

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

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

а)  $(n^3 - n) : 6$ ;

б)  $(n^5 - n) : 30$ ;

в)  $(n(n^2 + 5)) : 6$ ;

г)  $(n^7 - n) : 42$ ;

д)  $mn(m^4 - n^4) : 30$ ;

е)  $(n^5 - 5n^3 + 4n) : 120$ ;

е)  $(n^4 + 6n^3 + 11n^2 + 6n) : 24$ ;

ж)  $(n^3 + 11n) : 6$ ;

з)  $(n^2 + 3n + 5)$  не : 121.

1.11. Довести, що для довільного натурального числа  $n$ :

а)  $(2^{4n} - 6) : 10$ ;

б)  $(4^{2n} - 3^{2n} - 7) : 84$ ;

в)  $(6^{2n-1} + 1) : 7$ ;

г)  $(n + 1)(n + 2) \dots (n + n) : 2^n$ ;

д)  $(3^{2n} + 5)$  не : 8.

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

а)  $(5^{2n} - 1) : 24$ ; е)  $(10^n + 18n - 1) : 27$ ;

б)  $(10^{3n} - 1) : 27$ ; е)  $(3^{2n+3} + 40n - 27) : 64$ ;

в)  $(15^n - 1) : 7$ ; ж)  $(4^n + 6n - 1) : 9$ ;

г)  $(3^{6n} - 2^{6n}) : 35$ ; з)  $(10^{n+1} - 9n - 10) : 81$ ;

д)  $(11^{n+2} + 12^{2n+1}) : 133$ ; к)  $(9^{n+1} - 8n - 9) : 16$ .

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

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

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

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

а) довжина, при наймені, одного катета ділиться на 3;

б) довжина, при наймені, однієї із сторін ділиться на 5.

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

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

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

## § 2. Означення і властивості простих та складених чисел.

Решето Ератосфена. Канонічна форма натурального числа.

Розподіл простих чисел серед чисел

натурального ряду

### Література

[1] — § 7, с. 89—92; § 8, с. 95—99;

[2] — § 7, с. 86—91; § 8, с. 93—98;

[3] — гл. 11, § 1, с. 365—372;

[4] — гл. II, § 7, с. 124—134;

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

## ТЕОРЕТИЧНІ ВІДОМОСТІ

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

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

**Теорема Евкліда.** *Множина простих чисел нескінчена.*

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

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

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

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

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

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

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

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

Відомо, що  $\lim_{x \rightarrow \infty} [\pi(x) : \frac{x}{\ln x}] = 1$  (асимптотичний закон розподілу простих чисел).

Відомо також, що

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

(нерівності Чебишова).

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

## ПРИКЛАДИ РОЗВ'ЯЗУВАННЯ ЗАДАЧ

1. Просте чи складене число 323?

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

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

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

В результаті дістаемо, що 323 не ділиться на 7, 11, 13, а ділиться на 17. Відповідь. Число 323 є складеним.

**З ау в а ж е н н я.** Якщо існує точне значення  $\sqrt{n}$ , тобто  $\sqrt{n} = k$ ,  $k \in \mathbb{N}$ , то  $n$  є складеним числом, бо  $n = k^2$ .

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

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

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

3. Знайти канонічний розклад числа 4725.

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

Скорочено цей процес записують так:

$$\begin{array}{c|c} 4725 & 3 \\ 1575 & 3 \\ 525 & 3 \\ 175 & 5 \\ 35 & 5 \\ 7 & 7 \\ 1 & \end{array}$$

### Зауваження

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

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

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

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

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

в якої

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

Отже, якщо  $k$  складене, то

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

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

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

Таким чином, якщо зображення

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

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

Якщо, крім того,

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

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

#### Зауваження

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

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

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

5. Знайти канонічний розклад чисел 4725 і 1769.

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

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

### Задачі

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

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

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

2.3. Знайти канонічний розклад числа  $n$ , якщо:

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

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

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

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

2.5. Знайти канонічний розклад числа  $a$ , якщо:

- а)  $a = 2^6 + 3^6$ ;      д)  $a = 2^{18} + 3^{18}$ ;  
 б)  $a = 5^4 + 5^3 - 6$ ;      е)  $a = 235^2 + 972^2$ ;  
 в)  $a = 5^6 + 5^3 - 2$ ;      ж)  $a = 3^{10} + 3^5 + 1$ .  
 г)  $a = 7^8 + 7^4 - 6$ ;

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

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

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

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

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

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

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

2.11. Нехай  $p_k$  є  $k$ -те просте число ( $p_1 = 2$ ,  $p_2 = 3$ ,  $p_3 = 5$ ,  $p_4 = 7$  і т. д.). Довести, що:

- а)  $p_k < 2^{2^{k-1}}$ , причому рівність виконується тільки при  $k = 1$ ;  
 б)  $p_k > 2k$ , де  $k \geq 5$ ;  
 в)  $p_{k+1} < p_1 p_2 \dots p_k$ ,  $k > 1$ ,  
 г)  $p_1 p_2 \dots p_k > n$ , де  $p_k \leq n$  і  $n > 2$ .

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

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

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

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

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

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

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

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

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

**2.19.** Знайти натуральне число  $n$ , якщо:

а)  $n = 2^\alpha$ ,  $n + 1 = 3^\beta$ , де  $\alpha$ ,  $\beta$  — деякі натуральні числа;

б)  $n = 3^\alpha$ ,  $n + 1 = 2^\beta$ , де  $\alpha$ ,  $\beta$  — деякі натуральні числа.

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

**2.21.** Знайти  $n$  послідовних складених натуральних чисел, якщо:

а)  $n = 10$ ; б)  $n = 12$ ; в)  $n = 100$ ; г)  $n = 1000$ ; д)  $n = k$ .

**2.22.** Довести нескінченість множини простих чисел виду:

а)  $p = 3k + 2$ ,  $k \in \mathbb{N}$ ;      г)  $p = 4k + 3$ ,  $k \in \mathbb{N}$ ;

б)  $p = 3k + 1$ ,  $k \in \mathbb{N}$ ;      д)  $p = 6k + 1$ ,  $k \in \mathbb{N}$ ;

в)  $p = 4k + 1$ ,  $k \in \mathbb{N}$ ;      е)  $p = 6k + 5$ ,  $k \in \mathbb{N}$ .

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

#### Література

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

#### ТЕОРЕТИЧНІ ВІДОМОСТІ

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

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

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

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

Якщо  $a \mid b$ , то  $(a, b) = |b|$ .