

8. Степеневі лишки, первісні корені, індекси

8.1. Степеневі лишки

Нехай m, n — фіксовані натуральні числа і $c \not\equiv 0 \pmod{m}$. Розглянемо конгруенцію

$$x^k \equiv c \pmod{m}. \quad (8.1)$$

Якщо ця конгруенція має розв'язки, то число c називається *k-степеневим лишком* за модулем m . У протилежному разі говорять, що c є *k-степеневим нелишком* за модулем m . Для $k = 2$ і $k = 3$ говорять відповідно про *квадратичні* і *кубічні* лишки або нелишки.

Приклад. Нехай $m = 11$, а k дорівнює 2 або 3. З таблиці

$x \equiv 1, 2, 3, 4, 5, 6, 7, 8, 9, 10 \pmod{11}$
$x^2 \equiv 1, 4, 9, 5, 3, 3, 5, 9, 4, 1 \pmod{11}$
$x^3 \equiv 1, 8, 5, 9, 4, 7, 2, 6, 3, 10 \pmod{11}$

видно, що числа 1, 3, 4, 5, 9 є квадратичними лишками за модулем 11, а числа 2, 6, 7, 8, 10 — квадратичними нелишками. У той же час за модулем 11 будь-яке не кратне 11 число є кубічним лишком, а кубічних нелишків немає жодного.

Для взаємно простих чисел a і m завжди існує таке натуральне число n , що $a^n \equiv 1 \pmod{m}$ (наприклад, за теоремою Ойлера можна взяти $n = \varphi(m)$). Найменше таке n назовемо *порядком* числа a за модулем m і позначатимемо його символом $P_m(a)$.

Наприклад, порядок числа 3 за модулем 13 дорівнює 3, бо $3^1, 3^2 \not\equiv 1 \pmod{13}$, але $3^3 \equiv 1 \pmod{13}$.

Надалі впродовж усього цього розділу букви a і m позначатимуть взаємно прості числа і це, як правило, спеціально не застерігатиметься.

Відзначимо кілька властивостей функції $P_m(a)$.

Твердження 8.1. (a) Якщо $b \equiv a \pmod{m}$, то $P_m(b) = P_m(a)$.

(b) Якщо $P_m(a) = k$ та остача від ділення числа n на k дорівнює r , то $a^n \equiv a^r \pmod{m}$.

Доведення. (a) Якщо $b \equiv a \pmod{m}$, то для довільного $s \in \mathbb{N}$ $b^s \equiv a^s \pmod{m}$ (наслідок 2 з теореми 5.3). Тому з $a^{P_m(a)} \equiv 1 \pmod{m}$ випливає $b^{P_m(a)} \equiv 1 \pmod{m}$, а для довільного $1 \leq r < P_m(a)$ з $a^r \not\equiv 1 \pmod{m}$ випливає $b^r \not\equiv 1 \pmod{m}$.

$(\text{mod } m)$ випливає $b^r \not\equiv 1 \pmod{m}$.

(б) Якщо $P_m(a) = k$, то $a^k \equiv 1 \pmod{m}$. Нехай $n = k \cdot q + r$. Тоді $a^n = a^{k \cdot q + r} = (a^k)^q \cdot a^r \equiv 1^q \cdot a^r \equiv a^r \pmod{m}$ що й вимагалось. \square

Наслідок 1. (а) Конгруенція $a^s \equiv a^t \pmod{m}$ має місце тоді й лише тоді, коли $s \equiv t \pmod{P_m(a)}$. Зокрема, $a^s \equiv 1 \pmod{m}$ тоді й лише тоді, коли $P_m(a) | s$;

(б) $P_m(a) | \varphi(a)$;

(в) якщо $P_m(a) = n$, то для кожного $i \in \mathbb{N}$ має місце рівність $P_m(a^i) = \frac{n}{(i, n)}$.

Доведення. (а) Справді, нехай $a^s \equiv a^t \pmod{m}$. Без обмеження загальності можна вважати, що $s \geq t$. Із теореми Ойлера (теорема 5.10) випливає, що існує число b , для якого $ab \equiv 1 \pmod{m}$. Помноживши обидві частини конгруенції $a^s \equiv a^t \pmod{m}$ на b^{t-s} після очевидних скорочень одержимо $a^{s-t} \equiv 1 \pmod{m}$. Якщо остатча від ділення $s - t$ на $P_m(a)$ дорівнює r , то з твердження 8.1(б) тепер випливає, що $a^r \equiv 1 \pmod{m}$. Отже, $r = 0$ і $P_m(a) | s - t$, тобто $s \equiv t \pmod{P_m(a)}$.

Нехай тепер $s \equiv t \pmod{P_m(a)}$. Тоді s і t при діленні на $P_m(a)$ дають однакові остачі, а тому за твердженням 8.1(б) $a^s \equiv a^t \pmod{m}$.

Останню частину пункту (а) одержимо, якщо покладемо $t = 0$.

(б) Випливає з пункту (а), бо за теоремою Ойлера $a^{\varphi(m)} \equiv 1 \pmod{m}$.

(в) Нехай $(a^i)^k = a^{ik} \equiv 1 \pmod{m}$. Тоді з (а) випливає, що $ik \equiv 0 \pmod{n}$. Позначимо найбільший спільний дільник (i, n) чисел i та n через d . Тоді $i = di_1$, $n = dn_1$ і $dn_1 | di_1 k$, звідки $n_1 | i_1 k$. Але i_1 та n_1 — взаємно прості, тому $n_1 | k$ і $k \geq n_1$. З іншого боку, $(a^i)^{n_1} = a^{in_1} = a^{di_1 n_1} = (a^n)^{i_1} \equiv 1 \pmod{m}$. Отже, $n_1 = \frac{n}{(i, n)}$ є найменшим натуральним числом, для якого $(a^i)^k \equiv 1 \pmod{m}$, тобто $n_1 = P_m(a^i)$. \square

Задача 8.1. Для кожного з чисел від 2 до 9, взаємно простого з числом 10, знайти порядок цього числа за модулем 10.

Розв'язання. Серед даних чисел взаємно простими з 10 будуть числа 3, 7 і 9. За щойно доведеним наслідком (наслідок 1 (б)) їх порядки треба шукати серед дільників числа $\varphi(10) = 4$, тобто серед чисел 1, 2 і 4. Оскільки $3^1 \not\equiv 1 \pmod{10}$, $3^2 \not\equiv 1 \pmod{10}$, $7^1 \not\equiv 1 \pmod{10}$, $7^2 \not\equiv 1 \pmod{10}$, $9^1 \not\equiv 1 \pmod{10}$, і $9^2 \equiv 1 \pmod{10}$, то $P_m(3) = 4$, $P_m(7) = 4$, $P_m(9) = 2$. \square

Наслідок 2. Нехай $P_m(a) = k$. Тоді класи лишків $\bar{1} = \overline{a^0}, \bar{a^1}, \bar{a^2}, \dots, \bar{a^{k-1}}$ за модулем числа m є різними розв'язками конгруенції $x^k \equiv 1 \pmod{m}$.

Доведення. За попереднім наслідком (наслідок 1 (a)) класи лишків $\bar{1} = \overline{a^0}, \bar{a^1}, \bar{a^2}, \dots, \bar{a^{k-1}}$ є різними. Безпосередньо перевіряється, що всі вони є розв'язками конгруенції $x^k \equiv 1 \pmod{m}$. \square

Наприклад, $P_{18}(7) = 3$, тому класи лишків $\bar{1}, \bar{7}, \bar{7^2}$ є розв'язками конгруенції $x^3 \equiv 1 \pmod{18}$. Але ця конгруенція має й інші розв'язки, а саме $\bar{5}, \bar{11}$ і $\bar{17}$.

Для простого модуля p попередній наслідок можна посилити:

Наслідок 3. Якщо число p — просте і $P_p(a) = k$, то класи лишків $\bar{1} = \overline{a^0}, \bar{a^1}, \bar{a^2}, \dots, \bar{a^{k-1}}$ за модулем числа p дають усі k розв'язки конгруенції $x^k \equiv 1 \pmod{p}$.

Доведення. Це випливає з попереднього наслідку й теореми 7.2. \square

Задача 8.2. Знайти всі розв'язки конгруенції $x^5 \equiv 1 \pmod{11}$.

Розв'язання. Знайдемо спочатку число a , порядок якого за модулем 11 дорівнює 5. Перебираючи послідовно малі числа, знаходимо: $2^5 \not\equiv 1 \pmod{11}$, $3^5 \equiv 1 \pmod{11}$. За наслідком 3 з теореми 8.1 розв'язки даної конгруенції повністю вичерпуються такими класами лишків за модулем 11: $\bar{1}, \bar{3}, \bar{3^2} = \bar{9}, \bar{3^3} = \bar{5}, \bar{3^4} = \bar{4}$. \square

Твердження 8.2. (a) Якщо $P_m(a) = k, P_m(b) = l$ і числа k і l попарно взаємно прості, то $P_m(a \cdot b) = k \cdot l$.

(б) Якщо порядки $P_m(a_1), \dots, P_m(a_n)$ чисел a_1, \dots, a_n попарно взаємно прості, то $P_m(a_1 \cdots a_n) = P_m(a_1) \cdots P_m(a_n)$.

Доведення. (a) Справді, нехай $P_m(a \cdot b) = u$. Тоді $(ab)^u \equiv 1 \pmod{m}$ і $1 \equiv 1^l \equiv (ab)^{ul} \equiv a^{ul}b^{ul} \equiv a^{ul} \cdot 1 \equiv a^{ul} \pmod{m}$. Отже, за наслідком 1 a) з теореми 8.1 $k \mid ul$, і позаяк k і l попарно взаємно прості, то $k \mid u$. Analogічно отримуємо, що $l \mid u$. Але тоді $kl \mid u$. З іншого боку, з $(ab)^{kl} \equiv a^{kl}b^{kl} \equiv 1^l \cdot 1^k \equiv 1 \pmod{m}$ випливає, що $u \mid kl$. Тому $u = kl$.

(б) Ця частина легко доводиться за допомогою математичної індукції. Справді, для $n = 2$ це твердження збігається з уже доведеним твердженням (a). Припустимо тепер, що воно виконується для

$n = k \geq 2$. Тоді $P_m(a_1 \cdots a_k) = P_m(a_1) \cdots P_m(a_k)$ і це число взаємно просте з $P_m(a_{k+1})$. Тому для $n = k + 1$ отримуємо: $P_m(a_1 \cdots a_{k+1}) = P_m((a_1 \cdots a_k)a_{k+1}) = P_m(a_1 \cdots a_k)P_m(a_{k+1}) = P_m(a_1) \cdots P_m(a_k) \cdot P_m(a_{k+1})$.

□

Задача 8.3. Нехай $a > 1$ – натуральне число. Довести, що:

- (a) для кожного непарного простого числа p прості непарні дільники числа $a^p - 1$ або є дільниками числа $a - 1$, або мають вигляд $2px + 1$;
- (б) для кожного непарного простого числа p існує нескінченно багато простих чисел вигляду $2px + 1$;
- (в) прості дільники числа $2^{2^n} + 1$ мають вигляд $2^{n+1}x + 1$.

Розв'язання. (a) Якщо q – просте непарне число і $q | (a^p - 1)$, то $a^p \equiv 1 \pmod{q}$ і $P_q(a) | p$, тобто $P_q(a) = 1$ або $P_q(a) = p$. Якщо $P_q(a) = 1$, то $a \equiv 1 \pmod{q}$ і $q | (a - 1)$. Нехай тепер $P_q(a) = p$. Тоді співвідношення $P_q(a) | \varphi(q)$ (наслідок 1 (б) з теореми 8.1) набуває вигляду $p | (q - 1)$, звідки $q - 1 = 2px$ і $q = 2px + 1$.

(б) Із пункту (a) випливає, що простими числами вигляду $2px + 1$ будуть, наприклад, усі прості дільники числа $2^p - 1$. Тому прості числа такого вигляду існують. Нехай тепер d_1, \dots, d_k – довільні прості числа вигляду $2px + 1$. Розглянемо число $d^p - 1$, де $d = pd_1 \cdots d_k$. Жодне з чисел d_1, \dots, d_k не є його дільником. Із рівності $d^{p-1} + d^{p-2} + \cdots + d + 1 = (d - 1)(d^{p-2} + 2d^{p-3} + \cdots + (p - 1)) + p$ випливає, що кожний спільний дільник чисел $d - 1$ і $d^{p-1} + d^{p-2} + \cdots + d + 1$ має бути і дільником числа p . Але $d - 1 = pd_1 \cdots d_k - 1$ не ділиться на p . Тому числа $d - 1$ і $d^{p-1} + d^{p-2} + \cdots + d + 1$ – взаємно прості. Число $d^{p-1} + d^{p-2} + \cdots + d + 1$ як сума p непарних чисел також непарне. Нехай q – його непарний простий дільник. Оскільки q не ділить число $d - 1$, але ділить число $d^p - 1$, то за твердженням 8.2 (а) q має вигляд $q = 2px + 1$. Крім того, q відмінне від кожного з чисел d_1, \dots, d_k .

Таким чином, ми завжди можемо збільшити кількість простих чисел вигляду $2px + 1$ принаймні на 1. Тому таких чисел нескінченно багато.

(в) Нехай q – простий дільник числа $2^{2^n} + 1$. Тоді $2^{2^n} + 1 \equiv 0 \pmod{q}$, звідки $2^{2^{n+1}} - 1 = (2^{2^n} + 1)(2^{2^n} - 1) \equiv 0 \pmod{q}$, тобто $2^{2^{n+1}} \equiv 1 \pmod{q}$. Отже, $P_q(2) = 2^{n+1}$ і за наслідком 1 (б) $2^{n+1} | (q - 1)$. Тому $q = 2^{n+1}x + 1$. □

Задача 8.4. Довести, що кожне просте число p вигляду $p = 2^{2k} + 2^k + 1$ ділить число $2^{2^k+1} - 1$.

Розв'язання. Розглянемо число $p(2^k - 1) = 2^{3k} - 1$. Тоді $2^{3k} \equiv 1 \pmod{p}$. Нехай $P_p(2) = m$. За наслідком 1 (а) з теореми 8.1 $m \mid 3k$. Але з нерівності $2^{\frac{3k}{2}} < 2^{2k} < p$ випливає, що $m > \frac{3k}{2}$. Тому $m = 3k$. Крім цього, за наслідком 1 (б) з теореми 8.1 $m \mid \varphi(p)$, де $\varphi(p) = p - 1 = 2^k(2^k + 1)$, бо p – просте число. Отже, $3k \mid 2^k(2^k + 1)$. Число k не може бути парним, бо для $k = 2l$ число $2^{2k} + 2^k + 1 = 2^{4l} + 2^{2l} + 1 = (2^{2l} + 1)^2 - 2^{2l} = (2^{2l} + 2^l + 1)(2^{2l} - 2^l + 1)$ не є простим. Тому $3k \mid (2^k + 1)$ і $2^{2^k+1} \equiv 1 \pmod{p}$, тобто $p \mid (2^{2^k+1})$. \square

Задача 8.5. Довести, що для довільних натуральних чисел $a > 1$ і n число $\varphi(a^n - 1)$ ділиться на n .

Розв'язання. Із очевидної конгруенції $a^n \equiv 1 \pmod{a^n - 1}$ випливає, що $P_{a^n-1}(a) = n$. Але за наслідком 1 (б) з теореми 8.1 $P_{a^n-1}(a) \mid \varphi(a^n - 1)$, що й вимагається. \square

8.2. Первісні корені

Для взаємно простих чисел a і m число a називається *первісним коренем* за модулем m , якщо порядок a за цим модулем дорівнює $\varphi(m)$, тобто $P_m(a) = \varphi(m)$. Це поняття вперше ввів Ойлер.

Згідно з твердженням 8.1 (а) порядки $P_m(a)$ всіх чисел a , що належать одному й тому ж класові лишків за модулем m , одинакові. Тому $P_m(a)$ можна розглядати як функцію, визначену на множині класів лишків за модулем m , взаємно простих із модулем, і позначати $P_m(\bar{a})$. Тоді природно разом із числом a називати первісним коренем за модулем m і весь клас лишків \bar{a} за цим же модулем.

Постає питання про існування первісних коренів. Ойлер першим висловив припущення, що для кожного простого модуля p існує число, порядок якого дорівнює $p - 1 = \varphi(p)$. Згодом це довів Лежандр.

Теорема 8.1. За кожним простим модулем p існує рівно $\varphi(p - 1)$ класів первісних коренів.

Доведення. Доведемо спочатку існування первісних коренів. Нехай $\delta_1, \delta_2, \dots, \delta_r$ – усі можливі порядки за модулем p чисел $1, 2, \dots, p - 1$, а найменше спільне кратне τ цих порядків має канонічний розклад $\tau = p_1^{\alpha_1} \cdots p_k^{\alpha_k}$. Для кожного множника $p_s^{\alpha_s}$ цього розкладу повинен існувати порядок δ_j , який ділиться на цей множник. Тому δ_j можна записати у вигляді $\delta_j = b p_s^{\alpha_s}$. Нехай a_j – одне з чисел $1, 2, \dots, p - 1$,

для якого $P_p(a_j) = bp_s^{\alpha_s}$. Тоді, зокрема, $a_j^{\delta_j} \equiv 1 \pmod{p}$. Звідси маємо $a_j^{bp_s^{\alpha_s}} = (a_j^b)^{p_s^{\alpha_s}} \equiv 1 \pmod{p}$, отже, $P_p(a_j^b) = p_s^{\alpha_s}$. Позначимо число a_j^b через d_s , тоді для $d = d_1 \cdots d_k$ згідно з твердженням 8.2 (б) маємо $P_p(d) = \tau$ і за наслідком 1 (б) з теореми 8.1 $\tau \mid (p-1)$. Оскільки всі числа $\delta_1, \delta_2, \dots, \delta_r$ ділять τ , то за наслідком 1 (а) з теореми 8.1 кожне з чисел $1, 2, \dots, p-1$ є розв'язком конгруенції $x^\tau \equiv 1 \pmod{p}$. Але за теоремою 7.2 кількість таких розв'язків не може перевищувати степеня конгруенції, тобто $p-1 \leq \tau$. Тому $\tau = p-1$ і d – первісний корінь за модулем p .

Тепер доведемо таке допоміжне твердження:

Якщо існує хоча б одне число, порядок якого за простим модулем p дорівнює k , то такий порядок матиме щонайменше $\varphi(k)$ класів лишків за модулем p .

Справді, припустимо, що $P_p(a) = k$. Зокрема, тоді $a^k \equiv 1 \pmod{p}$ і, за наслідком 3, усі класи лишків $\overline{a^0}, \overline{a^1}, \overline{a^2}, \dots, \overline{a^{k-1}}$ є різними і є розв'язками конгруенції $x^k \equiv 1 \pmod{p}$. Нехай тепер показник s є взаємно простим із числом k і нехай $P_p(a^s) = l$. Тоді l є найменшим натуральним числом, для якого $(a^s)^l = a^{sl} \equiv 1 \pmod{p}$. Але $P_p(a) = k$, тому за наслідком 1 (а) з теореми 8.1 $k \mid sl$. Позаяк k і s взаємно прості, то $k \mid l$. З іншого боку, $(a^s)^k = (a^k)^s \equiv 1 \pmod{p}$. Тому, за тим же наслідком, $l \mid k$. Отже, $l = k$, тобто клас лишків $\overline{a^s}$ має порядок k .

Оскільки показників s , взаємно простих із числом k , буде рівно $\varphi(k)$, то щонайменше $\varphi(k)$ класів лишків матимуть за модулем p порядок k . Допоміжне твердження доведене.

Нехай тепер k – довільний дільник числа $p-1$ і $p-1 = kt$. Тоді з конгруенції $(d^t)^k = d^{kt} = d^{p-1} \equiv 1 \pmod{p}$ випливає, що $P_p(d^t) = k$. Разом із допоміжним твердженням це дає, що для кожного дільника k числа $p-1$ щонайменше $\varphi(k)$ класів лишків за модулем p мають порядок k . Позначимо кількість класів лишків порядку k через n_k . Тоді, з урахуванням твердження 2.1, одержуємо ланцюжок нерівностей:

$$p-1 \geq \sum_{k \mid p-1} n_k \geq \sum_{k \mid p-1} \varphi(k) = p-1 ,$$

з якого випливає, що для всіх дільників k числа $p-1$ $n_k = \varphi(k)$. Зокрема, число n_{p-1} первісних коренів дорівнює $\varphi(p-1)$. \square

З останньої частини доведення теореми 8.1 випливає таке

Твердження 8.3. Число класів лишків за модулем простого числа p , які за цим модулем мають порядок k , дорівнює $\varphi(k)$, якщо k ділить число $p - 1$, і 0 у протилежному разі.

Використовуючи алгебричну термінологію, теорему 8.1 можна переподумувати таким чином:

Теорема 8.1*. Якщо p — просте число, то в мультиплікативній групі кільця \mathbb{Z}_p рівно $\varphi(p - 1)$ елементів мають порядок $p - 1$.

Вправа 8.1. Довести, що коли g — первісний корінь за модулем m , то числа $g_0, g_1, g_2, \dots, g^{\varphi(m)-1}$ утворюють зведену систему лишків за модулем m .

Ефективного методу знаходження первісних коренів за даним простим модулем досі ще не знайдено. Для невеликих модулів їх можна шукати методом проб, перебираючи в певному порядку лишки за даним модулем і кожного разу з'ясовуючи, чи є цей лишок первісним коренем. Однак розумне впорядкування перебору дозволяє часто суттєво зменшити об'єм обчислень. Є два поширені способи такого впорядкування. Перший з них називається способом Ойлера і ґрунтуються на такій теоремі:

Теорема 8.2. Нехай p — просте число і $p - 1 = p_1^{\alpha_1} p_2^{\alpha_2} \cdots p_k^{\alpha_k}$ — канонічний розклад числа $p - 1$. Число a є первісним коренем за модулем p тоді й лише тоді, коли єжодна з конгруенцій

$$x^{p_i} \equiv a \pmod{p}, \quad i = 1, 2, \dots, k, \quad (8.2)$$

не має розв'язків.

Доведення. Нехай для деякого i одна з конгруенцій (8.2) має розв'язок x_0 . Піднесемо обидві частини цієї конгруенції до степеня $(p - 1)/p_i$: $x_0^{p-1} \equiv a^{(p-1)/p_i} \pmod{p}$. Але за теоремою Ферма $x_0^{p-1} \equiv 1 \pmod{p}$, тому матимемо $a^{(p-1)/p_i} \equiv 1 \pmod{p}$. Отже, $P_p(a) \leq (p - 1)/p_i < p - 1 = \varphi(p)$ і a не є первісним коренем. Таким чином, коли a — первісний корінь, то жодна з конгруенцій (8.2) розв'язків не має.

Припустимо тепер, що жодна з конгруенцій (8.2) не має розв'язків, але a не є первісним коренем. Тоді $P_p(a) = n$, де $n < p - 1$. За наслідком 1 (б) з теореми 8.1 $n | (p - 1)$, тобто $p - 1 = rn$. Припустимо, що одним із простих дільників числа r є p_i . Тоді $r = p_i l$. Оскільки $a^{ln} \equiv 1 \pmod{p}$, то для будь-якого x маємо

$$x^{p-1} - 1 = x^{p_i ln} - a^{ln} + a^{ln} - 1 = (x^{p_i} - a)(x^{p_i(ln-1)} + x^{p_i(ln-2)}a + \cdots +$$

$$+x^{p_i}a^{ln-2}+a^{ln-1})+(a^{ln}-1) \text{ або } x^{p-1}-1 \equiv x^{p_iln}-a^{ln}+a^{ln}-1= \\ =(x^{p_i}-a)(x^{p_i(ln-1)}+x^{p_i(ln-2)}a+\cdots+x^{p_i}a^{ln-2}+a^{ln-1}) \pmod{p}.$$

За теоремою Ферма конгруенція $x^{p-1}-1 \equiv 0 \pmod{p}$ має $p-1$ розв'язків, тому конгруенція $x^{p_i}-a \equiv 0 \pmod{p}$ має p_i розв'язків, що суперечить припущенням. Отже, a є первісним коренем. \square

Ця теорема дає такий алгоритм пошуку первісних коренів за модулем числа p . Нехай $p-1 = p_1^{\alpha_1}p_2^{\alpha_2}\cdots p_k^{\alpha_k}$ і $p_1 < p_2 < \cdots < p_k$. Підносимо кожне з чисел ряду

$$1, 2, 3, \dots, p-1 \quad (8.3)$$

до p_1 -го степеня й беремо найменші додатні лишки цих степенів за модулем числа p :

$$a_1, a_2, a_3, \dots, a_{p-1} \quad (8.4)$$

Для кожного числа a з ряду (8.4) конгруенція $x^{p_i} \equiv a \pmod{p}$ має розв'язок. Тому за теоремою 8.2 жодне з цих чисел не є первісним коренем за модулем числа p . Видаємо ці числа з ряду (8.3), а числа, що залишилися, підносимо до степеня p_2 і беремо найменші додатні лишки отриманих степенів за модулем числа p . Отримані числа знову не можуть бути первісними коренями, тому видаємо і їх з ряду (8.3) і т.д. Після k -го кроку у нас залишається тільки первісні корені за модулем числа p .

Задача 8.6. Знайти всі первісні корені за модулем числа 13.

Розв'язання. У нас $p = 13$ і $p-1 = 12 = 2^2 \cdot 3$. Підносимо числа $1, 2, \dots, 12$ до квадрату, одразу замінюючи квадрати найменшими додатними лишками за модулем 13. Потім числа, що не зустрічаються серед квадратів, підносимо до кубу. Результати обчислень подамо у вигляді таблиці

x	\equiv	1	2	3	4	5	6	7	8	9	10	11	12
x^2	\equiv	1	4	9	3	12	10	10	12	3	9	4	1
x^3	\equiv		8			8	8	5	5			5	

Числа, що не зустрічаються ні в другому, ні в третьому рядку, тобто числа 2, 6, 7, 11, і є первісними коренями за модулем числа 13. Як і стверджує теорема 8.1, їх буде $\varphi(12) = 4$. \square

Другий спосіб знаходження первісних коренів за модулем простого числа p називається *способом Гауса*. Він ґрунтуються на зауваженні, що достатньо знайти хоча б один первісний корінь a . Тоді всі інші первісні корені матимуть вигляд a^s , де показник s взаємно простий з числом $p - 1$. Отже, беремо будь-яке взаємно просте з p число a і, послідовно підносячи його до степеня 2, 3, ..., знаходимо його порядок $P_p(a) = n$. Якщо $n = p - 1$, то a і буде первісним коренем.

Якщо ж $n < p - 1$, то покажемо, як можна знайти число $a^{(1)}$, порядок якого буде більший за $P_p(a)$. Очевидно, що для довільного показника s порядок $P_p(a^s)$ числа a^s є дільником числа n . Крім того, із твердження 8.3 і доведення теореми 8.1 випливає, що степенями $\overline{a^0}, \overline{a^1}, \overline{a^2}, \dots, \overline{a^{n-1}}$ вичерпуються всі класи лишків за модулем p , порядки яких є дільниками числа n . Візьмемо тепер довільне число $b \not\equiv 0 \pmod{p}$, яке не конгруентне за модулем p жодному степеню числа a , і нехай $P_p(b) = n_1$. Якщо $n_1 > n$, то можна взяти $a^{(1)} = b$. У протилежному разі нехай $N = \text{НСК}(n, n_1)$. Оскільки $n_1 \nmid n$, то $N > n$. Нехай k — це добуток усіх тих множників $p_i^{\alpha_i}$ із канонічного розкладу $N = p_1^{\alpha_1} \cdots p_r^{\alpha_r}$, які ділять число n . Тоді $N = kl$, де $k \mid n$, $l \mid n_1$ і числа k та l — взаємно прості. Легко перевіряється, що $P_p(a^{n/k}) = k$ і $P_p(b^{n_1/l}) = l$. Тому

$$(a^{n/k}b^{n_1/l})^{kl} = (a^{n/k})^{kl}(b^{n_1/l})^{kl} \equiv 1 \pmod{p} \quad \text{i} \quad P_p(a^{n/k}b^{n_1/l}) \mid kl .$$

Позначимо $N_1 = P_p(a^{n/k}b^{n_1/l})$, $a_1 = a^{n/k}$, $b_1 = b^{n_1/l}$. Тоді $(a_1 b_1)^{N_1} = a_1^{N_1} b_1^{N_1} \equiv 1 \pmod{p}$. Нехай $N_2 = \alpha l - N_1$, де натуральне число α виберемо так, щоб N_2 було додатним. Із останньої конгруенції випливає, що $(a_1^{N_1} b_1^{N_1})^{N_2} = a_1^{N_1} b_1^{\alpha l} \equiv b_1^{N_2} \pmod{p}$. Але $b_1^{\alpha l} \equiv 1 \pmod{p}$, тому $a_1^{N_1} \equiv b_1^{N_2} \pmod{p}$. І позаяк порядки за модулем p степенів числа a_1 є дільниками числа k (наслідок 1 (б) з твердження 8.1), а порядки степенів числа b_1 — дільниками числа l , то $P_p(a_1^{N_1})$ є спільним дільником взаємно простих чисел k і l . Отже, $P_p(a_1^{N_1}) = 1$ і $a_1^{N_1} \equiv 1 \pmod{p}$. Звідси випливає, що $k \mid N_1$. Аналогічно доводиться, що $l \mid N_1$. Отже, $kl \mid N_1$, тобто $N \mid N_1$. Оскільки $N_1 \mid N$, то $N_1 = N$. Тому можна взяти $a^{(1)} = a_1 b_1$.

Таким чином будується ряд чисел $a, a^{(1)}, a^{(2)}, \dots$, для якого $P_p(a) < P_p(a^{(1)}) < P_p(a^{(2)}) < \dots$. Через скінченну кількість кроків прийдемо до числа g , для якого $P_p(g) = p - 1$, тобто до первісного кореня за модулем p .

Проілюструємо спосіб Гауса на розв'язанні наступної задачі.

Задача 8.7. Знайти всі первісні корені за модулем: (а) 23; (б) 109.

Розв'язання. (a) Візьмемо будь-яке число a , взаємно просте з 23, наприклад, $a = 2$. Знайдемо $P_{23}(2)$. Позаяк $P_{23}(2)$ має бути дільником числа $\varphi(23) = 22$, то досить обчислити тільки 2^2 і 2^{11} . $2^2 = 4 \not\equiv 1 \pmod{23}$, $2^{11} \equiv 1 \pmod{23}$. Отже, $P_{23}(2) = 11$. Шукаємо тепер b , відмінне від степенів $2^1 = 2$, $2^2 = 4$, $2^3 = 8$, $2^4 = 16$, $2^5 \equiv 9$, $2^6 \equiv 18$, $2^7 \equiv 13$, $2^8 \equiv 3$, $2^9 \equiv 6$, $2^{10} \equiv 12$ числа 2. Можна взяти, наприклад, $b = 5$. $5^2 \equiv 2 \not\equiv 1 \pmod{23}$. Крім того, за вибором числа 5, $P_{23}(5) \neq 11$. Отже, $P_{23}(5) = 22$ і 5 є первісним коренем за модулем числа 23. Іншими первісними коренями будуть $5^3 \equiv 10$, $5^5 \equiv 20$, $5^7 \equiv 17$, $5^9 \equiv 11$, $2^{13} \equiv 21$, $2^{15} \equiv 19$, $2^{17} \equiv 15$, $2^{19} \equiv 7$, $2^{21} \equiv 14$ (всього маємо $\varphi(22) = 10$ первісних коренів).

(б) Візьмемо $a = 2$ – найменше натуральне число, взаємно просте з числом 109. Знайдемо $P_{109}(2)$. Оскільки $p - 1 = 108 = 2^2 \cdot 3^3$, то $P_{109}(2)$ має бути одним із чисел 2, 3, 4, 6, 9, 12, 18, 27, 36, 54, 108. Але за модулем числа 109 $2^2 = 4 \not\equiv 1$, $2^3 = 8 \not\equiv 1$, $2^4 = 16 \not\equiv 1$, $2^6 = 64 \not\equiv 1$, $2^9 \equiv 76 \not\equiv 1$, $2^{12} \equiv 63 \not\equiv 1$, $2^{18} \equiv 108 \not\equiv 1$, $2^{27} \equiv 33 \not\equiv 1$, $2^{36} \equiv 1$, тому $P_{109}(2) = 36$. Тепер далі треба шукати число b , відмінне від степенів двійки. Виписувати всі 36 степенів двійки не дуже хочеться, тому варто спробувати інший шлях. Із спостережень відомо, що за простим модулем числа 2 і 3 часто або є первісними коренями (наприклад, у межах першої тисячі 2 є первісним коренем у 67 випадках, серед решти простих модулів ще в 40 випадках первісним коренем буде 3, і лише в 60 випадках ні 2, ні 3 не буде первісним коренем), або мають досить високі порядки. Тому варто знайти порядок $P_{109}(3)$ числа 3. Маємо: $3^2 = 9 \not\equiv 1$, $3^3 = 27 \not\equiv 1$, $4^4 = 81 \not\equiv 1$, $3^6 = 75 \not\equiv 1$, $3^9 \equiv 63 \not\equiv 1$, $3^{12} \equiv 66 \not\equiv 1$, $3^{18} \equiv 45 \not\equiv 1$, $3^{27} \equiv 1$, тому $P_{109}(3) = 27$. Отже, 3 також не є первісним коренем за модулем 109. Але 3 не є і степенем числа 2, бо $27 \nmid 36$. Тому в ролі b можна взяти число 3. Далі обчислюємо: $\text{HCK}(36, 27) = 108 = 4 \cdot 27$ і $4 \mid 36$, $27 \mid 27$. Тому для числа $a^{(1)} = a^{36/4}b^{27/27} = 2^9 3^1 = 1536 \equiv 10 \pmod{109}$ маємо $P_{109}(10) = \text{HCK}(36, 27) = 108$, тобто 10 є первісним коренем за модулем 109. Решта первісних коренів мають вигляд 10^s , де показник s взаємно простий з числом 108. Всього за модулем 109 буде $\varphi(108) = 36$ первісних коренів. \square

Для великих простих чисел p із двох запропонованих способів знаходження первісних коренів останнім часом перевагу віддають способу Гауса, бо існує достатньо обґрутована гіпотеза, що найменший додатний первісний корінь за модулем простого числа p має величину $O(\log^6 p)$.

Розглянемо тепер питання про існування первісних коренів за скла-

деним модулем m .

Теорема 8.3. *Первісні корені за модулем m існують тоді й лише тоді, коли m дорівнює 2, 4 або має вигляд p^α чи $2p^\alpha$, де p – довільне непарне просте число.*

Доведення. Достатність. Очевидно, що первісними коренями за модулями 2 і 4 будуть відповідно числа 1 і 3.

Доведемо тепер існування первісних коренів за модулем p^α . Для цього покажемо, що їх завжди можна знайти серед первісних коренів за модулем p . Точніше, доведемо, що коли g – первісний корінь за модулем непарного простого числа p , то існує таке ціле число x , що $h = g + px$ є первісним коренем за модулем p^j для всіх $j \in \mathbb{N}$. Справді, якщо g – первісний корінь за модулем p , то $P_p(g) = \varphi(p) = p - 1$ і $g^{p-1} = 1 + py$ для деякого цілого числа y . За формулою бінома Ньютона

$$(g + px)^{p-1} = g^{p-1} + \binom{p-1}{1} g^{p-2} px + \binom{p-1}{2} g^{p-3} p^2 x^2 + \dots$$

$$\dots + \binom{p-1}{p-2} gp^{p-2} x^{p-2} + p^{p-1} x^{p-1} = 1 + py + p((p-1)g^{p-2} x + z) ,$$

$$\text{де } z = \binom{p-1}{2} g^{p-3} px^2 + \dots + \binom{p-1}{p-2} gp^{p-3} x^{p-2} + p^{p-2} x^{p-1} \equiv 0 \pmod{p} .$$

Отже, $(g + px)^{p-1} \equiv 1 + h(y + (p-1)g^{p-2} x) \pmod{p^2}$. Коефіцієнт $(p-1)g^{p-2}$ при x не ділиться на p , тому x можна вибрати таким, щоб виконувалась умова

$$\text{НСД}(y + (p-1)g^{p-2} x, p) = 1 . \quad (8.5)$$

Позначимо $h = g + px$ і нехай $P_{p^j}(h) = d$. Тоді за наслідком 1 (б) з твердження 8.1 $d \mid \varphi(p^j) = p^{j-1}(p-1)$. Але h – первісний корінь за модулем p , бо $h = g + px \equiv g \pmod{p}$ і за твердженням 8.1 (а) $P_p(h) = P_p(g)$. Тому $(p-1) \mid d$ і $d = p^k(p-1)$ для деякого $k < j$.

Крім цього, оскільки число p – непарне, то

$$(h^{p-1})^{p^k} = \left(1 + py + p((p-1)g^{p-2} x + z)\right)^{p^k} = 1 + p^{k+1} v_k ,$$

де $(v_k, p) = 1$. Проте $h^d \equiv 1 \pmod{p^j}$. Отже, $j = k + 1$ і $d = \varphi(p^j)$, тобто $h = g + px$ є первісним коренем за модулем p^j . Таким чином,

існування первісних коренів за модулем p^j для всіх $j \in \mathbb{N}$ доведено. Враховуючи рівність $\varphi(2p^j) = \varphi(p^j)$, неважко також зрозуміти, що для кожного первісного кореня g за модулем p^j непарне з чисел g і $g + p^j$ буде первісним коренем за модулем $2p^j$.

Необхідність. Якщо модуль $m > 1$ має вигляд, відмінний від описаного в умові теореми, то або $m = 2^j$, де $j > 2$, або $m = m_1m_2$, де обидва множники m_1 і m_2 більші за 2 і взаємно прості. Досить довести, що в кожному з цих випадків первісних коренів не існує. Розберемося спочатку з першим випадком. Якщо $m = 8$, то $\varphi(8) = 4$ і первісні корені треба шукати серед чисел 1, 3, 5, 7. Але $P_8(1) = 1$ і $P_8(3) = P_8(5) = P_8(7) = 2$, тому первісних коренів за модулем 8 не існує.

Доведемо тепер, що із неіснування первісних коренів за модулем числа 2^l , $l > 2$, випливає неіснування первісних коренів і за модулем числа 2^{l+1} . Справді, неіснування первісних коренів за модулем числа 2^l означає, що для довільного непарного числа a виконується конгруенція $a^{2^{l-2}} \equiv 1 \pmod{2^l}$, бо за наслідком 1 (б) з твердження 8.1 порядок $P_{2^l}(a)$ має бути власним дільником числа $\varphi(2^l) = 2^{l-1}$. Отже, $a^{2^{l-2}} = 1 + b \cdot 2^l$. Але тоді $a^{2^{l-1}} = (1 + b \cdot 2^l)^2 = 1 + b \cdot 2^{l+1} + b^2 \cdot 2^{2l} \equiv 1 \pmod{2^{l+1}}$. Тому для кожного непарного числа a $P_{2^{l+1}}(a) \leq 2^{l-1} < \varphi(2^{l+1}) = 2^l$ і первісних коренів за модулем 2^{l+1} не існує.

Розглянемо тепер другий випадок. Із задачі 2.18 (а) випливає, що $\varphi(m_1) = 2k_1$, $\varphi(m_2) = 2k_2$. Нехай тепер a — довільне число, взаємно просте з m . Тоді a взаємно просте з кожним із множників m_1 і m_2 і за теоремою Ойлера число $a^{2k_1 k_2} - 1 = (a^{2k_1} - 1)(a^{2k_1(k_2-1)} + \dots) = (a^{2k_2} - 1)(a^{2k_2(k_1-1)} + \dots)$ ділиться на кожен з цих множників. Але тоді $a^{2k_1 k_2} - 1$ ділиться на $m = m_1 m_2$ і $P_m(a) \leq 2k_1 k_2 < \varphi(m) = \varphi(m_1 m_2) = \varphi(m_1)\varphi(m_2) = 4k_1 k_2$, тобто і в цьому випадку первісних коренів не існує. \square

Твердження 8.4. (а) Якщо первісні корені за модулем числа m існують, то їх буде $\varphi(\varphi(m))$.

(б) Для непарного простого числа p існує $\varphi(\varphi(p^\alpha))$ первісних коренів за модулем числа p^α ; кожен із них за модулем числа p породжує $\varphi(p^{\alpha-1})$ різних первісних коренів за модулем числа p^α ; первісний корінь g за модулем числа p тоді й тільки тоді буде первісним коренем і за модулем числа p^α , коли $g^{p-1} \equiv 1 \pmod{p}$ і $g^{p-1} \not\equiv 1 \pmod{p^2}$.

- (6) Для непарного простого числа p існує $\varphi(\varphi(2p^\alpha))$ первісних коренів за модулем числа $2p^\alpha$; кожний непарний первісний корінь за модулем числа p^α є первісним коренем і за модулем числа $2p^\alpha$.

Доведення. (a) Нехай g – первісний корінь за модулем числа m . Тоді $P_m(g) = \varphi(m)$ і всі взаємно прості з m класи лишків за модулем m вичерпуються степенями класу \bar{g} . За наслідком 1 (b) з твердження 8.1 рівно $\varphi(\varphi(m))$ з них матимуть порядок $\varphi(m)$, тобто будуть первісними коренями.

Твердження (b) і (c) очевидним чином випливають із твердження (a) та доведення теореми 8.3. \square

Задача 8.8. Знайти всі первісні корені за модулем числа 49.

Розв'язання. За твердженням 8.4 існує $\varphi(\varphi(49)) = \varphi(42) = 12$ первісних коренів за модулем 49. Кожен первісний корінь за модулем числа 7 породжує $\varphi(7^{2-1}) = \varphi(7) = 6$ первісних коренів за модулем 49. За модулем 7 маємо $\varphi(6) = 2$ первісних коренів, а саме 3 та 5. Оскільки $3^6 - 1 = 728 = 2^3 \cdot 7 \cdot 13$, то $3^6 \equiv 1 \pmod{7}$ і $3^6 \not\equiv 1 \pmod{7^2}$. Отже, 3 є первісним коренем за модулем 49. Тоді $P_{49}(3) = \varphi(49) = 42$ і за наслідком 1 (b) з твердження 8.1 всі первісні корені за модулем 49 матимуть вигляд 3^s , де показник s є взаємно простим з числом 42. Тому отримуємо такі первісні корені: $3^1 = 3$, $3^5 \equiv 47$, $3^{11} \equiv 12$, $3^{13} \equiv 10$, $3^{17} \equiv 26$, $3^{19} \equiv 38$, $3^{23} \equiv 40$, $3^{25} \equiv 17$, $3^{29} \equiv 5$, $3^{31} \equiv 45$, $3^{37} \equiv 24$, $3^{41} \equiv 33$ (всього 12 коренів). \square

Задача 8.9 (Теорема Вулстенхолма). Довести, що для кожного простого числа $p > 3$ чисельник суми $1 + \frac{1}{2} + \frac{1}{3} + \dots + \frac{1}{p-1}$ ділиться на p^2 .

Розв'язання. Запишемо p у вигляді $p = 2k + 1$ і виконаємо деякі перетворення даної суми:

$$\begin{aligned} 1 + \frac{1}{2} + \frac{1}{3} + \dots + \frac{1}{p-1} &= \left(1 + \frac{1}{p-1}\right) + \left(\frac{1}{2} + \frac{1}{p-2}\right) + \dots + \left(\frac{1}{k} + \frac{1}{p-k}\right) = \\ &= \frac{p}{1 \cdot (p-1)} + \frac{p}{2 \cdot (p-2)} + \dots + \frac{p}{k \cdot (p-k)} = p \left(\frac{1}{1 \cdot (p-1)} + \frac{1}{2 \cdot (p-2)} + \dots \right. \\ &\quad \left. \dots + \frac{1}{k \cdot (p-k)} \right) = \frac{p}{2} \left(\frac{p}{1 \cdot (p-1)} + \frac{p}{2 \cdot (p-2)} + \dots + \frac{p}{k \cdot (p-k)} + \right. \end{aligned}$$

$$\begin{aligned}
& + \frac{1}{(k+1) \cdot (p-k-1)} + \cdots + \frac{1}{(p-1) \cdot 1} \Big) = \frac{p}{2} \left(\frac{p}{1 \cdot (p-1)} + \frac{p}{2 \cdot (p-2)} + \cdots \right. \\
& \cdots + \frac{1}{(p-1) \cdot 1} \Big) = \frac{p}{2} \left(\frac{p}{1 \cdot (p-1)} + \cdots + \frac{1}{(p-1) \cdot 1} + 1 + \frac{1}{2^2} + \cdots + \frac{1}{(p-1)^2} - \right. \\
& \left. - \left(1 + \frac{1}{2^2} + \cdots + \frac{1}{(p-1)^2} \right) \right) = \frac{p}{2} \left(\left(\frac{1}{1 \cdot (p-1)} + \frac{1}{1^2} \right) + \left(\frac{1}{2 \cdot (p-2)} + \frac{1}{2^2} \right) + \right. \\
& \left. + \cdots + \left(\frac{1}{(p-1) \cdot 1} + \frac{1}{(p-1)^2} \right) - \left(1 + \frac{1}{2^2} + \cdots + \frac{1}{(p-1)^2} \right) \right) = \\
& = \frac{p}{2} \left(\frac{p}{1^2 \cdot (p-1)} + \frac{p}{2^2 \cdot (p-2)} + \cdots + \frac{p}{(p-1)^2 \cdot 1} - \left(1 + \frac{1}{2^2} + \cdots + \frac{1}{(p-1)^2} \right) \right).
\end{aligned}$$

Отже, для розв'язання задачі досить показати, що чисельник суми $1 + \frac{1}{2^2} + \cdots + \frac{1}{(p-1)^2}$ ділиться на p . Помноживши цю суму на взаємно просте з p число $((p-1)!)^2$, зводимо задачу до подільності на p цілого числа

$$\left(1 + \frac{1}{2^2} + \cdots + \frac{1}{(p-1)^2} \right) ((p-1)!)^2. \quad (8.6)$$

Нехай g — первісний корінь за модулем p . Тоді $g^{p-1} \equiv 1 \pmod{p}$ і $p-1$ є найменшим показником із такою властивістю. Із вправи 1 випливає, що $\{\overline{g^1}, \overline{g^2}, \dots, \overline{g^{p-1}}\} = \{\overline{1}, \overline{2}, \dots, \overline{p-1}\}$, тому

$$\begin{aligned}
& \left(1 + \frac{1}{2^2} + \cdots + \frac{1}{(p-1)^2} \right) ((p-1)!)^2 \equiv \\
& \equiv \left(\frac{1}{g^2} + \frac{1}{(g^2)^2} + \frac{1}{(g^3)^2} + \cdots + \frac{1}{(g^{p-1})^2} \right) ((p-1)!)^2 = \\
& = \frac{((p-1)!)^2 \left(\frac{1}{(g^{p-1})^2} \cdot \frac{1}{(g^2)^2} - \frac{1}{(g^2)^2} \right)}{\frac{1}{(g^2)^2} - 1} = \frac{(g^{2p-2} - 1)((p-1)!)^2}{g^{2p-2}(1 - g^2)} \pmod{p}.
\end{aligned}$$

Знаменник останнього дробу не ділиться на p . Справді, $g^{2p-2} \not\equiv 0 \pmod{p}$, бо g — первісний корінь і $g \not\equiv 0 \pmod{p}$; $g^2 \not\equiv 1 \pmod{p}$, бо з $p > 3$ випливає, що $2 < p-1 = P_p(g)$. Але чисельник ділиться на p , бо $(g^{2p-2} - 1) = (g^{p-1} - 1)(g^{p-1} + 1) \equiv 0 \pmod{p}$. Отже, число (8.6) ділиться на p . \square

8.3. Індекси

Загальновідомо, яку роль у різних розділах математики і в її застосуваннях відіграє поняття логарифма числа a за основою b (тобто показника степеня, до якого треба піднести число b , щоб отримати a). За аналогією в теорії чисел також розглядають показник степеня, до якого треба піднести число g , щоб отримати число, конгруентне числу a за даним модулем m . А саме, нехай g – первісний корінь за модулем числа m і a – довільне взаємно просте з m ціле число. Невід'ємне ціле число l називається *індексом* числа a за модулем m і основою g , якщо $g^l \equiv a \pmod{m}$. Позначають $l = \text{ind}_g a \pmod{m}$ або просто $l = \text{ind}_g a$.

Отже, згідно з означенням індексу, $g^{\text{ind}_g a} \equiv a \pmod{m}$.

Якщо $b \equiv a \pmod{m}$, то з $g^l \equiv a \pmod{m}$ випливає $g^l \equiv b \pmod{m}$, тобто індекс $\text{ind}_g a$ числа a є також індексом усіх чисел із класу лишків \bar{a} за модулем m . Тому природно число $\text{ind}_g a$ називати також індексом класу лишків \bar{a} .

Увів поняття індексу Гаус, і він же вперше дослідив основні властивості індексів.

Приклади.

(a) Із задачі 8.6 ми знаємо, що 2 є первісним коренем за модулем 13. Тоді з конгруенції $2^7 \equiv 11 \pmod{13}$ маємо, що $\text{ind}_{13} 11 = 7$ і для довільного числа $b \equiv 11 \pmod{13}$ також $\text{ind}_{13} b = 7$.

(b) $2^{13} \equiv 2 \pmod{13}$, отже, $\text{ind}_{13} 2 = 13$. Але разом із тим $2^1 \equiv 2 \pmod{13}$, тобто $\text{ind}_{13} 2 = 1$. Більше того, можна помітити, що для довільного числа $l \equiv 1 \pmod{12}$ виконується конгруенція $2^l \equiv 2 \pmod{13}$, і тому $l = \text{ind}_{13} 2$. Ми повернемось до цього в теоремі 8.4.

(c) Якщо основа g не є первісним коренем за модулем m , то $\text{ind}_g a$ може не існувати. Наприклад, 4 не є первісним коренем за модулем 17 і $\text{ind}_{17} 4 \pmod{17}$ не існує, бо конгруенція $4^l \equiv 3 \pmod{17}$ не виконується для жодного числа l (4^l може бути конгруентним за модулем 17 лише одному з чисел 1, 4, 13 або 16).

Виникають природні питання: для яких чисел g , m та a індекс $\text{ind}_g a \pmod{m}$ існує? Скільки може бути різних індексів для даного a ? Як описати ці індекси? Відповіді на ці питання дає

Теорема 8.4. *Нехай g – первісний корінь за модулем m . Тоді для кожного взаємно простого з m числа a існують індекси за основою g , тобто існують такі l , що $g^l \equiv a \pmod{m}$. Для фіксованого a множина таких індексів l збігається з множиною всіх невід'ємних цілих чисел із деякого класу лишків за модулем числа $\varphi(m)$.*

Доведення. Згідно з вправою 8.1 степені

$$g^0 \ g^1 \ g^2 \ \dots, g^{\varphi(m)-1} \quad (8.7)$$

первісного кореня g утворюють зведену систему лишків за модулем m . Візьмемо довільне взаємно просте з m число a . Тоді у зведеній системі лишків (8.7) існує єдине число, яке належить класу \bar{a} . Отже, для деякого l , $0 \leq l \leq \varphi(m)-1$, виконується конгруенція $g^l \equiv a \pmod{m}$, тобто індекс $\text{ind}_g a \pmod{m}$ існує і дорівнює l .

Доведемо тепер другу частину теореми. Справді, якщо $l = \text{ind}_g a \pmod{m}$ і $k = \text{ind}_g a \pmod{m}$, то $g^l \equiv a \pmod{m}$, $g^k \equiv a \pmod{m}$ і $g^l \equiv g^k \pmod{m}$. Оскільки $P_m(g) = \varphi(m)$, то за наслідком 1 (a) з твердження 8.1 $l \equiv k \pmod{\varphi(m)}$, тобто l і k належать одному класу лишків за модулем $\varphi(m)$. Навпаки, всі невід'ємні числа з цього класу є індексами числа a , бо за тим же наслідком із конгруенції $l \equiv k \pmod{\varphi(m)}$ і $g^l \equiv a \pmod{m}$ випливає конгруенція $g^k \equiv a \pmod{m}$. \square

За теоремою 8.4 індексами числа a за модулем m і основою g є всі невід'ємні цілі числа з певного класу лишків за модулем $\varphi(m)$. Найменше з цих чисел назовемо *головним значенням індексу*. Тоді, очевидно, головне значення індексу (якщо індекси $\text{ind}_g a \pmod{m}$ існують) визначене однозначно і не перевищуватиме числа $\varphi(m) - 1$.

Відзначимо ряд властивостей індексів.

Твердження 8.5. (a) Якщо g – первісний корінь за модулем m , а число a взаємно просте з m , то конгруенція $b \equiv a \pmod{m}$ має місце тоді й лише тоді, коли $\text{ind}_g b \equiv \text{ind}_g a \pmod{\varphi(m)}$.

(б) Якщо g – первісний корінь за модулем m , а числа a і b взаємно прості з m , то

$$\text{ind}_g ab \equiv \text{ind}_g a + \text{ind}_g b \pmod{\varphi(m)}. \quad (8.8)$$

(в) Нехай g – первісний корінь за модулем m , а кожне з чисел a_1, \dots, a_s взаємно просте з m . Тоді

$$\text{ind}_g(a_1 \cdots a_s) \equiv \text{ind}_g a_1 + \cdots + \text{ind}_g a_s \pmod{\varphi(m)}. \quad (8.9)$$

(г) Якщо g – первісний корінь за модулем m , а число a взаємно просте з m , то для кожного цілого числа $n \geq 0$ виконується конгруенція

$$\text{ind}_g a^n \equiv n \cdot \text{ind}_g a \pmod{\varphi(m)}. \quad (8.10)$$

(d) Нехай g – первісний корінь за модулем m , а числа a і b взаємно прості з m . Якщо через $\text{ind}_g \frac{a}{b}$ позначити індекс класу лишків \bar{r} , де $\frac{a}{b} \equiv r \pmod{m}$, то

$$\text{ind}_g \frac{a}{b} \equiv \text{ind}_g a - \text{ind}_g b \pmod{\varphi(m)}. \quad (8.11)$$

(e) Нехай g і h – два первісні корені за модулем m , а число a взаємно просте з m . Тоді

$$\text{ind}_g a \equiv \text{ind}_h a \cdot \text{ind}_h g \pmod{\varphi(m)}, \quad \text{ind}_h a \equiv \text{ind}_g a \cdot \text{ind}_g h \pmod{\varphi(m)}. \quad (8.12)$$

Доведення. (a) Це випливає з теореми 8.4.

(б) Згідно з означенням індексу $g^{\text{ind}_g ab} \equiv ab \equiv g^{\text{ind}_g a} \cdot g^{\text{ind}_g b} \equiv g^{\text{ind}_g a + \text{ind}_g b} \pmod{\varphi(m)}$. Оскільки $P_m(g) = \varphi(m)$, то за наслідком 1 (a) з твердження 8.1 має місце (8.8).

(в) Скористаємося методом математичної індукції. Для $s = 1$ конгруенція (8.9) очевидна. Припустимо, що (8.9) виконується для $s = k$, і розглянемо числа a_1, \dots, a_{k+1} , кожне з яких взаємно просте з m . Згідно з пунктом (a) $\text{ind}_g(a_1 \cdots a_{k+1}) \equiv \text{ind}_g(a_1 \cdots a_k) + \text{ind}_g a_{k+1} \pmod{\varphi(m)}$. За припущенням індукції $\text{ind}_g(a_1 \cdots a_k) \equiv \text{ind}_g a_1 + \cdots + \text{ind}_g a_k \pmod{\varphi(m)}$. З останніх двох конгруенцій випливає конгруенція (8.9) для $s = k + 1$.

(г) Для $n = 0$ конгруенція (8.10) виконується, бо $g^0 \equiv 1 \pmod{m}$ і $\text{ind}_g 1 \equiv 0 \pmod{\varphi(m)}$. Для $n > 0$ вона є частковим випадком конгруенції (8.9) для $a_1 = \cdots = a_n = a$.

(д) Якщо b і m взаємно прості, то з теореми 6.1 існує єдиний клас лишків \bar{r} за модулем m , для якого $\bar{b} \cdot \bar{r} = \bar{a}$, тобто $br \equiv a \pmod{m}$. Звідси $\text{ind}_g a \equiv \text{ind}_g b + \text{ind}_g r \pmod{\varphi(m)}$ або $\text{ind}_g \frac{a}{b} = \text{ind}_g r \equiv \text{ind}_g a - \text{ind}_g b \pmod{\varphi(m)}$.

(е) Нехай $\alpha \equiv \text{ind}_g a \pmod{\varphi(m)}$ і $\beta \equiv \text{ind}_g b \pmod{\varphi(m)}$. Тоді $a \equiv g^\alpha \equiv h^\beta \pmod{m}$. Звідси та з пункту (г) отримуємо: $\text{ind}_g a \equiv \alpha \equiv \beta \cdot \text{ind}_g h \equiv \text{ind}_g b \cdot \text{ind}_g h \pmod{\varphi(m)}$, що доводить першу з конгруенцій (8.12). Друга доводиться аналогічно. \square

Твердження 8.5 показує, що індекси за своїми властивостями дуже нагадують звичайні логарифми.

За теоремою 8.3 первісні корені за модулем m , а отже, і індекси за цим модулем, існують лише тоді, коли m є одним із чисел 2, 4, p^α , $2p^\alpha$,

де p — непарне просте число. Але, як видно з наступного твердження, індекси чисел за модулем $2p^\alpha$ і непарною основою g такі самі, як і за модулем p^α і тією ж основою g .

Твердження 8.6. *Нехай g — непарний первісний корінь за модулем p^α , де p — непарне просте число. Якщо числа a і $2p$ взаємно прості, то $\text{ind}_g a \pmod{p^\alpha} = \text{ind}_g a \pmod{2p^\alpha}$.*

Доведення. Позначимо $s = \text{ind}_g a \pmod{p^\alpha}$. Тоді $g^s \equiv a \pmod{p^\alpha}$. Крім того, при непарних a і g маємо $g^s \equiv a \pmod{2}$, так що $g^s \equiv a \pmod{2p^\alpha}$ і $s = \text{ind}_g a \pmod{2p^\alpha}$. \square

Таким чином, достатньо вміти будувати таблиці індексів за простими модулями і модулями вигляду p^α , де p — непарне просте число, причому процедура побудови в усіх випадках однакова. Розглянемо цю процедуру на прикладі.

Задача 8.10. Скласти таблицю індексів за модулем 25 і основою 3.

Розв'язання. $\varphi(25) = 20$, тому порядок числа 3 має бути дільником числа 20. Але $3^4 \equiv 6 \not\equiv 1 \pmod{25}$ і $3^{10} \equiv 24 \not\equiv 1 \pmod{25}$, тому $P_{25}3 = 20$ і 3 є первісним коренем за модулем 25. Далі знаходимо найменші додатні лишки степенів числа 3 за цим модулем: $3^0 \equiv 1, 3^1 \equiv 3, 3^2 \equiv 9, 3^3 \equiv 2, 3^4 \equiv 6, 3^5 \equiv 18, 3^6 \equiv 1, 3^7 \equiv 12, 3^8 \equiv 11, 3^9 \equiv 8, 3^{10} \equiv 24, 3^{11} \equiv 22, 3^{12} \equiv 16, 3^{13} \equiv 23, 3^{14} \equiv 19, 3^{15} \equiv 7, 3^{16} \equiv 21, 3^{17} \equiv 13, 3^{18} \equiv 14, 3^{19} \equiv 17$.

Одержані дані заносимо в таблицю індексів за модулем 25 і основою 3, причому розглядаємо лише числа, взаємно прості з модулем:

a	1	2	3	4	6	7	8	9	11	12
inda	0	3	1	6	4	15	9	2	8	7

a	13	14	16	17	18	19	21	22	23	24
inda	17	18	12	19	5	14	16	11	13	10

\square

За допомогою таблиць індексів можна легко розв'язувати різні двочленні конгруенції. Тому багато підручників з теорії чисел містять досить докладні таблиці індексів (див., наприклад, [3], [4]). Розглянемо кілька прикладів застосування таблиць індексів.

Задача 8.11. Знайти найменший натуральний показник α , для якого виконується конгруенція $3^\alpha \equiv 1 \pmod{23}$.

Розв'язання. Найменшим первісним коренем за модулем 23 є 5 (див. задачу 8.7). Тому розглянемо індекси лівої і правої частин даної конгруенції за основою 5. На підставі твердження 8.5 (г) отримуємо конгруенцію $\alpha \cdot \text{ind}_5 3 \equiv 0 \pmod{\varphi(23)}$. Використовуючи таблиці індексів, знаходимо: $\text{ind}_5 3 = 16$. Крім того, $\varphi(23) = 22$. Тому остання конгруенція набуває вигляду $16\alpha \equiv 0 \pmod{22}$ або $8\alpha \equiv 0 \pmod{11}$. Найменшим натуральним числом, яке її задоволяє, є, очевидно, $\alpha = 11$. \square

Задача 8.12. Розв'язати конгруенції: а) $16^x \equiv 11 \pmod{53}$; б) $37x \equiv 25 \pmod{89}$; в) $11x^3 \equiv 6 \pmod{79}$; г) $3x^2 - 8x + 44 \equiv 0 \pmod{47}$.

Розв'язання. (а) Найменшим первісним коренем за модулем 53 є 2. Тому проіндексуємо обидві частини даної конгруенції за основою 2: $x \cdot \text{ind}_2 16 \equiv \text{ind}_2 11 \pmod{\varphi(53)}$. За таблицями індексів знаходимо: $\text{ind}_2 16 = 4$, $\text{ind}_2 11 = 6$, що дає нам конгруенцію $4x \equiv 6 \pmod{52}$ або $2x \equiv 3 \pmod{26}$. Оскільки НСД(2, 26) = 2, а 3 на 2 не ділиться, то вихідна конгруенція розв'язків не має.

(б) 3 є первісним коренем за модулем 89, тому індексуємо обидві частини даної конгруенції за основою 3: $\text{ind}_3 37 + \text{ind}_3 x \equiv \text{ind}_3 25 \pmod{\varphi(89)}$. За таблицями індексів $\text{ind}_3 37 = 11$, $\text{ind}_3 25 = 52$, що дає нам конгруенцію $\text{ind}_3 x \equiv 41 \pmod{88}$. Звідси за тими ж таблицями індексів $x \equiv 56 \pmod{89}$.

(в) Індексуємо обидві частини конгруенції за основою 3: $\text{ind}_3 11 + 3 \cdot \text{ind}_3 x \equiv \text{ind}_3 6 \pmod{\varphi(79)}$. За таблицями індексів $\text{ind}_3 11 = 68$, $\text{ind}_3 6 = 5$, тому одержуємо конгруенцію $3 \cdot \text{ind}_3 x \equiv -63 \equiv 15 \pmod{78}$. Після скорочення на 3 матимемо: $\text{ind}_3 x \equiv 5 \pmod{26}$. Повертаючись назад до модуля 78, отримуємо 3 конгруенції $\text{ind}_3 x \equiv 5 + 0 \cdot 26 \equiv 5 \pmod{78}$, $\text{ind}_3 x \equiv 5 + 1 \cdot 26 \equiv 31 \pmod{78}$, $\text{ind}_3 x \equiv 5 + 2 \cdot 26 \equiv 57 \pmod{78}$. Звідси за таблицями індексів одержуємо розв'язки вихідної конгруенції: $x \equiv 6 \pmod{79}$, $x \equiv 59 \pmod{79}$, $x \equiv 14 \pmod{79}$.

(г) Помноживши обидві частини конгруенції на взаємно просте з 47 число 3, одержимо рівносильну її конгруенцію $9x^2 - 24x + 38 \equiv (3x - 4)^2 + 22 \equiv 0 \pmod{47}$. Після заміни $y = 3x - 4$ одержуємо $y^2 \equiv -22 \equiv 25 \pmod{47}$ або, після індексування за основою 5, $2 \cdot \text{ind}_5 y \equiv \text{ind}_5 25 \pmod{\varphi(47)}$, тобто $2 \cdot \text{ind}_5 y \equiv 2 \pmod{46}$. Після скорочення на 2 матимемо: $\text{ind}_5 y \equiv 1 \pmod{23}$. Повертаючись назад до модуля 46, отримуємо дві конгруенції

$$\text{ind}_5 y \equiv 1 + 0 \cdot 23 \equiv 1 \pmod{46}, \quad \text{ind}_5 y \equiv 1 + 1 \cdot 23 \equiv 24 \pmod{46}.$$

За таблицями індексів знаходимо $y \equiv 5 \pmod{47}$, $y \equiv 42 \pmod{47}$, звідки $3x \equiv 9 \pmod{47}$, $3x \equiv 46 \pmod{47}$, і, враховуючи, що за модулем 47 $3 \cdot 16 \equiv 1$, остаточно отримуємо, що $x \equiv 3 \pmod{47}$ або $x \equiv 31 \pmod{47}$. \square

Теорема 8.5. *Нехай первісні корені за модулем t існують і число a взаємно просте з t . Конгруенція*

$$x^n \equiv a \pmod{m} \quad (8.13)$$

має розв'язки тоді й лише тоді, коли виконується умова

$$a^{\varphi(m)/d} \equiv 1 \pmod{m}, \quad (8.14)$$

де $d = \text{НСД}(n, \varphi(m))$, причому в цьому випадку конгруенція (8.13) має за модулем t рівно d різних розв'язків. Зокрема, при $n = 2$ маємо критерій Ойлера того, чи є a квадратичним лишком за модулем t .

Доведення. Нехай g — первісний корінь за модулем t . Індексуємо обидві частини конгруенції (8.13) за основою g і одержуємо рівносильну початковій конгруенцію

$$n \cdot \text{ind}_g x \equiv \text{ind}_g a \pmod{\varphi(m)}. \quad (8.15)$$

Якщо n і $\varphi(m)$ взаємно прості, то конгруенція (8.15) має рівно 1 розв'язок. Нехай тепер $\text{НСД}(n, \varphi(m)) = d > 1$. Необхідно їй достатньою умовою існування розв'язків конгруенції (8.15) є $d \mid \text{ind}_g a$. Після скорочення (8.15) на d одержуємо конгруенцію $\frac{n}{d} \cdot \text{ind}_g x \equiv \frac{\text{ind}_g a}{d} \pmod{\frac{\varphi(m)}{d}}$, яка має рівно один розв'язок за модулем $\frac{\varphi(m)}{d}$. Це означає, що (8.15) (і рівносильна їй конгруенція (8.13)) має за модулем t рівно d різних розв'язків.

Умова $d \mid \text{ind}_g a$ означає, що для певного числа k виконується рівність $\text{ind}_g a = d \cdot k$. За означенням індексу маємо $a \equiv g^{\text{ind}_g a} = g^{dk} \pmod{m}$, звідки $a^{\varphi(m)/d} \equiv (g^{dk})^{\varphi(m)/d} = g^{k \cdot \varphi(m)} \pmod{m}$. Але за теоремою Ойлера $g^{k \cdot \varphi(m)} \equiv 1 \pmod{m}$, тому $a^{\varphi(m)/d} \equiv 1 \pmod{m}$.

Навпаки, нехай виконується умова (8.14). Тоді з конгруенції $g^{\text{ind}_g a} \equiv a \pmod{m}$ отримуємо $(g^{\text{ind}_g a})^{\varphi(m)/d} \equiv 1 \pmod{m}$. Оскільки g — первісний корінь, то $\varphi(m) \mid \frac{\varphi(m) \cdot \text{ind}_g a}{d}$. Отже, $\frac{\text{ind}_g a}{d}$ є цілим числом, тобто $d \mid \text{ind}_g a$. \square

Із доведення цієї теореми випливає такий

Наслідок 2. Якщо за даним модулем $t > 2$ індекси існують, то для довільної основи індекси квадратичних лишків будуть парними числами, а квадратичних нелишків — непарними.

Доведення. Із задачі 2.18 (а) випливає, що $\varphi(m)$ буде парним для кожного $m > 2$. Тому $\text{НСД}(2, \varphi(m)) = 2$. Але з доведення теореми 8.5 випливає, що a буде квадратичним лишком за модулем m (тобто конгруенція $x^2 \equiv a \pmod{m}$ матиме розв'язки) тоді й лише тоді, коли $\text{НСД}(2, \varphi(m)) | \text{ind}_g a$, тобто коли число $\text{ind}_g a$ є парним. \square

Задача 8.13. Визначити, які з чисел 15, 16, 17, 18, 19 є квадратичними лишками за модулем 41.

Розв'язання. За таблицями індексів знаходимо індекси даних чисел за основою 6: $\text{ind}_6 15 = 37$, $\text{ind}_6 16 = 24$, $\text{ind}_6 17 = 33$, $\text{ind}_6 18 = 16$, $\text{ind}_6 19 = 9$. За попереднім наслідком числа будуть квадратичними лишками тоді й лише тоді, коли їх індекси будуть парними. Отже, серед даних чисел квадратичними лишками є 16 та 18. \square

Дамо ще один приклад застосування таблиць індексів.

Задача 8.14. Знайти остачу від ділення: а) числа $7^{50} + 3$ на 43; б) числа 49^{100} на 1242.

Розв'язання. (а) Фактично нам потрібно знайти найменший невід'ємний розв'язок конгруенції $x \equiv 7^{50} + 3 \pmod{43}$. Оскільки 43 — просте число, то можна взяти первісний корінь g і після індексування за основою g перейти до рівносильної конгруенції $\text{ind}_g(x - 3) \equiv 50 \cdot \text{ind}_g 7 \pmod{\varphi(43)}$. За таблицями індексів для основи $g = 3$ знаходимо $\text{ind}_3 7 = 35$ і одержуємо конгруенцію $\text{ind}_3(x - 3) \equiv 50 \cdot 35 = 1750 \equiv 28 \pmod{42}$. За тими ж таблицями знаходимо $x - 3 \equiv 6 \pmod{43}$, звідки $x \equiv 9 \pmod{43}$ і остача від ділення числа $7^{50} + 3$ на 43 дорівнює 9.

(б) $1242 = 2 \cdot 3^3 \cdot 23$, тому за модулем 1242 індекси не існують. Але вони існують за взаємно простими модулями $2 \cdot 3^3 = 54$ і 23. Тому ми спочатку знайдемо остачі r_1 і r_2 від ділення 49^{100} на 54 і 23 відповідно, а потім будемо шукати остачу x від ділення на 1242 із системи конгруенцій

$$\begin{cases} x \equiv r_1 \pmod{54}, \\ x \equiv r_2 \pmod{23}. \end{cases}$$

$\varphi(27) = 18$. Оскільки жодне з чисел $5^6 - 1 = 15624$ і $5^9 - 1 = 1953124$ не ділиться на 27, то 5 є непарним первісним коренем за модулем 27. Згідно з твердженням 8.4 (б) 5 буде первісним коренем і за модулем 54. Тоді $r_1 \equiv 49^{100} \pmod{54}$ і $\text{ind}_5 r_1 \equiv 100 \cdot \text{ind}_5 49 \equiv 200 \cdot \text{ind}_5 7 \pmod{\varphi(54)}$. За твердженням 8.6 $\text{ind}_5 7 \pmod{54} = \text{ind}_5 7 \pmod{27}$. За таблицями індексів $\text{ind}_5 7 \pmod{27} = 14$. Звідси $\text{ind}_5 r_1 \equiv 200 \cdot 14 \equiv 10 \pmod{18}$. Але тоді $r_1 \equiv 510 \equiv 49 \pmod{54}$.

5 є первісним коренем і за модулем 27. Тому для r_2 маємо: $r_2 \equiv 49^{100} \equiv 3^{100} \pmod{23}$, звідки $\text{ind}_5 r_2 \equiv 100 \cdot \text{ind}_5 3 \pmod{\varphi(23)}$. За таблицями індексів $\text{ind}_5 3 \pmod{23} = 16$. Отже, $\text{ind}_5 r_2 \equiv 100 \cdot 16 \equiv 16 \pmod{22}$. Але тоді $r_2 \equiv 516 \equiv 3 \pmod{23}$.

Таким чином, приходимо до системи

$$\begin{cases} x \equiv 49 \pmod{54}, \\ x \equiv 3 \pmod{23}. \end{cases}$$

Розв'язуючи її за допомогою китайської теореми про лишки, знаходимо $x \equiv 49 \pmod{1242}$. Отже, остатча дорівнює 49. \square

8.4. Задачі для самостійного розв'язання

1. Для всіх чисел від 2 до $m - 1$, які взаємно прості з m , знайти їх порядки за модулем m : а) $m = 5$; б) $m = 8$; в) $m = 9$; г) $m = 11$.
2. Використовуючи індексування, визначити, які з чисел 15, 16, 17, 18, 19 є квадратичними лишками: а) за модулем 23; б) за модулем 29; в) за модулем 73.
3. Знайти всі первісні корені за модулем числа: а) 7; б) 11; в) 13; г) 19; д) 23; е) 31; є) 43; ж) 109; з) 191.
4. Довести, що для довільного простого числа p сума всіх різних первісних коренів за модулем p конгруентна $\mu(p - 1)$ за модулем p .
5. Довести, що для довільного натурального числа $a \neq 1$ і простого числа p кожний непарний простий дільник числа $a^p + 1$ або має вигляд $2px + 1$, або є дільником числа $a + 1$.
6. Нехай m і n — відмінні від 1 натуральні числа. Рахуємо числа 1, 2, ..., n у прямому порядку від 1 до n , далі у зворотному порядку від n до 2, потім знову у прямому порядку від 1 до n , далі у

зворотному порядку від n до 2, і т.д. При такому підрахунку виписуємо 1-е отримане число, потім $(m+1)$ -е, $(2m+1)$ -е, і т.д., поки не отримаємо n чисел. З цим новим рядом із n чисел повторюємо ту ж операцію, і т.д. Довести, що після виконання цієї операції k разів одержимо вихідний ряд 1, 2, ..., n тоді й лише тоді, коли $m^k \equiv \pm 1 \pmod{2n-1}$.

7. Довести, що 3 є первісним коренем за модулем кожного простого числа вигляду $2^n + 1$, $n > 1$.
8. Нехай p — просте число вигляду $4n + 1$. Якщо число $2p + 1$ теж просте, то 2 є первісним коренем за модулем $2p + 1$.
9. Нехай p — просте число вигляду $4n + 3$. Якщо число $2p + 1$ теж просте, то -2 є первісним коренем за модулем $2p + 1$.
10. Довести, що коли числа p і $4p+1$ — прості, то 2 є первісним коренем за модулем $4p + 1$.
11. Скласти таблицю індексів за модулем m і основою g , якщо: а) $m = 27$, $g = 5$; б) $m = 29$, $g = 2$.
12. Знайти показник α в конгруенціях: а) $5^\alpha \equiv 1 \pmod{7}$; б) $8^\alpha \equiv 1 \pmod{13}$; в) $12^\alpha \equiv 1 \pmod{17}$; г) $10^\alpha \equiv 1 \pmod{13}$; д) $27^\alpha \equiv 1 \pmod{17}$; е) $23^\alpha \equiv 1 \pmod{41}$.
13. Розв'язати конгруенції: а) $2^x \equiv 7 \pmod{67}$; б) $13^x \equiv 12 \pmod{47}$; в) $52^x \equiv 38 \pmod{61}$; г) $20^x \equiv 21 \pmod{41}$.
14. За допомогою таблиць індексів розв'язати лінійні конгруенції: а) $7x \equiv 23 \pmod{17}$; б) $39x \equiv 84 \pmod{97}$; в) $125x \equiv 7 \pmod{79}$; г) $4x \equiv 13 \pmod{37}$; д) $47x \equiv 13 \pmod{667}$.
15. Розв'язати двочленні конгруенції: а) $5x^4 \equiv 3 \pmod{11}$; б) $2x^8 \equiv 5 \pmod{13}$; в) $2x^3 \equiv 17 \pmod{41}$; г) $27x^5 \equiv 25 \pmod{31}$; д) $8x^{26} \equiv 37 \pmod{41}$; е) $x^{12} \equiv 37 \pmod{41}$; є) $x^5 \equiv 74 \pmod{71}$; ж) $x^2 \equiv 59 \pmod{67}$; з) $x^2 \equiv 56 \pmod{41}$.
16. Застосовуючи індексування, розв'язати конгруенції: а) $3x^2 - 5x - 2 \equiv 0 \pmod{11}$; б) $2x^2 - 7x + 28 \equiv 0 \pmod{43}$.
17. Використовуючи таблиці індексів, знайти остаточу від ділення: а) числа $37^{20} \cdot 23^{12}$ на 61; б) числа $9^{45} + 17$ на 56.

18. Довести, що коли g є первісним коренем за модулем простого числа p вигляду $p = 4k + 1$, то $p - g$ також є первісним коренем за цим модулем.
19. Нехай p — просте число, g і h — первісні корені за модулем p і $\alpha \cdot \text{ind}_g h \equiv 1 \pmod{p-1}$. Довести, що для кожного взаємно простого з p числа a виконується конгруенція $\text{ind}_h a \equiv \alpha \cdot \text{ind}_g a \pmod{p-1}$.
20. Нехай p — просте число, g і h — первісні корені за модулем p , $n > 1$ і $n|(p-1)$. Для взаємно простого з p числа a позначимо $r = \text{ind}_g a \pmod{p}$, $r_1 = \text{ind}_h a \pmod{p}$. Розіб'ємо всі взаємно прості з p числа на n сукупностей двома способами. Спочатку в сукупність $L(s, g)$ ($s = 0, 1, \dots, n-1$) об'єднуємо всі числа a з умовою $r \equiv s \pmod{n}$, а потім об'єднуємо в сукупність $L(s_1, h)$ ($s_1 = 0, 1, \dots, n-1$) всі числа a з умовою $r_1 \equiv s_1 \pmod{n}$. Довести, що:
- (а) $\{L(s, g) : s = 0, 1, \dots, n-1\} = \{L(s_1, h) : s_1 = 0, 1, \dots, n-1\}$;
 - (б) $L(s, g) = L(s_1, h)$ тоді і тільки тоді, коли $s_1 \equiv \alpha \cdot s \pmod{n}$, де α знаходиться з конгруенції $\alpha \cdot \text{ind}_g h \equiv 1 \pmod{p-1}$.

Література

- [1]. *Бейкер А.* Введение в теорию чисел. — Минск.: Вышэйшая школа, 1995.
- [2]. *Бородін О.І.* Теорія чисел. — К.: Вища школа, 1970.
- [3]. *Бухштаб А.А.* Теория чисел. — М.: Просвещение, 1966.
- [4]. *Виноградов И.М.* Основы теории чисел. — М.: Наука, 1972.
- [5]. *Завало С.Т., Костарчук В.М., Хаџет Б.І.* Алгебра і терія чисел. ч.1, ч.2. — К.: Вища школа, 1976.
- [6]. *Кнут Д.* Искусство программирования для ЭВМ. т.2 Получисленные алгоритмы. — М.: Мир, 1977.
- [7]. *Ляпин Е.С., Евсеев А.Е.* Алгебра и теория чисел. ч.1, ч.2. — М.: Просвещение, 1974, 1978.
- [8]. *Стахов А.П.* Коды золотой пропорции. — М.: Радио и связь, 1984.