Якщо $d = 2$, $p = 8k + 1$ або $p = 8k + 3$, то рівняння $x^2 + 2y^2 = p$ має розв'язки в Z .

Наслідок 1. Якщо $p = 4k + 1$ просте число, то існує $x, y \in Z$, що

$$x^2 + y^2 = p.$$

Наслідок 2. Якщо $p = 8k + 1$ або $p = 8k + 3$ – просте число, то існують $x, y \in Z$, що $p = x^2 + 2y^2$.

Теорема 1.9. Якщо натуральне число p, більше за одиницю, не ділиться на жодне з простих чисел, квадрати яких не перебільшують p, то число p просте.

Лема 1.1. Будь-яке натуральне число, більше за одиницю, має хоча б один простий дільник.

Вивчення простих чисел та поняття спільного дільника чисел пов'язане з поняттям взаємно простих чисел. Властивості взаємно простих чисел безпосередньо визначаються за допомогою основних теорем, що мають для них місце.

Теорема 1.10. Якщо числа a і b взаємно прості, то існують такі два цілі числа x_0 та y_0, що $ax_0 + by_0 = 1$.

Теорема 1.11. Якщо число n ділиться на кожне з двох взаємно простих чисел a, b, то воно ділиться і на їх добуток ab.

Теорема 1.12. Якщо добуток ac ділиться на b і якщо числа a і b взаємно прості, то c ділиться на b.

Теорема Ейлера. $2^q - 1$ ділиться на $p = 2q + 1$ при $q = 4k + 3$.

Теорема Крайчика. $2^q - 1$ ділиться на $p = 6q + 1$ при $p = a^2 + 27c^2$.

Також для простих чисел справедливі твердження:

1) $2^q - 1$ ділиться на

$$p = 8q + 1,\ p = a^2 + 64b^2\ (b \text{ – непарне});$$

2) $2^q - 1$ ділиться на

$$p = 16q + 1,\ p = a^2 + 256b^2 = c^2 + 32d^2,$$

де – b, d – парні числа.

РОЗДІЛ 2
ПРОСТІ ЧИСЛА ФЕРМА ТА МЕРСЕННА

2.1. Числа Мерсенна

Прості числа виду

$$M_p = 2^p - 1,$$

де p – також просте число, називають *простими числами Мерсенна* на честь французького математика і філософа Мерсенна (1588-1648), який у 1644 р. склав список таких чисел до 10^{79} (без помилок лише до 10^{18}) [24].

Зауважимо, що коли n – непарне складене число, то $2^n - 1$ буде також складеним числом. Адже, з

$$n = a \cdot b,\ 3 \le a \le n,\ 3 \le a \le n$$

випливає рівність:

$$2^{ab} - 1 = (2^a - 1) \cdot (2^{a(b-1)} + 2^{a(b-2)} + \ldots + 2^a + 1).$$

Крім того при будь-якому парному $n \ge 4$ числа виду

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

складені. Таким чином, якщо p не є простим числом, то серед чисел Мерсенна немає простих.

Числа Мерсенна відіграють важливу роль у зв‘язку з однією проблемою теорії чисел. Ще Евклід знав, що коли $2^p - 1$ є простим числом, то $2^{p-1}(2^p - 1)$ є так званим *досконалим числом*, тобто дорівнює сумі двох своїх власних дільників [15]. Наведемо приклади досконалих чисел

$$6 = 1 + 2 + 3,$$

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

Чи існує хоч одне непарне досконале число? Ця проблема не розв‘язана до цього часу. Відомо лише, що коли число й існує, то воно

не менше ніж 10^{100} [12].

Взагалі кажучи, не всі числа Мерсенна є простими. Справді,

$$M_2 = 2^2 - 1 = 3,$$

$$M_3 = 2^3 - 1 = 7,$$

$$M_5 = 2^5 - 1 = 31,$$

$$M_7 = 2^7 - 1 = 127$$

– прості числа, а

$$M_{11} = 2^{11} - 1 = 2047 = 23 \cdot 89$$

– складене число.

Загальний спосіб перевірки чисел Мерсенна на простоту полягає у безпосередньому підставленні значень p, але чим більше p, тим важче таку перевірку здійснити.

Проте у 1750 р. Л.Ейлеру вдалося довести [3], що M_{31} – просте число. До нього 8 простих чисел Мерсенна, які відповідають значенням

$$p = 2, 3, 5, 7, 13, 19, 31,$$

було вже знайдено.

Більш ста років ніхто не міг знайти простого числа Мерсенна, яке б перевищувало число Ейлера M_{31}. Але в 1876 р. було доведено [22], що число

$$2^{127} - 1 = 170141183460469231731687303715884105727$$

є простим. Воно має 39 цифр.

Прості числа Мерсенна, які не перевищують M_{127}, відповідають значенням p = 61, 89, 107. Після цього 75 років ніхто не міг знайти нового простого числа Мерсенна. Нові прості числа Мерсенна було відкрито за допомогою ЕОМ. Так, у 1952 р. встановили, що простими є числа M_p при

$$p = 521, 607, 1279, 2203, 2281,$$

у 1958 р. було знайдено просте число M_{3217}, у 1962 р. – ще два простих числа M_p, які відповідають значенням p = 4253, 4423, а у 1964 р. було доведено, що числа M_p при p = 9689, 9941, 11213 є простими [7].

Таким чином, з часів Евкліда до 1962 р., “урожай” простих чисел Мерсенна становив 23 числа.

У 1971 р. було доведено, що число M_p при p = 19937 теж є простим, а у 1978-1983 рр. знайдені ще 4 нових простих числа Мерсенна для $p \in [21000, 132049]$. Останнє з них $2^{132049} - 1$ має 39751 цифру.

Станом на сьогодні відомо 51 просте число Мерсенна $2^{82589933} - 1$. Це число з 24862048 цифр, записане за основою 10. З 1997 року усі прості числа Мерсенна були знайдені в рамках Great Internet Mersenne Prime Search, проекту розподілених обчислень.

Отже, якщо число M_n, де $n > 1$, просте, то і число n повинно бути простим, але не обов’язково навпаки.

Доведено, що якщо p – просте число, то кожен натуральний дільник числа M_p повинен бути виду $2kp + 1$, де k – ціле число ≥ 0. Тому, наприклад, дільниками числа M_{11} є числа

$$22k + 1, \text{ де } k = 0, 1, 4 \text{ і } 93.$$

Точно так само дільники числа

$$M_{101} = 2^{101} - 1$$

повинні бути виду $202k + 1$. На жаль, досі не знайдено ні одного простого дільника числа M_{101} (очевидно, число k тут дуже велике), хоча іншим шляхом доведено, що число M_{101} складене і є добутком двох різних простих чисел.

Доведено, що якщо q є просте число виду $8k + 7$, то $q \mid M_{\frac{q-1}{2}}$. Це дозволило показати, що серед чисел M_p, де p – просте число, багато є складеними. Наприклад,

$$47 \mid M_{23}, 167 \mid M_{83}, 263 \mid M_{131}, 359 \mid M_{179}, 383 \mid M_{191}, 479 \mid M_{239}.$$

Висунуто припущення (досі не доведене), що таких складених чисел існує нескінченно багато [17].

Один із найкращих способів генерування дуже великих простих

чисел використовує експоненціальні формули. Найстаріша експоненціальна формула для простих чисел названа іменем Мерсенна [19]. Нехай n – натуральне число. Як було зазначено вище, що n-им числом Мерсенна називається число виду:

$$M(n) = 2^n - 1$$

Ми вже бачили, що число $M(n)$ складене, якщо таким є і n. Для $n = rs$ маємо:

$$2^n - 1 = (2^r)^s - 1 = (2^r - 1)(\, 2^{r(s-1)} + 2^{r(s-2)} + \cdots + 2^r + 1$$

Отже, $M(r)$ – дільник числа $M(n) = M(rs)$. Звісно, $M(s)$ теж ділить $M(n)$.

Таким чином, при пошуку простих чисел Мерсенна ми можемо обмежитись дослідженням $M(p)$ з простими p. Проте твердження про простоту всіх таких $M(p)$ не є вірним. Розглянемо метод розкладання на множники чисел Мерсенна із простим, але не занадто великим показником. Головну рушійну силу методу дає загальна формула дільників числа $M(p)$, відкрита Ферма. Для доведення формули нам знадобиться один результат з теорії груп [14].

Лема 2.1. Нехай G – скінчена група з операцією * та $a \in G$. Натуральне число t задовольняє умові $a^t = e$ тоді, коли t ділиться на порядок елемента a.

Доведення.

Позначимо через t порядок елементів a. Подільність t на s означає рівність: $t = rs$ за деякого натурального r. В цьому випадку:

$$a^t = (a^s)^r = e$$

Для доведення протилежного твердження припустимо, що $a^t = e$. Оскільки порядок елемента є найменшим натуральним числом, при якому $a^s = e$, то $s \leq t$. Розділимо t на s із остачею:

$$t = sq + r \text{ , де } 0 \leq r < s.$$

Звідси отримуємо:

$$e = a^t = (a^s)^q * a^r = a^r$$

(За умовою, $a^s = e$). Але в наслідок нерівності $r < s$ і вибору s останнє співвідношення можливе, тільки якщо $r = 0$.

Повернемося до чисел Мерсенна. Припустимо, що q – простий дільник числа $M(p) = 2^p - 1$ відповідний простому $p \neq 2$. Тоді:

$$2^p \equiv 1 \pmod{q}.$$

Цю конгруенцію можна інтерпретувати як рівність у групі $U(q) = Z_q \setminus \{0\}$ [8], а саме:

$$\bar{2}^p = \bar{1}.$$

Що можна сказати про порядок елемента $\bar{2}$ групи $U(q)$? З попереднього співвідношення та леми 2.1 випливає, що він ділить p. Але p – просте число, отже, порядком елемента $\bar{2}$ може бути тільки або 1, або p. Припущення у тому, що $\bar{2}^p = \bar{1}$ призводить до суперечності: $\bar{1} = \bar{0}$ (через рівності $\bar{2} = \bar{1} + \bar{1}$). Отже, елемент $\bar{2}$ має порядок p у групі $U(q)$. З іншого боку, за теоремою Ферма:

$$\bar{2}^{q-1} = \bar{1} \text{ в } U(q).$$

І знову лема 2.1 каже нам, що порядок елемента $\bar{2}$ – ділить $q - 1$. Оскільки, як ми вже встановили, він дорівнює p, робимо висновок, що $q - 1 = kp$ для якогось натурального k.

Отримане співвідношення можна посилити. Дійсно, число $M(p) = 2^p - 1$ –непарне, тому всі його дільники теж непарні. Зокрема, різниця $q - 1$ – парна. Далі, з непарності p випливає, що число k у розкладанні $q - 1$ на множники має бути парним. Отже, $q - 1 = 2rp$ для деякого натурального числа r. Ми довели наступний результат.

Метод Ферма. Нехай $p \neq 2$ – просте число, та q – простий дільник числа Мерсенна $M(p)$. Тоді знайдеться таке натуральне r, що

$$q = 1 + 2rp.$$

Застосуємо сформульований метод для пошуку дільника числа

$M(11) = 2047$. Згідно з формулою, будь-який простий дільник числа $M(11)$має вигляд: $q = 1 + 22r$. Тепер ми маємо обчислити q при $r = 1, 2, \ldots$ і вибрати з отриманих результатів дільники числа $M(11)$. Перед початком обчислень корисно подумати, як далеко слід заходити у цьому процесі. Нагадаємо, якщо $q = 1 + 2rp$ – найменший простий дільник складеного числа $M(p)$ то:

$$\sqrt{M(p)} \geq q = 1 + 2rp$$

Оскільки $\sqrt{M(p)} < 2^{\frac{p}{2}}$, з останньої нерівності випливає, що

$$r < \frac{2^{\frac{p}{2}} - 1}{2p}$$

При $p = 11$ це обмеження залишає лише два можливих значення для r: 1 і 2. Підстановка $r = 1$ у формулу $q = 1 + 22r$ дає $q = 23$. Елементарний поділ показує, що 23 є множником числа $M(11) = 2047$. Інший його простий дільник – це $89 = 1 + 22 * 4$. Цікаво відзначити, що якби ми шукали дільники числа $M(11)$ методом спроб, то нам довелося б безуспішно ділити $M(11)$на кожне просте число, менше 23. А таких чисел 8.

Історія чисел Мерсенна – скарбниця курйозів та анекдотичних випадків. Один з найкращих – доповідь Коула (Cole) на засіданні Американського Математичного Товариства 1903 року. Він довів, що

$$M(67) = 193\,707\,721 * 761\,838\,257\,287,$$

перемножуючи ці числа у повній тиші. Аудиторія з ентузіазмом прийняла доказ! Простим способом отримати такий розклад поки що ніхто не зміг.

Чимало з відомих великих простих чисел – числа Мерсенна. Звичайно, є способи перевірки чисел Мерсенна на простоту кращі, ніж метод Ферма. Найчастіше вживаний з них – тест Люка-Лемера, який буде розглянуто далі.

2.2. Числа Ферма

Французький математик П. Ферма (1601-1665) був упевнений, що всі числа виду

$$F_k = 2^{2^k} + 1$$

прості (числа F_k називають *числами Ферма*) [13].

Перші 6 чисел дійсно виявилися простими:

$$F_0 = 2^{2^0} + 1 = 3, \quad F_1 = 2^{2^1} + 1 = 5, \quad F_2 = 2^{2^2} + 1 = 17,$$

$$F_3 = 2^{2^3} + 1 = 257, \quad F_4 = 2^{2^4} + 1 = 65537.$$

Проте, гіпотеза Ферма, взагалі кажучи, була помилковою. Ейлер у 1739 р. помітив [8], що число

$$F_5 = 4294967297 = 641 \cdot 6700417$$

вже не є простим. Крім того, він зазначив, що всі дільники числа $2^{2^k} + 1$ повинні мати вигляд $m \cdot 2^n + 1$.

Цікаво, що прості числа Ферма F_k відіграють важливу роль у задачі про можливість побудови правильного n–кутника за допомогою циркуля та лінійки. Ще математикам Стародавньої Греції було відомо, що за допомогою циркуля та лінійки можна побудувати правильний n–кутник при деяких значеннях n, наприклад:

3, 6, 12, 24, … ; 4, 8, 16, 32, … ; 5, 10, 20, 40, … ; 15, 30, 60, 120, … .

І от у 1801 р. німецький математик К.Ф. Гаусс (1777-1855) довів [19], що правильний n–кутник можна побудувати за допомогою циркуля та лінійки тільки тоді, коли число його сторін n дорівнює

$$2^\alpha \cdot p_1 \cdot \ldots \cdot p_s \ (\alpha \geq 0, s \geq 1)$$

де всі прості числа p_i є простими числами Ферма.

Зауважимо, що серед перших 1000 значень всього 54 числа такого виду.

Відкриття Гаусса загострило інтерес до пошуку простих чисел Ферма. Багато математиків шукали серед чисел Ферма прості. Але жодного нового числа Ферма навіть за допомогою ЕОМ так і не було знайдено.

Цікаву формулу запропонував і французький математик Лежандр [11]: $f(n) = 2n^2 + 29$. Вона дає прості числа для значень n від 0 до 28. Проте праці видатних математиків так і не дали позитивної відповіді на запитання про формулу довільного простого числа.

Розглянемо важливі твердження. що стосуються властивостей чисел Ферма.

Теорема 2.1. Якщо число F_n є, то число $3^{2^{2^n-1}} + 1$ ділиться на F_n.

Спочатку доведемо наступну лему.

Лема 2.2. Якщо k є ціле невід'ємне число і якщо число $p = 12k + 5$ є простим, то число $3^{6k+2} + 1$ ділиться на p.

Доведення.

Лема, очевидно, справедлива для $k = 0$, тому надалі будемо вважати, що k є числом натуральним. Нехай $p = 12k + 5$. Візьмемо добуток перших $6k + 2$ натуральних чисел, які діляться на 3, і розіб'ємо співмножники цього добутку на три групи. Віднесемо до першої групи перші $2k$ співмножника, до другої – наступні $2k + 1$ співмножники і до третьої – останні $2k + 1$ співмножники.

Співмножники першої групи дають добуток $3 \cdot 6 \cdot 9 \ldots 6k$. Співмножники другої групи, якщо їх записати у порядку спадання, дають добуток

$$(12k + 3) \cdot 12k \cdot (12k - 3) \ldots (6k + 6)(6k + 3),$$

який, враховуючи, що $p = 12k + 5$, можна записати у вигляді

$$(p - 2)(p - 5)(p - 8) \ldots [p - (6k + 2)].$$

Так як число співмножників непарне $(2k + 1)$, то останній добуток після розкриття дужок і зведення доданків, які діляться на p, дає нам число $pu - 2\cdot5\cdot8 \ldots (6k + 2)$, де u є деяке ціле число.

Співмножники третьої групи дають добуток

$$(12k + 6)(12k + 9)(12k + 12) \ldots (18k + 6) =$$

$$= (p + 1)(p + 4)(p + 7) \ldots (p + 6k + 1) = pv + 1\cdot4\cdot7 \ldots (6k + 1),$$

де v – натуральне число.

Таким чином, маємо

$$3\cdot6\cdot9 \ldots (18k + 6) =$$

$$= 3\cdot6\cdot9 \ldots 6k[pu - 2\cdot5\cdot8 \ldots (6k + 2)][pv + 1\cdot4\cdot7 \ldots (6k + 1)] =$$

$$= pw - 1\cdot2\cdot3\cdot4\cdot5\cdot6 \ldots (6k + 1)\cdot(6k + 2) = pw - (6k + 2)!,$$

де w – ціле число.

Але

$$3\cdot6\cdot9 \ldots (18k + 6) = (6k + 2)\,!3^{6k+2}.$$

Звідси ми робимо висновок, що число pw ділиться на $(6k + 2)$!, отже,

$$pw = (6k + 2)!t,$$

де t – ціле число. Але

$$6k + 2 < 12k + 5 = p,$$

і тому число $(6k + 2)$! не ділиться на p. Оскільки ж добуток $(6k + 2)!t$ ділиться на p, то t повинно ділитися на p, $t = ps$, звідки

$$w = (6k + 2)!s,$$

де s – ціле число. Таким чином, маємо $3^{6k+2} = ps - 1$, звідки випливає, що число $3^{6k+2} + 1$ ділиться на p, що й потрібно було довести.

Лему доведено.

Перейдемо тепер до доведення теореми 2.2.

Доведення.

Нехай n – деяке натуральне число. Тоді маємо $2^n = 2m$, де m – натуральне число, $F_n - 1 = 4^m$, звідки випливає, що число $F_n - 5$ ділиться на 4. З іншого боку, маємо

$$F_n - 1 = 4^m = (3+1)^m = 3t + 1,$$

де t – натуральне число. Звідси

$$F_n - 5 = 3(t-1),$$

так що число $F_n - 5$, яке ділиться на 4, ділиться і на 3, отже, це число ділиться на 12, і тому $F_n = 12k + 5$, де k – ціле число. Таким чином, за лемою 2.3, якщо число F_n просте, то число

$$3^{6k+2} + 1 = 3^{\frac{(F_n-1)}{2}} + 1 = 3^{2^{2^n-1}}$$

ділиться на F_n.

Теорему доведено.

Ми вже бачили, що й число $M(n) = 2^n - 1$ просте, то n теж просте. Це міркування наводить на думку спробувати пошукати значення при яких вираз $2^n - 1$ даватиме прості числа. Припустивши, що $p = 2^n - 1$ – просте, отримаємо:

$$\bar{2}^n = -\bar{1} \text{ в } U(p). \qquad (2.1)$$

Отже,

$$\bar{2}^{2n} = \bar{1} \text{ в } U(p).$$

Таким чином, за лемою 2.1 порядок елемента $\bar{2}$ групи $U(p)$ ділить $2n$. Як і в попередній ситуації, ми повинні точно визначити цей порядок. З рівності (2.1) випливає, що порядок елемента $\bar{2}$ не може ні дорівнювати n, ні бути його дільником. Але він усе-таки ділить $2n$ тому шуканий порядок може бути парним, тобто, рівним $2r$ при якомусь натуральному r. Очевидно, r ділить число n.

Тепер, за означенням порядку, $\bar{2}^{2r} = \bar{1}$ в $U(p)$, що можна записати у вигляді рівності в Z_p:

$$\bar{0} = \bar{2}^{2r} - \bar{1} = (\bar{2}^r - \bar{1})(\bar{2}^r + \bar{1}).$$

За нашим припущенням, p – просте число. Отже:

$$2^r \equiv 1 \pmod{p} \quad \text{або} \quad 2^r \equiv -1 \pmod{p}.$$

Отже, p ділить одне з чисел: $\bar{2}^r + \bar{1}$ або $\bar{2}^r - \bar{1}$. Але через співвідношення: $p = 2^n + 1$, $n \geq r$, таке можливе тільки, якщо $r = n$, тобто порядок елемента $\bar{2}$ групи $U(p)$ дорівнює $2n$.

У силу рівності $p - 1 = 2^n$, з теореми Ферма випливає, що:

$$\bar{2}^{2n} = \bar{1} \text{ в } U(p).$$

Тому порядок елемента $\bar{2}$ (а він дорівнює $2-n$) ділить число 2^n. Зокрема, n має бути степенем двійки. Отже, якщо число $2^n + 1$ – просте, то n – якась степінь двійки.

Саме з цієї причини у пошуках простих ми обмежуємося числами виду $F(k) = 2^{2^k}$, тобто числами Ферма. Ферма вважав, що всі такі числа прості. Це вірно для $F(k)$ при $0 \leq k \leq 4$. Однак у 1730 р. Ейлер показав, що число $F(5)$ складене [14]. Як не дивно, метод Ейлера близький до способу самого Ферма, який той використовував для пошуку дільників чисел Мерсенна. Розглянемо, як працює метод Ейлера.

Припустимо, що q – простий дільник числа $F(k)$. Тоді:

$$\bar{2}^{2^k} = -\bar{1} \text{ в } U(p) \qquad (2.2)$$

і, за лемою 2.1, порядок елемента $\bar{2}$ ділить 2^{k+1}. Але те ж рівняння гарантує, що цей порядок не може бути степенем двійки з показником менше $k + 1$. Отже, порядок елемента $\bar{2}$ в групі $U(p)$ точно дорівнює 2^{k+1}. Далі, за теоремою Ферма порядок елемента $\bar{2}$ повинен бути дільником числа $q - 1$; таким, що $q - 1 = 2^{k+1}r$.

Метод Ейлер. Якщо q – простий дільник числа $F(k)$, знайдеться таке натуральне r, що $q = 1 + 2^{k+1}r$.

Спираючись на метод Ейлера, знайдемо дільник числа $F(5) = 2^{35} + 1$. Перш за все, будь-який такий простий дільник можна подати у вигляді $q = 1 + 64r$. Таким чином, нам потрібно визначити, чи є серед натуральних чисел

$$q < \sqrt{2^{32} + 1} \leq 66\,000,$$

представлених як $q = 1 + 64r$, дільники числа $F(5)$. Обмеження для q дає оцінку $r < 1031$; на жаль, працювати з настільки великою границею незручно.

Найменше значення r, при якому число q просте, дорівнює 3, що відповідає $q = 193$. Обчислення показують:

$$2^{32} \equiv (2^8)^4 \equiv 64^4 \equiv 108 \pmod{193}.$$

Отже, 193 не ділить число $F(5)$. При $r = 4$ ми маємо $q = 257$, теж просте число, але

$$2^{32} \equiv 1 \pmod{257},$$

тобто, 257 також не є шуканим дільником. Наступне значення r, при якому q буде простим, це $r = 7$, причому $q = 449$. І знову мимо:

$$2^{32} \equiv (2^{16})^2 \equiv 431^2 \equiv 324 \pmod{449}.$$

Наступне просте $q = 577$, що відповідає $r = 9$. У цьому випадку

$$2^{32} \equiv 287 \pmod{577},$$

тобто, 577 не ділить $F(5)$. Нарешті, $r = 10$ дає довгоочікуваний дільник $q = 641$ числа $F(5)$.

Нам пощастило, що дільник виявився відносно малим, і всі необхідні обчислення при його пошуку можна виконати на електронному калькуляторі. Ейлер, звичайно, зробив їх вручну. На жаль, такий успіх випадає нечасто. Проблема в тому, що $F(k)$ є двічі показниковою функцією [12]. Тому навіть щодо невеликих значень k пошук дільників доводиться робити серед дуже великої кількості кандидатів, що практично неможливо здійснити методом Ейлера. Проте знайти дільник конкретного числа Ферма можна зручнішими методами. Більше того, є дуже ефективний тест, що визначає, чи це число Ферма є простим або складовим. Цей тест розглянемо далі.

Про числа Ферма відомо досить багато. Наприклад, виписані розклади на прості множники чисел $F(11)$ і всіх $F(k)$ при $k \leq 9$. Крім того, знайдений принаймні один дільник для кожного з чисел $F(k)$ при $k \leq 32$, за винятком $k = 14,\ 20,\ 22,\ 28$ і 31. Виходить, що серед чисел

Ферма, які ми знаємо, простими є тільки $F(0), \ldots, F(4)$ виникає припущення, що інших простих серед чисел Ферма немає.

Чому ж числа Ферма привертають таку велику увагу? Є кілька причин, і, звичайно ж, не остання серед них – наповнена драматичними подіями історія цих чисел. Крім того, вони є хорошим джерелом важких для розкладу на множники великих чисел, що робить їх прекрасним об'єктом для випробування можливостей нових алгоритмів. Алгоритми розкладу, в свою чергу, часто вимагають від комп'ютера величезної кількості простих арифметичних і логічних операцій, що повторюються. Тому їх перевірка на новостворюваних комп'ютерах досить ефективно допомагає виловити недоліки в конструкції.

Числа Ферма цікаві і з теоретичної точки зору. У 1801 р. Гаусс показав, що якщо правильний *n*-кутник можна побудувати за допомогою циркуля та лінійки, то *n* дорівнює деякому степеню двійки, помноженого на просте число Ферма [8]. Зокрема, правильний 17-кутник можна побудувати таким чином, оскільки $17 = F(2)$, а накреслити правильний семикутник, використовуючи тільки циркуль і лінійку, не вдасться, так як 7 не є числом Ферма.

Найбільш відоме складене число Ферма – це число $F(23\,471)$; його дільник дорівнює $5 * 2^{23\,473} + 1$ [9]. Число $F(23\,471)$ досить велике і виникає питання: за яким алгоритмом вдається знайти його дільник? Відповісти на нього легко. Це метод Ейлера, описаний вище. Проте замість того, щоб сліпо слідувати Ейлеру, ми перевернемо метод з ніг на голову. Ейлер починав із конкретного числа Ферма і намагався знайти його дільник. Ми ж візьмемо число, яке може бути дільником якогось $F(m)$ і шукатимемо відповідне *m*.

Алгоритм починається з вибору двох натуральних чисел: *k* і *n*,

перше з яких має бути непарним. Потім будується число $q = k * 2^n + 1$. З методу Ейлера випливає, що воно ділить число Ферма $F(m)$ тоді і лише тоді, коли

$$2^{2m} \equiv -1 \pmod{q}$$

Для роботи з великими числами, подібними до вищезазначеного, нам знадобиться дуже ефективний спосіб обчислення конгруенцій. Оскільки ми маємо справу тільки зі степенями двійки, знайти такий спосіб досить просто, оскільки

$$\left(2^{2^i}\right)^2 = 2^{2^{i+1}}$$

Тепер зробимо наступним чином. Для початку припустимо $r = 2^{2^5}$ і $i = 5$. Змінна i використовується для зберігання інформації про показник. Ми стартуємо з $i = 5$ тому, що $F(i)$ – просте при $i < n$. Суть алгоритму полягає в заміні r на віднімання числа r^2 по модулю q і збільшенні i на 1 у кожному циклі. Зупиняється алгоритм в одному з двох випадків: або $r = q - 1$, або $i = n$. У першому з них q ділить $F(i)$, а в другому q не є дільником жодного з $F(i)$. Нагадаємо, що якщо $q = k * 2^n + 1$ ділить число $F(i)$, то $i \leq n - 1$.

Цей метод з деякими удосконаленнями був використаний Гостином (Gostin) [6] щодо визначення дільників чисел $F(15), F(25), F(27)$ і $F(147)$. Він написав програму на мовах «Сі» та асемблері, розподіливши деякі процедури. На першому етапі програма генерує кілька мільйонів можливих значень чисел q. Потім з них

видаляються всі, що діляться на невеликі прості числа. Ті, що залишились, перевіряються конгруенціями, як пояснювалося вище.

Далі приведена частина таблиці з роботи. Вона містить ті значення натуральних *m*, *k* і *n*, для яких $k * 2^n + 1$ є множником числа $F(m)$.

m	*k*	*n*
15	17 753 925 353	17
64	17 853 639	67
353	18 908 555	355
885	16 578 999	887
1082	82 165	1084
1225	79 707	1231
1451	13 143	1454
3506	501	3508
6390	303	6393
9609	6021	6912

2.3. Тест Люка-Лемера

В цьому розділі розглянемо дуже хороший тест, який перевіряє на простоту числа Мерсенна. Першим його виявив Люка (відомий нам як творець «Ханойських веж» [3]) у 1878 р. Потім тест був удосконалений Лемером (D. H. Lehmer) у 1932 р., і тепер він називається тестом Люка-Лемера [15].

Головна складова частина тесту – послідовність натуральних чисел: $S_0, S_1, S_2, \ldots$, яка визначається рекурентною формулою

$$S_0 = 4 \quad \text{і} \quad S_{k+1} = S_k^2 - 2\,.$$

Спочатку ми покажемо, що члени послідовності можна записати у вигляді сум степенів деяких ірраціональних чисел. Нехай $\omega = 2 + \sqrt{3}$ і $\bar{\omega} = 2 - \sqrt{3}$. Доведемо індукцією по n, що

$$\omega^{2n} + \bar{\omega}^{2n} = S_n \tag{2.3}$$

Очевидно, $\omega + \bar{\omega} = S_0$. Припустимо, що $\omega^{2n-1} + \bar{\omega}^{2n-1} = S_{n-1}$. Піднесемо до квадрату обидві частини рівності, отримаємо:

$$\omega^{2n} + 2(\omega\bar{\omega})^{2n-1} + \bar{\omega}^{2n} = S_{n-1}^2.$$

Оскільки $\omega\bar{\omega} = 1$, звідси випливає співвідношення

$$\omega^{2n} + \bar{\omega}^{2n} = S_{n-1}^2 - 2,$$

що, за означенням, дає S_n.

Тест Люка-Лемера. Нехай p – просте число. Число Мерсенна $M(p)$ є простим тоді і тільки тоді, коли $S_{p-2} \equiv 0 (mod\ M(p))$.

Ми доведемо лише необхідність умови тесту, доведення достатності можна знайти у [26]. Будучи елементарним по суті, воно оперує ірраціональними числами таким способом, який важко обґрунтувати. Але якщо змиритися з ірраціональними числами, то в іншому проблем не буде, оскільки доведення близько дотримується схеми міркувань, розглянутої вище.

Доведення тесту Люка-Лемера проводиться мовою теорії груп [7], але групи, які застосовуються при цьому, більш специфічні, ніж $U(p)$.

Відправна точка міркувань – деяка підмножина у сукупності $\mathbb{Z}[\sqrt{3}]$ чисел виду $a + b\sqrt{3}$, де $a, b \in \mathbb{Z}$. Ці числа можна додавати і множити як дійсні. При цьому сума і добуток двох елементів з

$\mathbb{Z}[\sqrt{3}]$ залишається в даній множині. Більше того, подібно $\mathbb{Z}$ до сукупності $\mathbb{Z}[\sqrt{3}]$, будучи групою відносно додавання, не буде такою щодо множення. Усі згадані факти легко перевірити. Зауважимо, що кожне число $a \in \mathbb{Z}$ можна записати у вигляді $a = a + 0\sqrt{3}$, так що $\mathbb{Z} \subset \mathbb{Z}[\sqrt{3}]$.

Нехай тепер $q > 0$ – просте натуральне число. Введемо позначення $I(q) = \{q\alpha | \alpha \in \mathbb{Z}[\sqrt{3}]\}$. Зрозуміло, що $0 = 0q \in I(q)$. З рівності $q\alpha + q\beta = q(\alpha + \beta)$ випливає, що сума будь-яких двох чисел з $I(q)$ також належить $I(q)$. Більш того, для будь-якого $\alpha \in \mathbb{Z}[\sqrt{3}]$ як $q\alpha$, так і $-q\alpha$ лежать в $I(q)$. Таким чином, $I(q)$ – підгрупа в адитивній (по додаванню) групі $\mathbb{Z}[\sqrt{3}]$.

Відношення *конгруенції за модулем* $I(q)$ є відношенням еквівалентності [18] на множині $\mathbb{Z}[\sqrt{3}]$. Нагадаємо, що якщо $\alpha, \beta \in \mathbb{Z}[\sqrt{3}]$, то $\alpha \equiv \beta \ (mod\ I(q))$, коли $\alpha - \beta \in I(q)$.

Далі елемент $\alpha \in \mathbb{Z}[\sqrt{3}]$ записується у вигляді $a = a_1 + a_2\sqrt{3}$, де $\alpha_1, \alpha_2 \in \mathbb{Z}$. Розділивши a_1 і a_2 на q залишком, ми отримаємо $a_1 = qb_1 + r_1$ і $a_2 = qb_2 + r_2$ причому $0 \leq r_1, r_2 < q$. Позначивши суму $r_1 + r_2\sqrt{3}$ через ρ, можна записати $\alpha - \rho = q(b_1 + b_2\sqrt{3})$.

Отже, $\alpha \equiv \rho \ (mod\ I(q))$. Число ρ називається *наведеною формою* елемента α по модулю *I(q)*. Оскільки залишок від поділу цілих чисел визначений однозначно, кожен елемент із $\mathbb{Z}[\sqrt{3}]$ має тільки одну наведену форму по модулю *I(q)*. Зазначимо, що $\mathbb{Z}[\sqrt{3}]$ існує рівно q^2 різних наведених форм елементів по модулю *I(q)*.

Тепер кожен клас еквівалентності $\mathbb{Z}[\sqrt{3}]$ може бути поданий у наведеній формі. Більше того, два класи, що мають різні наведені форми, мають бути різними. Таким чином, множина $\mathbb{Z}_q[\sqrt{3}]$ класів еквівалентності по модулю *I(q)* містить точно q^2 елементів. Клас еквівалентності елемента $\alpha \in \mathbb{Z}[\sqrt{3}]$ по модулю *I(q)* ми позначатимемо через $\tilde{\alpha}$. Визначимо множення в $\mathbb{Z}_q[\sqrt{3}]$ за правилом $\tilde{\alpha}\tilde{\beta} = \widetilde{\alpha\beta}$.

Доведення незалежності результату множення від вибору представників класів аналогічно до відповідної перевірки для арифметики лишків. Якщо $a = a_1 + a_2\sqrt{3}$ і $\beta = b_1 + b_2\sqrt{3}$, то просте обчислення показує, що представник добутку $\tilde{\alpha}\tilde{\beta}$ має вигляд:

$$(a_1b_1 + 3a_2b_2) + (a_1b_2 + a_2b_1)\sqrt{3}.$$

Легко перевірити, що множення асоціативно, комутативне і має $\tilde{1}$ як одиничний елемент. Однак $\mathbb{Z}_q[\sqrt{3}]$ не є групою по множенню. Як і у випадку арифметики лишків, ми долаємо цю труднощі, вводячи множину $V(q)$ оборотних по множенню елементів з $\mathbb{Z}_q[\sqrt{3}]$. Вона

утворює групу, оскільки добуток оборотних елементів множини $\mathbb{Z}_q[\sqrt{3}]$ теж оборотний, що легко перевіряється. Внаслідок включення

$$V(q) \subset \mathbb{Z}_q[\sqrt{3}] \setminus \{\tilde{0}\}$$

порядок групи $V(q)$ обов'язково менше, ніж q^2. Зауважимо також, що рівність $\omega\bar{\omega} = 1$ говорить про оборотність елементів ω і $\bar{\omega}$, тобто $\omega, \bar{\omega} \in V(q)$. Тепер ми готові до доведення коректності тесту.

Доведення коректності тесту Люка-Лемера. Припустимо, що при деякому простому p число Мерсенна $M(p)$ ділить член послідовності S_{p-2}. Завдяки співвідношенню (2.3), знайдеться таке натуральне r, що

$$\omega^{2^{p-2}} + \bar{\omega}^{2^{p-2}} = rM(p).$$

Помножуючи цю рівність на $\omega^{2^{p-2}}$ та використовуючи тотожність, $\omega\bar{\omega} = 1$, отримуємо

$$\omega^{2^{p-2}} + 1 = rM(p)\bar{\omega}^{2^{p-2}} \tag{2.4}$$

Припустимо тепер, що число $M(p)$ складене і нехай q – його найменший простий множник. Приведемо наше припущення до протиріччя. Оскільки q ділить $M(p)$ з *(4.2)* випливає, що

$$\tilde{\omega}^{2^{p-1}} = -1 \tag{2.5}$$

в $\mathbb{Z}_q[\sqrt{3}]$. При піднесенні у квадрат рівність (2.5), маємо $\tilde{\omega}^{2^p} = \tilde{1}$.

Звідси, керуючись лемою 2.1, робимо висновок: порядок елемента

$\tilde{\omega}$ ділить 2^p . З іншого боку, рівняння (2.5) говорить нам, що він не може бути степенем двійки, меншим, ніж 2^p. Отже, порядок елемента $\tilde{\omega}$ в групі $V(q)$ дорівнює 2^p . Далі, за теоремою Лагранжа, порядок елемента $\tilde{\omega}$ ділить порядок групи $V(q)$ завдяки тому, що останній не перевищує $q^2 - 1$, отримуємо нерівність $2^p \leq q^2 - 1$. Пам'ятаючи тепер, що q – найменший простий дільник числа Мерсенна *M(p),* можна оцінити q^2 зверху: $q^2 \leq M(p)$. Таким чином,

$$2^p \leq q^2 - 1 < 2^p - 1,$$

що суперечить здоровому глузду. Отже, якщо *M(p),* ділить член послідовності S_{p-2}, то число *M(p)* просте, тобто ми довели потребу умови тесту.

Незважаючи на труднощі, пов'язані з доведенням коректності тесту, його дуже легко реалізувати та застосувати. У 1978 р. два старшокласники Лора Нікель (Nickel) і Курт Нолль (Noll) за допомогою тесту Люка-Лемера довели простоту числа, скориставшись локальною комп'ютерною мережею місцевого університету [14]. Їхній успіх був відбитий у передовиці «Нью-Йорк Таймс». Цей же тест лежить в основі GIMPS, пакету програм "Great Internet Mersenne Prime Search", яка є вільною у доступі (разом з текстами програм) програмною системою. Так що будь-який власник персонального комп'ютера може зайнятися пошуком великих простих чисел.

РОЗДІЛ 3
ПРОСТІ ЧИСЛА
В ШКІЛЬНОМУ КУРСІ МАТЕМАТИКИ

Розглянемо деякі питання з теорії простих чисел, які можна розглядати на факультативних заняттях, починаючи з сьомого класу. Тема є досить корисною для здобувачів, які приймають активну участь у математичних олімпіадах різного рівня. Для участі в олімпіаді здобувачі мають, окрім інших вимог, мати відповідні знання, оскільки знань з елементарної математики, набутих під час уроків з математики, недостатньо. Задачі математичних олімпіад мають на меті «виявляти рівень математичних здібностей і математичної підготовки учнів, рівень їх логічної культури, зокрема, володіння правилами логіки» [22]. Результати олімпіад залежать саме від розвитку вмінь та швидкості розв'язування нестандартних задач з математики.

Розглянемо приклади застосування основних властивостей простих чисел до розв'язування різноманітних задач.

Задача 3.1. Довести, що при будь-якому цілому k числа $2k + 1$ і $9k + 4$ є простими, а для чисел $2k – 1$ і $9k + 4$ знайти їх НСД в залежності від цілого числа k.

Розв'язання.

Числа $2k + 1$ і $9k + 4$ є взаємно простими, так як існують цілі $m = 9$ і $n = – 2$, що

$$9(2k + 1) – 2(9k + 4) = 1.$$

Так як $9k + 4 = 4(2k – 1) + (k + 8)$ і $2k – 1 = 2(k + 8) – 17$,

то

$$(9k + 4, 2k – 1) = (2k – 1, k + 8) = (k + 8, 17).$$

Таким чином, якщо число k при діленні на 17 дає в остачі 9, то $(k + 8, 17) = 17$ (в противному випадку, якщо 17 не ділить $k + 8$, то $(k + 8, 17) = 1$). Звідси випливає, що $(9k + 4, 2k – 1) = 17$, якщо k при

діленні на 17 дає остачу 9;

$$(9k + 4, 2k – 1) = 1,$$

якщо k при діленні на 17 дає остачу, відмінну від 9.

Задача 3.2. Знайти всі прості числа, які є одночасно сумами і різницями двох простих чисел.

Розв'язання.

Існує тільки одне таке просте число: 5. Насправді, припустимо, що просте число r є одночасно і сума, і різниця двох простих чисел. Число r, очевидно, повинно бути більше двох, і тому r є непарне просте число. Далі, так як r є сума, і різниця двох простих чисел, то одне із них повинно бути непарним, а інше парним, тобто числом 2.

Отже, маємо $r = p + 2 = q – 2$, де p і q є непарними простими числами. Але тоді

$$p, r = p + 2 \text{ і } q = r + 2$$

є трьома послідовними непарними простими числами, а, як відомо, існує тільки одна така трійка: 3, 5, 7 (так як із кожних трьох послідовних непарних чисел одне повинне ділитися на 3). Таким чином, маємо

$$r = 5 = 3 + 2 = 7 – 2.$$

Задача 3.3. Довести, що кожне просте число виду $4k + 1$ є довжиною гіпотенузи прямокутного трикутника, сторони якого виражаються натуральними числами.

Розв'язання.

Згідно з теоремою Ферма кожне просте число виду $4k + 1$ є сумою двох квадратів натуральних чисел. Тому для такого p: $p = a^2 + b^2$, де a і b – натуральні числа і причому різні (так як p – непарне), наприклад, $a > b$. Звідси

$$p^2 = (a^2 – b^2)^2 + (2ab)^2,$$

тобто p є гіпотенузою прямокутного трикутника, катетами якого є натуральні числа $a^2 – b^2$ і $2ab$. Так,

$$5^2 = 3^2 + 4^2,\ 13^2 = 5^2 + 12^2,\ 17^2 = 15^2 + 8^2,\ 29^2 = 21^2 + 20^2.$$

Задача 3.4. Довести, що рівняння

$$p^2 + q^2 = r^2 + s^2 + t^2$$

не має розв'язків в простих числах p, q, r, s, t.

Доведення.

Відмітимо перш за все, що якщо p, q, r, s і t є простими числами і

$$p^2 + q^2 = r^2 + s^2 + t^2,$$

то кожне із чисел p і q відмінне від кожного із чисел r, s і t. Дійсно, якби було, наприклад, $p = r$, то ми отримали б рівняння $q^2 = s^2 + t^2$, яке не має розв'язків в простих числах q, s, t, так як числа s і t не можуть бути обидва ні парними, ні непарними (в будь-якому із цих випадків було б $q = 2$, що неможливо, так як права частина > 4). Якщо ж взяти $s = 2$, то число 4 буде різницею двох квадратів натуральних чисел, що неможливо.

Якщо

$$p^2 + q^2 = r^2 + s^2 + t^2,$$

то усі числа p, q, r, s, t не можуть тут бути непарними. Якщо p – парне, з відси випливає, $p = 2$, то числа q, r, s, t повинні бути непарними, а так як квадрат непарного числа при діленні на 8 дає остачу 1, то ліва частина при діленні на 8 давала б остачу 5, права ж – остачу 3, що неможливо.

Якщо числа p і q обидва непарні, то ліва частина при діленні на 8 дає остачу 2, а в правій частині, як легко помітити, тільки одне з чисел може (і повинно) бути парним, наприклад, $r = 2$. Але тоді права частина при діленні на 8 дає остачу 6, що неможливо.

Задача 3.5. Знайти всі натуральні числа n, для яких кожне із шести чисел

$$n + 1, n + 3, n + 7, n + 9, n + 13 \text{ і } n + 15$$

є простим.

Розв'язання.

Існує тільки одне таке натуральне число: $n = 4$. Насправді, для $n = 1$ число $n + 3 = 4$ – складене, для $n = 2$ число $n + 7 = 9$ – складене,

для $n = 3$ число $n + 1 = 4$ – складене, для $n > 4$ всі наші числа > 5 і принаймні одне із них ділиться на 5, так як числа 1, 3, 7, 9, 13, і 15 при діленні на 5 дають відповідно остачі 1, 3, 2, 4, 3 і 0, тобто усі ймовірні остачі, звідки слідує, що і числа

$$n + 1, n + 3, n + 7, n + 9, n + 13 \text{ і } n + 15$$

при діленні на 5 дають усі ймовірні остачі і, звідси випливає, хоча б одне із них ділиться на 5 і як число, більше п'яти (так як $n > 4$), є складеним. Але для $n = 4$ ми отримуємо прості числа 5, 7, 11, 13, 17 і 19.

Задача 3.6. Знайти всі цілі числа $k \geq 0$, для яких послідовність

$$k + 1, k + 2, \ldots, k + 10$$

містить найбільше число простих чисел.

Розв'язання.

Існує тільки одне таке число: $k = 1$. Для нього послідовність

$$k + 1, k + 2, \ldots, k + 10 \qquad (3.1)$$

містить п'ять простих чисел: 2, 3, 5, 7, 11. Для $k = 0$ і $k = 2$ в послідовності (3.1) міститься тільки по чотири простих числа. Якщо ж $k \geq 3$, то в послідовності (3.1) немає числа 3.

Як відомо, серед трьох послідовних непарних чисел завжди одне ділиться на 3 [5]. Таким чином, в послідовності (3.1) існує принаймні одне непарне складене число. Далі, в послідовності (3.1) завжди існує п'ять парних чисел і, значить (для $k > 2$), складених. Отже, в послідовності (3.1) для $k \geq 3$ ми маємо принаймні шість складених чисел і, звідси випливає, не більше чотирьох простих чисел.

Задача 3.7. Знайти всі сотні послідовних натуральних чисел, які містять по 25 простих чисел.

Розв'язання.

Існує тільки шість таких сотень, а саме ті, першими членами яких є числа 1, 3, 4, 5, 10 і 11. Доведення цього твердження випливає з наступної леми: для $k > 11$ серед чисел $k, k + 1, \ldots, k + 99$ маємо принаймні 76 чисел, які діляться на 2, 3, 5, 7 або 11.

Для доведення леми складемо нескінченну зростаючу послідовність натуральних чисел, які діляться на 2, 3, 5, 7 або 11. Якщо число γ міститься в нашій послідовності, то в ній також міститься число $\gamma + 2310$, і навпаки (так як $2310 = 2 \cdot 3 \cdot 5 \cdot 7 \cdot 11$). Нехай $\gamma_1, \gamma_2, \ldots, \gamma_s$ – всі натуральні числа, які не перевищують 2310 і діляться на 2, 3, 5, 7 або 11. Тоді усі числа нашої послідовності містяться в s арифметичних прогресіях

$$2310t + \gamma_i, \text{ де } i = 1, 2, \ldots, s, \; t = 0, 1, 2, \ldots$$

Тепер достатньо виписати усі натуральні числа, які не перевищують 2310 + 100 і діляться на 2, 3, 5, 7 або 11, і впевнитися, що в кожній сотні чисел

$$k, k + 1, \ldots, k + 99 \text{ для } 1 \leq k \leq 2310$$

міститься принаймні 76 чисел із виписаної послідовності.

Задача 3.8. Знайти всі відрізки натурального ряду, які складаються з 21 числа і містять по 8 простих чисел.

Розв'язання цієї задачі пояснює наступне твердження: в кожному відрізку натурального ряду, який складається з 21 числа, міститься принаймні 14 чисел, що діляться хоча б на одне із чисел 2, 3 або 5.

Доведення твердження.

В кожному відрізку натурального ряду, який складається із 21 числа, міститься принаймні 10 чисел, що діляться на 2, і принаймні 10 послідовних непарних чисел, серед яких мається хоча б три числа, що діляться на 3. Таким чином, залишається показати, що в кожному відрізку натурального ряду, який складається з 21 числа, міститься принаймні одне число, що ділиться на 5, але не ділиться ні на 2, ні на 3. Нехай γ означає остачу від ділення числа x на 30. Тоді $x = 30t + \gamma$, де t – ціле число ≥ 0, а $\gamma = 0, 1, \ldots, 29$.

Якщо $\gamma \leq 5$, то

$$x \leq 30t + 5 < x + 20$$

і число $30t + 5$ є число послідовності $x, x + 1, \ldots, x + 20$, яке ділиться на 5, але не ділиться ні на 2, ні на3. Якщо ж $5 < \gamma \leq 25$, то

$$x \leq 30t + 25 > x + 20$$

і число $30t + 25$ є число послідовності $x, x + 1, \ldots, x + 20$, яке ділиться на 5, але не ділиться ні на 2, ні на 3. Якщо, нарешті, $25 < \gamma < 30$, то

$$x < 30t + 35 < x + 20$$

і число $30t + 35$ є число послідовності $x, x + 1, \ldots, x + 20$, яке ділиться на 5, але не ділиться ні на 2, ні на 3. Отже, твердження доведено.

З твердження безпосередньо випливає, що в кожному відрізку натурального ряду, який складається з 21 числа, будь-яке з яких > 5, ми маємо принаймні 14 складених чисел і , звідси слідує, що не більше 7 простих чисел. Для $x = 1$, 2 і 3 в послідовності $x, x + 1, \ldots, x + 20$ ми маємо по 8 простих чисел, а для $x = 4$ і $x = 5$ маємо по 7 простих чисел. Таким чином, в послідовності $x, x + 1, \ldots, x + 20$ ми маємо по 8 простих чисел тільки для $x = 1$, 2 і 3.

Задача 3.9. Довести, що існує нескінченно багато пар послідовних простих чисел, які не є парами простих чисел-близнюків.

Доведення.

Нехай p_k – k-е по порядку просте число і нехай p_{k_n} для натурального числа n означає найбільше просте число $\leq 6n + 1$. Так як числа

$$6n + 2 = 2(3n + 1),\ 6n + 3 = 3(2n + 1) \text{ і } 6n + 4 = 2(3n + 2)$$

є складеними, то зрозуміло, що $p_{k_n+1} \geq 6n + 5$ і, звідси випливає,

$$p_{k_n+1} - p_{k_n} \geq (6n + 5) - (6n + 1) = 4,$$

тобто послідовні прості числа p_{k_n} і p_{k_n+1} не складають пару простих чисел-близнюків.

Так як $p_{k_n+1} \geq 6n + 5$, а n може бути будь-яким натуральним числом, то таких пар чисел p_{k_n}, p_{k_n+1} існує нескінченно багато. Зазначимо, однак, що в такій парі p_{k_n}, p_{k_n+1} p_{k_n} може бути більшим

числом із деякої пари простих чисел-близнюків, а p_{k_n+1} – меншим числом із деякої іншої пари простих чисел-близнюків; наприклад: для $n = 1$ $p_{k_n} = 7$ є більше із пари чисел-близнюків 5 і 7, а $p_{k_n+1} = 11$ є менше із пари чисел-близнюків 11 і 13; для $n = 2$ $p_{k_n} = 13$ є більше із пари 11 і 13, а $p_{k_n+1} = 17$ є менше із пари 17 і 19; для $n = 17$ $p_{k_n} = 103 = 6 \cdot 17 + 1$ є більше із пари 101 і 103, а $p_{k_n+1} = 107$ є менше із пари 107 і 109.

Задача 3.10. Знайти п'ять найменших натуральних чисел n, для яких число $n^2 - 1$ є добутком трьох різних простих чисел.

Розв'язання.

Якщо для натурального числа n число $n^2 - 1$ є добутком трьох різних простих чисел, то, так як $2^2 - 1 = 3$, число n повинно бути > 2. З іншого боку, n повинно бути парним, так як інакше обидва співмножника правої частини рівності

$$n^2 - 1 = (n - 1)(n + 1)$$

були б парними і з'ясувалося би, що $2^2 | n^2 - 1$. При цьому числа $n - 1$ і $n + 1$, які обидва > 1 (так як $n > 2$), не можуть бути обидва складеними, інакше в цьому випадку число $n^2 - 1$ не є добутком трьох різних простих чисел. Звідси випливає, що одне із чисел $n - 1$ і $n + 1$ повинно бути простим, інше ж – добутком двох різних простих чисел. Для $n = 4$ маємо

$$n - 1 = 3,\ n + 1 = 5,$$

тобто ця умова не виконується. Аналогічно для $n = 6$, так як

$$n - 1 = 5,\ n + 1 = 7.$$

Для $n = 8$ маємо $n - 1 = 7$, $n + 1 = 3^2$.

Для $n = 10$ $n - 1 = 3^2$,

для $n = 12$ $n - 1 = 11$, $n + 1 = 13$.

Для $n = 14$ $n - 1 = 13$, $n + 1 = 3 \cdot 5$.

Найменше натуральне число n, для якого $n^2 - 1$ є добутком трьох різних простих чисел, є число $n = 14$, для якого

$$n^2 - 1 = 3 \cdot 5 \cdot 13.$$

Так як $16^2 - 1 = 3 \cdot 5 \cdot 17$, то наступним таким числом n є $n = 16$. Так як

$$18^2 - 1 = 17 \cdot 19, \quad 20^2 - 1 = 19 \cdot 21 = 3 \cdot 7 \cdot 19,$$

то третім по порядку таким числом n являється $n = 20$. Потім маємо

$$22^2 - 1 = 3 \cdot 7 \cdot 23,$$

і, значить, четверте шукане число є $n = 22$. Міркуючи таким чином далі, легко знайдемо, що п'яте шукане число є $n = 32$, для якого

$$n^2 - 1 = 3 \cdot 11 \cdot 31.$$

Отже, п'ятьма найменшими шуканими числами є 14, 16, 20, 22 і 32.

Задача 3.11. Визначити, чи є число 353 простим.

Розв'язання.

Оскільки $353 \leq 19^2$, то необхідно перевірити подільність даного числа на: 2, 3, 5, 7, 11, 13, 17. Зрозуміло, що оскільки число 353 непарне, то воно не ділиться на 2. Тепер використовуємо ознаки подільності на 3, 5, 7 та 11.

Оскільки число 353 не закінчується на 0 або 5, то воно не ділиться на 5. Знайдемо суму цифр даного числа: 3 + 5 + 3 = 11. Так як число 11 не ділиться на 3, то число 353 не ділиться на 3. Безпосередньою перевіркою встановлюємо, що дане число не ділиться на 7, 11, 13 та 17.

Таким чином, можна зробити висновок, що дане число – просте.

Задача 3.12. Які з чисел, розташовані між 2320 та 2350, є простими?

Розв'язання.

Маємо: $2320 \leq 48^2$, $2350 \leq 48^2$. Тобто нам необхідно перевірити подільність чисел, розташованих в даних межах, на прості числа:

2, 3, 5, 7, 11, 13, 17, 19, 23, 29, 31, 37, 41, 43, 47.

Між 2320 та 2350 розташовані наступні числі:

2321, 2322, 2323, 2324, 2325, 2326, 2327, 2328, 2329, 2330,

2331, 2332, 2333, 2334, 2335, 2336, 2337, 2338, 2339, 2340,

2341, 2342, 2343, 2344, 2345, 2346, 2347, 2348, 2349.

З цих чисел відразу можна відкинути ті, що діляться на 2 та на 5:

на 2 діляться:

2322, 2324, 2326, 2328, 2330, 2332, 2334,
2336, 2338, 2340, 2342, 2344, 2346;

на 5 діляться:

2325, 2330, 2335, 2340, 2345.

Залишаються числа:

2321, 2323, 2337, 2339, 2331, 2333,
2337, 2339, 2341, 2343, 2347, 2349.

Перевіряємо ці числа на подільність на 3:

2 + 3 + 2 + 1 = 8 – число 2321 не ділиться на 3,

2 + 3 + 2 + 3 = 10 – число 2323 не ділиться на 3,

2 + 3 + 3 + 7 = 15 – число 2337 ділиться на 3,

2 + 3 + 3 + 9 = 17 – число 2339 не ділиться на 3,

2 + 3 + 3 + 1 = 9 – число 2331 ділиться на 3,

2 + 3 + 3 + 3 = 11 – число 2333 не ділиться на 3,

2 + 3 + 3 + 7 = 15 – число 2337 ділиться на 3,

2 + 3 + 3 + 9 = 17 – число 2339 не ділиться на 3,

2 + 3 + 4 + 1 = 10 – число 2341 не ділиться на 3,

2 + 3 + 4 + 3 = 12 – число 2343 ділиться на 3,

2 + 3 + 4 + 7 = 16 – число 2347 не ділиться на 3,

2 + 3 + 4 + 9 = 18 – число 2349 ділиться на 3.

Отже, в результаті залишаються числа:

2321, 2323, 2339, 2333, 2339, 2341, 2347.

Безпосередньою перевіркою з‘ясовуємо, що:

- число 2221 ділиться на 7,
- число 2323 ділиться на 23.

Таким чином, простими є числа:

2339, 2333, 2339, 2341, 2347.

Задача 3.13. Перевірити, чи ділиться на 7 число 4136.

Розв‘язання.

Щоб дізнатися остачу від ділення натурального числа на 7, треба справа наліво підписати під цифрами цього числа коефіцієнти:

... –1, 2, 3, 1, –2, –3, –1, 2, 3, 1,

потім помножити кожну цифру на коефіцієнт, що стоїть під нею, і отримані добутки скласти; знайдена сума буде мати ту саму остачу від ділення на 7, що і дане число.

Діючи так, як вказано в правилі, ми знаходимо:

$$\begin{array}{cccc} 4 & 1 & 3 & 6 \\ \underline{-1} & \underline{2} & \underline{3} & \underline{1} \\ -4 & 2 & 9 & 6 \end{array}$$

$$(-4) + 2 + 6 = 13.$$

Таким чином, при діленні даного числа на 7 маємо остачу 13, тобто число 4136 не ділиться на 7.

Задача 3.14. Перевірити, чи ділиться на 7 число 8546216.

Розв‘язання.

Діючи так, як вказано в правилі, ми знаходимо:

$$\begin{array}{ccccccc} 8 & 5 & 4 & 6 & 2 & 1 & 6 \\ \underline{1} & \underline{-2} & \underline{-3} & \underline{-1} & \underline{2} & \underline{3} & \underline{1} \\ 8 & -10 & -12 & -6 & 4 & 3 & 6 \end{array}$$

$$8 + (-10 + (-12) + (-6) + 4 + 3 + 6 = -7.$$

Таким чином, дане число ділиться на 7.

Задача 3.15. Довести, що число $n^3 - n$ ділиться на 6.

Розв‘язання.

Для розв‘язання задачі застосуємо теорію порівнянь.

Ми доведемо, що число $n^3 - n$ ділиться на 2, і окремо доведемо, що воно ділиться на 3. Так як 2 і 3 взаємно прості, то звідси буде випливати за теоремою 2, що $n^3 - n$ ділиться на 6.

Якщо $n \equiv 0 \ (mod\ 2)$, то

$$n^3 - n \equiv 0^3 - 0 \equiv 0 \ (mod\ 2);$$

якщо $n \equiv 1 \ (mod\ 2)$, то

$$n^3 - n \equiv 1^3 - 1 \equiv 0 \ (mod\ 2).$$

Отже, в будь-якому випадку

$$n^3 - n \equiv 0 \ (mod\ 2),$$

тобто число $n^3 - n$ ділиться на 2.

Далі, якщо $n \equiv 0 \ (mod\ 3)$, то

$$n^3 - n \equiv 0^3 - 0 \equiv 0 \ (mod\ 3);$$

якщо $n \equiv 1 \ (mod\ 3)$, то

$$n^3 - n \equiv 1^3 - 1 \equiv 0 \ (mod\ 3);$$

якщо $n \equiv 2 \ (mod\ 3)$, то

$$n^3 - n \equiv 2^3 - 2 \equiv 0 \ (mod\ 3).$$

Отже, в будь-якому випадку

$$n^3 - n \equiv 0 \ (mod\ 3),$$

тобто $n^3 - n$ ділиться на 3.

Задача 3.16. Чи існує таке натуральне n, що число

$$\underbrace{111...11}_{n \quad цифр}$$

ділиться на 217?

Розв'язання.

Розглянемо числа

$$1,\ 11,\ 111,\ 1111,\ ...,\ \underbrace{111...11}_{218 \quad цифр}.$$

Кожне з них має якусь остачу від ділення на 217. Так як остач від ділення на 217 є 217 (тобто 0, 1, 2, ..., 216), а чисел в нас 218, то знайдуться серед них два числа, що мають однакові остачі від ділення на 217.

Нехай, наприклад,

$$\underbrace{111...11}_{k \quad цифр} \equiv \underbrace{111...11}_{k+l \quad цифр} \ (mod 217),$$

тоді різниця цих чисел ділиться на 217.

Підписавши перше число під другим та здійснюючи віднімання “стовпчиком”, ми побачимо, що різниця цих чисел має вигляд:

$$\underbrace{111...11}_{l \text{ цифр}}\underbrace{000...00}_{k \text{ цифр}},$$

тобто ця різниця дорівнює $10^k \cdot \underbrace{111...11}_{l \text{ цифр}}$. За доведеним це число ділиться на 217.

Залишається застосувати теорему 1.3: так як числа 10^k та 217 взаємно прості, то число $\underbrace{111...11}_{l \text{ цифр}}$ повинно ділитися на 217.

Ми бачимо, що відповідь на поставлене запитання позитивна. Можна навіть стверджувати, що існує число, що можна записати не більш, ніж 217 одиницями, і яке ділиться на 217.

ВИСНОВКИ

Самостійна теорія простих чисел є менш відомою спеціальною областю арифметики. Вона відрізняється просто формулюваннями постановок задач і в той же час складними, часто аналітичними, доведеннями. Багато проблем очікують ще свого рішення.

В ході виконання дослідження було розглянуто основні теоретичні відомості з теорії простих чисел; розкрито питання про прості числа, що задовольняють певним співвідношенням, зокрема, про числа Ферма та Мерсенна; розглянуто можливості застосування простих чисел до розв'язування різноманітних задач теорії чисел. Підсумовуючи результати дослідження, можна відмітити наступні твердження.

Прості числа виду $M(p) = 2^p - 1$, де p – також просте число, називають простими числами Мерсенна. Коли n – непарне складене число, то $2^n - 1$ буде також складеним числом.

Крім того при будь-якому парному $n \geq 4$ числа виду

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

складені. Таким чином, якщо p не є простим числом, то серед чисел Мерсенна немає простих.

Загальний спосіб перевірки чисел Мерсенна на простоту полягає у безпосередньому підставленні значень p, але чим більше p, тим важче таку перевірку здійснити. Станом на сьогодні відомо 51 просте число Мерсенна $2^{82589933} - 1$. Це число з 24862048 цифр, записане за основою 10. З 1997 року усі прості числа Мерсенна були знайдені в рамках Great Internet Mersenne Prime Search, проекту розподілених обчислень.

П. Ферма був упевнений, що всі числа виду $F_k = 2^{2^k} + 1$ прості (числа F_k називають числами Ферма). Проте, гіпотеза Ферма, взагалі кажучи, була помилковою. Ейлер зазначив, що всі дільники числа

$2^{2^k} + 1$ повинні мати вигляд $m \cdot 2^n + 1$.

Цікаво, що прості числа Ферма F_k відіграють важливу роль у задачі про можливість побудови правильного n–кутника за допомогою циркуля та лінійки. К.Ф. Гаусс довів, що правильний n–кутник можна побудувати за допомогою циркуля та лінійки тільки тоді, коли число його сторін n дорівнює $2^\alpha \cdot p_1 \cdot \ldots \cdot p_s$ ($\alpha \geq 0$, $s \geq 1$), де всі прості числа p_i є простими числами Ферма. Відкриття Гаусса загострило інтерес до пошуку простих чисел Ферма. Багато математиків шукали серед чисел Ферма прості. Але жодного нового числа Ферма навіть за допомогою ЕОМ так і не було знайдено.

Цікаву формулу запропонував Лежандр: $f(n) = 2n^2 + 29$. Вона дає прості числа для значень n від 0 до 28. Проте праці видатних математиків так і не дали позитивної відповіді на запитання про формулу довільного простого числа.

Числа Ферма мають цікаві властивості, зокрема: 1) якщо k є ціле невід'ємне число і якщо число $p = 12k + 5$ є простим, то число $3^{6k+2} + 1$ ділиться на p; 2) якщо число F_n є числом Ферма, то число $3^{2^{2^n-1}} + 1$ ділиться на F_n.

Прості числа є досить корисною темою для здобувачів, які приймають активну участь у математичних олімпіадах різного рівня, оскільки для участі в олімпіаді здобувачі мають, окрім інших вимог, мати відповідні знання, зокрема, і з теорії чисел. В роботі наведено низку прикладів розв'язування задач, пов'язаних із властивостями простих чисел, натуральних чисел, ознак подільності та ін.

СПИСОК ВИКОРИСТАНИХ ДЖЕРЕЛ

1. Айерлэнд К. Классическое введение в современную теорию чисел: Пер. с англ. / К. Айерлэнд, М. Роузен. – М.: Мир, 1987. – 416 с.
2. Бевз Г.П. Методика розв‘язування алгебраїчних задач / Г.П. Бевз. – К.: Рад. шк., 1995. – 240 с.
3. Боревич З. И. Теория чисел. Изд. 2-е. / З.И. Боревич, И.Р. Шафаревич. – М.: Наука, 1972. – 496 с.
4. Бородін О. І. Теорія чисел. Вид. 3-те, перероб. доп.: Підручник для фіз.-мат. факультетів пед. ін.-тів / О.І. Бородін. – К.: Вища школа, 1990. – 274 с.
5. Бухштаб А. А. Теория чисел / А.А. Бухштаб. – М.: Учпедгиз, 1960. – 396 с.
6. Венков Б.А. Избранные труды. Исследования по теории чисел / Б.А. Венков. – Л.: Наука, 1981. – 448 с.
7. Виноградов И.М. Основы теории чисел. / И.М. Виноградов. – М.: Наука, 1989. – 238 с.
8. Воронин С.М. Простые числа / С.М. Воронин. – М.: Знание, 1988. – 64 с.
9. Гайштут О.Г. Розв‘язування алгебраїчних задач: Посібник для вчителів / О.Г. Гайштут, Г.М. Литвиненко. – К.: Рад. шк., 1991. – 203 с.
10. Дополнительные главы по курсу математики 7-8 классов для факультативных занятий / Составитель К.П. Сикорский. – М.: Просвещение, 1979. – 206 с.
11. Задания для учащихся. 100 развивающих задач по теории чисел и арифметике. – М.: Наука, 1995. – 186 с.
12. Игошин В.И. Задачи и упражнения по математической логике и теории алгоритмов / В.И. Игошин. – М.: Издательский центр "Академия", 2007. – 304 с.

13. Клейн Ф. Элементарная математика с точки зрения высшей: В 2- х томах, т.1. Арифметика. Алгебра. Анализ. / Ф. Клейн. – М.: Наука, 1987. – 432 с.
14. Ляпин Е.С. Алгебра и теория чисел / Е.С. Лапин, А.Е. Евсеев. – М.: Просвещение, 1984. – 526 с.
15. Математика. Посібник для факультативних занять у 10 класі / За ред. проф. І.Є. Шиманського. – К.: Радянська школа, 2000. – 255 с.
16. Михелович Ш.Х. Теория чисел / Ш.Х. Михелович. – М.: Высшая школа, 1997. – 358 с.
17. Окунев Л.Я. Краткий курс теории чисел / Л.Я. Окунев. – М.: Учпедгиз, 1975. – 426 с.
18. Оре О. Приглашение в теорию чисел: Пер с англ. Изд. 2-е, стереотипное. / О. Оре. – М.: Едиториал УРСС, 2003. – 128 с.
19. Постников А.Г. Введение в аналитическую теорию чисел / А.Г. Постников. – М.: Наука, 1991. – 416 с.
20. Просветов Г.И. Теория чисел: задачи и решения: Учебно-практическое пособие / Г.И. Просветов. – М.: Издательство «Альфа-Пресс», 2010. – 72 с.
21. Расева Е. Математика и математики.: Пер. с англ. / Е. Расева, Р. Сикорский. – М.: Наука. Главная редакция физико-математической литературы, 1992. – 342 с.
22. Серпинский В. Что мы знаем и не знаем о простых числах: Пер. с польского Мельникова И. Г. / В. Серпинский. – М.: Наука, 1993. – 90 с.
23. Серпинский В. 250 задач по элементарной теории чисел / В. Серпинский. – М.: Просвещение, 1982. – 160 с.
24. Сивошинский И.Х. Задачи по математике для внеклассных занятий (9-10 класс) / И.Х. Сивошинский. – М.: Просвещение, 1988. – 486 с.

25. Справочник по элементарной математике / Под ред. Фильчакова П. Ф. – К.: Наукова думка, 1992. – 527 с.
26. Трост Э. Простые числа: Пер. с нем. Федельмана Н. И. / Под ред. Гельфонда А. О. – М.: Гос. изд. физ.-мат. лит.-ры, 1989. – 135 с.
27. Факультативный курс по математике 7-9 / Составитель И.Л. Никольская. – М.: Просвещение, 1991. – 214 с.
28. Фішман І.М. Методологічні питання шкільного курсу математики: Посібник для самоосвіти / І.М Фішман. – К.: Рад. шк., 1985. – 214 с.
29. Фридман Д.М. Как научиться решать задачи: Беседы о решении математических задач: Пособие для учащихся / Д.М. Фридман, Е.Н. Турецкий, В.Я. Стеценко. – М.: Просвещение, 1989. – 160 с.
30. Цейтен Г.Г. История математики в древности и в средние века / Г.Г Цейтен. – ГОНТИ, 1968. – 312 с.
31. Чарков И.И. Простые числа в курсе математики средней школы / И.И. Чарков // Математика в школе. – 1986. – № 5. – С.67-69.
32. Черватюк О.Г. Елементи цікавої математики на уроках математики / О,Г. Черватюк, Г.Д. Шиманська. – К.: Радянська школа, 1988. – 298 с.
33. Шмигевський М. Велика теорема Ферма / М. Шмигевський // Математика в школі. – 2006. – № 2. – С.51-56.
34. Ядренко М.Й. У світі математики / М.Й. Ядренко. – К.: Радянська школа, 1975. – 264 с.
35. Cohen H. A Course in Computational Algebraic Number Theory. New York: Springer-Verlag, 1996. 546 p.
36. Ribenboim P. The New Book of Prime Number Records. New York: SpringerVerlag, 1996. 541 p.