

## § 18. Конгруенції другого степеня, квадратичні лишки і квадратичні нелишки, символ Лежандра

### *Література*

- [1] — § 18, с. 184—192;
- [2] — § 18, с. 187—196;
- [10] — гл. V, § 1—4, с. 68—80;
- [11] — гл. 21, 22, с. 172—200;
- [12] — гл. III, § 10, с. 110—124;
- [14] — § 25—28, с. 105—136.

### ТЕОРЕТИЧНІ ВІДОМОСТІ

Конгруенцію другого степеня виду

$$a_1y^2 + a_2y + a_3 \equiv 0 \pmod{n}, \quad a_1 \not\equiv 0 \pmod{n} \quad (1)$$

зазвиди можна звести до двочленної конгруенції виду

$$x^2 \equiv a \pmod{m}, \quad (2)$$

де  $a = a_2^2 - 4a_1a_3$ ,  $x = 2a_1y + a_2$ ,  $m = 4an$ .

Для цього слід обидві частини і модуль конгруенції (1) домножити на 4 і зробити відповідні перетворення.

Якщо конгруенція (2) має хоча б один розв'язок, то  $a$  називається **квадратичним лишком за модулем  $m$** , у противному разі  $a$  називається **квадратичним нелишком за модулем  $m$** . При цьому  $(a, m) = 1$ .

Розв'язування конгруенції виду (2) за складеним модулем зводиться до розв'язування таких конгруенцій:

$$1) \quad x^2 \equiv a \pmod{p}, \quad \text{де } p \text{ — непарне просте число}; \quad (3)$$

$$2) \quad x^2 \equiv a \pmod{p^\alpha}, \quad \text{де } p \text{ — непарне просте число, } \alpha > 1; \quad (4)$$

$$3) \quad x^2 \equiv a \pmod{2^\alpha}, \quad \text{де } \alpha > 1. \quad (5)$$

Найбільш важливим є той випадок, коли модуль є непарним простим числом. При цьому досить обмежитися випадком, коли  $(a, p) = 1$ , оскільки в противному разі конгруенція (3) має єдиний розв'язок  $x \equiv 0 \pmod{p}$ .

Отже, надалі розглядатимемо таку конгруенцію:

$$x^2 \equiv a \pmod{p}, \quad (a, p) = 1, \quad \text{де } p \text{ — просте непарне число}. \quad (6)$$

Якщо  $a$  — квадратичний лишок за модулем  $p$ , то конгруенція (6) має два розв'язки.

Для будь-якого іростого непарного числа  $p$  половина лишків зведеній системи лишків є квадратичними лишками, а половина — квадратичними нелишками.

При простому непарному  $p$  число  $a$  є квадратичним лишком за модулем  $p$  тоді і тільки тоді, коли  $a^{\frac{p-1}{2}} \equiv 1 \pmod{p}$ , і квадратичним нелишком тоді і тільки

тоді, коли  $a^{\frac{p-1}{2}} \equiv -1 \pmod{p}$  (критерій Ейлера).

**Теорема Ейлера.** Добуток двох квадратичних лишків або нелишків є квадратичним лишком за модулем  $p$ ; добуток квадратичного лишку на нелишок є квадратичним нелишком.

Добуток ряду чисел  $a, b, \dots, c$  дає квадратичний лишок або нелишок залежно від того, парне чи непарне число нелишків буде серед множників.

Для ефективного використання критерію Ейлера вводиться так званий **символ Лежандра**  $\left( \frac{a}{p} \right)$  (читається: «символ Лежандра  $a$  відносно  $p$ », або коротше « $a$  відносно  $p$ », або « $a$  до  $p$ »),  $a$  називається **чисельником**, а  $p$  — **знаменником** символу Лежандра.

Символ Лежандра  $\left(\frac{a}{p}\right)$  визначається для всіх цілих чисел  $a$ , які не діляться на просте непарне число  $p$ , рівністю

$$\left(\frac{a}{p}\right) = \begin{cases} 1, & \text{якщо } a \text{ є квадратичним лишком за модулем } p, \\ -1, & \text{якщо } a \text{ є квадратичним нелишком за модулем } p. \end{cases}$$

Критерій Ейлера тоді коротко записується так:

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

**Основні властивості символу Лежандра:**

$$1^\circ. \text{ Якщо } a \equiv b \pmod{p}, \text{ то } \left(\frac{a}{p}\right) = \left(\frac{b}{p}\right);$$

$$2^\circ. \left(\frac{a^2}{p}\right) = 1;$$

$$3^\circ. \left(\frac{1}{p}\right) = 1;$$

$$4^\circ. \left(\frac{-1}{p}\right) = (-1)^{\frac{p-1}{2}};$$

$$5^\circ. \left(\frac{ab \dots c}{p}\right) = \left(\frac{a}{p}\right) \left(\frac{b}{p}\right) \dots \left(\frac{c}{p}\right);$$

$$6^\circ. \left(\frac{ab^2}{p}\right) = \left(\frac{a}{p}\right);$$

$$7^\circ. \left(\frac{a^n}{p}\right) = \left(\frac{a}{p}\right)^n;$$

$$8^\circ. \left(\frac{2}{p}\right) = (-1)^{\frac{p^2-1}{8}};$$

$$9^\circ. \text{ Якщо } p \text{ і } q — \text{різні непарні прості числа, то}$$

$$\left(\frac{q}{p}\right) = \left(\frac{p}{q}\right) \cdot (-1)^{\frac{p-1}{2} \cdot \frac{q-1}{2}}$$

(закон взаємності квадратичних лишків).

У загальненням символу Лежандра є **символ Якобі**  $\left(\frac{a}{m}\right)$  (читається: «символ Якобі  $a$  відносно  $m$ »). Він визначається для буль-яких непарних натуральних чисел  $m > 1$  і чисел  $a$ , взаємно простих з  $m$ , рівністю

$$\left(\frac{a}{m}\right) = \left(\frac{a}{p_1}\right) \left(\frac{a}{p_2}\right) \dots \left(\frac{a}{r}\right),$$

де  $m = p_1 \cdot p_2 \dots r$  є розкладом  $m$  на прості множники (серед них можуть бути і рівні), тобто як добуток символів Лежандра. Для символу Якобі зберігаються властивості 1) — 9) символу Лежандра, проте для символу Якобі йдея не про непарні прості числа  $p$ , а про непарні натуральні числа  $m > 1$ , для властивості 9) — про взаємно прості непарні числа, відмінні від 1. Тому при визначенні символу Лежандра зручно розглядати його як символ Якобі. При цьому часто немає потреби виділяти з чисельника символу його непарні прості множники.

Конгруенція  $x^2 \equiv a \pmod{p^n}$ , де  $p$  — непарне просте число,  $n > 1$ ,  $(a, p) = 1$ , має два розв'язки, якщо  $\left(\frac{a}{p}\right) = 1$ , і не має їх зовсім, якщо  $\left(\frac{a}{p}\right) = -1$ .

Для конгруенції  $x^2 \equiv a \pmod{2^n}$ ,  $(a, 2) = 1$ , необхідними умовами існування розв'язків є  $a \equiv 1 \pmod{4}$  при  $a = 2$ ;  $a \equiv 1 \pmod{8}$  при  $a > 3$ .

Якщо ці умови виконуються, то існує один розв'язок при  $a = 1$ ; два розв'язки при  $a = 2$  і чотири розв'язки при  $a > 3$ .

Для конгруенції загального виду  $x^2 \equiv a \pmod{m}$ ,  $m = 2^k p_1^{a_1} p_2^{a_2} \dots p_k^{a_k}$ ,  $(a, m) = 1$ , необхідними і достатніми умовами існування розв'язків є:  $a \equiv 1 \pmod{4}$  при  $a = 2$ ;  $a \equiv 1 \pmod{8}$  при  $a > 3$

$$\left( \frac{a}{p_1} \right) = \left( \frac{a}{p_2} \right) = \dots = \left( \frac{a}{p_k} \right) = 1.$$

Якщо жодну з цих умов не порушенено, то число розв'язків дорівнюватиме:  $2^k$  — при  $a = 0$  і  $a = 1$ ;  $2^{k+1}$  — при  $a = 2$ ;  $2^{k+2}$  — при  $a > 3$ .

### ПРИКЛАДИ РОЗВ'ЯЗУВАННЯ ЗАДАЧ

1. Звести конгруенцію другого степеня  $4x^2 - 11x - 3 \equiv 0 \pmod{13}$  до двочленної.  
**Розв'язання.** Для простого модуля старший коефіцієнт взаємно простий з ним. Тоді процес зведення заданої конгруенції до двочленної можна скоротити і навіть залишити модуль незмінним. Визначимо множник  $k$  так, щоб  $4k \equiv 1 \pmod{13}$ . Матимемо  $k \equiv 10 \pmod{13}$ . Домножуючи обидві частини заданої конгруенції на 10 за модулем 13, дістаємо

$$40x^2 - 110x - 30 \equiv 0 \pmod{13},$$

або

$$x^2 - 6x - 4 \equiv 0 \pmod{13}. \quad (1)$$

Виділімо в лівій частині цієї конгруенції повний квадрат

$$x^2 - 2 \cdot 3x + 9 - 9 - 4 \equiv 0 \pmod{13},$$

або

$$(x - 3)^2 - 13 \equiv 0 \pmod{13}.$$

Остаточно

$$(x - 3)^2 \equiv 0 \pmod{13}.$$

#### Зauważення

1. При розв'язуванні задач такого типу треба намагатися спростити процес виділення повного квадрату, для цього є різні способи. Зокрема, у розглянутому прикладі від заданої конгруенції можна було б перейти до такої конгруенції:

$$4x^2 - 24x - 16 \equiv 0 \pmod{13}. \quad (2)$$

Оскільки  $(4, 13) = 1$ , то на 4 можна скоротити обидві частини конгруенції (2):

$$x^2 - 6x - 4 \equiv 0 \pmod{13}.$$

Дістали конгруенцію (1).

2. Часто процес зведення конгруенції до двочленної завершується простим розв'язанням її. Так,

$$x - 3 \equiv 0 \pmod{13}, \text{ або } x \equiv 3 \pmod{13}.$$

2. Скільки розв'язків має конгруенція  $x^2 \equiv 219 \pmod{383}$ ?

**Розв'язання.** Знайдемо символ Лежандра  $\left( \frac{219}{383} \right)$ . Оскільки  $219 = 3 \cdot 73$ , а 383 — просте число, то, згідно з властивістю 5,

$$\left( \frac{219}{383} \right) = \left( \frac{3}{383} \right) \cdot \left( \frac{73}{383} \right).$$

Обчислимо окремо символи Лежандра  $\left(\frac{3}{383}\right)$  і  $\left(\frac{73}{383}\right)$ . Оскільки 3 і 383 — різні прості непарні числа, то внаслідок закону взаємності 9) дістаемо

$$\left(\frac{3}{383}\right) = \left(\frac{383}{3}\right) \cdot (-1)^{\frac{381-1}{2} \cdot \frac{3-1}{2}} = -\left(\frac{383}{3}\right).$$

За властивістю 1) маємо

$$\left(\frac{383}{3}\right) = \left(\frac{2}{3}\right),$$

бо  $383 \equiv 2 \pmod{3}$ .

За властивістю 8)

$$\left(\frac{2}{3}\right) = (-1)^{\frac{3^2-1}{8}} = -1.$$

Отже,  $\left(\frac{3}{383}\right) = -(-1) = 1$ . Щоб спростити запис, а також полегшити процес перевірки, доцільно при кожному переході під знаком рівності ставити номер властивості, на основі якої відбувається цей перехід. Наприклад,

$$\begin{aligned} \left(\frac{73}{383}\right)_9 &= \left(\frac{383}{73}\right) \cdot (-1)^{\frac{381-1}{2} \cdot \frac{73-1}{2}} = \left(\frac{383}{73}\right)_1 \left(\frac{18}{73}\right) = \\ &= \left(\frac{2 \cdot 3^2}{73}\right)_6 = \left(\frac{2}{73}\right)_8 = (-1)^{\frac{73^2-1}{8}} = 1. \end{aligned}$$

Остаточно

$$\left(\frac{219}{383}\right) = \left(\frac{3}{383}\right) \cdot \left(\frac{73}{383}\right) = 1 \cdot 1 = 1.$$

Таким чином, задана конгруенція має два розв'язки.

### Зауваження

1. Слід уважно застосовувати властивість 9), оскільки якщо хоч одне з чисел  $p$  чи  $q$  є складеним, застосування цієї властивості може привести до помилок в обчисленні символу Лежандра.

2. Розглядаючи символ Лежандра як окремий випадок символу Якобі і користуючись властивостями останнього, можна символ Лежандра обчислити швидше. Наприклад,

$$\begin{aligned} \left(\frac{219}{383}\right)_9 &= \left(\frac{383}{219}\right) \cdot (-1)^{\frac{383-1}{2} \cdot \frac{219-1}{2}} = -\left(\frac{383}{219}\right)_1 \left(\frac{164}{219}\right) = \\ &= \left(\frac{41 \cdot 2^2}{219}\right)_6 = -\left(\frac{41}{219}\right)_9 = -\left(\frac{219}{41}\right) \cdot (-1)^{\frac{219-1}{2} \cdot \frac{41-1}{2}} = \\ &= -\left(\frac{219}{41}\right)_1 = -\left(\frac{14}{41}\right)_6 = -\left(\frac{2}{41}\right) \cdot \left(\frac{7}{41}\right) = (-1)^{\frac{41^2-1}{8}} \left(\frac{7}{41}\right) = \\ &= -\left(\frac{7}{41}\right)_9 = -\left(\frac{41}{7}\right) (-1)^{\frac{41-1}{2} \cdot \frac{7-1}{2}} = -\left(\frac{41}{7}\right)_1 = -\left(\frac{-1}{7}\right)_4 = -(-1)^{\frac{7-1}{2}} = 1. \end{aligned}$$

3. Зауважимо, що коли  $p$  — просте непарне число, то символ Лежандра  $\left(\frac{a}{p}\right)$

є для конгруенції  $x^2 \equiv a \pmod{p}$  символом Якобі  $\left(\frac{a}{p}\right)$  і навпаки. Тому для

конгруенції за простим модулем можна не розрізняти символів Лежандра і Якобі, що дає змогу при обчисленні символів Лежандра не розкладати чисельник на прості множники. Треба тільки виділяти множники, що дорівнюють 2. Якщо  $\left(\frac{a}{p}\right) = 1$ , то ця конгруенція має два розв'язки; якщо  $\left(\frac{a}{p}\right) = -1$ , конгруенція розв'язків не має. Для конгруенції  $x^2 \equiv a \pmod{m}$ , де  $m$  — непарне складене число, символ Лежандра не існує, а символ Якобі існує. Проте, якщо символ Якобі  $\left(\frac{a}{m}\right) = 1$  і  $m$  — непарне складене число, то це ще не означає, що конгруенція  $x^2 \equiv a \pmod{m}$  має розв'язки. Так, конгруенція  $x^2 \equiv 2 \pmod{15}$  розв'язків не має, а символ Якобі для неї  $\left(\frac{2}{15}\right)_8 = (-1)^{\frac{15^2-1}{8}} = 1$ .

### Задачі

**16.1.** Розв'язати конгруенції, звівши їх до двочленних.

- а)  $3x^2 - 5x - 7 \equiv 0 \pmod{5}$ ;      е)  $3x^2 + 2x \equiv 1 \pmod{7}$ ;
- б)  $3x^2 - x \equiv 0 \pmod{5}$ ;      е)  $4x^2 \equiv 7x + 3 \pmod{11}$ ;
- в)  $2x^2 + 4x - 1 \equiv 0 \pmod{5}$ ;      ж)  $5x^2 + 7x + 1 \equiv 0 \pmod{13}$ ;
- г)  $2x^2 - 4x - 5 \equiv 0 \pmod{7}$ ;      з)  $4x^2 - 11x - 3 \equiv 0 \pmod{13}$ ;
- д)  $2x^2 + 5x - 1 \equiv 0 \pmod{7}$ ;

**16.2.** Розв'язати задані конгруенції, звівши їх до двочленних:

- а)  $3x^2 + 6x + 1 \equiv 0 \pmod{10}$ ;      е)  $12x^2 - 6x - 7 \equiv 0 \pmod{19}$ ;
- б)  $4x^2 + 3x + 3 \equiv 0 \pmod{15}$ ;      е)  $7x^2 + 15x - 11 \equiv 0 \pmod{23}$ ;
- в)  $3x^2 + 7x + 8 \equiv 0 \pmod{17}$ ;      ж)  $x^2 - 5x + 6 \equiv 0 \pmod{24}$ ;
- г)  $6x^2 + 3x + 1 \equiv 0 \pmod{17}$ ;      з)  $12x^2 - 8x - 15 \equiv 0 \pmod{44}$ ;
- д)  $3x^2 + 13x - 10 \equiv 0 \pmod{19}$ ;

**16.3.** Користуючись критерієм Ейлера, знайти всі квадратичні лишки за модулями: а) 5; б) 7; в) 11; г) 13; д) 17; е) 23; е) 37; ж) 53.

**16.4.** Розв'язати способом проб такі конгруенції:

- а)  $x^2 \equiv 2 \pmod{7}$ ;
- б)  $x^2 \equiv 4 \pmod{7}$ ;
- в)  $x^2 \equiv 3 \pmod{7}$ .

**16.5.** Обчислити символи Лежандра:

- а)  $\left(\frac{13}{7}\right)$ ;      б)  $\left(\frac{22}{13}\right)$ ;      в)  $\left(\frac{19}{67}\right)$ ;      г)  $\left(\frac{37}{67}\right)$ ;      д)  $\left(\frac{56}{73}\right)$ ;      е)  $\left(\frac{47}{73}\right)$ ;
- е)  $\left(\frac{54}{83}\right)$ ;      ж)  $\left(\frac{68}{113}\right)$ ;      з)  $\left(\frac{63}{131}\right)$ .

**16.6.** Користуючись символом Якобі, обчислити символи Лежандра:

- а)  $\left(\frac{283}{563}\right)$ ;      б)  $\left(\frac{251}{577}\right)$ ;      в)  $\left(\frac{241}{593}\right)$ ;      г)  $\left(\frac{323}{607}\right)$ ;      д)  $\left(\frac{346}{643}\right)$ ;      е)  $\left(\frac{3153}{1201}\right)$ ;
- е)  $\left(\frac{20470}{1847}\right)$ ;      ж)  $\left(\frac{2108}{2003}\right)$ ;      з)  $\left(\frac{3149}{5987}\right)$ .

**16.7.** Знайти кількість розв'язків таких конгруенцій:

- а)  $x^2 \equiv 3 \pmod{31}$ ;      е)  $x^2 \equiv 429 \pmod{563}$ ;
- б)  $x^2 \equiv 2 \pmod{31}$ ;      е)  $x^2 \equiv 579 \pmod{821}$ ;
- в)  $x^2 \equiv 5 \pmod{73}$ ;      ж)  $x^2 \equiv 728 \pmod{919}$ ;
- г)  $x^2 \equiv 3 \pmod{101}$ ;      з)  $x^2 \equiv 847 \pmod{1087}$ ;
- д)  $x^2 \equiv 226 \pmod{563}$ ;      к)  $x^2 \equiv 3766 \pmod{5987}$ .

**16.8.** Знайти  $x$ , якщо:

- а)  $\left(\frac{x}{3}\right) = 1$ ; б)  $\left(\frac{x}{5}\right) = 1$ ; в)  $\left(\frac{x}{7}\right) = 1$ ; г)  $\left(\frac{x}{11}\right) = 1$ ; д)  $\left(\frac{x}{15}\right) = 1$ ;  
е)  $\left(\frac{x}{15}\right) = -1$ .

**16.9.** Довести, що:

- а) конгруенція  $x^2 \equiv a \pmod{p}$  має розв'язки

$$x \equiv a^{k+1}, \quad p - a^{k+1} \pmod{p},$$

якщо  $p$  — просте число виду  $4k + 3$ , а число  $a$  — квадратичний лишок за модулем  $p$ ;

- б) конгруенція  $x^2 \equiv a \pmod{p}$  має розв'язки

$$x \equiv a^{k+1} \cdot 2^{(2k+1)t} \pmod{p},$$

де  $t = 0$  при  $a^{2k+1} \equiv 1 \pmod{p}$  і  $t = 1$  при  $a^{2k+1} \equiv -1 \pmod{p}$ , якщо  $p$  — просте число виду  $8k + 5$  і  $a$  — квадратичний лишок за модулем  $p$ ;

в) рівняння  $11y = 5x^2 - 7$  не виконується при жодних цілих числах  $x$  і  $y$ ;

г) при діленні добутку двох послідовних цілих чисел на число 13 остача ніколи не дорівнює 1;

- д)  $2^{\frac{p-1}{2}} \equiv \begin{cases} 1 \pmod{p}, & \text{якщо } p \text{ — просте число виду } 8k + 7, \\ -1 \pmod{p}, & \text{якщо } p \text{ — просте число виду } 8k + 3, \end{cases}$

- е)  $\left(\frac{a}{p}\right)\left(\frac{-a}{p}\right) = \begin{cases} 1, & \text{якщо } p \text{ — просте число виду } 4k + 1, \\ -1, & \text{якщо } p \text{ — просте число виду } 4k + 3; \end{cases}$

- ж)  $\left(\frac{3}{p}\right) = \begin{cases} 1, & \text{якщо } p \text{ — просте число виду } 12k + 1 \text{ або } 12k + 11, \\ -1, & \text{якщо } p \text{ — просте число виду } 12k + 5 \text{ або } 12k + 7; \end{cases}$

ж) конгруенція  $x^2 \equiv a \pmod{16}$ ,  $a \equiv 1 \pmod{8}$  має розв'язки:  $x \equiv x_0$ ,  $16 - x_0$ ,  $x_0 + 8$ ,  $8 - x_0 \pmod{16}$ , де  $x_0$  — один з розв'язків заданої конгруенції; аналогічно за модулем  $2^a$ ,  $a > 4$ ,

$$x \equiv x_0, 2^a - x_0, x_0 + 2^{a-1}, 2^{a-1} - x_0 \pmod{2^a}.$$

**16.10.** Використовуючи результати задач 16.9, а), б), розв'язати конгруенції:

- а)  $x^2 \equiv 2 \pmod{311}$ ; в)  $x^2 \equiv 7 \pmod{29}$ ;

- б)  $x^2 \equiv 3 \pmod{47}$ ; г)  $x^2 \equiv 3 \pmod{37}$ .

**16.11.** Чи проходять через точки з цілими координатами такі параболи:

- а)  $43y = x^2 - 42$ ; в)  $83y = x^2 - 34$ ;

- б)  $73y = x^2 - 37$ ; г)  $443y = x^2 - 152$ ?

**16.12.** Розв'язати в цілих числах рівняння:

- а)  $4x^2 - 5y - 6 = 0$ ; г)  $x^2 - 10x - 11y + 5 = 0$ ;

- б)  $15x^2 - 7y^2 - 9 = 0$ ; д)  $x^2 - 21x - 13y + 110 = 0$ .

- в)  $5x^2 - 11y - 7 = 0$ ;

**16.13.** Довести, що:

а) розв'язки конгруенції  $x^2 + 1 \equiv 0 \pmod{p}$ , де  $p$  — просте число виду  $4m + 1$ , мають вид  $x = 1 \cdot 2 \dots 2m$ ;  $p - 1 \cdot 2 \dots 2m \pmod{p}$ ;

б) конгруенція  $x^2 + 1 \equiv 0 \pmod{p}$  має розв'язки тоді і тільки тоді, коли  $p$  — просте число виду  $4m + 1$ ;

- в) конгруенція  $x^2 + 2 \equiv 0 \pmod{p}$  має розв'язки тоді і тільки тоді, коли  $p$  — просте число виду  $8m+1$  або  $8m+3$ ;
- г) конгруенція  $x^2 + 3 \equiv 0 \pmod{p}$  має розв'язки тоді і тільки тоді, коли  $p$  — просте число виду  $6m+1$ ;
- д) множина простих чисел виду  $4m+1$  нескінчена;
- е) множина простих чисел виду  $6m+1$  нескінчена;
- ж) канонічний розклад числа виду  $a^2 + b^2$ , де  $(a, b) = 1$ , містить тільки прості числа виду  $4m+1$ ;
- ж) незалежно від простого непарного модуля  $p$  конгруенції

$$(x^2 - 13)(x^2 - 17)(x^2 - 221) \equiv 0 \pmod{p},$$

$$(x^2 - 3)(x^2 - 5)(x^2 - 7)(x^2 - 11)(x^2 - 1155) \equiv 0 \pmod{p}$$

мають завжди хоч один розв'язок;

- з) конгруенція  $x^2 \equiv -7 \pmod{p^a}$ , де  $p$  — непарне просте число виду  $7n+1$ , має розв'язки при будь-якому натуральному  $a$ ;
- к) конгруенція  $x^2 \equiv -11 \pmod{4p}$ , де  $p$  — непарне просте число виду  $11n+2$ , не має розв'язків;
- л) для будь-якого натурального  $n$  число  $1 + 2 + \dots + n$  не може закінчуватися цифрою 7.

**16.14.** Використовуючи результат задачі 16.9, ж), розв'язати такі конгруенції:

- а)  $x^2 \equiv 9 \pmod{16}$ ;      д)  $x^2 \equiv 57 \pmod{64}$ ;  
 б)  $x^2 \equiv 17 \pmod{32}$ ;      е)  $x^2 \equiv 65 \pmod{128}$ ;  
 в)  $x^2 \equiv 25 \pmod{32}$ ;      е)  $x^2 \equiv 73 \pmod{128}$ ;  
 г)  $x^2 \equiv 41 \pmod{64}$ ;      ж)  $x^2 \equiv 145 \pmod{256}$ .

**16.15.** Розв'язати конгруенції:

- а)  $x^2 \equiv 7 \pmod{27}$ ;      в)  $x^2 \equiv 91 \pmod{243}$ ;  
 б)  $x^2 \equiv 59 \pmod{125}$ ;      г)  $x^2 - 3x + 2 \equiv 0 \pmod{400}$ .

**16.16.** Довести, що:

- а)  $\left(\frac{-6}{p}\right) = \begin{cases} 1, & \text{якщо } p \text{ — просте число і } p \equiv 1, 5, 7, 11 \pmod{24}, \\ -1, & \text{якщо } p \text{ — просте число і } p \equiv 13, 17, 19, 23 \pmod{24}; \end{cases}$
- б)  $\left(\frac{ab}{p}\right) = (-1)^{\frac{p-1}{2}}$ , якщо  $p$  — непарний простий дільник числа  $ax^2 + by^2$ , де  $a, b, x, y$  — цілі числа і  $(ax, by) = 1$ ;
- в)  $10541 = 83 \cdot 127$ , якщо  $10541 = 3 \cdot 59^2 + 2 \cdot 7^2$ ;
- г) непарні прості дільники  $p$  чисел виду  $x^2 + 2y^2$  при  $(x, y) = 1$  мають вид  $p = 8n+1$ ,  $p = 8n+3$ ;
- д) непарні прості дільники  $p$  чисел виду  $2x^2 - y$  і  $x^2 - 2y^2$  при  $(x, y) = 1$  мають вид  $p = 8n+1$ ,  $p = 8n+7$ .

**§ 17. Порядок числа і класу лишків за модулем.**

Первісні корені, існування їх та кількість  
за простим модулем

### Література

- [1] — § 19, с. 193—201;  
 [2] — § 19, с. 196—204;  
 [3] — гл. 12, § 5, с. 413—416;  
 [10] — гл. VI, § 1—3, с. 86—90;