

- 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;

- [11] — гл. 17, 18, с. 139—152;
[12] — гл. IV, § 1, 2, с. 125—136;
[14] — § 29, 30, с. 137—144.

ТЕОРЕТИЧНІ ВІДОМОСТІ

Нехай $a \in \mathbb{Z}$, $m \in \mathbb{N}$ і $(a, m) = 1$. Порядком числа a за модулем m називається таке найменше натуральне число δ , що $a^\delta \equiv 1 \pmod{m}$. Число δ позначають ще як $\delta = P_m(a)$ і називають показником, до якого належить число a за модулем m . Оскільки за теоремою Ейлера $a^{\varphi(m)} \equiv 1 \pmod{m}$, то число δ завжди існує і $\delta \leq \varphi(m)$. Якщо $\delta = \varphi(m)$, то число a називають первісним коренем за модулем m .

Якщо $a \equiv b \pmod{m}$, то $P_m(a) = P_m(b)$. Ця властивість дає змогу казати про порядок класу лишків, а саме: клас лишків $K_a^{(m)}$ має порядок δ за модулем m . Якщо порядок його представника за цим самим модулем дорівнює δ .

Якщо $\delta = \varphi(m)$, то клас лишків називається класом первісних коренів за модулем m .

Якщо $\delta = P_m(a)$, то числа $1 = a^0, a^1, a^2, \dots, a^{\delta-1}$ попарно неконгруентні між собою за модулем m .

Якщо a — первісний корінь за модулем m , тобто $P_m(a) = \varphi(m)$, то числа $1 = a^0, a^1, a^2, \dots, a^{\varphi(m)-1}$ утворюють зведену систему лишків за модулем m .

Якщо $P_m(a) = \delta$, то $a^k \equiv a^l \pmod{m}$ тоді і тільки тоді, коли $k \equiv l \pmod{\delta}$. Зокрема, $a^k \equiv 1 \pmod{m}$ тоді і тільки тоді, коли $k \vdash \delta$.

Якщо $P_m(a) = \delta$ і $a^k \equiv 1 \pmod{m}$, то $k \vdash \delta$.

Якщо $P_m(a) = \delta$, то $\varphi(m) \vdash \delta$.

Якщо $(P_m(a), P_m(b)) = 1$, то $P_m(a \cdot b) = P_m(a) \cdot P_m(b)$.

Якщо $P_m(x) = ab$, то $P_m(x^2) = b$.

Якщо $P_m(a), P_m(b), \dots, P_m(c)$ — попарно взаємно прості числа, то $P_m(ab \dots c) = P_m(a) P_m(b) \dots P_m(c)$. $P_m(a^s) = P_m(a)$ тоді і тільки тоді, коли $(s, P_m(a)) = 1$.

$$P_m(a^k) = \frac{P_m(a)}{(P_m(a), k)}.$$

Якщо $P_m(a) = k$, то класи лишків $K_a^{(m)}, K_{a^2}^{(m)}, \dots, K_{a^k}^{(m)}$ є різними розв'язками конгруенції $x^k \equiv 1 \pmod{m}$.

Якщо m — просте число, то зазначені класи лишків вичерпують усі розв'язки даної конгруенції.

За простим модулем p кожен дільник d числа $p-1$ є порядком для $\varphi(d)$ класів лишків. Зокрема, існує $\varphi(p-1)$ класів первісних коренів (теорема Гаусса).

Якщо g — первісний корінь за простим модулем p , то інші первісні корені містяться серед степенів g^2, g^3, \dots, g^{p-1} і мають вигляд g^k , де $(k, p-1) = 1$ і $k < p-1$.

Якщо $p-1 = q_1^{k_1} q_2^{k_2} \dots q_s^{k_s}$ — канонічний розклад числа $p-1$, то число g тоді і тільки тоді є первісним коренем за простим модулем p , коли

$$g^{\frac{p-1}{q_i^{k_i}}} \not\equiv 1 \pmod{p}$$

для всіх $i = 1, 2, \dots, s$.

Первісні корені існують тільки за модулями $m = 2, 4, p^\alpha$ і $2p^\alpha$, де p — просте непарне число, а $\alpha > 1$.

Нехай g — первісний корінь за простим модулем p . Тоді можна знайти таке число t , що число u , яке визначається з умови

$$(g + pt)^{p-1} = 1 + p^u,$$

не ділиться на p . Відповідне число $g + pl$ є первісним коренем за модулем p^a при будь-якому $a > 1$.

Нехай $a > 1$ і g — первісний корінь за модулем p^a . Непарне з чисел g і $g + p$ є також первісним коренем за модулем $2p^a$.

Якщо $c = \varphi(m)$ і q_1, q_2, \dots, q_k — різні прості дільники числа c , то число g , взаємно просте з m , тоді і тільки тоді є первісним коренем за модулем m ; коли

$$g^{\frac{c}{q_l}} \not\equiv 1 \pmod{m}$$

для всіх $l = 1, 2, \dots, k$.

ПРИКЛАДИ РОЗВ'ЯЗУВАННЯ ЗАДАЧ

1. Знайти порядок $P_m(a)$ числа a за модулем m , якщо:

- а) $a = 2, m = 15$; б) $a = 3, m = 15$; в) $a = 8, m = 15$.

Розв'язання. Щоб знайти порядок $P_m(a)$ числа a за модулем m , слід забезпечити виконання таких вимог:

- 1) $(a, m) = 1$;
- 2) $P_m(a)$ — дільник числа $\varphi(m)$;
- 3) $P_m(a)$ — найменше з тих натуральних чисел k , для яких виконується конгруенція

$$a^k \equiv 1 \pmod{m}.$$

а) Маємо $(2, 15) = 1$. Знаходимо $\varphi(15)$. Оскільки $15 = 3 \cdot 5$, то $\varphi(15) = 3 \cdot 5 \left(1 - \frac{1}{3}\right)\left(1 - \frac{1}{5}\right) = 8$.

Отже, $P_{15}(2)$ міститься серед чисел 1, 2, 4, 8. Записуємо послідовно:

$$\begin{aligned} 2^1 &\equiv 2 \not\equiv 1 \pmod{15}, \\ 2^2 &\equiv 4 \not\equiv 1 \pmod{15}, \\ 2^4 &\equiv 16 \equiv 1 \pmod{15}. \end{aligned}$$

Отже, $P_{15}(2) = 4$.

б) Оскільки $(3, 15) = 3 \neq 1$, то для числа $a = 3$ за модулем 15 порядку не існує.

в) Оскільки $(8, 15) = 1$ і $8 = 2^3$, то $P_{15}(8)$ існує, його визначають за формулою

$$P_{15}(2^3) = \frac{P_{15}(2)}{(P_{15}(2), 3)} = \frac{4}{(4, 3)} = 4.$$

Зauważення

1. Щоб знайти порядок $P_m(a)$ числа a за модулем m , слід використовувати обчислення, зроблені на попередньому етапі. Так, якщо вже знайдено $a^k \equiv a_0 \pmod{m}$, де $k | \varphi(m)$, то щоб знайти a^l , де $l > k$ і $l | \varphi(m)$, треба використати те, що $a^k \equiv a_0 \pmod{m}$.

2. Процес знаходження порядку числа може водночас бути процесом знаходження первісних коренів за даним модулем m . Для цього слід визначити, які з чисел мають порядок $\varphi(m)$.

2. Знайти всі первісні корені за модулем 7.

Розв'язання. Первісних коренів за простим модулем $p = 7$ є $\varphi(p - 1) = \varphi(6) = 2$. Вони містяться серед чисел ЗСЛ₇:

$$\text{ЗСЛ}_7 = \{1, 2, 3, 4, 5, 6\}.$$

Оскільки $p - 1 = 6$ у канонічному розкладі має вигляд $p - 1 = 2 \cdot 3$, то досліджувати слід числа виду $a^{\frac{p-1}{3}}$ і $a^{\frac{p-1}{2}}$, тобто числа a^2 і a^3 , де $a \in \text{ЗСЛ}_7$.

Знайдемо перший первісний корінь. Перевіряємо число 2 (эроздуміло, що число 1 тільки за модулем 2 є первісним і тому в інших випадках перевірка не має смислу).

$$2^2 \equiv -3 \pmod{7}, \quad 2^3 \equiv 1 \pmod{7}.$$

Оскільки $3 < 6$, то 2 не є первісним коренем за модулем 7.
Перевіряємо число 3:

$$3^2 \equiv 2 \pmod{7}, \quad 3^3 \equiv -1 \pmod{7}.$$

Тоді $3^6 \equiv 1 \pmod{7}$. Отже, порядком числа 3 є 6, тобто 3 є первісним коренем за модулем 7.

Другий первісний корінь міститься серед чисел виду 3^k , де $(k, p-1) = (k, 6) = 1$ і $1 < k < 6$. Ці умови задовільняє тільки число $k = 5$. Отже, другим первісним коренем є число 3^5 . Оскільки $3^6 \equiv 5 \pmod{7}$, то первісними коренями за модулем 7 є числа 3 і 5.

Задачі

17.1. Знайти порядок числа a за модулем m , якщо:

- а) $a = 2, m = 5$; ж) $a = 7, m = 20$;
- б) $a = 4, m = 5$; з) $a = 7, m = 22$;
- в) $a = 5, m = 8$; к) $a = 6, m = 39$;
- г) $a = 10, m = 13$; л) $a = 7, m = 43$;
- д) $a = 4, m = 15$; м) $a = 5, m = 108$;
- е) $a = 2, m = 15$; н) $a = 2, m = 133$.
- є) $a = 2, m = 17$;

17.2. Знайти порядки всіх класів лишків за модулем m , якщо:

- а) $m = 11$; б) $m = 19$; в) $m = 21$.

17.3. Знайти порядки чисел a, b, c, d за модулем m , якщо:

- а) $a = 7, b = 9, c = 12, m = 13$;
- б) $a = 5, b = 8, c = 13, m = 17$;
- в) $a = 5, b = 8, c = 10, d = 16, m = 33$;
- г) $a = 10, b = 25, c = 50, m = 39$;
- д) $a = 5, b = 15, c = 21, d = 35, m = 44$.

17.4. Знайти порядок числа: а) 10 за модулем $13 \cdot 31$; б) $m - 1$ за модулем m .

17.5. Знайти всі первісні корені за такими модулями: а) 11; б) 13; в) 15; г) 19; д) 49; е) 81.

17.6. Знайти число первісних коренів і найменший з них за такими модулями: а) 10; б) 18; в) 19; г) 31; д) 37.

17.7. Знайти найменший первісний корінь за такими модулями:
а) 7; б) 17; в) 23; г) 41; д) 53; е) 50; ж) 71; з) 242; к) 289;
л) 578; м) 625.

17.8. Знаючи, що 3 є первісним коренем за модулем 29, знайти решту первісних коренів за цим модулем.

17.9. Знаючи, що 2 задовільняє конгруенцію $x^8 \equiv 1 \pmod{17}$, знайти всі розв'язки цієї конгруенції.

17.10. Знаючи, що $P_{29}(4) = 14$, знайти решту чисел, які мають порядок 14 за модулем 29.

17.11. Знаючи, що 2 — первісний корінь за модулем 37, довести, що $2^{18} \equiv 6^2 \pmod{37}$.

17.12. Знаючи, що $P_{29}(12) = 4, P_{29}(23) = 7$, знайти $P_{29}(15)$.

17.13. Знайти всі натуральні значення x , які задовільняють конгруенції:

$$\text{а) } 4^x \equiv 1 \pmod{3}; \quad \text{г) } 2^x \equiv 1 \pmod{25};$$

- б) $5^x \equiv 1 \pmod{8}$; д) $6^x \equiv 1 \pmod{49}$;
 в) $5^x \equiv 1 \pmod{9}$; е) $2^x \equiv 1 \pmod{49}$.

17.14. Знаючи, що 2 є первісний корінь за модулем 131 , знайти всі розв'язки конгруенції $x^3 \equiv 16 \pmod{131}$.

17.15. Знайти ті значення b , при яких мають розв'язки конгруенції: а) $4^x \equiv b \pmod{9}$; б) $5^x \equiv b \pmod{9}$.

17.16. Нехай p — просте непарне число. Довести, що:

а) серед первісних коренів за модулем p не може бути квадратів;

б) $\left(\frac{a}{p}\right) = 1$, якщо a — первісний корінь за модулем p ;

в) $\left(\frac{a^{2n+1}}{p}\right) = 1$, якщо a — первісний корінь за модулем p і $n \in \mathbb{N}$;

г) $P_p(ab) = P_p(a) \cdot P_p(b)$, якщо $(P_p(a), P_p(b)) = 1$;

д) за модулем p існують первісні корені;

е) $a^k + 1 \equiv 0 \pmod{p}$, якщо $P_p(a) = 2k$;

ж) добуток двох первісних коренів за модулем p не є первісним коренем за цим модулем;

ж) якщо $n > 1$, то існує $(p-1) \cdot \varphi(p-1)$ різних первісних коренів за модулем p^n , не конгруентних за модулем p^2 ;

з) якщо $n > 1$, то існує тільки $\varphi(\varphi(p^n))$ різних первісних коренів за модулем p^n ;

к) якщо $n > 1$, то існує $\varphi(\varphi(p^n))$ різних первісних коренів за модулем $2p^n$;

л) $a \cdot b$ не є первісним коренем за модулем p , якщо a і b не є ними за цим самим модулем;

м) якщо p — число виду $4k+1$ і g — первісний корінь за модулем p ; то $p-g$ — первісний корінь за модулем p ;

н) $a^k \equiv -1 \pmod{p}$, якщо $P_p(a) = 2k$ і a не $\equiv 1 \pmod{p}$.

17.17. Довести, що не існує первісних коренів за модулем m , якщо:

а) $m = 8$;

б) $m = 2^\alpha$, $\alpha \geq 3$;

в) $m = 36$;

г) $m = 2^\alpha p$, де $\alpha > 1$ і p — непарне просте число;

д) m — непарне складене число, яке ділиться, принаймні, на два різних простих множники.

17.18. Нехай p — просте непарне число. Довести, що

а) p має вигляд $1 + k \cdot 2^{n+1}$, якщо $p/2^{2^n} + 1$ і $n > 1$;

б) p має вигляд $1 + k \cdot 2^n$, якщо $p/2^{2^n} - 1$ і $n > 1$;

в) прості непарні дільники числа $a^p - 1$, де $a \in \mathbb{N}$ і $a > 1$ є дільниками числа $a-1$ або мають вигляд $2px+1$;

г) прості непарні дільники числа $a^p + 1$ є дільниками числа $a+1$ або мають вигляд $2px+1$;

д) множина простих чисел виду $2px+1$, $x \in \mathbb{N}$, є нескінченною;

е) a є первісним коренем за модулем p^α , $\alpha \geq 2$, якщо a є первісним коренем за модулем p^2 ;

е) $P_{p^k}(a) = P_{2p^k}(a)$, якщо a — непарне число, $a \nmid p$, $k \in \mathbb{N}$; зокрема, довільний непарний первісний корінь g за модулем p^k є ним і за модулем $2p^k$.

17.19. Довести, що:

а) первісний корінь за модулем $m > 2$ завжди є квадратичним нелишком за модулем m ;

б) $P_{a^{m-1}}(a) = m$, якщо $a, m \in \mathbb{N}$ і $a > 1$;

в) $\varphi(a^m - 1) \equiv 0 \pmod{m}$, якщо $a, m \in \mathbb{N}$ і $a > 1$;

г) $P_m(a) = [P_{p_1^{a_1}}(a), P_{p_2^{a_2}}(a), \dots, P_{p_s^{a_s}}(a)]$, якщо $(a, m) = 1$ і $m = p_1^{a_1} p_2^{a_2} \dots p_s^{a_s}$ — канонічний розклад числа m ;

д) $P_{p^k}(a) = d$, якщо $a^d \equiv 1 \pmod{p^k}$, де $d = P_{p^{k-1}}(a)$, p — просте число, $k \in \mathbb{N}$, $k > 1$, і $(a, p^k) = 1$;

е) $P_{p^k}(a) = p^d$, якщо $a^d \not\equiv 1 \pmod{p^k}$, де $d = P_{p^{k-1}}(a)$, p — просте число, $k \in \mathbb{N}$, $k > 1$, і $(a, p^k) = 1$;

ж) $P_{5929}(16) = 1155$;

ж) число a є первісним коренем за модулем m тоді і тільки тоді, коли клас лішків $K_a^{(m)}$ є твірним елементом мультиплікативної групи кільця Z_m .

§ 18. Індекси за простим модулем. Двочленні конгруенції за простим модулем; таблиці індексів із застосуванням

Література

- [1] — § 19, с. 201—204;
- [2] — § 19, с. 204—207;
- [3] — гл. 12, § 5, с. 416—420;
- [10] — гл. VI, § 4, с. 90—92;
- [11] — гл. 19, гл. 20, с. 163—172;
- [12] — гл. IV, § 3, 4, с. 136—146;
- [13] — § 31, 32, с. 144—152.

ТЕОРЕТИЧНІ ВІДОМОСТІ

Нехай g — первісний корінь за простим модулем p , $a \in \mathbb{Z}$ і $(a, p) = 1$. Ціле невід'ємне число γ називається індексом числа a за модулем p при основі g , якщо

$$g^\gamma \equiv a \pmod{p}. \quad (1)$$

Взагалі, довільне значення x , яке задовольняє конгруенцію

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

називається індексом числа d за модулем m при основі b і позначається

$$x \equiv \text{ind}_b d \pmod{m}. \quad (3)$$

При цьому m може бути й складеним числом, проте

$$(d, m) = (b, m) = 1.$$

Означення індексу можна записати ще так:

$$b^{\text{ind}_b d} \equiv d \pmod{m}. \quad (4)$$