Львівський державний університет безпеки життєдіяльності

Марта СТАСЮК

ЕЛЕМЕНТИ МАТЕМАТИЧНИХ ОСНОВ КРИПТОГРАФІЇ

НАВЧАЛЬНИЙ ПОСІБНИК

Львів 2021

УДК
С

Рецензенти: **Роман ЗАТОРСЬКИЙ,** доктор фізико-математичних наук, професор, завідувач кафедри диференціальних рівнянь і прикладної математики Прикарпатського національного університету імені Василя Стефаника;

Наталія КУХАРСЬКА, кандидат фізико-математичних наук, доцент, доцент кафедри управління інформаційною безпекою Львівського державного університету безпеки життєдіяльності.

Рекомендовано до друку вченою радою
Львівського державного університету безпеки життєдіяльності
(протокол № від 2021 року)

Стасюк, Марта.
Елементи математичних основ криптографії : навчальний посібник / Марта СТАСЮК – Львів : ЛДУ БЖД, 2021. – 216 с.

У посібнику викладено елементи математичних основ криптографії.

Описані алгебраїчні структури, що використовує криптографія, розглянуто ряд питань теорії чисел, які є математичним фундаментом асиметричних криптосистем. Подані елементарні відомості з еліптичних кривих над скінченними полями. У посібнику поєднано теоретичні викладки математичних основ криптографії з демонстрацією їх застосувань на конкретних прикладах.

Для студентів та курсантів, що навчаються за спеціальністю «Кібербезпека», а також для усіх бажаючих ознайомитися з нестандартними математичними поняттями, які можуть зустрітися в їх науково-дослідницькій діяльності.

Зміст

Вступ

Навчальний посібник "Елементи математичних основ криптографії" написаний на основі курсу лекцій «Спеціальні розділи математики», який читається для курсантів та студентів спеціальності «Кібербезпека» у Львівському державному університеті безпеки життєдіяльності.

Цей посібник – вступ до математичних основ криптографії – науки про збереження таємниці інформації та її захисту.

Новітні методи захисту інформації базуються на певних математичних поняттях, які не є предметом вивчення класичних математичних курсів, а вивчають в таких розділах математики, як теорія груп, теорія скінченних кілець і полів, теорія чисел, теорія еліптичних кривих над скінченними полями.

Так, при формуванні відкритого і таємного ключів у криптосистемах з відкритим ключем використовують конгруенції, системи конгруенцій та методи їх розв'язування. Як відомо, ці математичні об'єкти та методи є предметом вивчення теорії чисел. Ймовірнісні криптосистеми вимагають володіння поняттями квадратичного лишка, символів Лежандра і Якобі. Криптосистема Ель-Гамаля використовує поняття первісного кореня та дискретного логарифма, які також вивчає теорія чисел. Багато криптологічних протоколів і криптосистем таких, як криптосистеми Ель-Гамаля, Шнорра, Чаума, криптосистема XTR, базуються на застосуванні теорії скінчених полів та многочленів над скінченими полями. Бурхливого розвитку набула сьогодні і криптографія на еліптичних кривих, що виправдовує необхідність ознайомити майбутніх фахівців із захисту інформації з елементарною теорією еліптичних кривих над скінченими полями.

Отже, для розуміння новітніх методів криптування і вміння їх застосовувати, слухачі повинні володіти

математичними основами понять і методів криптографії. Запропонований посібник покликаний ознайомити (хоча б на елементарному рівні) слухачів з цими методами і поняттями.

Матеріал посібника охоплює три розділи: 1.Алгебра, 2.Теорія чисел, 3.Еліптичні криві. Розділ «Теорія чисел» можна читати і використовувати незалежно від першого. Розділ «Еліптичні криві» суттєво використовує як перший, так і другий розділи.

Посібник адаптований до математичного рівня аудиторії, яка вивчала курси «Лінійна алгебра та аналітична геометрія», «Математичний аналіз», «Теорія ймовірностей і математична статистика» і супроводжується достатньою кількістю типових задач, які дозволяють перевірити розуміння вивчених абстрактних понять.

В посібнику наведено також зразки тестових і розрахункових завдань, які слухачі повинні виконати для складання заліку чи екзамену.

Сподіваюсь, що цей посібник буде корисним як для майбутніх спеціалістів в галузі інформаційної безпеки, так і для усіх бажаючих ознайомитися з нестандартними математичними поняттями, які можуть зустрітися в їх науково-дослідницькій діяльності.

Розділ 1. Алгебра

§ 1.1. *Групи.*

1.1.1. Основні визначення

Нехай задана деяка (скінченна чи нескінченна) множина G, на якій визначена операція множення «$\cdot$», тобто визначений закон, за яким кожній парі a,b елементів з множини G відповідає деякий елемент цієї множини, який називається добутком a і b та позначається символом $a\cdot b$.

Нехай ця операція справджує умови:

1. асоціативність $(a\cdot b)\cdot c = a\cdot(b\cdot c)$;

2. існування *одиничного(нейтрального)елемента,* який позначається e, і такого, що для довільного $a\in G$ справджується умова

$$a\cdot e = e\cdot a = a;$$

3. умова існування для довільного $a\in G$ *оберненого елемента* a^{-1} такого, що

$$a\cdot a^{-1} = a^{-1}\cdot a = e.$$

Визначення 1.1.1. Множина G з операцією множення «$\cdot$», що справджує умови $1-3$ називається *групою,* а операція множення «$\cdot$» $-$*груповою операцією.*

Визначення 1.1.2. Якщо в групі G для довільних елементів $a,b\in G$ виконується ще й умова

$$a\cdot b = b\cdot a,$$

то група G називається *комутативною* або *абелевою.*

Визначення 1.1.3. Група називається скінченною, якщо вона складається із скінченного числа елементів, в протилежному випадку група називається *нескінченною.*

Визначення 1.1.4. *Число елементів скінченної групи* називається її *порядком* і позначається $\operatorname{ord} G$.

Визначення 1.1.5. Нехай $G-$група. Підмножина $H \subset G$ називається *підгрупою* групи G, якщо H сама є групою з груповим законом групи G.

Приклади груп.

1.1.1. Група цілих чисел $\mathbb{Z} = \{0, \pm 1, \pm 2, ..., \pm n, ...\}$ відносно операції «$+$» (в цій групі $0-$нейтральний елемент, $-a-$ протилежний до $a \in \mathbb{Z}$, тобто "адитивно обернений").

1.1.2. Група ненульових раціональних чисел з груповою операцією $-$звичайним множенням «$\cdot$».

1.1.3. а) Група поворотів правильного трикутника (групова операція $-$це композиція поворотів).

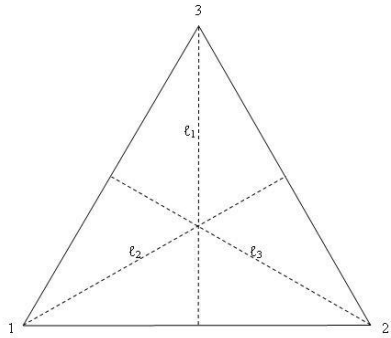

Рис.1

Є три повороти, які переводять правильний трикутник в себе: на 0^0, на 120^0 і на 240^0.

Помножити два повороти $-$це послідовно здійснити їх один за одним. Якщо позначити нульовий поворот через α_0, поворот на 120^0 через α_1, а поворот на 240^0 через α_2, то отримаємо правила множення поворотів:

$$\alpha_0 \cdot \alpha_0 = \alpha_0, \quad \alpha_0 \cdot \alpha_1 = \alpha_1 \cdot \alpha_0 = \alpha_1, \quad \alpha_0 \cdot \alpha_2 = \alpha_2 \cdot \alpha_0 = \alpha_2.$$

$$\alpha_1 \cdot \alpha_1 = \alpha_2, \quad \alpha_1 \cdot \alpha_2 = \alpha_2 \cdot \alpha_1 = \alpha_0, \quad \alpha_2 \cdot \alpha_2 = \alpha_1.$$

Легко перевірити, що для поворотів $\alpha_0, \alpha_1, \alpha_2$ справджується властивість асоціативності:

$$(\alpha_0 \cdot \alpha_1) \cdot \alpha_2 = \alpha_0 \cdot (\alpha_1 \cdot \alpha_2).$$

З правил множення поворотів випливає, що в множині $\{\alpha_0, \alpha_1, \alpha_2\}$ існує «одиничний елемент» α_0, тобто для $\alpha_i, \quad i = 1, 2$ маємо

$$\alpha_0 \cdot \alpha_i = \alpha_i \cdot \alpha_0 = \alpha_i.$$

З правил множення поворотів також випливає, що для $\alpha_i, \quad i = 0, 1, 2$ існує «обернений елемент», тобто такий елемент α_i^{-1}, для якого виконується правило

$$\alpha_i \cdot \alpha_i^{-1} = \alpha_0.$$

Легко бачити, що множина $\{\alpha_0, \alpha_1, \alpha_2\}$ поворотів правильного трикутника – це комутативна група порядку 3.

Правила множення поворотів трикутника доцільно подати у вигляді таблиці:

«•»	α_0	α_1	α_2
α_0	α_0	α_1	α_2
α_1	α_1	α_2	α_0
α_2	α_2	α_0	α_1

Таб. 1

б) Група поворотів правильного чотирикутника.

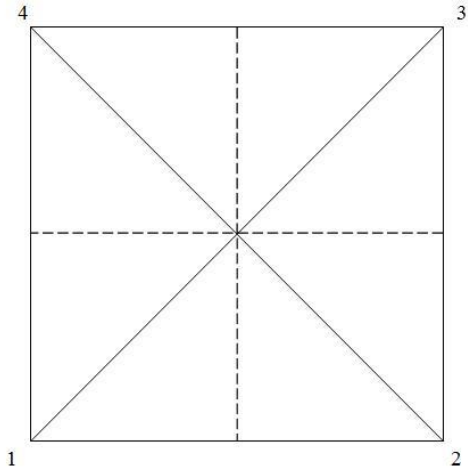

Рис.2

Повороти квадрата навколо центра O, подібно, як і для трикутника, позначимо відповідно: φ_0 – тотожний поворот, тобто поворот на кут 0^0, φ_1 – на 90^0, φ_2 – на 180^0, φ_3 – на 270^0

Аналогічно, як і для трикутника, можна написати таблицю множення поворотів квадрата.

1-й\2-й	φ_0	φ_1	φ_2	φ_3
φ_0	φ_0	φ_1	φ_2	φ_3
φ_1	φ_1	φ_2	φ_3	φ_0
φ_2	φ_2	φ_3	φ_0	φ_1
φ_3	φ_3	φ_0	φ_1	φ_2

Табл.2

Приклад підгрупи 1.1.4. Розглянемо всі симетрії правильного трикутника, до яких, окрім поворотів $\alpha_0, \alpha_1, \alpha_2$, відносяться ще й симетричні перетворення трикутника навколо його осей симетрії. Це три перетворення $\alpha_3, \alpha_4, \alpha_5$.

Перетворення α_3 залишає незмінною вершину 1, перетворення α_4 – незмінною вершину 2, а перетворення α_5 – вершину 3.

Правило множення всіх симетричних перетворень правильного трикутника аналогічно, як у випадку поворотів, подано в таблиці 3. З цієї таблиці видно, що ці перетворення утворюють групу, очевидно некомутативну.

«•»	α_0	α_1	α_2	α_3	α_4	α_5
α_0	α_0	α_1	α_2	α_3	α_4	α_5
α_1	α_1	α_2	α_0	α_4	α_5	α_3
α_2	α_2	α_0	α_1	α_5	α_3	α_4
α_3	α_3	α_5	α_4	α_0	α_2	α_1
α_4	α_4	α_3	α_5	α_1	α_0	α_2
α_5	α_5	α_4	α_3	α_2	α_1	α_0

Табл.3

З таблиці 3 видно, що група поворотів трикутника $\{\alpha_0, \alpha_1, \alpha_2\}$ – це *комутативна підгрупа* групи всіх симетрій правильного трикутника.

1.1.2. Циклічні групи.

Нехай a – довільний елемент групи G. Позначимо:

$$a \cdot a = a^2,$$
$$a \cdot a \cdot a = a^3,$$
$$\ldots\ldots\ldots\ldots,$$
$$a \cdot a \cdots a = a^n$$

Розглянемо елемент $a^{-1} \in G$ і позначимо:

$$a^{-1} \cdot a^{-1} = a^{-2},$$
$$a^{-1} \cdot a^{-1} \cdot a^{-1} = a^{-3},$$
$$\ldots\ldots\ldots\ldots\ldots,$$
$$a^{-1} \cdot a^{-1} \cdots a^{-1} = a^{-n}.$$

Покажемо, що

$$a^n \cdot a^{-n} = e. \qquad (1.1)$$

Дійсно, застосувавши метод математичної індукції, отримаємо

$$a^n \cdot a^{-n} = \left(a \cdot a^{n-1}\right) \cdot \left(a^{-(n-1)} \cdot a^{-1}\right) =$$
$$= a \cdot \left(a^{n-1} \cdot a^{-(n-1)}\right) \cdot a^{-1} = a \cdot e \cdot a^{-1} = e.$$

Покладемо, за визначенням, $a^0 = e.$ Далі для довільних цілих p, q маємо

$$a^p \cdot a^q = a^{p+q}.$$

Позначимо множину тих елементів групи G, які можна подати у вигляді a^n через $H(a)$, де a – елемент групи G. Попередні міркування доводять, що $H(a)$ – група. Дійсно

- $a^p \cdot a^q = a^{p+q} \in H(a), \quad p, q \in N;$
- існує $e = a^0$ такий, що $a \cdot e = e \cdot a = a;$
- для довільного $a \in H(a)$ існує a^{-1} такий, що $a \cdot a^{-1} = e.$

Група $H(a)$ називається *циклічною* групою, породженою елементом $a.$

Група $H(a)$, безумовно, є підгрупою групи G.

Визначення 1.1.6. Розглянемо групу $H(a)$, яка породжена елементом a, тобто має вигляд $\{a^n, n \in N\}$, де добуток $a \cdot a$ – визначений. Таку групу називатимемо *циклічною* групою, незалежно від того,чи є вона підгрупою якої-небудь групи, чи ні.

Зауважимо, що *циклічна* група – це *комутативна* група.

Приклади циклічних груп.

1.1.5. Група $m\mathbb{Z} = \{0, \pm m, \pm 2m, ..., \pm nm, ...\}$ є підгрупою групи $\mathbb{Z} = \{0, \pm 1, \pm 2, ..., \pm n, ...\}$ для довільного $m \in \mathbb{Z}$.

Група $m\mathbb{Z}$ – це циклічна група, породжена цілим додатним числом m відносно операції «+».

1.1.6. Група поворотів правильного трикутника $\{\alpha_0, \alpha_1, \alpha_2\}$ – циклічна група 3-го порядку з твірним елементом α_1 або α_2 (перевірити самостійно). Отже, тепер можна записати, наприклад,

$$\{\alpha_0, \alpha_1, \alpha_2\} = \{\alpha_1^0, \alpha_1^1, \alpha_1^2\}.$$

1.1.3. Група підстановок.

Довільне бієктивне (взаємно однозначне) відображення $\sigma : X_n \to X_n$, де X_n – довільна множина з n елементів, називається *підстановкою***.** Як правило, множину X_n вважають скінченним рядом цілих чисел: $X_n = \{1, 2, ..., n-1, n\}$.

Підстановки, зазвичай, позначаються малими грецькими літерами і записуються у вигляді таблиць:

$$\sigma = \begin{pmatrix} 1 & 2 & ... & n \\ i_1 & i_2 & ... & i_n \end{pmatrix}. \qquad (1.2)$$

Операція множення підстановок визначена згідно правил композиції відображень. Наприклад, для підстановок

$$\sigma = \begin{pmatrix} 1 & 2 & 3 & 4 \\ 2 & 3 & 4 & 1 \end{pmatrix}, \quad \tau = \begin{pmatrix} 1 & 2 & 3 & 4 \\ 4 & 3 & 2 & 1 \end{pmatrix}$$

$$\sigma \circ \tau = \begin{pmatrix} 1 & 2 & 3 & 4 \\ 1 & 4 & 3 & 2 \end{pmatrix}.$$

(підстановка τ переводить $1 \to 4,$ а підстановка σ переводить $4 \to 1,$ отже композиція $\sigma \circ \tau$ переводить $1 \to 1,$ ...., підстановка τ переводить $4 \to 1,$ а підстановка σ переводить $1 \to 2,$ отже композиція $\sigma \circ \tau$ переводить $4 \to 2$)

Зауважимо ,що

$$\tau \circ \sigma = \begin{pmatrix} 1 & 2 & 3 & 4 \\ 3 & 2 & 1 & 4 \end{pmatrix},$$

тобто множення підстановок $-$*некомутативна* операція.

Можна перевірити,що операція множення підстановок $-$асоціативна, тобто для довільних підстановок σ, τ, ω виконується співвідношення

$$(\sigma \circ \tau) \circ \omega = \sigma \circ (\tau \circ \omega).$$

Роль одиниці виконує підстановка e, яка не змінює своїх елементів:

$$e = \begin{pmatrix} 1 & 2 & \dots & n \\ 1 & 2 & \dots & n \end{pmatrix},$$

а оберненою до підстановки σ є підстановка

$$\sigma^{-1} = \begin{pmatrix} i_1 & i_2 & \dots & i_n \\ 1 & 2 & \dots & n \end{pmatrix}.$$

Отже підстановки (1.2) утворюють групу, яка називається *симетричною групою* n-го порядкуі позначається S_n.

Використовуючи основні поняття комбінаторики, можна довести важливу теорему $[1]$

Теорема 1.1.1 Порядок $|S_n|$ групи S_n дорівнює $n!$

Підстановка може деякі елементи переводити в інші, а деякі залишати на місці. Наприклад, підстановка

$$\sigma = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 \\ 3 & 2 & 4 & 6 & 5 & 1 \end{pmatrix}$$

залишає на місці елементи 2 і 5, а інші відображає по колу: $1 \to 3 \to 4 \to 6 \to 1$. Таку підстановку називатимемо *циклом* і позначатимемо $(1,\ 3,\ 4,\ 6)$.

Визначення 1.1.7. Циклом $(i_1, i_2, ..., i_k)$, де $i_1, i_2, ..., i_k$ – деякі числа із множини $\{1, 2, ..., n\}$ називається підстановка $\tau \in S_n$ така,що

$$\tau(i) = \begin{cases} i, i \notin \{i_1, i_2, ..., i_k\} \\ i_{t+1}, i = i_t, t \neq k \\ i_1, i = i_k. \end{cases} \qquad (1.3)$$

Визначення1.1.8. Два цикли називаються *незалежними*, якщо вони не мають спільних елементів.

Визначення1.1.9. *Транспозицією* називається двоелементний цикл.

Теорема 1.1.2. $[1]$ Якщо σ, τ – незалежні цикли, то

$$\sigma \circ \tau = \tau \circ \sigma.$$

Теорема 1.1.3. Кожна підстановка розкладається в добуток незалежних циклів. Цей розклад єдиний з точністю до порядку циклів.

Доведення цієї теореми можна знайти в $[1, 2]$.

Теорема1.1.4.Довільний цикл розкладається в добуток транспозицій.

Для доведення цієї теореми досить перевірити рівність.

$$(i_1, i_2, ..., i_k) = (i_1, i_k)(i_1, i_{k-1}) \cdots (i_1, i_3)(i_1, i_2).$$

Наслідок 1.1.1(з теорем 1.1.3,1.1.4)**.** Кожна підстановка розкладається в добуток скінченого числа *транспозицій.*

Визначення 1.1.10. *Перестановкою* $i_1, i_2, ..., i_n$ чисел з множини $\{1, 2, ..., n\}$ називається запис цих чисел в певному порядку.

Перестановки і підстановки пов'язані між собою. Якщо $\sigma = \begin{pmatrix} 1 & 2 & ... & n \\ i_1 & i_2 & ... & i_n \end{pmatrix}$ – підстановка,то $i_1, i_2, ..., i_n$ – перестановка.

Визначення1.1.11. Числа i_k, i_l утворюють *інверсію* в перестановці $i_1, i_2, ...i_k, ..., i_l, ...i_n$, якщо $i_k > i_l$, а $k < l$.

Визначення1.1.12.Перестановка $i_1, i_2, ..., i_n$ називається *парною*, якщо число її інверсій – парне і *непарною*в протилежному випадку.

Наприклад, підстановка $3, 5, 7, 1, 4, 2, 6$ – парна, бо має 10 інверсій:

$3,1;\quad 3,2;\quad 4,2;\quad 5,1;\quad 5,2;\quad 5,4;\quad 7,1;\quad 7,2;\quad 7,4;\quad 7,6.$

Перестановка $2, 1, 4, 3, 5, 7, 6$ має 3 інверсії:

$$2,1;\quad 4,3;\quad 7,6,$$

отже вона – непарна.

Визначення1.1.13. Підстановка $\sigma = \begin{pmatrix} 1 & 2 & ... & n \\ i_1 & i_2 & ... & i_n \end{pmatrix}$ називається *парною***,** якщо парною є перестановка $i_1, i_2, ..., i_n$ і *непарною* – в протилежному випадку (якщо перестановка $i_1, i_2, ..., i_n$ є непарною).

Теорема 1.1.5. Кожна парна підстановка розкладається в добуток парного числа транспозицій, а непарна – в добуток непарного числа транспозицій.

Доведення цієї теореми можна знайти в $[1, 2]$.

Якщо $\sigma = \tau_1 \cdot \tau_2 \cdots \tau_k -$ подання підстановки σ у вигляді добутку транспозицій $\tau_1, \tau_2, ..., \tau_k$, то число

$$\varepsilon_k = (-1)^k = \begin{cases} 1, & k = 2r \\ -1, & k = 2r-1, \quad r = 1,2,3,... \end{cases}$$

називається *сигнатурою* підстановки σ.

Отже, якщо підстановка парна,то її сигнатура дорівнює 1, а коли непарна, то -1.

Наслідок 1.1.2.$[1,2]$ Всі парні підстановки $n-$го порядку утворюють підгрупу $A_n \subset S_n$, порядок цієї групи $|A_n|$ дорівнює $\frac{n!}{2}$.

Група A_n називається *знакозмінною групою* n-го порядку.

Наступний приклад встановлює зв'язок між групою симетричних перетворень трикутника, які описані таблицями 2,3 і групою підстановок S_3 та її підгрупою A_3.

Приклади 1.1.7.

а) Розглянемо групу підстановок $G = S_3$:

$$P_0 = \begin{pmatrix} 1 & 2 & 3 \\ 1 & 2 & 3 \end{pmatrix}, \quad P_1 = \begin{pmatrix} 1 & 2 & 3 \\ 2 & 3 & 1 \end{pmatrix}, \quad P_2 = \begin{pmatrix} 1 & 2 & 3 \\ 3 & 1 & 2 \end{pmatrix},$$

$$P_3 = \begin{pmatrix} 1 & 2 & 3 \\ 1 & 3 & 2 \end{pmatrix}, \quad P_4 = \begin{pmatrix} 1 & 2 & 3 \\ 3 & 2 & 1 \end{pmatrix}, \quad P_5 = \begin{pmatrix} 1 & 2 & 3 \\ 2 & 1 & 3 \end{pmatrix}$$

та її підгрупу $U = A_3 = \{P_0, P_1, P_2\}$.

Якщо вершини трикутника перенумерувати так, як на рис.1,тотожному повороту α_0 поставимо у відповідність підстановку P_0, повороту α_1 – підстановку P_1, повороту α_2 – підстановку P_2,перетворенню $\alpha_3 - P_3$, перетворенню $\alpha_4 - P_4$, перетворенню $\alpha_5 - P_5$. Таким чином, група симетричних

перетворень трикутника еквівалентна (точне визначення буде згодом) групі підстановок S_3, а підгрупа поворотів $\{\alpha_0, \alpha_1, \alpha_2\}$ – еквівалентна підгрупі парних підстановок $A_3 \subset S_3$.

Отже працювати з симетричними перетвореннями трикутника – це те саме, що працювати з підстановками з S_3, що часто зручніше.

Приклад 1.1.8. Нехай задана підстановка

$$\tau = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 & 7 & 8 & 9 & 10 \\ 1 & 4 & 5 & 6 & 8 & 9 & 7 & 10 & 2 & 3 \end{pmatrix}.$$

Виконати наступні завдання:

а) подати підстановку у вигляді добутку циклів і транспозицій і зробити висновок про парність чи непарність підстановки;

б) знайти інверсії підстановки, що відповідає перестановці τ та підтвердити парність чи непарність заданої підстановки;

в) знайти τ^{18}.

Розвязання.

а) подамо підстановку τ у вигляді добутку циклів

$$\tau = (1)(7)(2 \quad 4 \quad 6 \quad 9)(3 \quad 5 \quad 8 \quad 10);$$

та добутку транспозицій

$$\tau = (2 \quad 9)(2 \quad 6)(2 \quad 4)(3 \quad 10)(3 \quad 8)(3 \quad 5);$$

б) знайдемо інверсії перестановки

$$1, \quad 4, \quad 5, \quad 6, \quad 8, \quad 9, \quad 7, \quad 10, \quad 2, \quad 3:$$

$$4,2; \quad 4,3; \quad 5,2; \quad 5,3; \quad 6,2; \quad 6,3; \quad 7,2; \quad 7,3;$$

$$8,2; \quad 8,3; \quad 8,7; \quad 9,2; \quad 9,3; \quad 9,7; \quad 10,2; \quad 10,3.$$

Оскільки кількість інверсій $k = 16$ – парна, то підстановка τ – парна.

Зауважимо, що кількість транспозицій підстановки τ є парним числом 6. Отже, парність чи непарність підстановки

можна встановлювати як з допомогою транспозицій, так і з допомогою інверсій, обрахованих для відповідної підстановки;

в)можна перевірити рівність

$$\tau^k = e = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 & 7 & 8 & 9 & 10 \\ 1 & 2 & 3 & 4 & 5 & 6 & 7 & 8 & 9 & 10 \end{pmatrix},$$

де $k = НСК(l_1, l_2, ..., l_m)$, а $l_1, l_2, ..., l_m$ – довжини циклів, на які розкладається підстановка (НСК$(l_1, l_2, ..., l_m)$ - це найменше спільне кратне чисел $l_1, l_2, ..., l_m$).

У випадку прикладу 1.1.8 $k = 4$. Тому

$$T^{18} = T^{16} \cdot T^2 = (\mathrm{T}^4)^4 \cdot T^2 = e \cdot T^2 =$$

$$= \begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 & 7 & 8 & 9 & 10 \\ 1 & 6 & 8 & 9 & 10 & 2 & 7 & 3 & 4 & 5 \end{pmatrix}.$$

Приклад 1.1.9. Використовуючи шифр підстановки, розшифрувати слово ІОВДРЖБАНЯЕН, якщо заданий ключ $K = \begin{pmatrix} 1 & 2 & 3 & 4 \\ 3 & 1 & 4 & 2 \end{pmatrix}$ періоду $l = 4$.

Розв'язання. Розіб'ємо слово на три блоки і розшифруємо кожен з них, використовуючи підстановку $K^{-1} = \begin{pmatrix} 1 & 2 & 3 & 4 \\ 2 & 4 & 1 & 3 \end{pmatrix}$ – обернену до K.

Маємо

ІОВД РЖБА НЯЕН

Застосувавши до кожного блоку підстановку K^{-1} прийдемо до блоків:

ВІДО БРАЖ ЕННЯ

З'єднавши ці блоки, отримуємо слово ВІДОБРАЖЕННЯ.

1.1.4. Група коренів з одиниці

Нагадаємо, як добути корінь $n-го$ *степеня з комплексного числа.* Нехай $z=a+bi.$

Визначення 1.1.14. Коренем $n-$го степеня з комплексного числа z називається будь-який розв'язок рівняння

$$x^n = z. \tag{1.4}$$

Позначимо через $\sqrt[n]{z}$ множину всіх коренів з комплексного числа z :

$$\sqrt[n]{z} = \left\{ u \in \mathbb{C} : u^n = z \right\}.$$

Наступне твердження описує сукупність всіх коренів з комплексного числа $z.$

Твердження1.1.1

$$\sqrt[n]{z} = \left\{ \sqrt[n]{|z|} \left(\cos\frac{\varphi+2k\pi}{n} + i\sin\frac{\varphi+2k\pi}{n} \right) \middle| \varphi = \arg z, \quad k = 0,1,2,...,n-1 \right\} \tag{1.5}$$

Доведення. Нехай комплексне число $u-$розв'язок рівняння (1.4). Подамо число u в тригонометричній формі $u=\rho(\cos\psi+i\sin\psi)$, де

$$\rho = |u|, \quad \psi = \arg u.$$

Підставляючи u в (1.4) івикористовуючи формулу Муавра $[1,2]$, отримуємо

$$|u|^n (\cos n\psi + i\sin n\psi) = |z|(\cos\varphi + i\sin n\varphi). \tag{1.6}$$

Із елементарної теорії комплексних чисел випливає, що два комплексні числа $-$рівні, якщо рівні їх модулі , а аргументи відрізняються на кількість повних обертів, тобто на число рівне $2\pi k, \quad k \in \mathbb{Z}.$ Тому з (1.6) прийдемо до співвідношень:

$$|u|^n = |z| \text{ або } |u| = \sqrt[n]{|z|},$$

$$n\psi - \varphi = 2k\pi \text{ або } \psi = \frac{\varphi + 2k\pi}{n}, \quad k \in \mathbb{Z}.$$

Отже для довільного $k \in \mathbb{Z}$ число

$$\sqrt[n]{|z|}\left(\cos\frac{\varphi + 2k\pi}{n} + i\sin\frac{\varphi + 2k\pi}{n}\right) \qquad (1.7)$$

є розв'язком рівняння (1.4). Перевіримо, що для $k = 0,1,2,...,n-1$ отримуємо різні корені рівняння (1.4). Справді, якби для $0 \le k_1 < k_2 \le n-1$ розв'язки були б однаковими, то $\frac{\varphi + 2k_2\pi}{n} - \frac{\varphi + 2k_1\pi}{n} = 2\pi l,$ або $k_2 - k_1 = nl, \quad l > 1,$ що неможливо. При $k \ge n$ поділимо ціле число k на число n з остачею, $k = d \cdot n + r, \quad 0 \le r \le n-1.$ Тоді маємо

$$\cos\frac{\varphi + 2k\pi}{n} + i\sin\frac{\varphi + 2k\pi}{n} = \cos\frac{\varphi + 2(dn + r)\pi}{n} + i\sin\frac{\varphi + 2(dn + r)\pi}{n} =$$

$$\cos\left(\frac{\varphi + 2\pi r}{n} + 2\pi d\right) + i\sin\left(\frac{\varphi + 2\pi r}{n} + 2\pi d\right) = \cos\frac{\varphi + 2\pi r}{n} + i\sin\frac{\varphi + 2\pi r}{n},$$

що й завершує доведення твердження 1.1.1.

Поклавши в (1.4) $z = 1$ і використавши (1.7) прийдемо до сукупності коренів $n-$го степеня з 1.

Визначення 1.1.15 .Коренями $n-$го степеня з 1 називають розв'язки рівняння $x^n = 1$**,** які за формулою (1.7) подаються у вигляді:

$$\sqrt[n]{1} = \left\{\cos\frac{2k\pi}{n} + i\sin\frac{2k\pi}{n}, \quad k = 0,1,2,...,n-1\right\} \qquad (1.8)$$

Для множини коренів $n-$го степеня з 1 прийнятне позначення C_n.

Теорема 1.1.6. Множина C_n –циклічна група $n-$го порядку відносно операції множення.

Дійсно, використовуючи дії над комплексними числами в тригонометричній формі,отримуємо

$$\left(\cos\frac{2\pi k_1}{n}+\sin\frac{2\pi k_1}{n}\right)\cdot\left(\cos\frac{2\pi k_2}{n}+i\sin\frac{2\pi k_2}{n}\right)=$$

$$=\left(\cos\frac{2\pi(k_1+k_2)}{n}+i\sin\frac{2\pi(k_1+k_2)}{n}\right)\in C_n$$

$$\left(\cos\frac{2\pi k}{n}+i\sin\frac{2\pi k}{n}\right)^{-1}=\left(\cos\frac{2\pi(n-k)}{n}+i\sin\frac{2\pi(n-k)}{n}\right)\in C_n$$

а, з використанням формули Муавра, приходимо до висновку: всі корені (1.8) є степенями кореня

$$\varepsilon=\cos\frac{2\pi}{n}+i\sin\frac{2\pi}{n}. \qquad (1.9)$$

Дійсно $\varepsilon^k=\cos\frac{2\pi k}{n}+i\sin\frac{2\pi k}{n}$, $k=0,1,2,...,n-1,$ отже група C_n-циклічна група, породжена, зокрема, коренем (1.9).

Визначення 1.1.16. Корінь $n-$го степеня з 1 називається *первісним,* якщо він не є коренем $m-$го степеня з 1 , де $1\le m<n$.

Приклад 1.1.10.

- числа i та $-i-$ первісні корені 4-го степеня з 1;
- $\varepsilon=\cos\frac{2\pi}{n}+i\sin\frac{2\pi}{n}-$ первісний корінь n-го степеня з 1.

Теорема 1.1.7. ε^k ,де ε визначений формулою (1.9), є первісним коренем $n-$го степеня з 1 тоді і тільки тоді, коли $\text{НСД}(k,n)=1,$ тобто, якщо числа k і $n-$ взаємно прості.

Доведення. Нехай ε^k – первісний корінь і нехай k і n не взаємно прості. Тоді існує їх спільний дільник $d = \text{НСД}(k,n)$ такий, що $k = k_1 d$, а $n = n_1 d$. Тоді

$$\left(\varepsilon^k\right)^{n_1} = \left(\varepsilon^{k_1 d}\right)^{n_1} = \left(\varepsilon^{k_1}\right)^{dn_1} = \left(\varepsilon^{k_1}\right)^{n} = \left(\varepsilon^{n}\right)^{k_1} = 1.$$

Отже ми отримали суперечність, що ε^k – первісний корінь, бо $\left(\varepsilon^k\right)^{n_1} = 1$, а $n_1 < n$.

Нехай тепер $\text{НСД}(k,n) = 1$. Покажемо, що ε^k – первісний корінь з 1. Якщо для деякого $m < n$ $\left(\varepsilon^k\right)^m = 1$, то $\cos\frac{2\pi km}{n} + i\sin\frac{2\pi km}{n} = 1$ і $\frac{2\pi km}{n} = 2\pi l$ і $km = nl$, звідки отримуємо, що n ділить m. А це неможливо, бо $m < n$.

Кількість первісних коренів n – го степеня з 1 дорівнює $\varphi(n)$, де $\varphi(n)$ – функція Ейлера, яка визначає число натуральних чисел k, що не перевищують n і взаємно прості з n. Детальніше цю функцію розглянемо в § 2.2.

Приклад 1.1.11. Знайти:

- всі нетривіальні підгрупи групи коренів з одиниці для $\sqrt[16]{1}$;
- всі первісні корені для $\sqrt[16]{1}$.

Розв'язання.

- нехай $\varepsilon = \cos\frac{2\pi}{n} + i\sin\frac{2\pi}{n}$. Тоді, за теоремою 1.1.6, степені ε^k, $k = 0,1,2,...,n-1$ утворюють циклічну групу коренів n – го степеня з 1.

Для $\sqrt[16]{1}$ маємо

$$\varepsilon = \cos\frac{2\pi}{16} + i\sin\frac{2\pi}{16} = \cos\frac{\pi}{8} + i\sin\frac{\pi}{8}.$$

Отже степені ε^k, $k = 0, 1, 2, \ldots$, утворюють циклічну групу 16-го порядку C_{16}. Ця група має наступні нетривіальні (відмінні від самої групи C_{16} і групи, що складається з $\varepsilon^0 = 1$) підгрупи:

- циклічна група8-го порядку,породжена коренем ε^2
$$\left\{\varepsilon^2\right\} = \left\{\varepsilon^2, \varepsilon^4, \varepsilon^6, \varepsilon^8, \varepsilon^{10}, \varepsilon^{12}, \varepsilon^{14}, \varepsilon^{16}\right\};$$
- циклічна група 4 -го порядку,породжена коренем ε^4
$$\left\{\varepsilon^4\right\} = \left\{\varepsilon^4, \varepsilon^8, \varepsilon^{12}, \varepsilon^{16}\right\};$$
- циклічна група 2 -го порядку,породжена коренем ε^8
$$\left\{\varepsilon^8\right\} = \left\{\varepsilon^8, \varepsilon^{16}\right\}.$$
- За теоремою 1.1.7. відомо, що ε^k, де ε визначений формулою
$$\varepsilon = \cos\frac{2\pi}{n} + i\sin\frac{2\pi}{n},$$
є первісним коренем $n-$го степеня з 1 тоді ітільки тоді, коли $(k, n) = 1.$

Очевидно, що числа $1, 3, 5, 7, 9, 11, 13, 15 -$ взаємно прості з 16 і менші за 16, тобто $\varphi(16) = 8.$ Тому маємо 8 первісних коренів 16-го степеня з1:
$$\varepsilon, \varepsilon^3, \varepsilon^5, \varepsilon^7, \varepsilon^9, \varepsilon^{11}, \varepsilon^{13}, \varepsilon^{15}.$$

Всі перелічені степені первісного кореня ε, в свою чергу, є твірними елементами циклічної групи C_{16}.

1.1.5. Фактор-група.

Нехай A і B – довільні множини. Відображення $f: A \to B$, яке кожному елементу $a \in A$ ставить у відповідність один і тільки один елемент $b = f(a) \in B$ породжує два важливі поняття:

- образ відображення $\operatorname{Im} f = \{ f(a), a \in A \}$ – це сукупність елементів $b = f(a)$ множини B;
- прообраз $f^{-1}(b) = \{ a \in A : f(a) = b \}$ елемента $b \in B$.

Визначення 1.1.17.

Відображення $f: A \to B$ називаються *сюр'єктивним,* якщо $\operatorname{Im} f = B$.

Відображення $f: A \to B$ називаються *ін'єктивним,* якщо з $a' \neq a \in A$ випливає, що $f(a') \neq f(a)$.

Відображення $f: A \to B$ називаються *бієктивним (*взаємно-однозначним*),* якщо це відображення є *сюр'єктивним та ін'єктивним* одночасно.

Справедливі дві майже очевидні теореми [1].

Теорема 1.1.8. Нехай $f: A \to B$ – відображення множин .Тоді повні прообрази $f^{-1}(b)$ всіх елементів $b \in B$ утворюють розбиття множини A на класи. Множина таких класів є у взаємно однозначній відповідності із множиною B.

Теорема 1.1.9. Нехай задане деяке розбиття множини A на класи. Це розбиття породжує відображення множини A на деяку множину B всіх класів даного розбиття. Відображення f ставить у відповідність кожному елементу $a \in A$ клас, до якого належить цей елемент.

Приклад 1.1.12. Розподілимо курсантів та студентів Львівського державного університету безпеки життєдіяльності (ЛДУБЖД) за навчально-науковими

інститутами:навчально-науковий інститут цивільного захисту (ННІЦЗ), навчально-науковий інститут пожежної та техногенної безпеки (ННІПТБ), навчально-науковий інститут психології та соціального захисту (ННІПСЗ). Тоді множина A – це множина всіх курсантів і студентів ЛДУБЖД, а множина B – це множина інститутів ННІЦЗ, ННІПТБ, ННІПСЗ.

За теоремою 1.1.8 кожному інституту (множина B) відповідає множина (клас) курсантів і студентів, які навчаються уцьому інституті (прообраз елемента множини B) . Наприклад, прообразом інституту ННІЦЗ є множина усіх курсантів та студентів цього інституту.

Теорема 1.1.9 визначає відображення f таким чином: кожному курсанту чи студенту ЛДУБЖД (множина A) поставимо у відповідність інститут, в якому він(вона) навчається(елемент групи B).

Відношення еквівалентності.

Нехай задане розбиття деякої множини M на класи.

Визначення 1.1.18. Назвемо два елементи a, b множини M еквівалентними відносно розбиття множини M на класи, якщо вони належать одному класу.

Еквівалентні елементи позначаються $a \sim b$. Відношенню еквівалентності притаманні такі властивості:

1. рефлексивність $a \sim a$;
2. симетрія: $a \sim b \Rightarrow b \sim a$;
3. транзитивність: $a \sim b$ і $b \sim c \Rightarrow a \sim c$.

Припустимо, навпаки, що для пар $a, b \subset M$ можна встановити відношення еквівалентності $\sim$, яке справджує вимоги 1-3. Тоді таке відношення еквівалентності визначає розбиття множини M на класи, що не перетинаються. Дійсно, поставимо у відповідність елементу $a \in M$ клас K_a, що містить цей елемент.

Покажемо, що класи K_a не перетинаються. Якщо б K_a і K_b для $a \neq b$ перетинались, тобто мали спільний елемент c, то $a \sim c$ і $b \sim c$, а отже й $a \sim b$. Нехай $y \in K_b$, тоді $y \sim b$ і отже $y \sim a$, тому $y \in K_a$ і навпаки. Ці міркування можна сформулювати у вигляді

Теорема 1.1.10. Кожне розбиття на класи деякої множини M визначає між елементами множини деяке відношення еквівалентності, що наділене властивостями 1-3.

Навпаки, кожне відношення еквівалентності, що встановлене між елементами множини M з властивостями 1-3, розбиває множину M на класи, що не перетинаються.

Приклад 1.1.13 .

- Нехай M – множина всіх прямих на площині. Введемо відношення еквівалентності в цій множині наступним чином:

$l_1 \sim l_2$ тоді і тільки тоді, коли l_1 паралельна l_2.

Легко переконатись, що запропоноване відношення еквівалентності справджує умови $1-3$.

- Подібність трикутників на площині – це відношення еквівалентності (Перевірити самостійно).

Лівобічні та правобічні суміжні класи.

Нехай задана деяка група G та її підгрупа U. Введемо відношення еквівалентності для двох довільних елементів групи G відносно підгрупи таким чином:

$$a \sim b, \text{ якщо } a^{-1} \cdot b \in U. \qquad (1.10)$$

Така еквівалентність називається *лівою еквівалентністю.*

Перевіримо, що відношення еквівалентності, яке визначене співвідношенням (1.10) справджує умови $1-3$.

1. $a \sim a$, так як $a^{-1} \cdot a = e \in U$;

2. якщо $a \sim b$, то $b \sim a$. Дійсно $\left(a^{-1} \cdot b\right)^{-1} = b^{-1} \cdot a \in U$, отже $b \sim a$;
3. оскільки $a \sim b$, то $a^{-1} \cdot b \in U$, оскільки $b \sim c$, то $b^{-1} \cdot c \in U$. Тоді $a^{-1} \cdot b \cdot b^{-1} \cdot c = a^{-1} \cdot c \in U$, тому $a \sim c$.

Тоді, за теоремою 1.1.10, група G відношенням еквівалентності (1.10) розбивається на класи еквівалентних елементів $\grave{K}_a$, які називаються *лівобічними суміжними класами*. Елементи довільного класу $\grave{K}_a$ – це елементи вигляду

$$\grave{K}_a = \{x = a \cdot u, x \in G, u \in U\} = aU \qquad (1.11)$$

Клас $\grave{K}_1 = U$ об'єднує всі елементи групи G, які еквівалентні елементу e.

Оскільки з (1.11) маємо, що $\grave{K}_a = aU, a \in G$ і з $u_1 \neq u_2$ випливає, що $a \cdot u_1 \neq a \cdot u_2$, то відображення $f : U \to aU$ – взаємно однозначне. А це означає, що кожен клас $\grave{K}_a$ має однакову кількість елементів, яка дорівнює порядку підгрупи U.

З цього факту, у випадку скінченої групи G, випливає

Теорема Лагранжа 1.1.11. Порядок довільної підгрупи скінченої групи – дільник порядку групи.

Дійсно, якщо n – порядок групи G, а m – порядок групи U, а l – кількість класів $\grave{K}_a$, то із попередніх міркувань отримуємо, що

$$n = m \cdot l.$$

Аналогічно, як у випадку *лівої еквівалентності*, можна ввести *праву еквівалентність* довільних двох елементів групи G за підгрупою $U \subset G$, а саме

$$a \sim b, \text{ якщо } b \cdot a^{-1} \in U. \qquad (1.12)$$

Відношення еквівалентності (1.12) справджує вимоги $1-3$ і називається *правою еквівалентністю.* Як і у випадку лівої еквівалентності, співвідношення (1.12) розбиває групу G на еквівалентні класи, які називаються *правобічними суміжними класами* і позначаються

$$K'_a = Ua, \quad a \in U.$$

Виникає запитання: коли $\grave{K}_a = K'_a$ або $aU = Ua$? (тобто, коли лівобічні суміжні класи групи G за підгрупою U співпадають з правобічними суміжними класами). З рівності

$$aU = Ua$$

випливає рівність

$$U = a^{-1}Ua, \quad a \in G. \tag{1.13}$$

Співвідношення (1.13) дає підстави для важливого

Визначення 1.1.7. Підгрупа U групи G, для якої виконується співвідношення (1.13), називається ***інваріантною підгрупою*** групи G або *нормальним дільником* групи G.

Отже у випадку, коли підгрупа $U \subset G$ – інваріантна підгрупа, маємо

$$\grave{K}_a = K'_a = K_a. \tag{1.14}$$

Зауважимо, що в комутативній групі всі підгрупи є *інваріантними* і рівність (1.14) виконується автоматично.

Приклад1.1.14.

а) Розглянемо групу підстановок $G = S_3$:

$$P_0 = \begin{pmatrix} 1 & 2 & 3 \\ 1 & 2 & 3 \end{pmatrix}, \quad P_1 = \begin{pmatrix} 1 & 2 & 3 \\ 2 & 3 & 1 \end{pmatrix}, \quad P_2 = \begin{pmatrix} 1 & 2 & 3 \\ 3 & 1 & 2 \end{pmatrix},$$

$$P_3 = \begin{pmatrix} 1 & 2 & 3 \\ 1 & 3 & 2 \end{pmatrix}, \quad P_4 = \begin{pmatrix} 1 & 2 & 3 \\ 3 & 2 & 1 \end{pmatrix}, \quad P_5 = \begin{pmatrix} 1 & 2 & 3 \\ 2 & 1 & 3 \end{pmatrix}$$

та її підгрупу $U = A_3 = \{P_0, P_1, P_2\}$.

Легко переконатись, що $U = A_3$ – інваріантна підгрупа S_3.

Зауважимо,що

$$P_3^{-1} = P_3, \quad P_4^{-1} = P_4, \quad P_5^{-1} = P_5.$$

Отже

$$P_3^{-1} U P_3 \subset U, \quad P_4^{-1} U P_4 \subset U, \quad P_5^{-1} U P_5 \subset U. \qquad (1.15)$$

Це твердження випливає з теореми 1.1.5. Можна перевірити, що кожна з підстановок P_0, P_1, P_2 підгрупи A_3 – парна, а кожна підстановка P_3, P_4, P_5 – непарна. Отже,в цьому випадку, група S_3 розбита на 2 класи (праві суміжні класи співпадають з лівими), які містять по 3 підстановки: клас $A_3 = \{P_0, P_1, P_2\}$ і клас непарних підстановок $\{P_3, P_4, P_5\}$.

б) Наведемо приклад неінваріантної підгрупи $U \subset S_3$, яка складається з двох підстановок: $U = \{P_0, P_5\}$. Ця підгрупа породжує різні суміжні класи $K_a \neq K'_a$, а саме:

$$K_a = \{\langle P_0, P_5\rangle, \langle P_1, P_3\rangle, \langle P_2, P_4\rangle\} \quad K'_a = \{\langle P_0, P_5\rangle, \langle P_2, P_3\rangle, \langle P_1, P_4\rangle\}.$$

Фактор-група за інваріантною підгрупою.

Отже нехай U – інваріантна підгрупа групи G, яка розбиває G на суміжні класи V. Покажемо, що в множині V можна визначити групову операцію «$\bullet$» , тобто з множини класів V утворити групу.

Нехай v_1, v_2 – довільні елементи з V. Виберемо $x_1 \in v_1, x_2 \in v_2$ *і через* $v_3 = v_1 \cdot v_2$ позначимо клас, що містить елемент $x_1 \cdot x_2$.

Покажемо, що вибраний добуток $v_1 \cdot v_2$ не залежить від вибору елементів x_1, x_2. Нехай $x_1^1 \neq x_1 \in v_1, \quad x_2^1 \neq x_2 \in v_2$. Тоді

$$x_1 \cdot x_2 \cdot \left(x_1^1 \cdot x_2^1\right)^{-1} = x_1 \cdot x_2 \cdot \left(x_2^1\right)^{-1} \cdot \left(x_1^1\right)^{-1} =$$

$$= x_1 \cdot u_1 \cdot \left(x_1^1\right)^{-1} = u_2 \cdot x_1 \cdot \left(x_1^1\right)^{-1} = u_2 \cdot u_3 \in U.$$

Отже

$$x_1 \cdot x_2 \sim x_1^1 \cdot x_2^1.$$

Перевіримо закони групи.

• можна перевірити, що добуток класів $v_1 \cdot v_2$ справджує умові асоціативності, оскільки закон асоціативності виконується в групі G.

• одиницею в V є клас U, тобто сама інваріантна підгрупа. Дійсно, оскільки для довільного $a \in v$ виконуються рівності $a \cdot e = e \cdot a = a$, то для довільного $v \in V$ отримуємо $v \cdot U = U \cdot v = v$.

• існує обернений до класу v клас v^{-1}. Дійсно, якщо $a \in v$, то клас v^{-1} – це клас, до якого належить елемент a^{-1}. Тоді

$$v \cdot v^{-1} = U,$$

оскільки $a \cdot a^{-1} = e$.

Множина класів V з груповим законом, який визначений вище, називається *фактор-групою* групи G за інваріантною підгрупою U і позначається G/U.

1.1.6. Гомоморфізми груп.

Нехай G і H – групи. Відображення $f : G \to H$ називається *гомоморфізмом груп*, якщо для довільних $x_1, x_2 \in G$ виконується умова

$$f\left(x_1 \cdot x_2\right) = f\left(x_1\right) \cdot f\left(x_2\right). \qquad (1.16)$$

Твердження 1.2. Множина $f\left(G\right) \subset H$, яка називається образом гомоморфізму (1.16) і позначається $\mathrm{Im}\, f$, є групою.

Твердження можна легко довести самостійно в якості вправи.

Визначення 1.1.8. Взаємно однозначний *гомоморфізм* груп (1.16) називається *ізоморфізмом.*

Приклад 1.1.15. Група симетрій правильного трикутника $\{\alpha_0, \alpha_1, \alpha_2, \alpha_3, \alpha_4, \alpha_5\}$ ізоморфна симетричній групі $S_3 = \{P_0, P_1, P_2, P_3, P_4, P_5\}$. Пропонуємо перевірити це твердження самостійно.

Визначення 1.1.9. Нехай $f : G \to H$ – гомоморфізм груп. Множина $\{x \in G : f(x) = e \in H\}$ називається ядром гомоморфізму і позначається $Kerf$.

Твердження 1.3. $Kerf$ – підгрупа групи G.

Дійсно, нехай $a_1, a_2 \in Kerf$, тобто $f(x_1) = e_H$, $f(x_2) = e_H$. Тоді:

- $f(x_1 \cdot x_2) = e_H \cdot e_H = e_H$;
- $f(e_G) = e_H$;
- $f(x_1^{-1}) = (f(x_1))^{-1}$ через те, що

$$f(x_1 \cdot x_1^{-1}) = f(x_1) \cdot f(x_1^{-1}) = f(e_G) = e_H.$$

І на завершення наведемо формулювання важливої теореми відомої алгебристки Еммі Нетер [1, 2].

Теорема про гомоморфізми 1.12. Нехай $f : G \to H$ – гомоморфізм груп. Тоді

1. $Kerf$ – інваріантна підгрупа групи G.

2. Довільна інваріантна підгрупа U групи G – це ядро деякого гомоморфізму, а саме:

$$f : G \to G / U.$$

3. Для того, щоб гомоморфізм $f : G \to H$ був ізоморфізмом необхідно і досить, щоб $Kerf = \{e_G\}$, тобто щоб

ядро гомоморфізму містило тільки один елемент – одиницю e_G.

Приклад 1.1.16. Розглянемо множину цілих чисел $\mathbb{Z}=\{0,\pm1,\pm2,...\}$ та її підгрупу $m\mathbb{Z}=\{\pm m,\pm 2m,...\}$, яка породжена фіксованим цілим додатним числом m.

Операція «$\cdot$» в цих групах – це операція «$+$», відносно якої і група $\mathbb{Z}$, і її група $m\mathbb{Z}$ – комутативні групи з нейтральним елементом 0.

Факторизуючи групу $\mathbb{Z}$ за підгрупою $m\mathbb{Z}$, прийдемо до фактор-групи $\mathbb{Z}/m\mathbb{Z}$, яка складається з класів $\bar{0},\bar{1},\bar{2},...,\overline{m-1}$. Клас $\bar{0}$ – це підгрупа $m\mathbb{Z}$, клас $\bar{1}$ – це множина цілих чисел, які при діленні на m дають остачу 1, клас $\bar{2}$ – це множина цілих чисел, які при діленні на m дають остачу 2,..., клас $\overline{m-1}$ – це множина цілих чисел, які при діленні на m дають остачу $m-1$. Легко переконатись, що

- для кожного класу $\bar{k}$ справджується співвідношення $\bar{0}+\bar{k}=\bar{k}+\bar{0}=\bar{k}$;
- для кожного класу $\bar{k}$ існує клас $-\bar{k}$ такий, що $\bar{k}+\left(-\bar{k}\right)=-\bar{k}+\bar{k}=\bar{0}$.

Приклад 1.1.17. Розглянемо конкретне значення $m=5$. Опишемо операцію додавання в фактор-групі $\mathbb{Z}/5\mathbb{Z}$, тобто в множині класів $\{\bar{0},\bar{1},\bar{2},\bar{3},\bar{4}\}$ таблицею 4.

Можна перевірити, що ненульові класи фактор-групи $\mathbb{Z}/5\mathbb{Z}$ утворюють групу і відносно операції множення.

«+»	$\bar{0}$	$\bar{1}$	$\bar{2}$	$\bar{3}$	$\bar{4}$

$\bar{0}$	$\bar{0}$	$\bar{1}$	$\bar{2}$	$\bar{3}$	$\bar{4}$
$\bar{1}$	$\bar{1}$	$\bar{2}$	$\bar{3}$	$\bar{4}$	$\bar{0}$
$\bar{2}$	$\bar{2}$	$\bar{3}$	$\bar{4}$	$\bar{0}$	$\bar{1}$
$\bar{3}$	$\bar{3}$	$\bar{4}$	$\bar{0}$	$\bar{1}$	$\bar{2}$
$\bar{4}$	$\bar{4}$	$\bar{0}$	$\bar{1}$	$\bar{2}$	$\bar{3}$

Табл.4

Задамо операцію множення таблицею 5

« ·»	$\bar{1}$	$\bar{2}$	$\bar{3}$	$\bar{4}$
$\bar{1}$	$\bar{1}$	$\bar{2}$	$\bar{3}$	$\bar{4}$
$\bar{2}$	$\bar{2}$	$\bar{4}$	$\bar{1}$	$\bar{3}$
$\bar{3}$	$\bar{3}$	$\bar{1}$	$\bar{4}$	$\bar{2}$
$\bar{4}$	$\bar{4}$	$\bar{3}$	$\bar{2}$	$\bar{1}$

Табл.5

Легко перевірити самостійно, що множина класів $\{\bar{1},\bar{2},\bar{3},\bar{4}\}$ утворює групу відносно операції «$\cdot$». З таблиці 5 бачимо, як знайти обернені елементи в цій групі: $\bar{2}^{-1}=\bar{3},\quad \bar{3}^{-1}=\bar{2},\quad \bar{4}^{-1}=\bar{4}.$

1.2. Кільця

1.2.1.Основні визначення.

Множина K з двома операціями «+» і« $\bullet$ » (додавання і множення) називається кільцем, якщо в цій множині справджуються аксіоми:

- відносно операції додавання $K-$ це *комутативна група* з нулем $0 \in K$ і протилежним елементом $-x$ для довільного $x \in K$.
- множення справджує закон *асоціативності*:

$$(x \cdot y) \cdot z = x \cdot (y \cdot z);$$

- операції множення та додавання пов'язані законом *дистрибутивності*:

$$x \cdot (y + z) = x \cdot y + x \cdot z, \quad (y + z) \cdot x = y \cdot x + z \cdot x.$$

Кільце називається **комутативним**, якщо для довільних $x, y \in K$ справджується рівність

$$x \cdot y = y \cdot x$$

Елемент кільця e називається *одиничним елементом***,** якщо для довільних $x \in K$ справджується рівність

$$x \cdot e = e \cdot x = x.$$

Легко перевірити, що одиничний елемент (якщо він існує) – єдиний.

В кожному кільці справедливі такі співвідношення для довільних $x, y \in K$:

- $x \cdot 0 = 0 \cdot x = 0;$
- $x \cdot (-y) = (-x) \cdot y = -x \cdot y;$
- $(-x) \cdot (-y) = xy.$

Визначення 1.2.1. Підмножина $A \subset K$ називається **підкільцем** в K, якщо A є кільцем відносно тих же операцій «+» і « $\bullet$ », що і в кільці A.

Приклади кілець:

1.2.1. $\mathbb{Z}=\{0\pm1,\pm2,...,\pm n,...\}, \mathbb{Q}=\left\{\frac{m}{n}, m,n\in\mathbb{Z}, n\neq 0\right\}$ – комутативні кільця з одиницею $e=1.$

1.2.2. Нехай A – довільна непорожня множина, $M=2^A$ – множина всіх підмножин множини A. Визначимо на множині M операції: для довільних $X, Y\subset M$

- $X\oplus Y=(X\cup Y)\setminus(X\cap Y)$;
- $X\odot Y=X\cap Y$,

де $X\cup Y$, $X\cap Y$ – об'єднання та перетин множин відповідно. M є кільцем відносно цих операцій.

1.2.3. Кільце цілих гаусових чисел $\mathbb{Z}[i]\overset{df}{=}\{a+bi \mid a,b\in\mathbb{Z}\}$ із операціями додавання і множення, як в множині комплексних чисел.

1.2.4. Кільце $M_n(R)$ квадратних матриць розміру $n\times n$ з елементами з $\mathbb{R}$, де $\mathbb{R}$ – множина дійсних чисел.

Операції додавання і множення в цьому кільці – це операції над квадратними матрицями однакових розмірів, які, як пригадуємо з курсу лінійної алгебри, можна виконувати завжди. Одиницею в цьому кільці є одинична матриця E_n. Закони асоціативності та дистрибутивності також справджуються [1, 2].

1.2.5. У ланцюжку $6\mathbb{Z}\subset 2\mathbb{Z}\subset\mathbb{Z}$ кожне попереднє кільце лежить в наступному. Нагадаємо,що

$$2\mathbb{Z}=\{0,\pm2,\pm4,\pm6,...,\pm2n,...\},$$

$$6\mathbb{Z}=\{0,\pm6,\pm12,\pm18,...,\pm6n,...\}$$

Визначення 1.2.2. [1, 2] Підкільце H кільця K називається *ідеалом***,** якщо виконується умова: з $a\in H$ і $x\in K$, випливає, що $ax\in H$.

Твердження 1.2.1. Ідеал складається з необоротних (таких, для яких не існує обернений) елементів кільця, нуль завжди лежить в ідеалі.

Визначення 1.2.3. Ідеал H комутативного кільця K називається *головним* , якщо існує елемент $a \in K$ такий, що $H = \{ax, x \in K\}$. В цьому випадку говорять, що ідеал H – це головний ідеал, породжений елементом $a \in K$.

Приклад 1.2.6. Нехай $\mathbb{Z}$ – кільце цілих чисел. Тоді $m\mathbb{Z} = \{0, \pm m, \pm 2m \pm 3m, ...\}$ – ідеал в $\mathbb{Z}$. Більш того, цей ідеал – головний.

Дійсно,

- $mx_1 - mx_2 \in m\mathbb{Z}$;
- $\forall a \in \mathbb{Z}\ a \cdot mx_1 = max_1 \in m\mathbb{Z}$;
- ціле число m породжує цей ідеал, бо кожний елемент ідеалу $m\mathbb{Z}$ – це число кратне m.

Визначення 1.2.4. Ідеал $H \subset K$ називається *простим* , якщо з включення $ab \in H$ випливає: $a \in H$ або $b \in H$.

Приклад 1.2.7. Головний ідеал $p\mathbb{Z}$, породжений простим числом $p \in \mathbb{Z}$, – простий ідеал в кільці $\mathbb{Z}$.

Приклад 1.2.7. Головний ідеал $6\mathbb{Z}$ – не є простимв кільці $\mathbb{Z}$.

Дійсно, з рівності $2 \cdot 3 \in 6\mathbb{Z}$ не випливає, що $2 \in 6\mathbb{Z}$ або $3 \in 6\mathbb{Z}$, бо число 2 – не є кратне числа 6, а число 3 – не є кратне числа 6.

1.2.2. Фактор-кільце

Нехай H – ідеал в кільці K. Тоді, оскільки ідеал H – це підгрупа адитивної групи кільця K, то , як і у випадку групи, в кільці K можна ввести відношення еквівалентності наступним чином:

$a \sim b$ тоді і тільки тоді, коли $a - b \in H$

Зауважимо, що оскільки ідеал H – комутативна підгрупа кільця K, то нема потреби розрізняти лівобічне та правобічне відношення еквівалентності.

Нехай $K/H=\{a+H \mid a\in K\}$ – множина всіх суміжних класів кільця K за ідеалом H. Позначимо $a+H=\bar{a}$. Визначимо на множині K/H операції додавання і множення суміжних класів:

$$\bar{a}+\bar{b}=\overline{a+b},\quad \bar{a}\cdot\bar{b}=\overline{a\cdot b}. \qquad (1.17)$$

Можна перевірити, як і у випадку груп, що ці операції визначені коректно.

Визначення 1.2.5. Множина суміжних класів K/H є кільцем відносно операцій додавання й множення суміжних класів (1.17) і називається фактор-кільцем кільця K за ідеалом H.

Зауважимо, що, якщо K – кільце з одиницею e, то K/H – також кільце з одиницею $\bar{e}=e+H$.

Приклад 1.2.8. Важливим прикладом фактор-кільця є кільце класів лишків $\mathbb{Z}/m\mathbb{Z}$. Елементами цього фактор-кільця є суміжні класи (див. приклад 1.1.16.) $\{a+m\mathbb{Z}, a\in\mathbb{Z}\}$. Оскільки $a=mk+r,\ 0\le r\le m-1,$ то представником суміжного класу може бути вибрана одна з остач від ділення числа a на число m. А, оскільки цими остачами є числа $0,1,2,...,m-1,$ то суміжні класи фактор-кільця $\mathbb{Z}/m\mathbb{Z}$ – це класи $\bar{1},\bar{2},...,\overline{m-1}$.

Розглянемо, наприклад, кільце лишків $\mathbb{Z}/6\mathbb{Z}$ і визначимо в ньому операції додавання та множення таблицями. Таблиці додавання і множення для кільця лишків $\mathbb{Z}/5\mathbb{Z}$ наведені в прикладі 1.1.17., (Табл.4,5).

+	$\bar{0}$	$\bar{1}$	$\bar{2}$	$\bar{3}$	$\bar{4}$	$\bar{5}$

$\overline{0}$	$\overline{0}$	$\overline{1}$	$\overline{2}$	$\overline{3}$	$\overline{4}$	$\overline{5}$
$\overline{1}$	$\overline{1}$	$\overline{2}$	$\overline{3}$	$\overline{4}$	$\overline{5}$	$\overline{0}$
$\overline{2}$	$\overline{2}$	$\overline{3}$	$\overline{4}$	$\overline{5}$	$\overline{0}$	$\overline{1}$
$\overline{3}$	$\overline{3}$	$\overline{4}$	$\overline{5}$	$\overline{0}$	$\overline{1}$	$\overline{2}$
$\overline{4}$	$\overline{4}$	$\overline{5}$	$\overline{0}$	$\overline{1}$	$\overline{2}$	$\overline{3}$
$\overline{5}$	$\overline{5}$	$\overline{0}$	$\overline{1}$	$\overline{2}$	$\overline{3}$	$\overline{4}$

Табл.6

•	$\overline{1}$	$\overline{2}$	$\overline{3}$	$\overline{4}$	$\overline{5}$
$\overline{1}$	$\overline{1}$	$\overline{2}$	$\overline{3}$	$\overline{4}$	$\overline{5}$
$\overline{2}$	$\overline{2}$	$\overline{4}$	$\overline{0}$	$\overline{2}$	$\overline{4}$
$\overline{3}$	$\overline{3}$	$\overline{0}$	$\overline{3}$	$\overline{0}$	$\overline{3}$
$\overline{4}$	$\overline{4}$	$\overline{2}$	$\overline{0}$	$\overline{4}$	$\overline{2}$
$\overline{5}$	$\overline{5}$	$\overline{4}$	$\overline{3}$	$\overline{2}$	$\overline{1}$

Табл. 7

Визначення 1.2.6. Елементи $a \neq 0,\ b \neq 0$ кільця K називають *дільниками нуля*, якщо $a \cdot b = 0.$ Кільце без дільників нуля називається *цілісним (або областю цілісності).*

Таблиця 7 прикладу 1.2.8. показує, що кільце $\mathbb{Z}/6\mathbb{Z}$ має дільники нуля, наприклад, $\overline{2}$ і $\overline{3}$ чи $\overline{3}$ і $\overline{4}$, і отже не є областю цілісності.

Визначення 1.2.7. Комутативне кільце P з одиничним елементом $e \neq 0$ називається *полем* , якщо для кожного ненульового елемента $a \in P$ існує обернений відносно множення елемент $a^{-1} \in P$.

Приклад 1.2.9. Множина $\mathbb{Q}$ раціональних чисел та множина $\mathbb{R}$ дійсних чисел є полями відносно звичайних операцій додавання та множення.

Приклад 1.2.10. Фактор- кільце $\mathbb{Z}/5\mathbb{Z}$, як видно з таблиць 4,5 прикладу 1.1.17, є полем.

Узагальнює останній приклад наступне

Твердження 1.2.1. Кільце класів лишків $\mathbb{Z}/m\mathbb{Z}$ – поле тоді і тільки тоді, коли m – просте число.

• Нехай $m = p$ – просте число. Покажемо, що для класу $\overline{a} \in \mathbb{Z}/p\mathbb{Z}$ існує клас $\overline{b} \in \mathbb{Z}/p\mathbb{Z}$ такий, що $\overline{a} \cdot \overline{b} = \overline{e}$. Розглянемо елементи

$$\overline{a}, \overline{2a}, \overline{3a}, ..., \overline{(p-1)a}. \qquad (1.18)$$

Ці елементи відмінні від нуля, бо $\overline{a} \neq \overline{0}$. До того ж всі елементи з послідовності (1.18) – різні: з рівності $\overline{ka} = \overline{la}$, $k < l$ випливало б $\overline{(k-l)a} = \overline{0}$, що невірно. Отже, послідовність елементів (1.18) співпадає з послідовністю якимось чином переставлених елементів

$$\overline{1}, \overline{2}, ..., \overline{p-1}.$$

Зокрема, при певному $b, 1 \leq b \leq p-1$ матимемо $\overline{a} \cdot \overline{b} = \overline{1}$. А це означає, що $\overline{b}$ – обернений елемент до елемента $\overline{a}$, тобто $\mathbb{Z}/p\mathbb{Z}$ – поле.

• Навпаки, нехай $\mathbb{Z}/m\mathbb{Z}$ – поле, тоді m – просте. Доведемо цей факт від супротивного. Якщо m не є простим,

то $\mathbb{Z}/m\mathbb{Z}$ – не є полем. Справді, в цьому випадку $m = m_1 \cdot m_2, \quad 1 < m_1, m_2 < m$. Тоді $\overline{m} = \overline{m_1} \cdot \overline{m_2} = \overline{0}, \overline{m_1} \neq \overline{0}, \overline{m_2} \neq \overline{0}$.

Якби для $\overline{m_1}$ існував обернений елемент $\overline{m_1}^{-1}$, то ми мали б $\overline{m_1}^{-1} \cdot \overline{m_1} \cdot \overline{m_2} = \overline{1} \cdot \overline{m_2} = \overline{m_2} = \overline{0}$ що невірно. Отже, це протиріччя й завершує доведення твердження.

Очевидним є наступне

Твердження 1.2.2. Поле не має дільників нуля.

Зауважимо, що твердження 1.2.1. дає нам сукупність скінчених полів, які мають широке застосування як в теорії чисел, так і в криптографії.

1.2.3. Ділення в кільцях. Дільники одиниці та прості елементи в кільцях.

Перш ніж вводити поняття евклідового кільця, потрібно нагадати і систематизувати загальні поняття, що стосуються подільності елементів в комутативному кільці.

Визначення 1.2.8. Нехай K – кільце з одиницею та без дільників нуля. Нехай $a, b \in K$. Кажуть, що b ділить a (a ділиться на b) і пишуть $b \mid a$, якщо існує елемент $c \in K$ такий, що $a = b \cdot c$.

З визначення 1.2.8. випливають такі найпростіші властивості подільності.

- якщо $b \mid a_1$ і $b \mid a_2$, то $b \mid a_1 + a_2$;
- якщо $b \mid a$ і $c \in K$, то $b \mid ac$.

Визначення 1.2.9. Якщо $a \in K$ і $a \mid e$, то a називається *дільником одиниці (або одиницею)* кільця K.

Приклад 1.2.11.

- В кільці $\mathbb{Z}$ є два дільники одиниці: ± 1.
- В кільці цілих чисел Гауса $\mathbb{Z}[i] = \{a + bi, \quad a, b \in \mathbb{Z}\}$ є чотири одиниці: $\pm 1, \quad \pm i$.

Дійсно, якщо $a+bi-$ одиниця , то існує число $c+di$ таке, що $(a+bi)\cdot(c+di)=1.$ Знайдемо спряжене до останнього $(a-bi)\cdot(c-di)=1$ і помножимо ці дві рівності.

Маємо

$$\left(a^2+b^2\right)\cdot\left(c^2+d^2\right)=1.$$

Ця рівність можлива , якщо $a=\pm1$ або $b=\pm1,$ що й приводить до одиниць $\pm1,\ \pm i.$

- В кільці $\mathbb{Z}\left(\sqrt{2}\right)\overset{df}{=}\left\{a+b\sqrt{2},a,b\in\mathbb{Z}\right\}$ із звичними операціями додавання і множення елемент $1+\sqrt{2}$ є дільником 1, бо $\left(\sqrt{2}+1\right)\left(\sqrt{2}-1\right)=1.$ Якщо $n\in\mathbb{N},$ то $\left(\sqrt{2}+1\right)^n\left(\sqrt{2}-1\right)^n=1,$ тому в кільці $\mathbb{Z}\left(\sqrt{2}\right)$ існує безліч дільників одиниці .

Визначення 1.2.10. Ненульові елементи $a,b\in K$ називаються *асоційованими*, якщо $a\,|\,b$ і $b\,|\,a.$

Твердження 1.2.3. Елементи $a,b\in K-$ асоційовані тоді і тільки тоді, коли $a=bu,$ де $u\,|\,e.$

Дійсно, якщо $a=bu,\ \ b=av,$ тобто $a(e-vu)=0,$ то $e-vu=0$ і $uv=e.$

Навпаки, якщо $a=bu,\ \ uv=e,$ то $av=bav=b.$ Отже, $a\,|\,b$ і $b\,|\,a.$

Визначення 1.2.11. Елемент $p\in K$ називається *простим,* якщо p не ділить одиницю і з того, що $a\,|\,p$ випливає, що або $a\,|\,e,$ або $a-$ асоційований з p .

Приклад 1.2.12.

1. Числа $\pm 2, \pm 3, \pm 5, \pm 7, \ldots$ в кільці $\mathbb{Z}$ є простими елементами, додатні числа $2, 3, 5, 7, \ldots$ в цьому кільці називаються *простими* числами.

2. В кільці $\mathbb{Z}[i]$ елемент 3 є простим, а елемент 5 – ні.

Дійсно, якби число 3 не було простим, то справджувався б розклад $(a+bi)(c+di)=3$, а отже і розклад $(a-bi)(c-di)=3$. Тому мала б виконуватись рівність $(a^2+b^2)(c^2+d^2)=9$. Оскільки $a+bi$ не ділить 1,то $a^2+b^2=3$. Проте остання рівність не виконується для жодних цілих a і b. Тому $3 \in \mathbb{Z}[i]$ – простий елемент.

Для 5 маємо розклад $5=(2-i)(2+i)$. Отже $5 \in \mathbb{Z}[i]$ – не є простим.

Останній приклад показує, що відомому ще з шкільної арифметики поняттю *простого* числа слід надавати точного визначення, як тільки ми працюємо не в звичному кільці цілих чисел $\mathbb{Z}$.

Визначення 1.2.12. Нехай a, b – ненульові елементи кільця K. Елемент d кільця K називається *найбільшим спільним дільником* елементів a і b, позначають (a,b) або НСД(a,b), якщо d – спільний дільник a, b і d ділиться на кожний інший спільний дільник елементів a і b.

Зауважимо,що НСД(a,b) визначається з точністю до асоційованості.

Приклад 1.2.13.

1. Вкільці $\mathbb{Z}$ маємо: $-7=(21,35)$, $7=(21,35)$.

2. $(3, 2+i)=1$.

Оскільки $3-$простий елемент в $\mathbb{Z}[i]$, то досить показати, що 3 не ділить $2+i$. Якби $3\,|\,2+i$, то для деякого числа $a+bi\in\mathbb{Z}[i]$ мали б розклад $3(a+bi)=2+i$ і, перейшовши до спряжених чисел, отримали б $3(a-bi)=2-i$. Після множення прийшли б до рівності $9(a^2+b^2)=5$ з цілими a,b, що неможливо. Це й доводить, що $(3,2+i)=1$.

Аналогічно, *найбільшим спільним дільником* ненульових елементів $a_1,a_2,...,a_k$ називається такий спільний дільник цих елементів, який ділиться на кожний інший їх спільний дільник.

Визначення 1.2.13. Елементи $a_1,a_2,...,a_k$ називають *взаємно простими*, якщо їх найбільший спільний дільник дорівнює одиниці.

Прості елементи в кільці породжують важливе поняття факторіального кільця.

Визначення 1.2.14. Область цілісності K називають *факторіальним кільцем*, якщо для K справджуються такі властивості:

1) кожний елемент $a\in K$ можна подати у вигляді добутку $a=u\cdot p_1\cdot p_2\cdots p_l$, де $u\,|\,1$, а p_i, $1\le i\le l-$ прості елементи з K. (якщо $l=0$, то $a=u$);

2) якщо $a=u\cdot p_1\cdot p_2\cdots p_l=u'\cdot q_1\cdot q_2\cdots q_s$, де $u\,|\,e$, $u'\,|\,e$, а $p_1,p_2,...,p_l,q_1,q_2,...,q_s-$прості елементи з K, то $l=s$ і кожний елемент p_i асоційований з деяким елементом q_j $1\le i,j\le l$.

Факторіальним кільцем є кільце цілих чисел $\mathbb{Z}$, в якому простими елементами є числа $\pm2,\pm3,\pm5,\pm7,...$

Не всі кільця – факторіальні. Далі наведемо

Приклад нефакторіального кільця 1.2.14.

Розглянемо кільце $\mathbb{Z}\left(\sqrt{-5}\right)=\left\{a+b\sqrt{-5}\,\middle|\,a,b\in\mathbb{Z}\right\}$. Знайдемо дільники 1 вцьому кільці.

Зауважимо, що якщо $\left(a+b\sqrt{-5}\right)\left(c+d\sqrt{-5}\right)=1$, то й $\left(a-b\sqrt{-5}\right)\left(c-d\sqrt{-5}\right)=1$. Тому $a^2+5b^2=1$, а це можливо тільки тоді, коли $a=\pm1,\quad b=0$. Розглянемо рівність

$$21=3\cdot7=\left(1+2\sqrt{-5}\right)\left(1-2\sqrt{-5}\right).$$

Покажемо, що 3, 7. $\left(1+2\sqrt{-5}\right)$, $\left(1-2\sqrt{-5}\right)$ – прості елементи кільця $\mathbb{Z}\left(\sqrt{-5}\right)$, які не є асоційованими з 1. Розглянемо,наприклад, елемент $\left(1-2\sqrt{-5}\right)$. Якщо

$$\left(a+b\sqrt{-5}\right)\left(c+d\sqrt{-5}\right)=1-2\sqrt{-5},$$

то $\left(a-b\sqrt{-5}\right)\left(c-d\sqrt{-5}\right)=1+2\sqrt{-5}$.Звідси $\left(a^2+5b^2\right)\left(c^2+5d^2\right)=21$, тому $a^2+5b^2=3$ або $a^2+5b^2=7$, що неможливо. Отже елемент$1-2\sqrt{-5}$ – простий елемент кільця $\mathbb{Z}\left(\sqrt{-5}\right)$. Аналогічно можна довести простоту інших трьох елементів: 3, 7, $\left(1+2\sqrt{-5}\right)$. Тому подання числа $21\in\mathbb{Z}\left(\sqrt{-5}\right)$ у вигляді добутку простих неоднозначне.

1.2.4. Евклідові кільця.

Евклідові кільця мають важливі застосування, як в алгебрі й теорії чисел, так і в криптографії. Найважливішими прикладами евклідових кілець є кільце цілих чисел $\mathbb{Z}$ та кільце многочленів $P[X]$ з коефіцієнтами з деякого, часто скінченного, поля P. Кільце $P[X]$ ми детально розглянемо в

наступному пункті. В евклідових кільцях працює алгоритм Евкліда, який дозволяє знаходити найбільший спільний дільник елементів кільця. Цей алгоритм дуже корисний в багатьох застосуваннях.

Визначення 1.2.15. Область цілісності K називається евклідовим кільцем, якщо існує відображення $\delta : K \setminus \{0\} \to \mathbb{N}$, що має властивості:

1. $\delta(ab) \geq \delta(a)$;
2. для довільних $a, b \in K$ існують $d, r \in K$ такі,що

$$a = bd + r, \qquad (1.19)$$

де $\delta(r) < \delta(b)$ або $r = 0$.

Рівність (1.19) називають діленням з остачею, q називають *неповною часткою, а r – остачею.*

Приклад 1.2.15.

1. $\mathbb{Z}$ – евклідове кільце,в якому для довільного $a \in \mathbb{Z}$ $\delta(a) = |a|$. (Перевірити,що $\delta(a) = |a|$ справджує умови 1,2 визначення 1.2.15)

2. Кільце цілих гаусових чисел $\mathbb{Z}[i]$ – евклідове, якщо $\delta(m + in) = m^2 + n^2$.

Алгоритм Евкліда.

Позначимо в (1.19) $q = q_1$, $r = r_2$. Тоді маємо

$$a = bq_1 + r_2,$$

де $\delta(r_2) < \delta(b)$ або $r_2 = 0$.

Якщо $r_2 \neq 0$, то поділимо b на r_2, маємо

$$b = r_2 q_2 + r_3,$$

де $\delta(r_3) < \delta(r_2)$ або $r_3 = 0$, і так далі. Продовжуючи ділення з остачею, отримаємо ряд рівностей:

$$
\begin{aligned}
&a = bq_1 + r_2, \quad \delta(r_2) < \delta(b),\\
&b = r_2q_2 + r_3, \quad \delta(r_3) < \delta(r_2),\\
&r_2 = r_3q_3 + r_4, \ \delta(r_4) < \delta(r_3),\\
&\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\\
&r_i = r_{i+1}q_{i+1} + r_{i+2}, \ \delta(r_{i+2}) < \delta(r_{i+1}),\\
&\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\\
&r_{n-2} = r_{n-1}q_{n-1} + r_n, \quad \delta(r_n) < \delta(r_{n-1}),\\
&r_{n-1} = r_nq_n.
\end{aligned}
\qquad (1.20)
$$

Процедуру послідовного ділення з остачею, визначену рівностями (1.20), називають *алгоритмом Евкліда* знаходження найбільшого спільного дільника в евклідових кільцях.

Твердження 1.2.4. Остання ненульова остача r_n в (1.20) є найбільшим спільним дільником елементів a, b евклідового кільця $K[1,2]$.

Доведення.

- Спочатку покажемо, що $r_n \mid a$ і $r_n \mid b$. З останньої рівності (1.20) маємо $r_n \mid r_{n-1}$. Тоді з передостанньої випливає, що $r_n \mid r_{n-2}$. І так далі, рухаючись угору від рівності до рівності в (1.20), отримаємо, що $r_n \mid r_3$ і $r_n \mid r_2$, а отже й $r_n \mid a$ і $r_n \mid b$.
- Залишається довести, що r_n ділиться на кожен інший спільний дільник елементів a і b. Дійсно, якщо $c \mid a$ і

$c \mid b$, то перша рівність в (1.20) показує, що $c \mid r_2$, а друга показує, що $c \mid r_3$. І так далі, рухаючись вниз від рівності до рівності в (1.20), отримуємо, що $c \mid r_{n-2}$ і $c \mid r_{n-1}$, а тому й з останньої рівності в (1.20) отримаємо, що $c \mid r_n$.

Наслідок 1.2.1.(з алгоритму Евкліда) Нехай $d = (a,b)-$ найбільший спільний дільник елементів a і b евклідового кільця K. Тоді існують $u, v \in K$ такі, що $au + bv = d$.

Доведення. З передостанньої рівності маємо $d = r_{n-2} - r_{n-1}q_{n-1}$. Тоді з попередньої рівності отримуємо, що $d = r_{n-2} - (r_{n-3} - r_{n-2}q_{n-2})q_{n-1} = r_{n-3}u' + r_{n-2}v'$ для деяких $u', v' \in K$. Конкретний вигляд елементів u', v' кільця K нас не цікавить. Рухаючись угору в (1.20), виразимо r_{n-2} через r_{n-3} і r_{n-4} і так далі. Дійшовши до першої рівності в (1.20), отримаємо рівність $au + bv = d$.

Наслідок 1.2.2. Нехай a і b – взаємно прості елементи евклідового кільця K. Тоді існують $u, v \in K$ такі, що $au + bv = 1$.

Наслідок 1.2.2.випливає з Наслідку 1.2.1.

Приклад 1.2.16.

Використовуючи алгоритм Евкліда,знайти:

- найбільший спільний дільник $d = (735, 266)$;
- цілі числа u і v, для яких справджується рівність:
$$735 \cdot u + 266 \cdot v = d.$$
- Знайти інверсію числа $c = 101$ відносно числа $a = 735$.

Розв'язання.

- Застосуємо алгоритм Евкліда для знаходження $d = (735, 266)$:

$$735 = 266 \cdot 2 + 203,$$
$$266 = 203 \cdot 1 + 63,$$
$$203 = 63 \cdot 3 + 14,$$
$$63 = 14 \cdot 4 + 7,$$
$$14 = 7 \cdot 2.$$

Отже $(735, 266) = 7$.

- Використаємо рівність $63 = 14 \cdot 4 + 7$.
  Маємо
  $7 = 63 - 14 \cdot 4 = 63 - (203 - 63 \cdot 3) \cdot 4 = 63 \cdot 13 - 203 \cdot 4 =$
  $(266 - 203) \cdot 13 - 203 \cdot 4 = 266 \cdot 13 - 203 \cdot 17 = 266 \cdot 13 -$
  $(735 - 266 \cdot 2) \cdot 17 = 266 \cdot 47 - 735 \cdot 17 = 12502 - 12495 = 7$
  Отже $u = -17, \quad v = 47.$

- Нагадаємо, що *інверсією числа* c відносно числа a, за умови, що $\text{НСД}(c, a) = 1$, називається число y таке, що $c \cdot y = \overline{1}$. у фактор-кільці $\mathbb{Z} / 735\mathbb{Z}$.
  Для розв'язання цієї задачі використаємо алгоритм Евкліда. Маємо

$$735 = 101 \cdot 7 + 28,$$
$$101 = 28 \cdot 3 + 17,$$
$$28 = 17 \cdot 1 + 11,$$
$$17 = 11 \cdot 1 + 6,$$
$$11 = 6 \cdot 1 + 5,$$
$$6 = 5 \cdot 1 + 1.$$

Знайдемо y.

$$1 = 6 - 5 \cdot 1 = 6 - (11 - 6 \cdot 1) \cdot 1 = 6 \cdot 2 - 11 = (17 - 11 \cdot 1) \cdot 2 - 11 =$$
$$= 17 \cdot 2 - 11 \cdot 3 = 17 \cdot 2 - (28 - 17 \cdot 1) \cdot 3 = 17 \cdot 5 - 28 \cdot 3 =$$

$$=(101-28\cdot 3)\cdot 5-28\cdot 3=101\cdot 5-28\cdot 18=101\cdot 5-(735-101\cdot 7)\cdot 18=$$
$$=101\cdot(5+7\cdot 18)-735\cdot 18=-735\cdot 11+101\cdot 131.$$

Отже, за визначенням, інверсія числа $c=101$ відносно $a=735$ дорівнює $y=131$.

Виконаємо перевірку, яку доцільно завжди робити при відшуканні інверсії числа. Маємо $101\cdot 131=13231=735\cdot 18+1 \equiv \bar{1}$.

Справедливі наступні важливі твердження, які пов'язують наведені вище визначення і які наведемо тут без доведення [1, 2, 6]..

Твердження 1.2.5. Кожне евклідове кільце – факторіальне.

Твердження 1.2.6. В евклідовому кільці всі ідеали – головні.

1.2.5. Кільце многочленів від однієї змінної

Важливим прикладом евклідового кільця є сукупність многочленів з коефіцієнтами з деякого кільця або поля.

Нехай K – кільце з одиницею. Побудуємо нове кільце A, елементами якого є нескінченні впорядковані послідовності

$$f=(f_0, f_1,..., f_i,...), \qquad (1.21)$$

де $f_i \in K$, $i=0,1,2,...$, причому всі f_i, окрім, можливо, скінченного їх числа, дорівнюють нулеві. Визначимо в цьому кільці операції додавання і множення:

$$f+g=(f_0+g_0, f_1+g_1,..., f_i+g_i,...),$$
$$f\cdot g=(h_0, h_1,..., h_i,...), \text{ де } h_i=\sum_{k+m=i} f_k g_m, \quad i=0,1,2,...,$$

якщо $f=(f_0, f_1,..., f_i,...)$, $g=(g_0, g_1,..., g_i,...)$.

Покажемо, що $A-$ кільце. Справді додавання в A зводиться до додавання елементів кільця K. Операція додавання в кільці $K-$ асоціативна і комутативна.

Операція віднімання визначена наступним чином:

$$f-g=(f_0-g_0, f_1-g_1,..., f_i-g_i,...).$$

Покажемо, що операція множення – асоціативна. Справді, якщо $f=(f_0, f_1,..., f_i,...)$, $g=(g_0, g_1,..., g_i,...)$, $h=(h_0, h_1,..., h_i,...)$, то на $i-$у місці в добутку $(fg)h$ маємо елемент

$$\sum_{s+t=i}\Big(\sum_{k+l=s} f_k g_l\Big)h_t=\sum_{k+l+t=i} f_k g_l h_t,$$

а в добутку $f(gh)$ на $i-$у місці маємо

$$\sum_{k+j=i} f_k\left(\sum_{l+t=j} g_l h_t\right)=\sum_{k+l+t=i} f_k g_l h_t.$$

Отже $(fg)h=f(gh)$, що й доводить асоціативність множення.

Покажемо, що операції додавання і множення пов'язані законом дистрибутивності.Справді, нехай

$$f=(f_0, f_1,..., f_i,...),\quad g=(g_0, g_1,..., g_i,...),\quad h=(h_0, h_1,..., h_i,...).$$

Тоді на $i-$у місці в послідовності $(f+g)h$ є елемент $\sum_{k+l=i}(f_k+g_k)h_l$, а в послідовності $fh+gh-$ елемент $\sum_{k+l=i} f_k h_l+\sum_{k+l=i} g_k h_l$. Оскільки

$$\sum_{k+l=i}(f_k+g_k)h_l=\sum_{k+l=i} f_k h_l+\sum_{k+l=i} g_k h_l,$$

то $(f+g)h=fh+gh$ і закон дистрибутивності виконується.

Зауважимо, що множення в A комутативне, якщо кільце $K-$ комутативне.

Одиницею в A є послідовність $(1,0,0,...,0,...)$ за умови, що в K є одиниця 1.

Таким чином, доведено, що сукупність нескінченних впорядкованих послідовностей A утворює кільце (кільце є комутативне, якщо $K-$ комутативне і має одиницю, якщо кільце K має одиницю). Це кільце називається *кільцем многочленів* над кільцем K, а його елементи називаються *многочленами.*

Послідовності $(a,0,0,...,0,...)$ додаються і множаться так, як елементи кільця K. Це дозволяє ототожнити такі послідовності з елементами кільця K, тобто вважати, що $a=(a,0,0,...,0,...)$ для кожного $a\in K$.

Позначимо $X=(0,1,0,...,0,...)$ і назвемо X змінною над K. Легко переконатись, що $X^2=(0,0,1,0,...,0,...)$, $X^3=(0,0,0,1,0,...,0,...)$ і т.д. Оскільки $K\subset A$, то

$$(0,0,...,0,a,0,...,0,...)=aX^n=X^na.$$

Отже, якщо f_n- останній, відмінний від нуля член послідовності $f=(f_0,f_1,...,f_n,...)$, то $f=f_0+f_1X+f_2X^2+\cdots+f_nX^n=f(X)$, що і є стандартним записом многочлена f. Елементи $f_0,f_1,...,f_n\subset K$ називаються *коефіцієнтами* многочлена f, а елемент f_n- *старшим коефіцієнтом.*

Побудоване кільце многочленів $f(X)$ над кільцем або полем K *позначають* $K[X]$.

Натуральне число n, яке фігурує в записі многочлена $f(X)$ називають *степенем* многочлена $f(X)$ і позначають $n = \deg f$.

Легко переконатись, що

$$\deg(f+g) \le \max(\deg f + \deg g),$$
$$\deg(f \cdot g) \le \deg(f) + \deg(g).$$

Можна перевірити, що у випадку, коли $K-$ кільце без дільників нуля, то

- остання нерівність стає рівністю, тобто маємо
$$\deg(f \cdot g) = \deg(f) + \deg(g);$$
- кільце $K[X]$ також без дільників нуля.

Слід відрізняти формальні многочлени (1.21), від многочленів, як функцій.

Нехай $f(X) = f_0 + f_1 X + f_2 X^2 + \cdots + f_n X^n$. Якщо змінній X у $f(X)$ надамо певного значення $X = a \in K$, то отримаємо елемент $f(a) \in K$, який назвемо значенням многочлена при $X = a$. Оскільки для кожного $a \in K$ многочлен $f(a) \in K$ визначений єдиним чином, то $f(X)$ можна вважати функцією від змінної X.

Слід зауважити, що многочлени не завжди можна ототожнювати з функціями. Наприклад, многочлени $f(X) = X$ і $g(X) = X^2$ над полем $\mathbb{Z}/2\mathbb{Z}$ визначають одну функцію із $\mathbb{Z}/2\mathbb{Z}$ в $\mathbb{Z}/2\mathbb{Z}$ (Перевірити самостійно).

Поєднує поняття формального многочлена і многочлена, як функцію, наступна

Теорема 1.2.1. Нехай $K-$ підкільце комутативного кільця R. Для кожного елемента $t \in R$ існує єдиний

гомоморфізм $\pi_t : \mathrm{K}[X] \to R$ такий, що $\pi_t(a) = a$ для довільного $a \in K$ і $\pi_t(X) = t.$

Дійсно, нехай такий гомоморфізм існує. Тоді, оскільки, $\pi_t(f_i) = f_i$ для кожного коефіцієнта f_i многочлена $f(X)$ і $\pi_t(X^k) = (\pi_t(X))^k = t^k,$ то $\pi_t(f) = f_0 + f_1 t + f_2 t^2 + \cdots + f_n t^n$ і $\pi_t(f)$ визначений однозначно.

Якщо $x \in K$ і $f(X) = a_0 + a_1 X + a_2 X^2 + \cdots + a_n X^n \in R[X]$ то $\pi_x(f) = a_0 + a_1 x + a_2 x^2 + \cdots + a_n x^n$ – це функція, яка набуває значень в $R.$ На множині всіх таких функцій $R[x]$ введемо операції додавання і множення:

$$\pi_x(f) + \pi_x(g) = \pi_x(f + g),$$
$$\pi_x(f) \cdot \pi_x(g) = \pi_x(f \cdot g).$$

Відносно цих операцій $R[x]$ є кільцем і відображення $\pi_x : \mathrm{R}[X] \to R[x]$ є сюр'єктивним гомоморфізмом кілець.

Гомоморфізм $\pi_x : \mathrm{R}[X] \to R[x]$ називають *гомоморфізмом підстановки.* Він відіграватиме важливу роль в конструкції скінченних полів.

Зауважимо наступне: якщо $R-$ нескінченне поле, то гомоморфізм $\pi_x : \mathrm{R}[X] \to R[x]-$ ін'єктивне відображення; це твердження не справджується у випадку скінченного поля. Наприклад, два різні многочлени $f(X) = X$ і $g(X) = X^2$ із $\mathbb{Z}/2\mathbb{Z}[X]$ відображаються в одну і ту ж функцію $h(x) \in \mathbb{Z}/2\mathbb{Z}[x]$ таку, що: $h(0) = 0, \quad h(1) = 1.$

Ділення в кільці многочленів

Нехай $K = P -$ поле. Тоді для визначення ділення в кільці многочленів $P[X]$ важливе значення має твердження про ділення з остачею:

Твердження 1.2.7. Для довільних многочленів $f(x), g(x) \in P[X]$ існують такі $h(x), r(x) \in P[X]$, що виконується рівність

$$f(x) = g(X) \cdot h(X) + r(X), \qquad (1.22)$$

де $\deg r(X) < \deg g(X)$ або $\deg r(x) = 0.$

Рівність (1.22) називають *діленням з остачею*, $h(x)$ називають *неповною часткою, а* $r(x) -$ *остачею.* Детальне доведення твердження 1.2.7 можна знайти, наприклад, в $[1,2]$.

Твердження 1.2.8. Кільце многочленів $P[X] -$ евклідове кільце.

Дійсно, у відображенні $\delta : P[X] \setminus \{0\} \to \mathbb{N}$ покладемо $\delta(f(X)) = \deg f(X) -$ степінь многочлена $f(X)$. Властивість 1 очевидна, а властивість 2 випливає з твердження 1.2.7.

Окрім того, в $P[X]$ працює алгоритм Евкліда знаходження найбільшого спільного дільника многочленів $f(X)$ і $g(X)$:

$$\begin{aligned}
&f(X) = g(X)h_1(X) + r_2(X), \quad \deg r_2(X) < \deg g(X),\\
&g(X) = r_2(X)h_2(X) + r_3(X), \quad \deg r_3(X) < \deg r_2(X),\\
&r_2(X) = r_3(X)h_3(X) + r_4(X), \quad \deg r_4(X) < \deg r_3(X),\\
&\qquad \ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots \ldots \qquad (1.23)
\end{aligned}$$

$$r_{n-2}(X)=r_{n-1}(X)h_{n-1}(X)+r_n(X),\deg r_n(X)<\deg r_{n-1}(X)$$
$$r_{n-1}(X)=r_n(X)h_n(X).$$

Як і в (1.20) остання ненульова остача $r_n(X)$ є найбільшим спільним дільником многочленів $f(X),g(X)$ евклідового кільця $P[X]$.

З алгоритму Евкліда, що справджується в евклідових кільцях, випливає наслідок для випадку кільця $P[X]$

Наслідок 1.2. Для довільних двох многочленів $f(X),g(X)\in P[X]$ існують многочлени $U(X),\mathrm{V}(X)\in P[X]$ такі, що справджується рівність

$$f(X)\cdot U(X)+g(X)\cdot V(X)=D(X), \qquad (1.24)$$

де $D(X)-$ найбільший спільний дільник многочленів $f(X)$ і $g(X)$.

Приклад 1.2.17. Знайти НСД(f,g) над $\mathbb{Z}/2\mathbb{Z}\overset{df}{=}F_2$, де

$$f(X)=X^6+X^5+X^4+1,\ g(X)=X^5+X+1.$$

Розв'язання. Застосуємо до цих многочленів алгоритм Евкліда (1.23), використовуючи ділення з остачею (1.22):

$$X^6+X^5+X^4+1=(X^5+X+1)(\mathrm{X}+1)+X^4+X^2,$$
$$X^5+X+1=(X^4+X^2)X+X^3+X+1,$$
$$X^4+X^2=(X^3+X+1)X+X,$$
$$X^3+X+1=X\cdot X^2+X+1,$$
$$X=(X+1)\cdot 1+1,$$
$$X+1=1\cdot(X+1).$$

Отже остання ненульова остача $R_6 = 1$ і є найбільший спільним дільником многочленів $f(X)$ і $g(x)$ над полем F_2. А це означає,що многочлени $f(X)$ і $g(X)$ – взаємно прості.

Приклад 1.2.18.ЗнайтиНСД(f, g) над $\mathbb{Z}/3\mathbb{Z} \overset{df}{=} F_3$, де

$$f(X) = X^8 + 2X^5 + X^3 + X^2 + 1,$$
$$g(X) = 2X^6 + X^5 + 2X^3 + 2X^2 + 2.$$

Розв'язання.

- як і в попередньому випадку, застосуємо до многочленів f, g алгоритм Евкліда:

$$X^8 + 2X^5 + X^3 + X^2 + 1 =$$
$$= \left(2X^6 + X^5 + 2X^3 + 2X^2 + 2\right)\left(2X^2 + 2X + 2\right) +$$
$$+2X^5 + X^4 + 2X^3 + 2X^2 + 2X,$$
$$2X^6 + X^5 + 2X^3 + 2X^2 + 2 =$$
$$= \left(2X^5 + X^4 + 2X^3 + 2X^2 + 2X\right) \cdot X + X^4 + 2,$$
$$2X^5 + X^4 + 2X^3 + 2X^2 + 2X =$$
$$= \left(X^4 + 2\right)\left(2X + 1\right) + 2X^3 + 2X^2 + X + 1,$$
$$X^4 + 2 = \left(2X^3 + 2X^2 + X + 1\right)\left(2x + 1\right) + 2x^2 + 1,$$
$$2x^3 + 2X^2 + X + 1 = \left(2X^2 + 1\right) \cdot \left(X + 1\right).$$

Отже остання ненульова остача $r_5(X) = 2X^2 + 1$ і є найбільшим спільним дільникоммногочленів $f(X)$ і $g(X)$.

- для заданих многочленів $f(x)$ та $g(x)$ знайдемо многочлени $U(x)$ і $V(x)$ в представленні (1.24). Для розв'язання цієї задачі запишемо алгоритм Евкліда для многочленів $f(X), g(X)$ в компактній формі:

$$\begin{aligned} f &= g\cdot\left(2X^2+2X+2\right)+r_2,\\ g &= r_2\cdot X+r_3,\\ r_2 &= r_3\cdot\left(2X+1\right)+r_4,\\ r_3 &= r_4\cdot\left(2X+1\right)+2X^2+1,\\ r_4 &= r_5\cdot\left(X+1\right). \end{aligned} \qquad (1.25)$$

Отже остання ненульова остача $r_5\left(X\right)=2X^2+1$ і є найбільшим спільним дільником многочленів $f\left(X\right)$ і $g\left(X\right)$. Зауважимо, що в полі F_3 виконуютьсярівності: $2^{-1}=2$, $-1=2$, $-2=1$, які використані при діленні многочленів з остачею.

Знайдемо невідомі многочлени $U\left(x\right)$ і $V\left(x\right)$, рухаючись в (1.25) знизу вгору, починаючи з передостанньої рівності. Маємо

$$\begin{aligned} r_5 &= r_3-r_4\left(2X+1\right)=r_3-\left[r_2-r_3\left(2X+1\right)\right]\cdot\left(2X+1\right)=\\ &=r_3\left(X^2+X+2\right)-r_2\left(2X+1\right)=\\ &=\left(g-r_2\cdot X\right)\left(X^2+X+2\right)-r_2\left(2X+1\right)=\\ &=g\left(X^2+X+2\right)-r_2\left(X^3+X^2+X+1\right)=\\ &g\left(X^2+X+2\right)-\left[f-g\left(2X^2+2X+2\right)\right]\cdot\left(X^3+X^2+X+1\right)=\\ &-f\cdot\left(X^3+X^2+X+1\right)+g\cdot\left(2X^5+X^4+X^2+2X+1\right), \end{aligned}$$

тобто

$U\left(X\right)=-\left(X^3+X^2+X+1\right),\quad V\left(X\right)=2X^5+X^4+X^2+2X+1.$

Для впевненості у правильності розв'язання задачі слід перевірити, чи рівність (1.24) справджується. Для цього

потрібно перемножити многочлени $f \cdot U$ і $g \cdot V$ з врахуванням рівностей в F_3 : $2^{-1} = 2,\ -1 = 2,\ -2 = 1$.

$$f \cdot U + g \cdot V =$$
$$-\left(X^8 + 2X^5 + X^3 + X^2 + 1\right)\left(X^3 + X^2 + X + 1\right) +$$
$$\left(2X^6 + X^5 + 2X^3 + 2X^2 + 2\right)\left(2X^5 + X^4 + X^2 + 2X + 1\right) =$$
$$-\left(X^{11} + X^{10} + X^9 + 2X^7 + X^5 + 2X^4 + 2X^2 + X + 1\right) +$$
$$+X^{11} + X^{10} + X^9 + 2X^7 +$$
$$+X^5 + 2X^4 + X^2 + X + 2 = -X^2 + 1 = 2X^2 + 1.$$

Оскільки кільце многочленів $-$це евклідове кільце, то, на основі твердження 1.2.5, це кільце $-$факторіальне. Виникає запитання: які многочлени є *простими елементами* кільця $P[X]$? Відповідь на це запитання залежить від поля P. В тому випадку, коли $P = \mathbb{C} -$ поле комплексних чисел, основна теорема алгебри доводить, що *простими елементами* в $P[X]$ є лінійні многочлени $x - a$, де $a \in \mathbb{C}$. У випадку, коли $P = \mathbb{R} -$ поле дійсних чисел, *простими елементами є*, як лінійні многочлени $x - a,\ a \in \mathbb{R}$, так і квадратні тричлени $x^2 + px + q,\ p, q \in \mathbb{R}$ з від'ємним дискримінантом $p^2 - 4q < 0$. У випадках скінченних полів маємо різноманіття *різних простих елементів* у різних полях. Так, наприклад, в кільці $F_2[X]$ маємо наступні прості (незвідні) многочлени:

- многочлени 1-го степеня: $x,\quad x+1$;
- многочлен 2-го степеня: $x^2 + x + 1$;
- многочлени 3-го степеня: $x^3 + x + 1,\quad x^3 + x^2 + 1$.

В кільці $F_3[X]$ незвідними многочленами 2-го степеня є многочлени:

$x^2+1, x^2+x+1, x^2+x+2, 2x^2+2, 2x^2+x+1, 2x^2+2x+1.$

Отже й факторизація, тобто розклад многочлена з кільця $P[X]$, де P – скінчене поле, в добуток *простих многочленів* в кожному кільці многочленів – інший.

1.2.6. Застосування методів алгебри до шифрування

Дипломатичні, військові і промислові секрети, як правило, передаються або зберігаються не у початковому вигляді, а після шифрування. На відміну від тайнопису, що приховує сам факт наявності повідомлення, шифрування передаються відкрито, а закривається тільки зміст. Отже криптографія забезпечує збереження змісту повідомлення за допомогою *шифрування* й відкриття його *розшифруванням,* які виконують за спеціальними *криптографічними алгоритмами* з допомогою *ключів* у відправника і одержувача.

Розглянемо класичну схему передачі секретних повідомлень криптографічним перетворенням, де зазначені етапи й учасники цього процесу.

	Шифрування	**Передача**	**Розшифрування**
Текст	листок	$\rightarrow$	листок
Ключ	конверт	$\rightarrow$	конверт
	Відправник	Канал зв’язку	Одержувач

Зі схеми можна побачити такі особливості й відмінності від звичайних комунікаційних каналів. Відправник шифрує повідомлення за допомогою ключа, отримане шифрування передається по відкритому каналу зв’язку одержувачу, в той

час, як ключ відправляється йому по закритому каналу, що гарантує таємність. Маючи ключ і шифрування, одержувач виконує розшифровування й відновлює вихідне повідомлення.

Криптографічні перетворення використовуються для досягнення двох цілей щодо захисту інформації. По-перше, вони забезпечують недоступність її для осіб, що не мають ключа, по-друге, підтримують із необхідною надійністю виявлення несанкціонованих підмін.

До необхідних аксесуарів криптографічної техніки, крім алгоритмів шифрування й розшифрування, належать секретні ключі. Їх роль така ж, як і в ключів від сейфа.

Наведемо кілька прикладів афінного шифрування, які використовують викладений алгебраїчний апарат.

Лінійний шифр. Розглянемо лінійний афінний шифр.

Домовимось, *що* $n-$*символьний алфавіт будемо ототожнювати зкільцем* $\mathbb{Z}/n\mathbb{Z}=\mathbb{Z}_n$, *тобто кожна буква замінюється своїм номером у алфавіті, причому нумерація починається з нуля*.

Наприклад, латинська абетка ототожнюється з $\mathbb{Z}_{26}$, а українська – із $\mathbb{Z}_{33}$. Літері **а** української абетки відповідає **0,** літері **б** – **1**, літері **в** – **2** і т.д. Тепер до букв відкритого тексту можна вільно застосовувати операції додавання та множення в кільці $\mathbb{Z}_{33}$.

Отже для лінійного шифру маємо:

Ключ: число a таке, що

- $0<a<n$;
- $\text{НСД}(a,n)=1$.

Шифрування: У повідомленні кожна буква x замінюється буквою $E(x)=\overline{ax}\equiv ax(\bmod n)$, тобто кожній букві x заданого алфавіту ставимо у відповідність представника класу $\overline{ax}$ у фактор-кільці $\mathbb{Z}_n$.

Дешифрування: У криптотексті кожна буква x' замінюється буквою $D(x') = \overline{a'x'} \equiv a'x' \pmod{n}$, де $a' \equiv a^{-1} \pmod{n}$ – дешифруючий ключ. Зауважимо, що рівність $a \equiv b \pmod{n}$ – це формальний запис еквівалентності чисел a і b в кільці $\mathbb{Z}_n$, тобто приналежність цих чисел до одного класу в $\mathbb{Z}_n$. Згодом ми пов'яжемо цей запис з конгруенціями.

Припустимо, що повідомлення записуються українською абеткою без пропусків та розділових знаків, тобто $n = 33$.

Приклад 1.2.19. Розглянемо процедуру шифрування української приказки

ВИЩЕ СЕБЕ НЕ ПІДСКОЧИШ

Використаємо ключ $a = 2$ (очевидно, що НСД$(2, 33) = 1$).

Шифрування. У цифровій формі, з використанням алфавіту в табл. 8, наша приказка має вигляд

2 10 29 621 6 1 617 619 11 5 21 14 18 27 10 28

Множення кожної цифри на 2 за модулем 33 дасть цифрову послідовність

4 20 25 129 12 2 121 12 5 22 10 9 28 3 21 20 23,

яка відповідає *криптотексту*

ҐРХЇ ЗЇВЇ БЇ ДТИЗШГСРУ

Дешифрування. Знайдемо дешифруючий ключ $2' = 2^{-1} \pmod{33}$.

Поділимо 33 на 2 з остачею. Маємо

$$33 = 2 \cdot 16 + 1,$$

звідки $1 = 33 - 2 \cdot 16$. Тому

$$2' = 2^{-1} \pmod{33} \equiv -16 \pmod{33} \equiv 17 \pmod{33}.$$

Отже дешифруючий ключ $2'=17$. Помножимо кожну цифру, що відповідає буквам криптотексту, на $17\pmod{33}$ і отримаємо послідовність чисел

2 10 29 621 6 1 617 619 11 5 21 14 18 27 10 28,

якій відповідає наша приказка.

Шифр Хілла. Не вдаючись до історії виникнення шифрів, яка є безумовно цікавою та вимагає детального аналізу, зупинимось на шифрі Хілла, який є *біграмним* і демонструє використання скінчених кілець.

Почнемо з вибору $n-$символьного алфавіту й кодуємо кожну букву одним із чисел з множини $\{0,1,2,...,n-1\}$. Якщо це український алфавіт, то $n=33$, якщо латинський, то $n=26$.

А 0	Б 1	В 2	Г 3	Г 4	Д 5	Е 6	Є 7	Ж 8	З 9	И 10
І 11	Ї 12	Й 13	К 14	Л 15	М 16	Н 17	О 18	П 19	Р 20	С 21
Т 22	У 23	Ф 24	Х 25	Ц 26	Ч 27	Ш 28	Щ 29	Ь 30	Ю 31	Я 32

Табл. 8

Поставимо у відповідність кожній біграмі (α,β) число

$$P=33\alpha+\beta\in\{0,1,2,...,33^2-1\}. \qquad (1.26)$$

Наприклад, біграмі «НІ» відповідає число $P=33\cdot17+11=572$. Далі введемо правила шифрування й лешифрування, тобто задамо функції шифрування й дешифрування, які повинні здійснювати ін'єктивне відображення:

$$P\xrightarrow{f}C\xrightarrow{f^{-1}}P,$$

де $P-$множина відкритих повідомлень (в цьому випадку бігам), але вже у формі чисел із кільця $\mathbb{Z}/33^2\mathbb{Z}=$

$\{0,1,2,...,33^2-1\}$. Отже функція шифрування повинна здійснювати перестановку на множині $\mathbb{Z}/33^2\mathbb{Z}$. Вибір функції шифрування f у шифрі Хілла вибрана у вигляді афінного перетворення

$$f(P)=C=aP+b(\mathrm{mod}\,33^2),$$

де $a,b\in\mathbb{Z}/33^2\mathbb{Z}$. Зауважимо, що алгебраїчна рівність $C=aP+b(\mathrm{mod}\,33^2)$ означає рівність елементів в кільці $\mathbb{Z}/33^2\mathbb{Z}$. В § 2.4 ми розглянемо конгруенції та їх властивості. Зв'язок конгруенцій із скінченими кільцями і виправдовує позначення $C=aP+b(\mathrm{mod}\,33^2)$

Для того, щоб існувало обернене відображення f^{-1} необхідно вимагати, щоб НСД$(a,33^2)=1$, тобто a і 33^2 були взаємно прості. А це означає, що в кільці $\mathbb{Z}/33^2\mathbb{Z}$ для елемента a існує обернений елемент a^{-1}(інверсія елемента a відносно числа 33^2).В цьому випадку

$$P=f^{-1}(C)=a^{-1}C-a^{-1}b\left(\mathrm{mod}\,33^2\right).$$

Приклад 1.2.20.Закодувати біграму «НІ» за допомогою функції шифрування $f(P)=5P+6\left(\mathrm{mod}\,33^2\right)$.

Оскільки НСД$(5,33)=1$, то так визначена функція шифрування – коректна, тобто здійснює ін'єктивне відображення. Отже, оскільки «НІ» $\to P=572$, то

$$f(P)=5\cdot 572+6\equiv 688\left(\mathrm{mod}\,33^2\right).$$

Зважаючи на те, що $688=33\cdot 20+28$, то коду $(20,28)$ відповідає біграма «РШ». Отже відкритий текст «НІ» переходить з допомогою функції шифрування f у шифрований текст «РШ».

Для того, щоб знайти функцію розшифрування f^{-1} потрібно знайти 5^{-1} за модулем $33^2 = 1089$, тобто інверсію числа 5 за модулем 1089. Це можна здійснити, використовуючи алгоритм Евкліда для чисел $33^2 = 1089$ і 5 в $\mathbb{Z}$ (див. приклад 1.2.16).Маємо

$$1089 = 5 \cdot 217 + 4,$$
$$5 = 4 \cdot 1 + 1,$$

Звідки $1 = 5 \cdot 128 - 1089$. Отже $5^{-1} \left(\mathrm{mod}\, 33^2\right) = 128$. Тому

$$f^{-1}(C) = f^{-1}(688) = 218 \cdot 688 - 218 \cdot 6 = 572 \left(\mathrm{mod}\, 33^2\right).$$

Повернувшись від числа 572 до біграми за правилом $P = 33\alpha + \beta,$, отримуємо

$$572 = 33 \cdot 17 + 11,$$

Тобто $\alpha = 17, \beta = 11,$ що є закодованим словом «HI».

Це означає, що одержувач криптотексту «РШ» швидко поставить йому у відповідність число 688 за правилом (1.26) та, використовуючи таблицю , і знаючи числа $5, 6$ за правилом знаходження f^{-1} знайде число $P = 572,$ якому відповідає біграма «HI».

Вибір параметрів a і b використовує частотний аналіз, який полягає в тому, що у довгій послідовності шифрованого тексту виділяють найчастіше уживані біграми й порівнюють їх з відомими частотами біграм українського тексту.

Лінійний шифр $k-$го порядку (Хілла). Відкрите повідомлення при такому шифруванні розбивається на $k-$грами. Кожній $k-$грамі ставимо у відповідність вектор X (тобто матриця розміру $k \times 1$). Криптотекст задається з допомогою *ключа* $A \in GL_k\left(\mathbb{Z}_n\right)$.

Нагадаємо, що $GL_k\left(\mathbb{Z}_n\right)$ – це множина оборотних матриць розміру $k \times k$ з коефіцієнтами з кільця $\mathbb{Z}_n = \mathbb{Z} / n\mathbb{Z},$

де n – число букв алфавіту, яким користуєтьсявідправник (для українського алфавіту $n = 33$, якщо не враховані пробіли чи розділові знаки).

Шифрування: З допомогою необоротної над $\mathbb{Z}_n$ матриці A знайдемо криптотекст $C = AX = X'$.

Дешифрування: $D(X') = D(AX) = A^{-1}X' = A^{-1}AX = X$, тобто дешифрування здійснюється з допомогою оберненої до матриці A над кільцем $\mathbb{Z}_n$ матриці A^{-1}.

Розглянемо докладніше випадок $k = 2$, тобто біграмний лінійний шифр. В якості ключа виберемо довільну матрицю

$$A = \begin{pmatrix} a & b \\ c & d \end{pmatrix} \in GL_2(\mathbb{Z}_n) \qquad (1.27)$$

з $\det A \neq 0$ і $\text{НСД}(\det A, n) = 1$.

Приклад 1.2.21. Нехай потрібно зашифрувати з допомогою біграмного лінійного шифру слово «ЗАВТРА» з ключем $A = \begin{pmatrix} 1 & 1 \\ 26 & 1 \end{pmatrix}$.

Розв'язання.Поставимо у відповідність біграмам «ЗА», «ВТ», «РА» вектори, використовуючи табл.1.

$$\text{«ЗА»} \to \begin{pmatrix} 9 \\ 0 \end{pmatrix};\ \text{«ВТ»} \to \begin{pmatrix} 2 \\ 22 \end{pmatrix};\ \text{«РА»} \to \begin{pmatrix} 20 \\ 0 \end{pmatrix}.$$

Отримаємо відкритий текст: $\begin{pmatrix} 9 & 2 & 20 \\ 0 & 22 & 0 \end{pmatrix}$. Знайдемо криптотекст, використовуючи ключ A. Отримаємо

$$\begin{pmatrix} 1 & 1 \\ 26 & 1 \end{pmatrix} \cdot \begin{pmatrix} 9 & 2 & 20 \\ 0 & 22 & 0 \end{pmatrix} (\text{mod}\, 33) = \begin{pmatrix} 9 & 24 & 20 \\ 3 & 8 & 25 \end{pmatrix}$$

Отже криптотекст – це стовпці: $\begin{pmatrix} 9 \\ 3 \end{pmatrix}, \begin{pmatrix} 24 \\ 8 \end{pmatrix}, \begin{pmatrix} 20 \\ 25 \end{pmatrix}$. Відповідні біграми за таблицею 1 – наступні: «ЗГ», «ФЖ»,

«РХ». Таким чином, одержувач отримав шифрований текст «ЗГФЖРХ».

Далі одержувач хоче розшифрувати його. Для цього потрібно знайти обернену до A матрицю за правилами лінійної алгебри. Така матриця існує, оскільки виконуються вимоги(1.27).Знайдемо

$$\det A \equiv 1-26 \pmod{33} \equiv -25 \pmod{33} \equiv 8 \pmod{33},$$

$$\text{НСД}(8,33)=1.$$

Тому

$$A^{-1} = 8^{-1}\begin{pmatrix} 1 & -1 \\ -26 & 1 \end{pmatrix} \equiv 8^{-1}\begin{pmatrix} 1 & 32 \\ 7 & 1 \end{pmatrix} \pmod{33}.$$

Знайдемо 8^{-1}, використовуючи ділення з остачею

$$33 = 8\cdot 4+1 \Rightarrow 1 = 33-8\cdot 4,$$

звідки отримуємо $8^{-1} \equiv -4 \pmod{33} \equiv 29 \pmod{33}$. Тому

$$A^{-1} \equiv \begin{pmatrix} 29 & 4 \\ 5 & 29 \end{pmatrix}.$$

Застосуємо до стовпців криптотексту матрицю A^{-1}. Маємо

$$\begin{pmatrix} 29 & 4 \\ 5 & 29 \end{pmatrix} \cdot \begin{pmatrix} 9 & 24 & 20 \\ 3 & 8 & 25 \end{pmatrix} = \begin{pmatrix} 9 & 2 & 20 \\ 0 & 22 & 0 \end{pmatrix}.$$

Отже ми прийшли до відкритого тексту «ЗАВТРА».

Приклад 1.2.22.Олексій отримав криптотекст «ЛУКЩГС» і ключ $A = \begin{pmatrix} 1 & 2 & 3 \\ 1 & 4 & 7 \\ 3 & 6 & 10 \end{pmatrix}$. Розшифрувати цей криптотекст.

Розв'язання. Знайдемо тривимірні вектори, які відповідають 3-грамам «ЛУК», «ЩГС», використовуючи таблицю 1.

$$\text{«ЛУК»} \to \begin{pmatrix} 15 \\ 23 \\ 14 \end{pmatrix}, \text{«ЩГС»} \to \begin{pmatrix} 29 \\ 3 \\ 21 \end{pmatrix}.$$

Знайдемо обернену до A матрицю A^{-1} з елементами кільця $\mathbb{Z}_{33}$. Спочатку обчислимо $\det A = 2$. Для побудови A^{-1} потрібно знайти 2^{-1}. Легко переконатись, як і в попередньому прикладі, що $2^{-1} \pmod{33} \equiv 17$ і обернена матриця має вигляд

$$A^{-1} \equiv 17 \begin{pmatrix} 31 & 31 & 2 \\ 11 & 1 & 29 \\ 27 & 0 & 2 \end{pmatrix} \pmod{33}.$$

Знайдемо добуток матриць

$$17 \begin{pmatrix} 31 & 31 & 2 \\ 11 & 1 & 29 \\ 27 & 0 & 2 \end{pmatrix} \cdot \begin{pmatrix} 15 & 29 \\ 23 & 3 \\ 14 & 21 \end{pmatrix} = \begin{pmatrix} 9 & 22 \\ 0 & 20 \\ 2 & 0 \end{pmatrix},$$

якийрозкриває надісланий текст. Маємо

$$\begin{pmatrix} 9 \\ 0 \\ 2 \end{pmatrix} \to \text{«ЗАВ»} \begin{pmatrix} 22 \\ 20 \\ 0 \end{pmatrix} \to \text{«ТРА»}$$

і надісланий текст розшифровано, це – «ЗАВТРА»

На жаль, стандартний лінійний шифр Хілла вразливий до атаки за обраним відкритим текстом. Криптоаналітик, який перехопить n^2 пар символів повідомлення зможе скласти систему лінійних рівнянь, яку зазвичай нескладно розв'язати. Якщо система виявиться несумісною, то необхідно додати ще кілька пар символів повідомлення. Розрахунки такого характеру засобами алгоритмів лінійної алгебри вимагає небагато часу.

Тому запропонований алгоритм шифрування носить навчально-тренувальний характер.

1.3.Поля

1.3.2. *Основні відомості з теорії полів.*

Нехай F – поле і $P \subset F$.

Визначення 1.3.1 Якщо P – поле з операціями, індукованими з поля F (тими ж, як і у полі F) , то P називається «*підполем*» поля F , а F «*надполем*» або *розширенням поля* P .

Той факт, що поле F є розширенням поля P, позначається $F : P$.

Визначення 1.3. 2. *Простим* або *елементарним полем* називається поле, яке не має власних «підполів».

Опишемо всі елементарні підполя в полі F.

Нехай P – елементарне підполе в полі K. Оскільки «1» $\in P$, то

$$n \cdot 1 = 1 + 1 + \cdots + 1 \in P,$$

$$-n \cdot 1 = -(n \cdot 1) \in P,$$

і тому $n \cdot 1 \in P$ для довільного $n \in \mathbb{Z}$. Рівності

$$n \cdot 1 + m \cdot 1 = (n + m) \cdot 1,$$

$$n \cdot 1 \cdot m \cdot 1 = (n \cdot m) \cdot 1$$

породжують гомоморфізм:

$$\lambda : \mathbb{Z} \supset n \to n \cdot 1 \in P \qquad (1.28)$$

Тут можливі два варіанти:

- ядро гомоморфізму (1.28)

$$Ker\lambda = \{n : \lambda(n) = n \cdot 1 = 0\} \neq \{0\}.$$

Тоді, оскільки ядро гомоморфізму – це головний ідеал в множині $\mathbb{Z}$, то $Ker\lambda = m\mathbb{Z}$, який породжує гомоморфізм $\mathbb{Z} / Ker\lambda \simeq \operatorname{Im}\lambda$ (теорема 1.1.12).

Такий випадок ми розглядали в § 1.2.для гомоморфізму кілець $\lambda : \mathbb{Z} \to \mathbb{Z} / m\mathbb{Z} = \{\bar{0}, \bar{1}, \bar{2}, ..., \overline{m-1}\}$. В цьому випадку

кожному $n \in \mathbb{Z}$ гомоморфізм λ ставив у відповідність $\lambda(n) = \bar{1} \cdot n = (1 + m\mathbb{Z}) \cdot n$ і очевидно, що $Ker\lambda = m\mathbb{Z} \neq \{0\}$.

Оскільки $\mathrm{Im}\,\lambda \subset P$, то $\mathrm{Im}\,\lambda \simeq \mathbb{Z}/m\mathbb{Z}$ не має дільників нуля. Тому $m -$ просте число із $\mathbb{Z}$. Отже $\mathbb{Z}/m\mathbb{Z} = \mathbb{Z}/p\mathbb{Z} \simeq \mathrm{Im}\,\lambda \subset P -$ поле (Твердження 1.2.1.).

• ядро гомоморфізму (1.28) $Ker\lambda = \{0\}$. Тоді $\mathbb{Z} \simeq \mathrm{Im}\,\lambda \subset P$ і тому елементарне поле P ізоморфне полю раціональних чисел $\mathbb{Q}$.

Таким чином приходимо до висновку: *елементарними полями* є лише наступні поля:

• $\mathbb{Q}$ *– поле раціональних чисел;*

• *скінченні поля* $\mathbb{Z}/p\mathbb{Z} = F_p$, *де* $p -$ *просте число*.

В алгебраїчній і літературі з криптографії часто поле F_p позначають $GF(p)$.

Визначення 1.3.3. Найменше $p \in N$ ($N -$ сукупність додатних цілих чисел) таке, що $p \cdot 1 = 0$, називається характеристикою поля F і позначається $charF$.

Справедливим є

Твердження 1.3.1. $[1, 2, 6]$

• $charF = 0$ тоді і тільки тоді, коли $F -$ розширення поля раціональних чисел $\mathbb{Q}$;

• $charF = p > 0$ тоді і тільки тоді, коли $F -$ розширення поля $\mathbb{Z}/p\mathbb{Z} = F_p$.

Визначення 1.3.4. Нехай $P \subset F$, $\alpha \in F$. Поле, утворене можливими раціональними комбінаціями елемента α, назвемо «простим розширенням» поля P і позначимо $P(\alpha)$.

Очевидно, що

$$P(\alpha)=\left\{\frac{f(\alpha)}{g(\alpha)}: f,g\in k[x],\quad g(\alpha)\neq 0\right\}.$$

Визначення 1.3.5.Елемент $\alpha\in F$ називається алгебраїчним над полем P, якщо існує многочлен $g\in k[X]$ такий , що $g(\alpha)=0.$

Визначення 1.3.6.Нехай $F:P$ і $\alpha\in F$. В множині

$$\{g(X)\in K[X],\quad g(\alpha)=0\}$$

виберемо многочлен найменшого степеня зі старшим коефіцієнтом одиницею. Такий многочлен називається *мінімальним многочленом* елемента α.

Справедлива наступна

Теорема 1.3.1. Нехай $F:P$, $\alpha\in F-$алгебраїчний елемент над P, а $f(X)\in P[X]-$ мінімальний многочлен елемента α. Тоді

- кожен многочлен $g(X)\in F[X]$, для якого $g(\alpha)=0,$ ділиться на $f(X)$;
- мінімальний многочлен визначений однозначно;
- мінімальний многочлен *незвідний* над полем P;

*Доведення***.** Дійсно,

- Нехай $g(\alpha)=0$. Поділимо $g(X)$ на $f(X)$ з остачею.
  $g(X)=f(X)\cdot q(X)+r(X),\quad \deg r(X)<\deg f(X).$
  Тоді $g(\alpha)=r(\alpha)=0$. Оскільки $\deg r(X)<\deg f(X)$, то $r(X)=0.$
- Нехай f і f_1- два мінімальні многочлени елемента α. Отже $\deg f=\deg f_1$. Тому $f_1(X)=f(X)\cdot q(X).$ Оскільки $\deg q(X)=0,$ то $q(X)=1,$ тобто $f_1=f.$

• Якщо б мінімальний многочлен f розкладався на множники($f(X)=g(X)\cdot h(X)$), то α був би коренем або $g(X)$, або $h(X)$, що заперечує мінімальність $f(X)$.

Визначення 1.3.7. Степінь мінімального многочлена алгебраїчного елемента α називається *степенем елемента* α і позначається $\deg\alpha$.

Довільний інший корінь α' мінімального многочлена алгебраїчного елемента α називається *спряженим* до α.

Визначення 1.3.7. Нехай $F:P.$ Тоді F можна розглядати, як *векторний простір* над полем $k.$ Розмірність цього простору позначимо $[F:P]$ і назвемо *степенем* F над P або *степенем розширення.*

Якщо степінь $[F:P]-$ скінченний, то розширення називається *скінченним*, в іншому випадку розширення називається *нескінченним.*

Степені трьох полів пов'язує

Теорема 1.3.2.[1,2,4,6] Нехай $P,F,L-$ три поля, для яких $P\subset F\subset L.$ Тоді

$$[L:F]\cdot[F:P]=[L:P].$$

Визначення 1.3.8. Нехай $F:P.$ Якщо кожний елемент поля F алгебраїчний над $P,$ то таке розширення називається *алгебраїчним.*

Теорема 1.3.3. Кожне скінченне розширення поля – алгебраїчне.

Дійсно, нехай $F-$ скінченне розширення поля P і $[F:P]=n.$ Якщо $\alpha\in F-$ довільний елемент, то множина $\{\alpha^0,\alpha^1,\alpha^2,...,\alpha^n\}-$ лінійно залежна, бо містить $n+1$ елементів. Отже існують такі (не всі рівні нулю) елементи $a_0,a_1,a_2,...,a_n\subset P$, що $a_0+a_1\alpha+a_2\alpha^2+...+a_n\alpha^n=0$

(визначення лінійної залежності). Тому елемент $\alpha-$ алгебраїчний над P.

Справедлива важлива

Теорема 1.3.4. Нехай поле F – розширенням поля P, $\alpha-$ алгебраїчний над P і $p(X)\in P[X]-$ мінімальний многочлен для α. Тоді:

- розширення $P(\alpha)-$ скінчене над P, при цьому $[P(\alpha):P]=\deg p(X)$;
- $P(\alpha)\simeq P[X]\big/\big(p(X)k[X]\big)$, тобто розширення поля $P(\alpha)$ ізоморфне фактор-кільцю кільця многочленів $P[X]$ за головним ідеалом цього кільця, що породжений мінімальним многочленом $p(X)$.

Доведення. Розглянемо гомоморфізм підстановки τ

$$\tau: f(X)\to f(\alpha)\in F,\quad f(X)\in P[X]$$

Оскільки елемент $\alpha-$ алгебраїчний над P, то $Ker\tau\neq\{0\}-$ головний ідеал в $P[X]$, а так як $P[X]$ є кільцем головних ідеалів, а ядро гомоморфізму є ідеалом в $P[X]$, то

$$Ker\tau=\big(q(X)\big)=q(X)P[X] \qquad (1.29)$$

для деякого $q(X)\in P[X]$. З (1.29) випливає, що $q(\alpha)=0$. Отже, за теоремою 1.3.1, многочлен $q(X)$ ділиться на мінімальний многочлен $p(X)$ і тому $Ker\tau=\big(p(X)\big)=p(X)P[X]$.

За властивістю гомоморфізму кілець маємо

$$P[X]\big/\big(p(X)P[X]\big)\simeq \operatorname{Im}\tau.$$

Оскільки $p(X)$ – незвідний над P (тобто $p(X)$ – простий елемент в $P[X]$), то $\mathrm{Im}\,\tau$ – поле і $P(\alpha) \simeq P[X] \big/ \big(p(X)P[X]\big)$. Отже доведений 2-й пункт твердження теореми.

Доведемо перший. Нехай $\deg p(X) = n$. Тоді елементи $1, \alpha, \alpha^2, ..., \alpha^{n-1}$ – лінійно незалежні і утворюють базу в $P[\alpha]$ [6]. Для кожного $f(\alpha) \in P[\alpha]$, де $f(X) \in P[X]$ знайдуться такі $q(X)$ і $r(X)$, що

$$f(X) = q(X) \cdot p(X) + r(X), \quad \deg r(X) < n.$$

Отже $f(\alpha) = r(\alpha)$. Тому $r(\alpha)$ виражається через $1, \alpha, \alpha^2, ..., \alpha^{n-1}$. Ці елементи породжують $P[\alpha]$, що й завершує доведення теореми.

Зауважимо, що теорема 1.3.4. – конструктивна. Вона дає можливість будувати поля $P(\alpha)$. Для цього потрібно:

- найти мінімальний многочлен $p(X)$ для α;
- визначити його степінь;
- сконструювати поле

$P(\alpha) = \left\{\beta = c_0 + c_1\alpha + c_2\alpha^2 + \cdots + c_{n-1}\alpha^{n-1}, \quad c_i \in P\right\}$ з використанням співвідношення $p(\alpha) = 0$.

1.3.2. Скінченні поля.

Поле називається *скінченним,* якщо множина його елементів – скінченна.

Твердження 1.3.2.

• Довільне скінченне поле F характеристики p містить просте підполе з p елементів і є його скінченним розширенням.

• Число елементів скінченного поля F характеристики p дорівнює $q = p^n$.

Доведення першого твердження випливає з попередніх міркувань.

Доведемо друге. Оскільки F – скінчене розширення поля F_p, то F – векторний простір над F_p. Отже, існує база $h_1, h_2, ..., h_n$ така, що для довільного $h \in F$ маємо

$$h = a_1 \cdot h_1 + a_2 \cdot h_2 + \cdots + a_n \cdot h_n, \qquad (1.30)$$

де a_i, $i = \overline{1,n}$ – елементи з F_p і число елементів в (1.30) дорівнює p^n. Тому $q = p^n$, і $F = F_q$.

Твердження 1.3.3. $[1,6]$ Нехай F – поле характеристики p. Тоді для $a, b \in K$ справедливі рівності:

$$(a \pm b)^p = a^p \pm b^p.$$

Дійсно,

$$(a+b)^p = a^p + C_p^1 a^{p-1} b + \cdots + C_p^k a^{p-k} b^k + \cdots + b^k = a^p + b^p,$$

оскільки C_p^k ділиться на p.

Наслідок з твердження 1.3.3. $[6]$ Нехай F – поле характеристики p. Тоді для $a, b \in K$ справедливі рівності:

$$(a \pm b)^{p^n} = a^{p^n} \pm b^{p^n}.$$

Доведення виконаємо індукцією за n. Дійсно

$$(a \pm b)^{p^n} = \left[(a \pm b)^{p^{n-1}} \right]^p = \left(a^{p^{n-1}} \pm b^{p^{n-1}} \right)^p = a^{p^n} \pm b^{p^n}.$$

Визначення 1.3.10. Полем розкладу H многочлена $f(x)$ над полем F називається поле, в якому многочлен $f(x)$ розкладається на лінійні множники.

Виникає запитання, як конструктивно описати скінченні розширення поля F_p. Відповідь на це запитання дає наступна теорема.

Теорема 1.3.5. Нехай $p-$ просте число, $n-$ натуральне число, а $q=p^n$. Тоді поле розкладу H многочлена $f=x^q-x$ над полем F_p- це скінченне поле, що складається з $q=p^n$ елементів.

Доведення. Розглянемо многочлен $f=x^q-x$. Легко перевірити, що сума, різниця, добуток і частка коренів x і y многочлена f є також коренями цього многочлена. Тому множина всіх коренів многочлена $f=x^q-x$ утворює підполе в полі H. Оскільки $f'=qx^{q-1}-1=-1\neq 0,$ то всі корені многочлена $f-$ різні, тобто поле містить $q=p^n$ елементів$[6]$.

Наслідок з теореми 1.3.5. Для довільного натурального n і простого p існує скінченне поле, що містить $q=p^n$ елементів. Цим полем є поле розкладу многочлена $f=x^q-x$.

Наведемо без доведення два твердження про мультиплікативні групи (групи відносно операції «$\cdot$») скінченного поля, які можуть бути корисними при конструктивній побудові скінченних полів$[1,2,4,6]$.

Твердження 1.3.4. Нехай $F-$поле, $F^\times-$ мультиплікативна група поля F. Множина

$$G=\{a\in F:\quad a^n=1\}$$

всіх коренів $n-$го степеня з 1 утворює скінчену підгрупу в $F^\times$.

Твердження 1.3.5. Довільна скінчена підгрупа Γ мультиплікативної групи довільного поля F – циклічна.

1.3.3. Побудова скінченних полів

Побудова скінченних полів базується на теоремі 1.3.4. і основних відомостях про скінченні поля.

Основою такої побудови є наступні твердження:

1. Довільне скінченне поле має характеристику $p > 0$ і складається з p^n елементів.

2. Якщо $f(x)-$ незвідний многочлен $n-$го степеня , коефіцієнти якого належать полю F_p, а $\alpha-$його корінь , то $F_{p^n} = F_p(\alpha)-$ це лінійний простір розмірності n над полем F_p з базою $1, \alpha, \alpha^2, ..., \alpha^{n-1}$, тобто

$$F_{p^n} = \left\{ a_0 + a_1\alpha + a_2\alpha^2 + \cdots + a_{n-1}\alpha^{n-1}, \quad f(\alpha) = 0 \right\}, \quad a_i \in F_p,\ i = \overline{0, n-1}. \tag{1.31}$$

3. Якщо $F-$ скінченне поле, що складається з p^n елементів, то його мультиплікативна група $F^\times -$ циклічна і породжена деяким елементом ξ який називається *примітивним елементом* поля K, тобто

$$F^\times = \left\{ 1, \xi, \xi^2, ..., \xi^{p^n-1} \right\}, \quad \xi^{p^n} = 1. \tag{1.32}$$

Число l примітивних коренів поля F визначене рівністю

$$l = \varphi\left(p^n - 1\right), \tag{1.33}$$

де $\varphi(x)-$ функція Ейлера.

На основі цих тверджень побудуємо конкретні скінчені поля.

Приклад 1.3.1. Побудувати поле $F_9 = F_{3^2}$.

Згідно твердження 2 для побудови поля F_9 потрібно знайти незвідний над F_3 многочлен $f(x)$ 2-го степеня. Таким многочленом є, наприклад, многочлен $f(x)=x^2+1$. Нехай $u-$ його корінь. Тоді за формулою (1.31) маємо

$$F_9 = F_3(u) = \{a_0 + a_1 u, \quad a_0, a_1 \in F_3, \quad u^2 = 2\} =$$
$$= \{0,1,2,u,2u,1+u,1+2u,2+u,2+2u\}.$$

Можна перевірити, що одним із примітивних елементів поля є $\xi = 1+u$. Дійсно

$$\xi^0 = 1, \quad \xi^1 = 1+u, \quad \xi^2 = 1+2u+u^2 = 2u,$$
$$\xi^3 = 2u(1+u) = 2u+2u^2 = 2u+1,$$
$$\xi^4 = 4u^2 = 2,$$
$$\xi^5 = 2(u+1) = 2u+2,$$
$$\xi^6 = 2(u+1)^2 = \text{u}, \quad \xi^7 = u(u+1) = 2+u.$$

Таким чином, степенями ξ вичерпані всі ненульові елементи поля F_9.

Зауважимо, що поле F_9 має чотири примітивні елементи, бо за формулою (1.33) $l = \varphi(8) = 4$. Цими елементами є:

$$\xi_1 = 1+u, \quad \xi_2 = 1-u = 1+2u, \quad \xi_3 = 2+u, \quad \xi_4 = 2-u = 2+2u.$$

Для прикладу 1.3.1 можна написати таблиці додавання і множення, які дозволять миттєво відшукати протилежні та обернені елементи до всіх елементів поля:

Додавання

0	1	2	u	$u+1$	$u+2$	$2u$	$2u+1$	$2u+2$
1	2	0	$u+1$	$u+2$	u	$2u+1$	$2u+2$	$2u$
2	0	1	$u+2$	u	$u+1$	$2u+2$	$2u$	$2u+1$
u	$u+1$	$u+2$	$2u$	$2u+1$	$2u+2$	0	1	2
$u+1$	$u+2$	u	$2u+1$	$2u+2$	$2u$	1	2	0
$u+2$	u	$u+1$	$2u+2$	$2u$	$2u+1$	2	0	1
$2u$	$2u+1$	$2u+2$	0	1	2	u	$u+1$	$u+2$
$2u+1$	$2u+2$	$2u$	1	2	0	$u+1$	$u+2$	u
$2u+2$	$2u$	$2u+1$	2	0	1	$u+2$	u	$u+1$

Таб.9

Множення

1	2	u	$u+1$	$u+2$	$2u$	$2u+1$	$2u+2$
2	1	$2u$	$2u+2$	$2u+1$	u	$u+2$	$u+1$
u	$2u$	2	$u+2$	$2u+2$	1	$u+1$	$2u+1$
$u+1$	$2u+2$	$u+2$	$2u$	1	$2u+1$	2	u
$u+2$	$2u+1$	$2u+2$	1	u	$u+1$	$2u$	2

$2u$	u	1	$2u+1$	$u+1$	2	$2u+2$	$u+2$
$2u+1$	$u+2$	$u+1$	2	$2u$	$2u+2$	u	1
$2u+2$	$u+1$	$2u+1$	u	2	$u+2$	1	$2u$

Таб.10

Знайдемо, наприклад, з таблиці 9 елемент поля F_9 – протилежний до елемента $2u+1$, тобто елемент $-(2u+1)$. Оскільки $(2u+1)+(u+2)=0$, то $-(2u+1)=u+2$.

Аналогічно, знайдемоз таблиці 10 елемент поля F_9 – обернений до елемента $2u+1$, тобто елемент $(2u+1)^{-1}$. Оскільки $(2u+1)\cdot(2u+2)=1$, то $(2u+1)^{-1}=2u+2$.

Приклад 1.3.2. Використовуючи незвідний над F_2 многочлен $f=x^3+x+1$, побудувати поле $F_{2^3}=F_8$.

Легко переконатись, що $f(x)=x^3+x+1$ – незвідний над полем F_2. Нехай α – його корінь. Тоді за (1.31) маємо

$$F_8=F_2(\alpha)=\{0,1,\alpha,1+\alpha,\alpha^2,\alpha^2+1,\alpha^2+\alpha,\alpha^2+\alpha+1\}$$

Для поля F_8 можна також скласти таблиці додавання та множення. Наведемо таблицю множення. (Таблицю додавання скласти самостійно)

1	α	$\alpha+1$	α^2	α^2+1	$\alpha^2+\alpha$	$\alpha^2+\alpha+1$
α	α^2	$\alpha^2+\alpha$	$\alpha+1$	1	$\alpha^2+\alpha+1$	α^2+1

$\alpha+1$	$\alpha^2+\alpha$	α^2+1	$\alpha^2+\alpha+1$	α^2	1	α
α^2	$\alpha+1$	$\alpha^2+\alpha+1$	$\alpha^2+\alpha$	α	α^2+1	1
α^2+1	1	α^2	α	$\alpha^2+\alpha+1$	$\alpha+1$	$\alpha^2+\alpha$
$\alpha^2+\alpha$	$\alpha^2+\alpha+1$	1	α^2+1	$\alpha+1$	α	α^2
$\alpha^2+\alpha+1$	α^2+1	α	1	$\alpha^2+\alpha$	α^2	$\alpha+1$

Таб.11

Можна перевірити, що мультиплікативна група $F_8^{\times}$ поля F_8 – це циклічна група 7-го порядку з твірним елементом α Дійсно,

$$\alpha^3=\alpha+1,\quad \alpha^4=\alpha^2+\alpha,\quad \alpha^5=\alpha^3+\alpha^2,\quad \alpha^6=\alpha^2+1,\quad \alpha^7=1.$$

Кількість примітивних елементів в цьому випадку дорівнює $\varphi(7)=6,$ тобто це всі, відмінні від одиниці, елементи поля.

Приклад 1.3.3. Побудувати поле $F_{16}=F_{2^4}$.

Використаємо незвідний многочлен 4-го степеня $f(x)=x^4+x+1$ над полем F_2. Нехай α – його корінь. Тоді, за (1.31), маємо

$$F_{16}=F_2(\alpha)=\left\{a_0+a_1\alpha+a_2\alpha^2+a_3\alpha^3,\quad \alpha^4+\alpha+1=0\right\}=$$

$$=\left\{0,1,\alpha,1+\alpha,\alpha^2,1+\alpha^2,\alpha+\alpha^2,\right\}\cup$$

$$\cup\left\{\begin{matrix}1+\alpha+\alpha^2,\alpha^3,1+\alpha^3,1+\alpha+\alpha^3,\alpha^2+\alpha^3,\\ 1+\alpha^2+\alpha^3,\alpha+\alpha^2+\alpha^3,\alpha+\alpha^3,1+\alpha+\alpha^2+\alpha^3\end{matrix}\right\}.$$

Легко перевірити, що один з примітивних елементів поля за формулою (1.32) в F_{16} – це $\xi = \alpha$. Іншими примітивними елементами поля є:

$$\alpha^2, 1+\alpha, 1+\alpha^2, 1+\alpha+\alpha^3, \alpha+\alpha^2+\alpha^3, 1+\alpha^2+\alpha^3, 1+\alpha^3,$$

оскільки за (1.33) $l = \varphi(15) = 8$.

Через те, що операції в полі F_{16} не задані таблицями, подібними до таблиць 9-11, то відшукання оберненого до довільного елемента цього поля проводимо за наступною схемою.

Оскільки для довільного $h(x) \in F_{16}[X]$ НСД$(h, f) = 1$, то існують многочлени $u(x)$ і $v(x)$ такі, що

$$f(x)\cdot u(x) + h(x)\cdot v(x) = 1.$$

Оскільки $f(\alpha) = 0$, $h(\alpha)\cdot v(\alpha) = 1$, то $h^{-1}(\alpha) = v(\alpha)$.

Наприклад, знайдемо обернений до елемента $\alpha^3 + \alpha + 1$. Маємо

$$\alpha^4 + \alpha + 1 = (\alpha^3 + \alpha + 1)\alpha + \alpha^2 + 1,$$

$$\alpha^3 + \alpha + 1 = (\alpha^2 + 1)\alpha + 1.$$

Отже,

$$(\alpha^3 + \alpha + 1)(\alpha^2 + 1) - (\alpha^4 + \alpha + 1)\alpha = 1.$$

Тому $(\alpha^3 + \alpha + 1)^{-1} = \alpha^2 + 1$.

Приклад 1.3.4. Побудувати поле $F_{49} = F_{7^2}$. Поле F_{7^2} є лінійним простором розмірності 2 над полем F_7. Побудуємо це поле, використавши незвідний многочлен 2-го степеня $p(X) = X^2 + 1$ над полем F_7. Нехай X – корінь многочлена $p(X) = X^2 + 1$. Тоді за формулою (1) отримаємо

$$F_{7^2} = \{a_0 + a_1 X, \quad a_0, a_1 \in F_7, \quad X^2 + 1 = 0\}.$$

Можна переконатись, що мультиплікативна група поля F_{7^2} – циклічна група порядку 48 з примітивним елементом, наприклад, $\alpha = 2X + 1$. Дійсно,

$$\alpha^2 = 4X + 4, \quad \alpha^3 = 5X + 3, \quad \alpha^4 = 4X, \quad \alpha^5 = 4X + 6,$$
$$\alpha^6 = 2X + 5, \quad \alpha^7 = 5X + 1 \quad \alpha^8 = 5,$$
$$\alpha^9 = 3X + 5, \quad \alpha^{10} = 6X + 6, \quad \alpha^{11} = 4X + 1, \quad \alpha^{12} = 6X,$$
$$\alpha^{13} = 6X + 2, \; \alpha^{14} = 3X + 4, \; \alpha^{15} = 4X + 5,$$
$$\alpha^{16} = 4, \quad \alpha^{17} = X + 4, \quad \alpha^{18} = 2X + 2, \quad \alpha^{19} = 6X + 5, \; \alpha^{20} = 2X,$$
$$\alpha^{21} = 2X + 3, \quad \alpha^{22} = X + 6,$$
$$\alpha^{23} = 6X + 4, \quad \alpha^{24} = 6, \quad \alpha^{25} = 5X + 6, \quad \alpha^{26} = 3X + 3,$$
$$\alpha^{27} = 2X + 4, \; \alpha^{28} = 3X,$$
$$\alpha^{29} = 3X + 1, \quad \alpha^{30} = 5X + 2, \quad \alpha^{31} = 2X + 6, \quad \alpha^{32} = 2,$$
$$\alpha^{33} = 4X + 2, \; \alpha^{34} = X + 1, \; \alpha^{35} = 3X + 6,$$
$$\alpha^{36} = X, \quad \alpha^{37} = X + 5, \quad \alpha^{38} = 4X + 3, \quad \alpha^{39} = 3X + 2,$$
$$\alpha^{40} = 3, \quad \alpha^{41} = 6X + 3, \quad \alpha^{42} = 5X + 5,$$
$$\alpha^{43} = X + 2, \quad \alpha^{44} = 5X, \quad \alpha^{45} = 5X + 4, \quad \alpha^{46} = 6X + 1,$$
$$\alpha^{47} = X + 3, \quad \alpha^{48} = 1.$$

Таким чином, ми перебрали усі 48 елементів мультиплікативної групи поля $F_{49} = F_{7^2}$, тобто побудували це поле.

Зауважимо, що за формулою (1.33), в полі F_{7^2} існує $l = \varphi(48) = 16$ примітивних елементів. Це такі елементи:

$$\alpha = 2X + 1, \; \alpha^5 = 4X + 6, \; \alpha^7 = 5X + 1, \; \alpha^{11} = 4X + 1,$$
$$\alpha^{13} = 6X + 2, \; \alpha^{17} = X + 4, \; \alpha^{19} = 6X + 5,$$
$$\alpha^{23} = 6X + 4, \; \alpha^{25} = 5X + 6, \; \alpha^{29} = 3X + 1, \; \alpha^{31} = 2X + 6,$$
$$\alpha^{35} = 3X + 6, \; \alpha^{37} = X + 5, \; \alpha^{41} = 6X + 3,$$

$$\alpha^{43} = X + 2, \quad \alpha^{47} = X + 3.$$

Зауважимо, що теорія скінченних полів має широке застосування в криптографії. Відомо [9,10,13–19], що є багато криптологічних протоколів і криптосистем, що базуються на застосуванні скінченних полів. Сюди відносяться схеми Ель-Гамаля, Advanced Encryption Standard, схема Шнорра, алгоритм Чаума, криптосистема XTR та ряд інших.

Дослідження многочленів над скінченими полями привели до створення коду БЧХ, частинним випадком якого є широко відомий код Ріда-Соломона, що має широке застосування в криптографії.

Розділ 2. Теорія чисел.

2.1. Елементарні поняття теорії чисел.

Теорія чисел займається вивченням цілих чисел. Цілими числами називаються числа: $0, \pm1, \pm2, \pm3, ..., \pm n, ...$ Множину цілих чисел позначимо

$$\mathbb{Z} = \{0, \pm1, \pm2, \pm3, ..., \pm n, ...\}, \qquad (2.1)$$

а самі числа позначатимемо малими літерами латинського алфавіту $a, b, c, ...$

Сума, різниця і добуток цілих чисел – ціле число. Проте, частка цілих чисел може виявитись і не цілим числом.

В тому випадку, коли частка від ділення a на b – ціле число, позначимо його буквою q. Тоді маємо

$$a = bq, \qquad (2.2)$$

скажемо, що a ділиться на b, або b ділить a і позначимо це так

$$b \mid a. \qquad (2.3)$$

При цьому число a називають *кратним* числа b, а число b – *дільником* числа a.

Наведемо найпростіші властивості подільності цілих чисел:

1. $\forall a \in \mathbb{Z}\ a \mid a, 1 \mid a$;
2. якщо $a \mid b$ і $b \mid a$, то $a = \pm b$;
3. якщо $b \mid a$ і $c \mid b$, то $c \mid a$ – властивість транзитивності;
4. якщо $c \mid a$ і $c \mid b$, то $c \mid a \pm b$;
5. якщо $b \mid a$, то $c \mid ab\ \forall b \in \mathbb{Z}$.

Важливу роль в теорії подільності цілих чисел відіграє наступна теорема про «ділення з остачею».

Теорема 2.1.1 Довільне ціле число a єдиним чином можна подати у вигляді:

$$a = bq + r, \quad 0 \le r < b \qquad (2.4)$$

Число q називається *неповною часткою,* а число r – *остачею.*

Дійсно, одне із зображень числа a в такій формі отримаємо, взявши за bq найбільше кратне числа b, що не перевищує a.

Єдиність зображення (2.4) випливає з наступних міркувань: якщо a має інше зображення

$$a = b_1 q_1 + r_1, \quad 0 \le r_1 < b_1 \ , \qquad (2.5)$$

то, віднімаючи (2.5) від (2.4), отримаємо

$$0 = b(q - q_1) + r - r_1$$

і отже $b \mid r - r_1$. Оскільки $|r - r_1| < b,$ то це можливо тільки за умови $r = r_1$, а отже $q = q_1$.

Приклад 2.1.1. Нехай $a = 144, \quad b = 14$

Тоді $117 = 14 \cdot 12 + 9, \quad 0 < 9 < 14$ і тому 12 – неповна частка, а 9 – остача.

НСД, алгоритм Евкліда

Визначення 2.1.1. Надалі будемо розглядати тільки додатні числа. Довільне ціле число, яке ділить одночасно цілі числа $a, b, ..., m$ називається їх *спільним дільником.*

Визначення 2.1.2. Найбільший із спільних дільників називається *найбільшим спільним дільником* і позначається НСД$(a, b, ..., m)$, або простіше

$$(a, b, ..., m) \qquad (2.6)$$

Визначення 2.1.3. Якщо $(a,b,...,m)=1$, то числа $a,b,...,m$ називаються *взаємно простими.*

Визначення 2.1.4.Якщо кожне з чисел $a,b,...,m$ – взаємно просте з кожним іншим з них, то числа $a,b,...,m$ називаються *попарно простими*.

Очевидно, що попарно прості числа завжди і взаємно прості, проте протилежне твердження, взагалі кажучи, невірне. У випадку двох чисел поняття «*попарно прості*» і «*взаємно прості*» співпадають.

Приклад 2.1.2.

- Числа $6,10,15$ – взаємно прості, бо $(6,10,15)=1$, хоч і не є попарно простими, оскільки $(6,10)=2,\ (6,15)=3\ \ (10,15)=5.$
- Числа $8,13,21$ – попарно прості, бо $(8,13)=1\ \ (8,21)=1\ \ (13,21)=1,$ а отже $8,13,21$ – взаємно прості.

Вкажемо деякі властивості спільних дільників.

1. Якщо $a\,|\,b$, то $(a,b)=b.$
2. Якщо $a=bq+r$, то $(a,b)=(b,c)$.
3. Алгоритм Евкліда застосовується для знаходження (a,b).

Використовуючи формулу ділення з остачею (2.5), матимемо ряд рівностей:

$$\begin{aligned} &a=bq_1+r_2, \quad 0<b<r_2,\\ &b=r_2q_2+r_3, \quad 0<r_3<r_2,\\ &r_2=r_3q_3+r_4, \quad 0<r_4<r_3,\\ &\ldots\ldots\ldots\ldots\ldots\ldots\ldots \qquad (2.7)\\ &r_{n-2}=r_{n-1}q_{n-1}+r_n, \quad 0<r_n<r_{n-1}, \end{aligned}$$

$$r_{n-1} = r_n q_n.$$

Цей ряд скінчений, оскільки $b > r_2 > r_3 > \cdots > r_{n-1} > \cdots$ і не може складатись із більшого числа, ніж b чисел. Використовуючи властивість 2, отримаємо:

$$(a,b) = (b,r_2) = (r_2,r_3) = \cdots = (r_{n-1},r_n) = r_n. \qquad (2.8)$$

З (2.8) випливає

Теорема 2.1.2. Найбільший спільний дільник чисел a і b – це остання, відмінна від нуля, остача r_n в ряді рівностей (2.7), тобто

$$(a,b) = r_n. \qquad (2.9)$$

Приклад 2.1.3. Застосовуючи алгоритм Евкліда, знайти $(6188, 4709)$.

Розв'язання. Маємо

$$6188 = 4709 \cdot 1 + 1479,$$
$$4709 = 1479 \cdot 3 = 272,$$
$$1479 = 272 \cdot 5 + 119,$$
$$272 = 119 \cdot 2 + 34,$$
$$119 = 34 \cdot 3 + 17,$$
$$34 = 17 \cdot 2.$$

Отже $(6188, 4709) = 17.$

Відзначимо властивості НСД чисел a і b.

1. Для довільного додатного m маємо

$$(am, bm) = (a,b)m.$$

2. Якщо δ – довільний спільний дільник чисел a і b, то

$$\left(\frac{a}{\delta}, \frac{b}{\delta}\right) = \frac{(a,b)}{\delta}.$$

3. Зокрема, $\left(\frac{a}{(a,b)},\frac{b}{(a,b)}\right)=1.$

4. Якщо $(a,b)=1$, то $(ac,b)=(c,b)$.

5. Якщо $(a,b)=1$ і $b \mid ac$, то $b \mid c$.

6. Якщо кожне з чисел $a_1,a_2,...,a_m$ взаємно просте з кожним із чисел $b_1,b_2,...,b_n$, то $(a_1a_2\cdots a_m, b_1b_2\cdots b_n)=1.$

7. Щоб знайти НСД чисел $a_1,a_2,...,a_n$ складемо ряд чисел:

$(a_1,a_2)=d_2,\quad (d_2,a_3)=d_3\quad (d_3,a_4)=d_4\quad \cdots\quad (d_{n-1},a_n)=d_n.$

Тоді $(a_1,a_2,...,a_n)=d_n.$

Найменше спільне кратне

Визначення 2.1.5. Довільне ціле число, яке є кратним даних чисел називається їх *спільним кратним.*

Визначення 2.1.6.Найменше з додатних спільних кратних чисел a і b, називається *найменшим спільним кратним* цих чисел і позначається $[a,b]$.

Встановимо зв'язок між (a,b) і $[a,b]$.

Нехай M – довільне спільне кратне цілих чисел a і b. Тоді $M=a\cdot k$ і число $\frac{a\cdot k}{b}$ повинно бути цілим. Нехай $(a,b)=d$ і $a=a_1\cdot d,\quad b=b_1\cdot d$. Тоді маємо $\frac{a\cdot k}{b}=\frac{a_1\cdot k}{b_1}$, де $(a_1,b_1)=1$. Оскільки $\frac{a_1\cdot k}{b_1}$ – ціле, то $b_1 \mid k$, тобто $k=b_1\cdot t=\frac{b}{d}\cdot t$, де t – ціле. Отже

$$M = \frac{ab}{d} \cdot t \qquad (2.10)$$

дає загальний вигляд всіх кратних чисел a і b. Найменше з них отримаємо при $t = 1$. Отже для найменшого спільного кратного m чисел a і b маємо

$$m = \frac{a \cdot b}{d}, \qquad (2.11)$$

яку можна записати у вигляді

$$(a,b) \cdot [a,b] = a \cdot b. \qquad (2.12)$$

Щоб знайти НСК кількох чисел $a_1, a_2, ..., a_n$ складемо ряд чисел:

$$[a_1, a_2] = m_2, [m_2, a_3] = m_3, \quad \cdots, \quad [m_{n-1}, a_n] = m_n$$

Тоді $m_n = [a_1, a_2, ..., a_n]$.

Зауважимо, що найменше спільне кратне попарно простих чисел дорівнює їх добутку.

Прості числа

Визначення 2.1.7. Ціле число, яке більше за 1 і ділиться тільки на 1 і на самого себе, називається *простим*.

Ціле число, яке має інші додатні дільники, окрім 1 і самого себе, називається *складеним*.

Відзначимо деякі властивості *простих чисел.*

1. Найменший, відмінний від 1, дільник цілого числа, яке більше від 1 – це *просте* число.

2. Найменший *простий дільник складеного числа* a не перевищує $\sqrt{a}$.

3. Кількість простих чисел – нескінченна (Евклід).

Дійсно, якщо $p_1, p_2, ..., p_k$ – різні прості, то можна отримати нове просте число p_{k+1}, яке є дільником суми

$p_1 \cdot p_2 \cdots p_k + 1$. Якби p_{k+1} співпадало з одним з простих $p_1, p_2, ..., p_k$, наприклад з простим p_l, то ми б отримали

$$p_1 \cdot p_2 \cdots p_l \cdots p_k + 1 = p_l M.$$

З останньої рівності випливало б, що p_l ділить 1, що неможливо.

4. Для довільного цілого числа a і простого p маємо: або $(a, p) = 1$, або $p \mid a$.

5. Якщо $p \mid a \cdot b \cdots l$, то p ділить хоча б один із множників $a, b, ..., l$.

Основна теорема арифметики.

Довільне ціле число $a > 1$ можна подати у вигляді добутку простих, враховуючи їх кратність, а саме:

$$a = p_1^{\alpha_1} \cdot p_2^{\alpha_2} \cdots p_k^{\alpha_k}. \qquad (2.13)$$

Подання числа a у формі (2.13) називається *канонічним розкладом* числа a на співмножники.

Приклад 2.1.4. Знайдемо канонічний розклад числа $a = 588000$.

Розв'язання.

$$588000 = 2^5 \cdot 3 \cdot 5^3 \cdot 7^2.$$

Критерій простоти

Для складання таблиці *простих* чисел, які не перевищують N, існує простий спосіб, що називається *решетом Ератосфена*. Він полягає в наступному:

Виписуємо числа

$$1, 2, ..., N. \qquad (2.14)$$

Перше число, яке більше за 1, – це число 2. Це число – просте. Закреслимо з ряду (2.14) всі числа кратні 2.

Наступне за 2, не закреслене число −це 3. Воно також просте. Закреслимо в ряді (2.14) всі числа,які кратні 3. Перше не закреслене число −це просте число 5. І так далі…Коли вказаним способом закреслені всі числа, які кратні простим, що менші від простого числа p, то всі не закреслені, які менші ніж p^2, будуть простими.

Дійсно, довільне складене число a, що менше p^2, вже закреслене, як кратне його найменшого простого дільника меншого за $\sqrt{a} < p$.

Отже, використовуючи алгоритм Ератосфена, маємо користуватись такими рекомендаціями:

- приступаючи до викреслювання кратних простого числа p, слід починати це викреслювання з p^2;
- складання таблиці простих чисел, які не перевищують числа N, слід завершити, як тільки закреслені всі складені, які кратні простим, що не перевищують $\sqrt{N}$.

Алгоритм Ератосфена дуже простий, але, якщо число a дуже велике, то час роботи алгоритму надто довгий. Даний алгоритм дозволяє будувати множину простих чисел, але він незручний для перевірки простоти заданого числа. Проте, ідея решета та її узагальнення на даний час часто використовуються для «просівання» множин чисел, що володіють тими чи іншими властивостями. До того ж, розробляються спеціальні мікропроцесори, на яких операції «просівання» виконуються дуже ефективно.

Іншими алгоритмами простоти є : тест Вільсона, тест на основі теореми Ферма, тест Рабина-Міллера, ймовірнісний тест Соловея-Штрассена. Однак, описання цих тестів вимагає хоча б елементарного знайомства з

теорією чисел (теорією конгруенцій, теоремами Ейлера та Ферма, квадратичних лишків, символів Лежандра, Якобі, дискретним логарифмуванням, тощо)[3,7,9,16.17].

Ці поняття ми опишемо в наступних параграфах.

2.2. Важливі функції теорії чисел.

2.2.1. Функції $[x], \{x\}$

Визначення 2.2.1. $[x]$ – це функція, яка визначена для довільного дійсного x і є найбільшим цілим числом, що не перевищує x.

Функція $[x]$ називається *цілою частиною x.*

Приклад2.2.1.

$[7]=7, \quad [2,6]=2, \quad [-4,7]=-5.$

Визначення 2.2.2. $\{x\}$ – це функція, яка визначена наступним чином

$$\{x\} \overset{df}{=} x-[x]. \qquad (2.15)$$

Функція $\{x\}$ називається *дробовою частиною x.*

Приклад 2.2.2.

$$\{7\}=7-7=0, \quad \{2,6\}=2,6-2=0,6,$$

$$\{-4,75\}=-4,75+5=0,25.$$

Властивості функцій $[x]$ та $\{x\}$

1. Для довільного дійсного числа x виконується подвійна нерівність

$$[x] \le x < [x]+1$$

2. Для довільного цілого k та дійсного x маємо

$$[k+x]=k+[x].$$

3. Якщо x – дійсне число, а n – ціле число, то $n \le x$ тоді і тільки тоді, коли $n \le [x]$.

4. Для довільного дійсного числа x і довільного натурального числа d справджується

$$\left|\{n \in N : n \le x, d \mid n\}\right| = [x \mid d].$$

5. Для довільного дійсного x виконується

$$[[x]] = [x]$$

6. Для довільного дійсного додатного числа x і довільного натурального числа d справджується

$$[x \mid d] = [[x] \mid d].$$

7. Для довільного дійсного x виконується

$$0 \le \{x\} < 1.$$

8. Для довільного цілого k та дійсного x маємо

$$\{k + x\} = \{x\}.$$

9. Якщо

$$n! = p_1^{\alpha_1} \cdot p_2^{\alpha_2} \cdots p_k^{\alpha_r},$$

де p_i пробігає всі прості числа, які не перевищують n, то показники α_i визначаться співвідношенням

$$\alpha_i = \left[\frac{n}{p_i}\right] + \left[\frac{n}{p_i^2}\right] + \left[\frac{n}{p_i^3}\right] + \cdots \qquad (2.16)$$

Приклад 2.2.3. Подати $40!$ у вигляді добутку степенів простих.

Розв'язання. Маємо

$$40! = 2^{\alpha_1} \cdot 3^{\alpha_2} \cdot 5^{\alpha_3} \cdot 7^{\alpha_4} \cdot 11^{\alpha_5} \cdot 13^{\alpha_6} \cdot 17^{\alpha_7} \cdot 19^{\alpha_8} \cdot 23^{\alpha_9} \cdot 29^{\alpha_{10}} \cdot 31^{\alpha_{11}} \cdot 37^{\alpha_{12}}.$$

Знайдемо показники простих чисел, які входять в останній розклад, використовуючи (2.16):

$$\alpha_1 = \left[\frac{40}{2}\right] + \left[\frac{40}{2^2}\right] + \left[\frac{40}{2^3}\right] + \left[\frac{40}{2^4}\right] + \left[\frac{40}{2^5}\right] =$$

$$= 20 + 10 + 5 + 2 + 1 = 38,$$

$$\alpha_2 = \left[\frac{40}{3}\right] + \left[\frac{40}{3^2}\right] + \left[\frac{40}{3^3}\right] = \left[13\frac{1}{3}\right] + \left[4\frac{1}{9}\right] + \left[1\frac{13}{27}\right] =$$

$$= 13 + 4 + 1 = 18,$$

$$\alpha_3 = \left[\frac{40}{5}\right] + \left[\frac{40}{5^2}\right] = 8 + 1 = 9, \quad \alpha_4 = \left[\frac{40}{7}\right] = \left[5\frac{5}{7}\right] = 5,$$

$$\alpha_5 = \left[\frac{40}{11}\right] = \left[3\frac{7}{11}\right] = 3, \quad \alpha_6 = \left[\frac{40}{13}\right] = \left[3\frac{1}{13}\right],$$

$$\alpha_7 = \left[\frac{40}{17}\right] = \left[2\frac{6}{17}\right] = 2, \quad \alpha_8 = \left[\frac{40}{19}\right] = \left[2\frac{2}{19}\right] = 2,$$

$$\alpha_9 = \left[\frac{40}{23}\right] = \left[1\frac{17}{23}\right] = 1, \quad \alpha_{10} = \left[\frac{40}{29}\right] = \left[1\frac{11}{29}\right] = 1,$$

$$\alpha_{11} = \left[\frac{40}{31}\right] = \left[1\frac{9}{31}\right] = 1, \quad \alpha_{12} = \left[\frac{40}{37}\right] = \left[1\frac{3}{37}\right] = 1.$$

Отже остаточно отримаємо

$$40! = 2^{38} \cdot 3^{18} \cdot 5^9 \cdot 7^5 \cdot 11^3 \cdot 13^3 \cdot 17^2 \cdot 19^2 \cdot 23 \cdot 29 \cdot 31 \cdot 37.$$

Мультиплікативні функції

Визначення 2.2.3. Арифметична функція $f(n)$ називається *мультиплікативною*, якщо $f(1) = 1$ і $f(m \cdot n) = f(m) \cdot f(n)$ для довільних взаємно простих натуральних чисел m та n і *цілком мультиплікативною*, якщо $f(m \cdot n) = f(m) \cdot f(n)$ для довільних натуральних m та n.

Приклад 2.2.4. Функція $f(n) = n^{\alpha}$ – цілком мультиплікативна, бо

$$f(m\cdot n)=(m\cdot n)^{\alpha}=m^{\alpha}\cdot n^{\alpha}=f(m)\cdot f(n).$$

Властивості мультиплікативних функцій

1. Добуток мультиплікативних функцій – мультиплікативна функція.

2. Якщо $f(n)$ – мультиплікативна функція, то функція $h(n)=\sum_{d|n} f(d)$ – також мультиплікативна.

3. Мультиплікативна функція повністю визначається її значеннями на степенях простих чисел:

$$f\left(p_1^{\alpha_1}\cdot p_2^{\alpha_2}\cdots p_s^{\alpha_s}\right)=f\left(p_1^{\alpha_1}\right)\cdot f\left(p_2^{\alpha_2}\right)\cdots f\left(p_s^{\alpha_s}\right).$$

4. Якщо $f(n)$ – мультиплікативна функція, то

$$f(m)\cdot f(n)=f\left((m,n)\right)\cdot f\left([m,n]\right).$$

Функції $\tau(n)$ ***і*** $\sigma(n)$

Визначення 2.2.4. Функція $\tau(n)\overset{df}{=}\sum_{d|n}1$ визначає число дільників натурального числа n.

Функція $\sigma(n)\overset{df}{=}\sum_{d|n}d$ визначає суму дільників натурального числа n.

Приклад 2.2.6.

$\tau(6)=4$, бо дільниками числа 6 є числа $1,2,3,6$;

$$\sigma(6)=1+2+3+6=12;$$

$\tau(13)=2$, бо дільниками числа 13 є числа $1,13$;

$$\sigma(13)=1+13=14.$$

Властивості функцій $\tau(n)$ *і* $\sigma(n)$

1. $\tau\left(p_1^{\alpha_1}\cdot p_2^{\alpha_2}\cdots p_s^{\alpha_s}\right)=(\alpha_1+1)(\alpha_2+1)\cdots(\alpha_s+1).$

2. $\sigma\left(p_1^{\alpha_1}\cdot p_2^{\alpha_2}\cdots p_s^{\alpha_s}\right)=\dfrac{p_1^{\alpha_1+1}}{p_1-1}\cdot\dfrac{p_2^{\alpha_2+1}}{p_2-1}\cdots\dfrac{p_s^{\alpha_s+1}}{p_s-1}.$

3. $\tau(n)-$ мультиплікативна функція.

4. $\sigma(n)-$ мультиплікативна функція.

Приклад 2.2.7. Обчислити $\tau\left(\sigma(120)\right).$

Оскільки $120=2^3\cdot3\cdot5,$ то, за властивістю 2, маємо

$$\sigma(120)=\sigma\left(2^3\cdot3\cdot5\right)=\frac{2^4-1}{2-1}\cdot\frac{3^2-1}{3-1}\cdot\frac{5^2-1}{5-1}=$$

$$=15\cdot4\cdot6=2^3\cdot3^2\cdot5.$$

Тоді, за властивістю 1 отримуємо

$$\tau\left(\sigma(120)\right)=\tau\left(2^3\cdot3^2\cdot5\right)=(3+1)(2+1)(1+1)=24.$$

Функція Ейлера

Визначення 2.2.5. Для заданого натурального числа n функція Ейлера $\varphi(n)$ визначається, як число натуральних чисел, які не перевищують n і взаємно прості з n.

Приклад 2.2.8.

$$\varphi(1)=1,\quad \varphi(2)=1,\quad \varphi(3)=2,$$

$$\varphi(4)=2,\quad \varphi(5)=4,\quad \varphi(6)=2.$$

Властивості функції Ейлера

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

2. $\varphi\left(p^{\alpha}\right)=p^{\alpha}-p^{\alpha-1}.$

3. Функція $\varphi(n)$ – мультиплікативна. Якщо $n = p_1^{\alpha_1} \cdot p_2^{\alpha_2} \cdots p_s^{\alpha_s}$, то $\varphi(n)$ обчислюється за однією з формул:

$$\varphi(n) = n\left(1-\frac{1}{p_1}\right)\left(1-\frac{1}{p_2}\right)\cdots\left(1-\frac{1}{p_s}\right),$$

$$\varphi(n) = \left(p_1^{\alpha_1} - p_1^{\alpha_1-1}\right)\left(p_1^{\alpha_1} - p_1^{\alpha_1-1}\right)\cdots\left(p_s^{\alpha_s} - p_s^{\alpha_s-1}\right).$$

4. $\sum_{d|n} \varphi(d) = n$ (тотожність Гауса).

Приклад 2.2.9. Обчислити функцію Ейлера чисел 7, 81, 60, 405, використовуючи властивості 1 – 4.

Розв'язання.

- $\varphi(7) = 7-1 = 6,$
- $\varphi(81) = \varphi\left(3^4\right) = 3^4 - 3^3 = 81-27 = 54,$
- $\varphi(60) = \varphi\left(2^2 \cdot 3 \cdot 5\right) = 60\left(1-\frac{1}{2}\right)\left(1-\frac{1}{3}\right)\left(1-\frac{1}{5}\right) = 16,$
- $\varphi(405) = \varphi(81 \cdot 5) = \varphi(81)\varphi(5) = 54 \cdot 4 = 216.$

Приклад 2.2.10. Перевірити тотожність Гауса для $n = 12$.

Розв'язання.

$$\varphi(1)+\varphi(2)+\varphi(3)+\varphi(4)+\varphi(6)+\varphi(12) =$$
$$= 1+1+2+2+2+4 = 12.$$

Приклад 2.2.11. Нехай $n = p \cdot q$, де p і q – прості, проте невідомі числа. Припустимо, що функція Ейлера $\varphi(n)$ – відома. Показати, що множники p, q можна однозначно визначити за відомими n і $\varphi(n)$.

Розв'язання. Зауважимо, що $\varphi(n)=n-p-q+1$ для $n=p\cdot q$. Тому числа p,q можна визначити із системи

$$\begin{cases} p\cdot q=n, \\ p+q=n+1-\varphi(n), \end{cases}$$

тобто з квадратного рівняння

$$x^2-\left(n+1-\varphi(n)\right)x+n=0,$$

за умови, що воно має цілі розв'язки.

Наприклад, якщо $n=7373$, а $\varphi(7373)=7200$, то два прості множники цього числа є коренями рівняння

$$x^2-174x+7373=0.$$

Розв'язавши це рівняння, отримаємо два розв'язки $x_1=101,\quad x_2=73$. Отже

$$7373=101\cdot 73.$$

Функція Мебіуса

Визначення 2.2.6. Функція Мебіуса $\mu(n)$ визначена для довільного натурального числа n і набуває тільки трьох числових значень $\{-1,0,1\}$ в залежності від розкладу числа n на прості множники, а саме

$$\mu(n)=\begin{cases} 1, & для \quad n=1, \\ (-1)^s, & для \quad n=p_1\cdot p_2\cdots p_s,\ p_i\neq p_j, i\neq j, \\ 0, & якщо \quad \exists p:\ p^2\,|\,n. \end{cases} \qquad (2.17)$$

Приклад 2.2.12. Обчислити функцію Мебіуса чисел $6,\ 70,\ 50$.

Розв'язання.

- Оскільки $6=2\cdot 3$, $s=2$, то, за визначенням (2.17), маємо $\mu(6)=(-1)^2=1$.

- Оскільки $70 = 2 \cdot 5 \cdot 7$, $s = 3$, та, за визначенням (2.17), маємо $\mu(70) = (-1)^3 = -1$.
- Оскільки $50 = 2 \cdot 5^2$, тобто існує $p = 5$ таке, що $5^2 \mid 50$, то, за визначенням (2.17), отримуємо $\mu(50) = 0$.

Приклад 2.2.13. Відомо $[18, 20]$, що число $a_p(n)$ незвідних і нормованих (зі старшим коефіцієнтом 1) многочленів степеня n над полем F_p обчислюється з допомогою функції Мебіуса за формулою:

$$a_p(n) = \frac{1}{n} \sum_{m \mid n} p^{\frac{n}{m}} \mu(m). \qquad (2.18)$$

У формулі (2.18) сумування відбувається за цілими числами m, що ділять n.

Обчислимо $a_2(2), a_2(3), a_2(4)$ за формулою (2.18)

Розв'язання. Маємо:

$$a_2(2) = \frac{1}{2}(2^2 - 2) = 1;$$

$$a_2(3) = \frac{1}{3}(2^3 - 2) = \frac{1}{3}(8 - 2) = 2;$$

$$a_2(4) = \frac{1}{4}(2^4 - 2^3) = \frac{1}{4}(16 - 4) = 3.$$

Неважко переконатись, що незвідними нормованими многочленами

2-го, 3-го і 4-го степеня над полем F_2 є многочлени:

- $n = 2; : f(x) = x^2 + x + 1;$
- $n = 3; : f_1(x) = x^3 + x + 1, \quad f_2(x) = x^3 + x^2 + 1;$

- $n=4$;

$$g_1(x)=x^4+x^3+1,\quad g_2(x)=x^4+x+1,\quad g_3(x)=x^4+x^3+x^2+1.$$

2.3. Ланцюгові дроби.

2.3.1. Скінченні ланцюгові дроби та їх властивості

Нехай $\frac{a}{b}$ – раціональне число з додатним знаменником, тобто a,b – цілі числа. Застосуємо до чисел a і b алгоритм Евкліда (2.7). Маємо:

$$\begin{aligned}
&a=bq_1+r_2, \quad \frac{a}{b}=q_1+\frac{1}{\frac{b}{r_2}},\\
&b=r_2q_2+r_3, \quad \frac{b}{r_2}=q_2+\frac{1}{\frac{r_2}{r_3}},\\
&\qquad\qquad\qquad\qquad\qquad\qquad\qquad\qquad\qquad\qquad (2.19)\\
&r_{n-2}=r_{n-1}q_{n-1}+r_n, \quad \frac{r_{n-2}}{r_{n-1}}=q_{n-1}+\frac{1}{\frac{r_{n-1}}{r_n}},\\
&r_{n-1}=r_nq_n, \quad \frac{r_{n-1}}{r_n}=q_n.
\end{aligned}$$

Тоді дріб $\frac{a}{b}$ можна записати у вигляді

$$\frac{a}{b}=q_1+\cfrac{1}{q_2+\cfrac{1}{q_3+\ddots+\cfrac{1}{q_n}}}. \qquad (2.20)$$

Визначення 2.3.1. Числа $q_1, q_2, ..., q_n$ називаються *неповними частками* послідовних поділів у алгоритмі Евкліда, а вираз (2.20) – *скінченним ланцюговим дробом,* який позначимо

$$\frac{a}{b} = [q_1, q_2, ..., q_n] \qquad (2.21)$$

Визначення 2.3.2. Дроби

$$\delta_1 = q_1, \quad \delta_2 = q_1 + \frac{1}{q_2}, \quad \delta_3 = q_1 + \frac{1}{q_2 + \dfrac{1}{q_3}}, \quad ..., \ (2.22)$$

називаються *підхідними дробами*.

Для підхідних дробів $\delta_s, \quad s = 2, 3, ..., n,$ справджується *рекурентна формула* [5]

$$\frac{P_s}{Q_s} = \frac{q_s P_{s-1} + P_{s-2}}{q_s Q_{s-1} + Q_{s-2}}, \quad P_0 = 1, \quad Q_0 = 0, \quad P_1 = q_1, \quad Q_1 = 1. \ (2.23)$$

Дійсно, покладаючи $P_0 = 1, \quad Q_0 = 0$ та позначивши підхідний дріб δ_s дробом $\frac{P_s}{Q_s}, \quad s = 2, 3, ..., n,$ маємо

$$\delta_1 = \frac{q_1}{1} = \frac{P_1}{Q_1};$$

$$\delta_2 = \frac{q_1 + \dfrac{1}{q_2}}{1} = \frac{q_1 q_2 + 1}{q_2} = \frac{q_2 P_1 + P_0}{q_2 Q_1 + Q_0} = \frac{P_2}{Q_2};$$

$$\delta_3 = \frac{\left(q_2 + \dfrac{1}{q_3}\right) P_1 + P_0}{\left(q_2 + \dfrac{1}{q_3}\right) Q_1 + Q_0} = \frac{q_3 P_2 + P_1}{q_3 Q_2 + Q_1} = \frac{P_3}{Q_3}.$$

Застосувавши метод математичної індукції (це можна зробити самостійно), прийдемо до рекурентної формули (2.23).

Отже, чисельники та знаменники підхідних дробів δ_s, $s=2,3,...,n$ можна послідовно обчислювати за такими двочленними рекурентними формулами:

$$P_s = q_s P_{s-1} + P_{s+2},$$
$$Q_s = q_s Q_{s-1} + Q_{s+2}, \qquad (2.24)$$
$$P_0 = 1, \quad Q_0 = 0, \quad P_1 = q_1, \quad Q_1 = 1.$$

Обчислення доцільно проводити засхемою, яка відображена в наступній таблиці

q_s		q_1	q_2	$\cdots$	q_{s-2}	q_{s-1}	q_s	$\cdots$	q_{n-1}	q_n
P_s	1	q_1	P_2	$\cdots$	P_{s-2}	P_{s-1}	P_s	$\cdots$	P_{n-1}	P_n
Q_s	0	1	Q_2	$\cdots$	Q_{s-2}	Q_{s-1}	Q_s	$\cdots$	Q_{n-1}	Q_n

Таб.12

Приклад 2.3.1. Подати у вигляді ланцюгового дробу число $\frac{105}{38}$. Знайти підхідні дроби за вказаною схемою (з використанням формул (2.24)).

Розв'язання. Використаємо алгоритм Евкліда для знаходження НСД$(105,38)$:

$$105 = 38 \cdot 2 + 29,$$
$$38 = 29 \cdot 1 + 9,$$
$$29 = 9 \cdot 3 + 2,$$
$$9 = 2 \cdot 4 + 1,$$
$$2 = 1 \cdot 2.$$

Отже

$$\frac{105}{38}=2+\cfrac{1}{1+\cfrac{1}{3+\cfrac{1}{4+\cfrac{1}{2,}}}}$$

або, в більш компактному вигляді

$$\frac{105}{38}=[2,1,3,4,2].$$

В цьому випадку таблиця 6 набуває вигляду

q_s		2	1	3	4	2
P_s	1	2	3	11	47	105
Q_s	0	1	1	4	17	38

Слід зауважити, що у випадку нескоротного дробу, останній підхідний дріб співпадає з вихідним дробом, тобто $\frac{P_n}{Q_n}=\frac{a}{b}$.

Властивості підхідних дробів

1. $P_s\cdot Q_{s-1}-P_{s-1}\cdot Q_s=(-1)^s;$ (2.25)
2. $Q_s\geq 2^{\frac{s-1}{2}};$
3. $\frac{P_s}{Q_s}-\frac{P_{s-1}}{Q_{s-1}}=\frac{(-1)^s}{Q_s\cdot Q_{s-1}};$

4. $$\frac{P_{s-2}}{Q_{s-2}} - \frac{P_s}{Q_s} = \frac{(-1)^s q_s}{Q_s \cdot Q_{s-1}}. \qquad (2.26)$$

Доведемо важливу в подальших застосуваннях формулу (2.25).

Маємо

$$\frac{P_s}{Q_s} - \frac{P_{s-1}}{Q_{s-1}} = \frac{h_s}{Q_s \cdot Q_{s-1}},$$

де

$$h_s = P_s \cdot Q_{s-1} - Q_s \cdot P_{s-1}.$$

Оскільки, за формулами (2.24),

$$h_s = (q_s P_{s-1} + P_{s-2}) Q_{s-1} - (q_s Q_{s-1} + Q_{s-2}) P_{s-1} =$$
$$= -(P_{s-1} \cdot Q_{s-2} - Q_{s-1} \cdot P_{s-2}) = -h_{s-1},$$

і $h_1 = q_1 \cdot 0 - 1 \cdot 1 = -1$, то $h_s = (-1)^s$, звідки й випливає співвідношення (2.25).

З (2.25) також отримуємо

$$(P_s, Q_s) = (P_{s-1}, Q_{s-1}) = 1.$$

А це означає, що підхідні дроби $\frac{P_s}{Q_s}$, $s = 2, 3, ..., n$ – *нескоротні.*

Доведення властивості 3 негайно випливає з формули (2.25).

Доведемо властивість 4.

$$\frac{P_{s-2}}{Q_{s-2}} - \frac{P_s}{Q_s} = \frac{P_{s-2} \cdot Q_s - Q_{s-2} \cdot P_s}{Q_s \cdot Q_{s-2}} =$$
$$= \frac{(q_s Q_{s-1} + Q_{s-2}) P_{s-2} - (q_s P_{s-1} + P_{s-2}) Q_{s-2}}{Q_s \cdot Q_{s-2}} =$$

$$= \frac{q_s\left(P_{s-2}\cdot Q_{s-1} - P_{s-1}\cdot Q_{s-2}\right)}{Q_s \cdot Q_{s-2}} = \frac{(-1)^s q_s}{Q_s \cdot Q_{s-2}}.$$

Отже властивість (2.26) доведена.

Зробимо важливі висновки з формули (2.26), а саме:

- підхідні дроби парних порядків утворюють спадну послідовність і наближають вихідний дріб «зверху»:

$$\frac{a}{b} < \cdots < \frac{P_6}{Q_6} < \frac{P_4}{Q_4} < \frac{P_2}{Q_2};$$

- підхідні дроби непарних порядків утворюють зростаючу послідовність і наближають вихідний дріб «знизу»:

$$\frac{P_1}{Q_1} < \frac{P_3}{Q_3} < \frac{P_5}{Q_5} < \cdots < \frac{a}{b}.$$

Приклад 2.3.2. Знайдемо підхідні дроби для скінченого ланцюгового дробу $\frac{105}{38} = [2,1,3,4,2]$.

Розв'язання.

$$\frac{P_1}{Q_1} = \frac{2}{1}, \quad \frac{P_2}{Q_2} = \frac{3}{1}, \quad \frac{P_3}{Q_3} = \frac{11}{4}, \quad \frac{P_4}{Q_4} = \frac{47}{17}, \quad \frac{P_5}{Q_5} = \frac{105}{38}.$$

Отже отримуємо такі оцінки:

$$\frac{2}{1} < \frac{11}{4} < \frac{105}{38} < \frac{47}{17} < \frac{3}{1}.$$

2.3.2.Нескінченні ланцюгові дроби

Нехай α – довільне дійсне число. Позначимо $q_1 = [\alpha]$, де $[\alpha]$ – ціла частина дійсного числа α, див. 2.2.1. Тоді маємо ($\{\alpha\}$ – дробова частина числа α)

$$\alpha = [\alpha] + \{\alpha\} = q_1 + \frac{1}{\alpha_2}, \quad \alpha_2 > 1.$$

Так само для нецілих $\alpha_2, \alpha_3, ..., \alpha_{s-1}$ дістанемо

$$\alpha_2 = [\alpha_2] + \{\alpha_2\} = q_2 + \frac{1}{\alpha_3}, \quad \alpha_3 > 1,$$

$$\text{.....} \quad (2.27)$$

$$\alpha_{s-1} = [\alpha_{s-1}] + \{\alpha_{s-1}\} = q_{s-1} + \frac{1}{\alpha_s}, \quad \alpha_s > 1,$$

$$\text{.....},$$

Визначення 2.3.3.Нескінченним ланцюговим дробом називається дріб, отриманий процедурою (2.27), тобто

$$\alpha = q_1 + \cfrac{1}{q_2 + \cfrac{1}{q_3 + \ddots + \cfrac{1}{q_{s-1} + \cfrac{1}{\alpha_s}}}}. \quad (2.28)$$

$$\ddots$$

Для ірраціонального числа (тобто для $\alpha \neq \frac{m}{n}$, $m, n \in Z$) вказаний в (2.27) процес, взагалі кажучи, нескінченний.

Позначимо ланцюговий дріб (2.28), як і випадку скінченного ланцюгового дробу

$$\alpha = [q_1, q_2, ..., q_{s-1}, ...]. \quad (2.29)$$

Приклад 2.3.3. Розвинути $\sqrt{7}$ у ланцюговий дріб.

Розв'язання.Маємо

$$q_1 = \left[\sqrt{7}\right] = 2,$$

$$q_2 = \left[\frac{1}{\sqrt{7}-2}\right] = \left[\frac{\sqrt{7}+2}{3}\right] = 1,$$

$$q_3=\left[\frac{1}{\frac{\sqrt{7}+2}{3}-1}\right]=\left[\frac{3}{\sqrt{7}-1}\right]=\left[\frac{\sqrt{7}+1}{2}\right]=1,$$

$$q_4=\left[\frac{1}{\frac{\sqrt{7}+1}{2}-1}\right]=\left[\frac{2}{\sqrt{7}-1}\right]=\left[\frac{\sqrt{7}+1}{3}\right]=1,$$

$$q_5=\left[\frac{1}{\frac{\sqrt{7}+1}{3}-1}\right]=\left[\frac{3}{\sqrt{7}-2}\right]=\left[\sqrt{7}+2\right]=4,$$

$$q_6=\left[\frac{1}{\sqrt{7}-2}\right]=\left[\frac{\sqrt{7}+2}{3}\right]=1,$$

$$\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots,$$

Оскільки $q_2=q_6=\dfrac{\sqrt{7}+2}{3}$, то наступні неповні частки будуть повторюватись *періодично,* тому

$$\sqrt{7}=[2,1,1,1,4,1,1,1,4,1,\ldots], \qquad (2.30)$$

тобто ірраціональне число $\sqrt{7}$ розвинуте у періодичний ланцюговий дріб (2.30).

Зауважимо, що підхідні дроби нескінченного ланцюгового дробу (2.29) визначаються двочленними рекурентними формулами (2.23), як і у випадку скінченного ланцюгового дробу.

Їх властивості $1-4$ аналогічні й для нескінченного випадку.

Проте, нескінченні ланцюгові дроби для точного, а не формального визначення, потребують граничного

переходу, тобто використання поняття границі послідовності [11].

Визначення 2.3.4. Якщо $[q_1, q_2, ..., q_{s-1}, ...]$ – нескінченний ланцюговий дріб і послідовність підхідних дробів $\delta_1, \delta_2, ..., \delta_s, ...$ – збіжна до числа α, то кажуть, що ланцюговий дріб збіжний і

$$\alpha = [q_1, q_2, ..., q_{s-1}, ...].$$

Дамо далі точне визначення періодичного ланцюгового дробу.

Визначення 2.3.5. Нескінченний ланцюговий дріб називається *періодичним*, якщо існують $m, n \in \mathbb{N}$ такі, що $q_n = q_{n+s}$ для всіх $n \geq m$ Число s називається *довжиною періоду.*

Введемо для періодичних ланцюгових дробів наступне позначення

$$[q_1, q_2, ..., q_m, q_{m+1}, ..., q_{m+s-1}, q_m, q_{m+1}, ...] =$$
$$= \left[q_1, q_2, ..., q_{m-1}, \overline{q_m, ..., q_{m+s-1}} \right].$$

Визначення 2.3.6. Дійсне число α називається *квадратичною* і*ррaціональністю*, якщо α – корінь квадратного рівняння

$$ax^2 + bx + c = 0$$

з цілими коефіцієнтами $a, b, c.$

Зауважимо, що кожну квадратичну ірраціональність можна записати у вигляді $\frac{P + \sqrt{D}}{Q}$ або $\frac{P - \sqrt{D}}{Q}$, де $P, Q, D \in \mathbb{Z}, \quad D > 0.$

Подамо, без доведення, важливу теорему, яка виправдовує нашу увагу до неперервних періодичних ланцюгових дробів [11].

Теорема 2.3.1 .Кожний нескінченний періодичний ланцюговий дріб

$$\left[q_1, q_2, ..., q_{m-1}, \overline{q_m, ..., q_{m+s-1}}\right]$$

дорівнює деякій квадратичній ірраціональності.

2.4.Конгруенції.

1.4.1. Основні властивості конгруенцій

Метод конгруенцій був створений видатним німецьким математиком К.Ф.Гаусом. Це –формальний метод, однак з його допомогою часто можна досить легко отримувати результати, які неможливо отримати іншими методами.

Нехай m – ціле додатне число, $a, b \in \mathbb{Z}$.

Визначення 2.4.1.Число a називається конгруентним до числа b за модулем m якщо m ділить різницю $a-b$ (тобто $m \mid a-b$) . Позначимо цю конгруенцію так

$$a \equiv b \pmod{m}. \qquad (2.31)$$

Приклад 2.4.1.

- $12 \equiv 2 \pmod{5}$, бо $12-2=10=5\cdot 2$;
- $11 \neq 2 \pmod{5}$, бо $11-2=9 \neq 5\cdot k, \quad k \in \mathbb{Z}$.

Властивості конгруенцій

Конгруенціям притаманні властивості звичайних рівностей. Розглянемо ці властивості. Перші три властивості конгруенцій, які ми далі сформулюємо, визначають на множині цілих чисел $\mathbb{Z}$ відношення еквівалентності(див. розділ 1).

1. $a \equiv a \pmod{m}$ (рефлексивність)
2. Якщо $a \equiv b \pmod{m}$, то $b \equiv a \pmod{m}$ (симетрія).

Дійсно, якщо $m|a-b$, то $m|-(a-b)$, отже $m|b-a$.

3. Якщо $a \equiv b \pmod m$ і $b \equiv c \pmod m$, то $a \equiv c \pmod m$ (транзитивність).

Дійсно, якщо $m|a-b$ і $m|b-c$, то $m|(a-b)+(b-c)$, тобто $m|a-c$, і тому $a \equiv c \pmod m$.

4. Якщо $a \equiv b \pmod m$ і $c \equiv d \pmod m$, то $a \pm c \equiv b \pm d \pmod m$.

Дійсно, якщо $m|a-b$ і $m|c-d$, то $m|(a \pm c)-(b \pm d)$, тобто $a \pm c \equiv (b \pm d) \pmod m$.

5. Якщо $a \equiv b \pmod m$ і $k \in \mathbb{Z}$, то $a \pm k \equiv b \pm k \pmod m$.

Дійсно, додаючи конгруенції: $a \equiv b \pmod m$ і $k \equiv k \pmod m$, отримуємо

$$a \pm k \equiv b \pm k \pmod m.$$

6. З властивості 5 випливає, що можна переносити з протилежним знаком члени з одного боку конгруенції в інший.

7. Якщо $a \equiv b \pmod m$ і $c \equiv d \pmod m$, то $a \cdot c \equiv b \cdot d \pmod m$, тобто конгруенції можна перемножувати.

Дійсно, оскільки $m|a-b$ і $a = b + mq_1$, а $m|c-d$ і $c = d + mq_2$, *де* $q_1, q_2 \in \mathbb{Z}$, то $a - b = mq_1$, $c - d = mq_2$, або

$$ac = bd + m(dq_1 + bq_2 + q_1 q_2).$$

Отже

$$m|ac - bd, \text{ тобто } ac \equiv bd \pmod m.$$

З властивості 7 випливають властивості 8,9,10.

8. Обидві частини конгруенції можна множити на одне і те ж ціле число, тобто якщо

$$a \equiv b \pmod{m} \text{ то } ak \equiv bk \pmod{m}, \quad k \in \mathbb{Z}.$$

9. Обидві частини конгруенції можна піднімати до одного і того ж цілого додатного степеня, тобто, якщо

$$a \equiv b \pmod{m}, \text{ то } a^k \equiv b^k \pmod{m}, \quad k \in \mathbb{N}.$$

10. Обидві частини конгруенції можна скорочувати на спільний цілий множник, якщо цей множник – взаємно простий з модулем, тобто якщо

$$ak \equiv bk \pmod{m} \text{ і } (k,m) = 1, \text{ то } a \equiv b \pmod{m}.$$

11. Якщо ж $ak \equiv bk \pmod{m}$, $(k,m) = d$, $m = m_1 d$ і $k = k_1 d$, то тобто обидві частини конгруенції та модуль можна скорочувати на спільний дільник.

$$ak_1 \equiv bk_1 \pmod{m_1},$$

12. Нехай $P(x)$ – многочлен з цілими коефіцієнтами, x, y – змінні. Тоді з конгруенції $x \equiv y \pmod{m}$ випливає $P(x) \equiv P(y) \pmod{m}$.

13. Якщо конгруенція справджується за декількома модулями, то вона справджується і за найменшим спільним кратним цих модулів, тобто з конгруенцій :

$$a \equiv b \pmod{m_1}, \quad a \equiv b \pmod{m_2}, \quad \cdots, \quad a \equiv b \pmod{m_k}$$

випливає конгруенція

$$a \equiv b \left(\mathrm{mod}\left[m_1, m_2, ..., m_k\right]\right).$$

Ця властивість негайно випливає з низки поділів:

$$m_1 \mid a-b, \quad m_2 \mid a-b, \quad \cdots, \quad m_k \mid a-b.$$

Тому, з визначення $\left[m_1, m_2, ..., m_k\right]$, випливає, що $\left[m_1, m_2, ..., m_k\right] \mid a-b.$

14. Якщо конгруенція справджується за модулем m, то вона справджується і за довільним дільником m.

Дійсно, з $m \mid a-b$ і $d \mid m$ випливає, що $d \mid a-b$ і тому $a \equiv b \pmod{d}$.

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

Ця рівність випливає з рівності $a = b + mt, \quad t \in \mathbb{Z}$.

Зауважимо, що властивість 12 є основою для виведення ознак подільності цілих чисел. Як ілюстрацію, розглянемо, наприклад, подільність на число 11.

Приклад 2.4.2. *Ознака подільності цілого числа N на* 11.

Нехай ціле число N виражається в десятковій системі числення цифрами $a_0, a_1, a_2, ..., a_n$, тобто

$$N = a_0 10^n + a_1 10^{n-1} + a_2 10^{n-2} + \cdots a_{n-1} 10 + a_n.$$

Оскільки $10 \equiv -1 \pmod{11}$, то, за властивістю 12, маємо

$$N = (-1)^n a_0 + (-1)^{n-1} a_1 + \cdots + (-1) a_{n-1} + a_n \pmod{11},$$

або

$$N = \left((a_n + a_{n-2} + \cdots) - (a_{n-1} + a_{n-3} + \cdots) \right) \pmod{11}.$$

Таким чином, отримуємо *ознаку подільності цілого числа N на* 11: число N ділиться на 11 тоді і тільки тоді, коли сума цифр, що стоїть на парних місцях мінус сума цифр, що стоїть на непарних місцях ділиться на 11.

Приклад 2.4.3. Перевірити, що число 582758 ділиться на 11.

Розв'язання. За ознакою подільності на 11, маємо

$$(8+7+8)-(5+2+5) = 23-12 = 11.$$

Отже число 582758 ділиться на 11. Дійсно $582758 = 11 \cdot 52978$.

2.4.2. Повна та зведена системи лишків

Числа, які при діленні на m дають однакову остачу, за властивостями конгруенцій 1-3, утворюють класи еквівалентності. Кількість таких класів дорівнює m, бо остачі r при діленні на m можуть набувати значень $0,1,2,...,m-1$.

Визначення 2.4.2. Довільне число класу, що відповідає остачі r, називається *лишком* за модулем m.

Визначення 2.4.3. Лишок, який дорівнює r, називається *найменшим невід'ємним лишком*.

Взявши з кожного класу по одному лишку, отримаємо *повну систему лишків за модулем* m.

Найчастіше користуються наступними повними системами лишків:

$$0,1,2,...,m-1; \qquad (2.32)$$

для $m=2k+1$ $$-\frac{m-1}{2},...,-1,0,1,...,\frac{m-1}{2}; \qquad (2.33)$$

для $m=2k$ $$-\frac{m}{2}+1,...,-1,0,1,...,\frac{m}{2}; \qquad (2.34)$$

або $$-\frac{m}{2},...,-1,0,1,...,\frac{m}{2}-1. \qquad (2.35)$$

Для повної системи лишків справджується наступне

Твердження 2.4.1. Якщо $(a,m)=1$ і x утворює повну систему лишків за модулем m, то $ax+b$, де $b\in\mathbb{Z}$, також утворює повну систему лишків за модулем m.

Для доведення цього твердження досить переконатись у тому, що ax_1+b, та ax_2+b, – не конгруентні за модулем m, як тільки x_1 та x_2 – не конгруентні за модулем m.

Припустимо, що навпаки $ax_1+b\equiv ax_2+b\pmod m$, тоді $ax_1\equiv ax_2\pmod m$ і через те, що $(a,m)=1$, то $x_1\equiv x_2\pmod m$, що приводить до протиріччя, бо ми припустили, що x_1 та x_2 – не конгруентні за модулем m.

Розглянемо такі класи лишків за модулем m, які – взаємно прості з цим модулем.

Взявши від кожного такого класу по одному лишку, отримаємо *зведену систему лишків* за модулем m.

Для зведеної системи лишків справедливе твердження, подібне до твердження 2.4.1 для повної системи лишків.

Твердження 2.4.2. *Якщо* $(a,m)=1$ і x *пробігає зведену систему лишків за модулем* m, *то* ax *також пробігає зведену систему лишків за* модулем m.

Це твердження доводиться аналогічно, як і твердження 2.4.1.

Приклад2.4.3.

- повною системою лишків за модулем 11 є, наприклад, як (2.32):

$$0,1,2,3,...,9,10;$$

- або, як (2.33):

$$-5,-4,-3,-2,-1,0,1,2,3,4,5;$$

- повною системою лишків за модулем 10 є, наприклад, як (2.34):

$$-4,-3,-2,-1,0,1,2,3,4,5;$$

- або, як (2.35):

$$-5,-4,-3,-2,-1,0,1,2,3,4;$$

- зведеною системою лишків за модулем 42 є

$$1,5,11,13,17,19,23,25,29,31,37,41.$$

Число класів цієї системи лишків дорівнює

$$l=\varphi(42)=\varphi(2\cdot3\cdot7)=1\cdot2\cdot6=12.$$

2.4.3. Теореми Ейлера і Ферма.

Теореми Ейлера і Ферма є дуже важливими теоремами теорії чисел.

Зокрема, теорема Ферма дозволяє тестувати число на простоту і ввести важливе в криптографії поняття *псевдопростого числа*.

Теорема Ейлера. Для $(a,m)=1$ і $m\in\mathbb{N}$ справджується конгруенція

$$a^{\varphi(m)}\equiv1(\bmod m), \qquad (2.36)$$

де $\varphi(m)$ – функція Ейлера числа m.

Доведення. Якщо x пробігає зведену систему лишків за модулем m

$$x=r_1,r_2,...,r_l,\quad l=\varphi(m),$$

то найменші невід'ємні лишки чисел $ax=\rho_1,\rho_2,...,\rho_l$ пробігатимуть, за твердженням 2.4.2., таку ж саму систему лишків, проте в іншому порядку, тобто

$$ar_1\equiv\rho_1(\bmod m),\quad ar_2\equiv\rho_2(\bmod m),\quad \cdots,\quad ar_l\equiv\rho_l(\bmod m). \qquad (2.37)$$

Перемножуючи конгруенції (2.37), отримаємо

$$a^l r_1r_2\cdots r_l\equiv\rho_1\rho_2\cdots\rho_l\,(\bmod m). \qquad (2.38)$$

Скоротивши (2.38) на добуток $r_1r_2\cdots r=\rho_1\rho_2\cdots\rho_l$, який є взаємно простим з m, матимемо

$$a^l\equiv1(\bmod m),$$

або

$$a^{\varphi(m)}\equiv1(\bmod m).$$

Теорема Ферма. Нехай p – просте число і $(p,a)=1$. Тоді

$$a^{p-1} \equiv 1 (\mathrm{mod}\, p). \qquad (2.39)$$

Дійсно, оскільки $\varphi(p)=p-1$, то з теореми Ейлера випливає формула (2.39), тобто теорема Ферма.

Теорема Ферма інколи формулюється у вигляді

$$a^{p} \equiv a (\mathrm{mod}\, p). \qquad (2.40)$$

Формула (2.40) отримується з (2.39) множенням обох частин конгруенції (2.39) на a.

Приклад 2.4.4. Знайти найменший додатний лишок числа 13^{26} за модулем 10.

Розв'язання. Оскільки $13 \equiv 3 (\mathrm{mod} 10)$, то $13^{26} \equiv 3^{26} (\mathrm{mod} 10)$. Так як $(3,10)=1$, то, застосувавши теорему Ейлера, де $\varphi(10)=\varphi(2)\cdot\varphi(5)=4$, дістанемо $3^4 \equiv 1 (\mathrm{mod} 10)$, а отже $3^{26} \equiv (3^4)^6 \cdot 3^2 \equiv 9 (\mathrm{mod} 10)$. Тому $13^{26} \equiv 9 (\mathrm{mod} 10)$. Отже найменшим додатним лишком числа 13^{26} за модулем 10 – це 9.

Приклад 2.4.5. Знайти остачу від ділення числа $5^{5^{1000}}$ на 325.

Розв'язання. Зауважимо, що остача x від ділення числа $5^{5^{1000}}$ на 325 справджує конгруенцію

$$5^{5^{1000}} \equiv x (\mathrm{mod}\, 325), \quad 0 \le x < 325.$$

Оскільки $\left(5^{5^{1000}}, 325\right) = \left(5^{5^{1000}}, 13\cdot 25\right) = 25 = 5^2$, то прийдемо до еквівалентної конгруенції

$$5^{5^{1000}-2} \equiv x_1 (\mathrm{mod} 13), \quad x = 5^2 \cdot x_1.$$

Знайдемо остачу $0 \le y < 12$ від ділення $5^{1000}-2$ на $\varphi(13)=12$. Тоді справджуються конгруенції

$$5^{1000}-2 \equiv y \pmod{12}$$

і

$$5^{5^{1000}-2} \equiv 5^{y} \pmod{13} \equiv x_1 \pmod{13}.$$

Далі , оскільки, $(5,12)=1$ і $\varphi(12)=4$, то $5^4 \equiv 1 \pmod{12}$. Отже

$$5^{1000}-2=$$

$$5^{4\cdot 250}-2=\left(5^4\right)^{250}-2 \equiv 1-2 \equiv -1+12 \equiv 11 \pmod{12}$$

і $y \equiv 11 \pmod{12}$. Тому $5^{11} \equiv x_1 \pmod{13}$. Так як $5^{11} \equiv 5^3 \pmod{13} \equiv 8 \pmod{13}$, то $x_1 = 8$ і $x = 25 \cdot 8 = 200$. Отже остача від ділення $5^{5^{1000}-2}$ на 325 дорівнює 200.

2.4.4. Тестування простоти

Теорема Ферма стверджує, що якщо число $n-$ просте, то для довільного $a \in \{2,3,...,n-1\}$ виконується (2.39), тобто

$$a^{n-1} \equiv 1 \pmod{n}. \qquad (2,41)$$

Зауважимо, що протилежне твердження , взагалі кажучи, невірне.

З цього твердження випливає, що якщо конгруенція $(2,41)$ не виконується хоча б для одного $a \in \{2,3,...,n-1\}$, то число $n-$ складене.

Тому можна запропонувати наступний ймовірнісний тест простоти [3]:

1. вибираємо випадкове $a \in \{2,3,...,n-1\}$ і перевіряємо з допомогою алгоритму Евкліда умову $(a,n)=1$. Якщо ця умова не виконується, то $n-$ складене;

2. перевіряємо умову $(2,41)$. Якщо $(2,41)$ не виконується,то число $n-$ складене;

3. якщо конгруенція $(2,41)$ справджується, то відповідь невідома, але можна повторити тест ще декілька разів. При його використанні виникає одна з двох ситуацій:

- число $n-$ просте і тест завжди говорить «невідомо»;
- число $n-$ складене і тест з ймовірністю не менше $\frac{1}{2}$ дає відповідь «$n-$ складене».

Визначення 2.4.4. Непарне число n, яке справджує конгруенцію (2.41), але не є простим, *називається псевдопростим числом Ферма за основою* a.

Деякі складені числа є псевдопростими за довільною основою. Такі псевдопрості числа називаються *числами Кармайкла*, найменше з яких є число $561=3\cdot11\cdot17$.

2.5. Розв'язування лінійних конгруенцій та систем конгруенцій.

2.5.1. Основні поняття про конгруенції з однією змінною

Надалі будемо вивчати конгруенції з однією змінною подібно до алгебраїчних рівнянь з однією змінною. Проте між рівняннями і конгруенціями є й відмінності, оскільки рівняння та їх розв'язки розглядаються в полі дійсних чи

комплексних чисел, а конгруенції та їх розв'язки – в скінчених кільцях чи полях.

Розглянемо конгруенцію вигляду

$$f(x) \equiv 0 (\mathrm{mod}\, m), \qquad (2.42)$$

де $f(x) = a_0 x^n + a_1 x^{n-1} + a_2 x^{n-2} + \cdots a_n$ – многочлен з цілими коефіцієнтами.

Визначення 2.5.1. Якщо коефіцієнт a_0 многочлена $f(x)$ не ділиться на m, то n називають *степенем конгруенції.*

Визначення 2.5.2. *Розв'язати конгруенцію* (2.42) – це знайти всі значення невідомої x, що справджують цю конгруенцію.

Якщо конгруенцію (2.42) справджує значення x_1, то цю ж конгруенцію справджує і довільне $x \equiv x_1 (\mathrm{mod}\, m)$. Отже весь клас $x \equiv x_1 (\mathrm{mod}\, m)$ вважатимемо розв'язком конгруенції (2.42).

При такому визначенні розв'язку конгруенція (2.42) *матиме стільки розв'язків, скільки лишків повної системи лишків справджує* (2.42).

Приклад 2.5.1. Знайти розв'язки конгруенції

$$x^5 + x + 1 \equiv 0 (\mathrm{mod}\, 7). \qquad (2.43)$$

Розв'язання. Серед повної системи лишків за модулем 7 знайдемо перебором розв'язки конгруенції (2.43). Такими розв'язками є лишки: $x_1 = 2, \quad x_2 = 4.$ Тому розв'язками конгруенції (2.43) є два класи:

$$x \equiv 2 (\mathrm{mod}\, 7), \quad x \equiv 4 (\mathrm{mod}\, 7)$$

і конгруенція (2.43) має два розв'язки.

Приклад 2.5.2. Знайти розв'язки конгруенції

$$x^4 + 2x - 1 \equiv 0 \pmod 7. \qquad (2.44)$$

Розв'язання. Легко переконатись, що жоден лишок з повної системи лишків $0,1,2,3,4,5,6$ за модулем 7 не справджує конгруенцію (2.44), тобто задана конгруенція *не має розв'язків*. Таку конгруенцію називають *несумісною.*

2.5.2. Розв'язування лінійної конгруенції з використанням теореми Ейлера

Кожна конгруенція 1-го степеня (лінійна конгруенція) може бути записана у вигляді

$$ax \equiv b \pmod m. \qquad (2.45)$$

Нехай $(a,m)=1$. Тоді конгруенція (2.45) має єдиний розв'язок.

Дійсно, оскільки $(a,m)=1$, то, за теоремою Ейлера,

$$a^{\varphi(m)} \equiv 1 \pmod m.$$

Припустимо, що конгруенція (2.45) – має розв'язок α. Тоді

$$a\alpha \equiv b \pmod m. \qquad (2.46)$$

Помножимо обидві частини (2.46) на $a^{\varphi(m)-1}$. Матимемо

$$a^{\varphi(m)}\alpha \equiv ba^{\varphi(m)-1} \pmod m.$$

Використовуючи теорему Ейлера, прийдемо до подання єдиного розв'язку конгруенції (2.45) у вигляді

$$\alpha \equiv ba^{\varphi(m)-1}. \qquad (2.47)$$

Приклад 2.5.3. Розв'язати конгруенцію

$$5x \equiv 3 \pmod{12}.$$

Розв'язання. Оскільки $(5,12)=1,$ то конгруенція має єдиний розв'язок, який знайдемо у формі (2.47). Оскільки $\varphi(12)=\varphi(3)\cdot\varphi(4)=2\cdot 2=4,$ то

$$\alpha = 3\cdot 5^3 = 3\cdot 125 = 375 \equiv 3(\mathrm{mod}12).$$

Запропонований спосіб відшукання розв'язку лінійної конгруенції (2.45) у формі (2.47) для великих m – громіздкий і вимагає піднесення до високого степеня за модулем. Ця задача заслуговує окремої уваги і буде розглянута далі.

2.5.3. Розв'язування лінійної конгруенції з використанням ланцюгових дробів.

Вкажемо інший підхід до відшукання єдиного, в сенсі визначення 5.2.2., розв'язку лінійної конгруенції (2.45), який ґрунтується на використанні скінчених ланцюгових дробів.

1. Припустивши, що $(a,m)=1,$ розкладемо раціональний дріб $\dfrac{m}{a}$ в скінченний ланцюговий дріб

$$\frac{m}{a}=[q_1,q_2,...,q_n] \qquad (2.48)$$

і розглянемо два останні підхідні дроби для ланцюгового дробу (2.48)

$$\frac{P_{n-1}}{Q_{n-1}},\quad \frac{P_n}{Q_n}=\frac{m}{a}.$$

За властивістю 1 підхідних дробів ланцюгового дробу маємо

$$mQ_{n-1}-aP_{n-1}=(-1)^n,\quad aP_{n-1}\equiv(-1)^{n-1}(\mathrm{mod}\,m),$$

звідки отримуємо

$$a(-1)^{n-1} P_{n-1} b \equiv b(\mathrm{mod}\, m).$$

Отже, розв'язок конгруенції (2.45) можна записати у формі

$$x \equiv (-1)^{n-1} P_{n-1} b(\mathrm{mod}\, m). \qquad (2.49)$$

Приклад 2.5.4. Розв'язати конгруенцію

$$37x \equiv 25(\mathrm{mod}107).$$

Розв'язання. Для того, щоб переконатись в тому, що $(37,107)=1$, застосуємо алгоритм Евкліда.

Маємо

$$107 = 37 \cdot 2 + 33,$$
$$37 = 33 \cdot 1 + 4,$$
$$33 = 4 \cdot 8 + 1,$$
$$4 = 1 \cdot 4.$$

Отже $(37,107)=1$ і ця конгруенція має єдиний розв'язок. Окрім того, ця процедура дала можливість подати раціональний дріб $\frac{107}{37}$ у вигляді ланцюгового дробу, а саме

$$\frac{107}{37} = [2,\ 1,\ 8,\ 4].$$

Складемо таблицю чисельників підхідних дробів $\frac{P_k}{Q_k}$, $k = 0,1,2,3,4$, використовуючи рекурентну формулу (2.24)

	2	1	8	4
1	2	3	26	107

Тоді розв'язок конгруенції $37x \equiv 25 (\mathrm{mod} 107)$ знайдемо за формулою (2.49). Тут $n = 4, \quad P_3 = 26, \quad b = 25$ і остаточно маємо

$$x \equiv (-1)^3 \cdot 26 \cdot 25 \equiv -650 (\mathrm{mod} 107) \equiv 99 (\mathrm{mod} 107).$$

2. Нехай $(a, m) = d$ *і* d *не ділить* b. Тоді конгруенція $(2,45)$ – несумісна.

Для доведення цього факту підемо від супротивного, тобто припустимо, що конгруенція (2.45) має розв'язок, тобто існує α, для якого

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

Ця конгруенція еквівалентна рівності

$$b = a\alpha - mq,$$

де $q \in \mathbb{Z}$. Оскільки $d \mid ax - mq$, то $d \mid b$. А ця подільність заперечує припущення, що d не ділить b. Це протиріччя й доводить твердження про несумісність лінійної конгруенції (2.45) при зазначених умовах.

Приклад 2.5.5. Розв'язати конгруенцію

$$4x \equiv 17 (\mathrm{mod} 10).$$

Розв'язання. Оскільки $(4,10) = 2$ і 2 не ділить 17, то конгруенція не має розв'язків.

3. *Нехай* $(a, m) = d$ *і* d *ділить* b. Тоді конгруенція (2.45) має d різних розв'язків, а саме:

$$\alpha, \quad \alpha + \frac{m}{d}, \quad \alpha + \frac{2m}{d}, \quad ..., \quad \alpha + \frac{(d-1)m}{d},$$

де α – розв'язок конгруенції

$$\frac{a}{d} x \equiv \frac{b}{d} (\mathrm{mod}\, m_1); \quad m_1 = \frac{m}{d} \qquad (2.50)$$

Дійсно, після скорочення конгруенції $ax \equiv b \pmod m$, на $d = (a, m)$, прийдемо до конгруенції (2.50), яка має єдиний розв'язок.

Нехай α – найменший додатний лишок розв'язку конгруентності (2.50). Тоді всі розв'язки цієї конгруенції знайдуться у формі

$$x \equiv \alpha \pmod{m_1}, \quad m_1 = \frac{m}{d}. \qquad (2.51)$$

Числа (2.51) за модулем m утворюють не один розв'язок, а стільки розв'язків, скільки є чисел (2.51) в повній системі лишків $0, 1, 2, ..., m-1$. Легко бачити, що в цей ряд потрапляють числа:

$$\alpha, \quad \alpha + m_1, \quad \alpha + 2m_1, \quad ..., \quad \alpha + (d-1)m_1, \quad (2.52)$$

Тобто конгруенція (2.45) в цьому випадку має d розв'язків (2.52).

Приклад 2.5.6. Розв'язати конгруенцію

$$111x \equiv 75 \pmod{321}. \qquad (2.53)$$

Розв'язання. Оскільки $d = (111, 321) = 3$ і 3 ділить 75, то конгруенція (2.53) має 3 розв'язки, які знайдемо за формулами (2.52) :

$$x_0 \equiv 99 \pmod{321}, \quad x_1 \equiv 99 + 107 \equiv 206 \pmod{321},$$

$$x_2 \equiv 99 + 2 \cdot 107 \equiv 313 \pmod{321}.$$

Зауважимо, що після скорочення конгруенції (2.53) на 3, прийдемо до конгруенції прикладу 2.5.4. $37x \equiv 25 \pmod{107}$, розв'язок якої $x \equiv 99 \pmod{107}$ вже знайдено.

2.5.4. Китайська теорема про лишки.

Розглянемо найпростішу лінійну систему конгруенцій

$$x \equiv b_1 \pmod{m_1}, \ldots, x \equiv b_k \pmod{m_k} \qquad (2.54)$$

з однією змінною, проте з різними і попарно простими модулями.

Розв'язати систему (2.54) можна , застосовуючи наступну теорему

Теорема 2.5.1.(Китайська теорема про лишки).Нехай для системи (2.54) числа M_s і M_s' $s = \overline{1,k}$ визначені умовами:

$$M_i m_i = m_1 \cdot m_2 \cdots m_k,$$
$$M_i M_i' \equiv 1 \pmod{m_i}, \quad i = \overline{1,k}.$$

і нехай

$$x_0 = M_1 M_1' b_1 + M_2 M_2' b_2 + \cdots + M_k M_k' b_k. \qquad (2.55)$$

Тоді розв'язок системи (2.54) визначиться конгруенцією

$$x \equiv x_0 \pmod{m_1 \cdot m_2 \cdots m_k}. \qquad (2.56)$$

Доведення. Дійсно, оскільки для довільного $i \neq j$, $i = \overline{1,k}$ $m_i \mid M_j$, то

$$x_0 \equiv M_i M_i' b_i \pmod{m_i}.$$

Отже, система (2.54) еквівалентна до системи:

$$x \equiv x_0 \pmod{m_1}, \quad x \equiv x_0 \pmod{m_2}, \quad \cdots, \quad x \equiv x_0 \pmod{m_k}.$$

Враховуючи властивість конгруенцій 13, отримуємо, що систему (2.54) справджують ті і тільки ті значення x, які справджують конгруенцію (2.56).

Приклад 2.5.7. Знайти натуральне число, яке не перевищує 100 і яке при діленні на 3,5, і 7 дає остачі 2,4 і 3 відповідно.

Розв'язання. Позначимо невідоме число x. Тоді для його відшукання, вийшовши з умови прикладу, отримаємо систему конгруенцій:

$$x \equiv 2(\mathrm{mod}\,3), \quad x \equiv 4(\mathrm{mod}\,5), \quad x \equiv 3(\mathrm{mod}\,7).$$

Розв'яжемо цю систему конгруенцій, використовуючи КТЛ, тобто формули $(2.55), (2.56)$. Маємо

$$M_1 = \frac{3\cdot 5\cdot 7}{3} = 35, \quad M_2 = \frac{3\cdot 5\cdot 7}{5} = 21, \quad M_3 = \frac{3\cdot 5\cdot 7}{7} = 15.$$

$$2M_1' \equiv 1(mod\,3), \quad M_2' \equiv 1(mod\,5), \quad M_3' \equiv 1(mod\,7),$$

З конгруенції $2M_1' \equiv 1(mod\,3)$, методом підбору, знайдемо

$$M_1' \equiv 2(\mathrm{mod}\,3).$$

Отже, подамо розв'язок (2.56) системи прикладу 2.5.7, з використанням формули (2.55) у вигляді

$$x_0 = 35\cdot 2\cdot 2 + 21\cdot 1\cdot 4 + 15\cdot 1\cdot 3 =$$

$$= 140 + 84 + 75 = 269 \equiv 59(\mathrm{mod}\,3\cdot 5\cdot 7) \equiv 59(\mathrm{mod}105).$$

Перевіркою переконуємось, що цей розв'язок справджує кожну з конгруенцій системи прикладу 2.5.7.

Розглянемо тепер загальний випадок, коли модулі $m_1, m_2, ..., m_k$ можуть і *не бути взаємно простими*. З'ясуємо, за яких умов система конгруенцій (2.54) сумісна. Для цього доведемо спочатку наступне

Твердження 2.5.1. Якщо $m = p_1^{\alpha_1} p_2^{\alpha_2} \cdots p_n^{\alpha_n}$ – канонічний розклад числа m, то конгруенція

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

еквівалентна до системи конгруенцій:

$$x \equiv a \left(\mathrm{mod}\, p_1^{\alpha_1}\right),\ x \equiv a \left(\mathrm{mod}\, p_2^{\alpha_2}\right),$$
$$\cdots, \qquad (2.57)$$
$$x \equiv a \left(\mathrm{mod}\, p_n^{\alpha_n}\right).$$

Доведення. Якщо β – довільний розв'язок конгруенції (2.54), то $m \mid \beta - a$, а тому $p_i^{\alpha_i} \mid \beta - a$, тобто $\beta \equiv a \left(\mathrm{mod}\, p_i^{\alpha_i}\right)$, $i = \overline{1,n}$. А це означає, що β – розв'язок системи конгруенцій (2.57).

Навпаки, якщо β – розв'язок системи конгруенцій (2.54), то, за властивістю 13, $\beta \equiv a (\mathrm{mod}\, m)$, оскільки $m = \left[p_1^{\alpha_1} p_2^{\alpha_2} \cdots p_n^{\alpha_n} \right]$.

Наслідок 2.5.1. Система конгруенцій

$x \equiv b_1 (\mathrm{mod}\, m_1)$, $x \equiv b_2 (\mathrm{mod}\, m_2)$, $\cdots$, $x \equiv b_k (\mathrm{mod}\, m_k)$

еквівалентна до системи конгруенцій

$x \equiv b_1 (\mathrm{mod}\, q_1)$, $x \equiv b_2 (\mathrm{mod}\, q_2)$, $\cdots$, $x \equiv b_t (\mathrm{mod}\, q_t)$, $k \le t$,

де $q_1, q_2, ..., q_t$ – степені множників $m_1, m_2, ..., m_k$.

Ознаку сумісності системи конгруенцій (2.54) при довільних m_i, $i = \overline{1,k}$ пропонує наступна теорема, яку приймемо без доведення.

Теорема 5.2.2. Система конгруенцій (2.54) сумісна тоді і тільки тоді, коли

$$b_i \equiv b_j \left(\mathrm{mod}\left(m_i, m_j\right)\right), \quad i \ne j, \quad i, j = \overline{1,k}. \qquad (2.58)$$

(нагадаємо, що $\left(m_i, m_j\right)$ – найбільший спільний дільник чисел m_i, m_j).

Приклад 2.5.8. Дослідити систему конгруенцій на сумісність

$$x \equiv 7 (\mathrm{mod} 15), \quad x \equiv 2 (\mathrm{mod} 35), \quad x \equiv 16 (\mathrm{mod} 21). \ (2.59)$$

Якщо система сумісна, то знайти її розв'язок.

Перевіряємо виконання умови сумісності для (2.59):

$$(15,35)=5,\quad 7\equiv 2(\mathrm{mod}\,5);$$
$$(15,21)=3,\quad 7\equiv 16(\mathrm{mod}\,3);$$
$$(35,21)=7,\quad 2\equiv 16(\mathrm{mod}\,7);$$

Оскільки

$$15=3\cdot 5,\quad 35=5\cdot 7,\quad 21=3\cdot 7,$$

то, за наслідком із твердження 5.2.1., система (2.54) еквівалентна до системи:

$$x\equiv 7(\mathrm{mod}\,3),\quad x\equiv 7(\mathrm{mod}\,5),\quad x\equiv 2(\mathrm{mod}\,5),$$
$$x\equiv 2(\mathrm{mod}\,7),\quad x\equiv 16(\mathrm{mod}\,3),\quad x\equiv 16(\mathrm{mod}\,7).$$

Відкидаючи зайві конгруенції, прийдемо до такої системи конгруенцій:

$$x\equiv 1(\mathrm{mod}\,3),\quad x\equiv 2(\mathrm{mod}\,5)\quad x\equiv 2(\mathrm{mod}\,7).$$

Розв'яжемо останню, застосувавши КТЛ. Маємо

$$M_1=5\cdot 7=35,\quad M_2=3\cdot 7=21,\quad M_3=3\cdot 5=15,$$
$$2M_1'\equiv 1(\mathrm{mod}\,3),\quad M_2'\equiv 1(\mathrm{mod}\,5),\quad M_3'\equiv 1(\mathrm{mod}\,7).$$

Методом підбору знаходимо $M_1'\equiv 2(\mathrm{mod}\,3)$. Тоді за формулою (2.56) , з використанням (2.55) отримуємо розв'язок конгруенції (2.59), а саме

$$x_0=35\cdot 2+21\cdot 2+15\cdot 2=142\equiv 37(\mathrm{mod}\,105).$$

Перевіркою переконуємось, що цей розв'язок справджує кожну з конгруенцій системи (2.59). Дійсно,

$$37\equiv 7(\mathrm{mod}\,15),\quad 37\equiv 2(\mathrm{mod}\,35)\quad 37\equiv 16(\mathrm{mod}\,21).$$

2.5.5. Піднесення до степеня за модулем

Піднесення до степеня за модулем використовується в багатьох задачах теорії чисел. Ця задача може бути сформульована, як задача обчислення функції $f(x) = x^l$, де $x-$елементк ільця $\mathbb{Z}_m$. Прямолінійна програма для цієї функції виражається такою процедурою і має складність $l-1$:

$$\begin{aligned} z_1 &= x \cdot x, \\ z_2 &= z_1 \cdot x, \\ z_3 &= z_2 \cdot x, \\ &\cdots\cdots\cdots \\ z_{l-1} &= z_{l-2} \cdot x. \end{aligned} \qquad (2.60)$$

В цьому алгоритмі завжди можна вважати, що $l < m.$ Інакше, можна скористатись теоремою Ейлера, щоб понизити показник. Якщо ми використаємо для розв'язання задачі піднесення до степеня за модулем наведену прямолінійну процедуру (2.60), то отримаємо експоненціальний алгоритм з довжиною входу порядку $\log m,$ а кількість операцій має порядок m.

Проте, є ощадливіший алгоритм, який був відомий ще до нашої ери в Індії. Це $-$бінарний метод, який базується на поданні показника l у двійковій системі числення. Для обчислення x^d подамо показник d у вигляді

$$d = (d_n, d_{n-1}, ..., d_1, d_0), \quad d_i \in \{0,1\}, \quad d = \sum_{i=0}^{n} d_i 2^i.$$

Тоді результат піднесення до степеня x^d за модулем m можна виразити такою рекурентною процедурою

$$\left(\left(\left(\left(x^{d_n}\right)^2 x^{d_{n-1}}\right)^2 x^{d_{n-2}}\right)^2 \cdots\right)^2 x^{d_0} = \tag{2.61}$$

$$= x^{d_n 2^n + d_{n-1} 2^{n-1} + d_{n-2} 2^{n-2} + \cdots + d_0 2^0} = x^d.$$

При цьому витрачається $n + \sum_{i=0}^{n-1} d_i \le 2n \le 2\log_2 d$ множень.

2.5.6. Застосування лінійних конгруенцій та бінарного алгоритму піднесення до степеня в криптосистемі RSA

Запропонована в 1977 р. криптосистема RSA є чи не найпотужнішою криптосистемою з відкритим ключем.

Генерація ключів в криптосистемі RSA полягає у виборі досить великих простих чисел p і q. Для їх добутку визначена функція Ейлера $\varphi(n) = \varphi(pq) = n - p - q + 1$. Далі випадковим чином вибирають елемент e такий, що не перевищує значення $\varphi(n)$ і $\text{НСД}(e, \varphi(n)) = 1$. Тоді знаходять інверсію d до елемента e за модулем $\varphi(n)$, тобто розв'язують конгруенцію

$$ed \equiv 1 \left(\mathrm{mod}\, \varphi(n)\right). \tag{2.62}$$

Конгруенцію (2.62) можна розв'язати, наприклад, методом ланцюгових дробів. Як результат отримують :

Відкритий ключ: e, n;

Таємний ключ: d.

Шифрування відбувається блоками. Для цього повідомлення записують у цифровій формі і розбивають на блоки так, що кожен блок визначає число, яке не перевищує n. Блок M розглядається як елемент кільця $\mathbb{Z}_n = \mathbb{Z} / n\mathbb{Z}$.

Алгоритм шифрування E в системі RSA полягає у піднесенні M до степеня e за модулем n.

$$E(M) = M^e \pmod n \qquad (2.63)$$

Отже (2.63) – це блок криптотексту $C = E(M)$.

Алгоритм дешифрування D блоку криптотексту C полягає у піднесенні C до степеня d – таємного ключа цієї криптосистеми, тобто

$$D(C) = C^d \pmod n.$$

Отже , як бачимо, і для шифрування криптотексту, так і для його дешифрування в системі RSA потрібно вміти підносити число до степеня за модулем. Оскільки числа p, q, n при описаному формуванні ключів повинні бути достатньо великими, то потрібно мати ефективні алгоритми піднесення до степеня за модулем. Одним з таких алгоритмів є відомий ще до нашої ери в Індії бінарний метод, який описаний вище.

Приклад 2.5.9. Нехай $p = 53, q = 67$. Тоді $n = 3551$ і $\varphi(n) = 3432$. Зашифрувати з допомогою криптосистеми RSA повідомлення «HI».

Розв'язання. Виберемо $e = 1021$ і, розв'язавши конгруенцію $1021d \equiv 1 \pmod{3432}$, знайдемо $d = 1237$. Отже маємо:

Відкритий ключ: 3551, 1021;

Таємний ключ 1237.

Шифрування. Припустимо,що нам потрібно надіслати повідомлення «HI», якому відповідає цифрова форма $M = 1711$. Подаючи число $e = 1021$ двійковим числом $e = 1111111101$ і застосувавши процедуру (2.61), знайдемо числовий криптотекст $C = 1711^{1021} \pmod{3551} \equiv 1844 \pmod{3551}$.

Дешифрування. Подаючи таємний ключ $d=1237$ двійковим числом $d=10011010101$ і застосувавши рекурентну процедуру (2.61), прийдемо до вихідного тексту в цифровій формі $D(C)=1844^{1237}\equiv 1711(\mathrm{mod}\,3551)$.

2.6. Квадратичні лишки.

Квадратичні лишки мають ряд застосувань в криптографії та в криптології. Зокрема, на мові символа Якобі, який є узагальненням символа Лежандра, формулюється тест простоти Соловея-Штрассена $[3,10]$

Квадратичні лишки використовуються також й при ймовірнісному криптуванні. Поняття псевдоквадрата, з допомогою якого створюють відкритий ключ при ймовірнісному криптуванні також передбачає знайомство з символамиЛежандра та Якобі.

2.6.1.Визначення та властивості.

Розглянемо конгруенцію

$$x^2\equiv a(\mathrm{mod}\,m) \qquad (2.64)$$

за умови, що $(a,m)=1$.

Визначення 2.6.1.

- Якщо конгруенція (2.64) має розв'язок, то число a називається *квадратичним лишком за модулем* m.
- Якщо конгруенція (2.64) не має розв'язків, то число a називається *квадратичним нелишком за модулем* m.

Приклад 2.6.1. Переірити, що:

а) число 8 – квадратичний лишок за модулем 17;

б) число 12 – квадратичний нелишок за модулем 17.

Розв'язання.

а) Легко переконатись, що

$$5^2 \equiv 8 (\mathrm{mod} 17),$$

тобто конгруенція (2.64) справджується для $a = 8, \quad x = 5.$

б) Перевірку твердження, що $a = 12 -$ квадратичний нелишок за модулем 17 здійснимо, перебравши всі квадрати із зведеної системи лишків за модулем 17:

$$2^2 = 4, \quad 3^2 = 9, \quad 4^2 = 16, \quad 5^2 = 25 \equiv 8, \quad 6^2 = 36 \equiv 2,$$

$$7^2 = 49 \equiv 15, \; 8^2 = 64 \equiv 13, \; 9^2 = 81 \equiv 13,$$

$$10^2 = 100 \equiv 15, \; 11^2 = 121 \equiv 2,$$

$$12^2 = 144 \equiv 8, \; 13^2 = 169 \equiv 16, \; 14^2 = 196 \equiv 9,$$

$$15^2 = 225 \equiv 4, \; 16^2 = 256 \equiv 1.$$

Як бачимо, серед цих квадратів нема числа 12, а тільки числа $1, 2, 4, 8, 9, 13, 15, 16$. Отже $12 -$ квадратичний нелишок за модулем 17.

Розглянемо далі квадратичну конгруенцію за простим модулем, тобто

$$x^2 \equiv a (\mathrm{mod}\, p), \quad (a, p) = 1. \qquad (2.65)$$

Вкажемо основні властивості квадратичної конгруенції (2.65).

Властивість 1. *Якщо* $a -$ квадратичний лишок за модулем p, то конгруенція (2.65) має два розв'язки.

Дійсно, якщо $x_1 -$ розв'язок конгруенції (2.65), то $-x_1$ також є розв'язком конгруенції (2.65), оскільки $(-x_1)^2 = x_1^2 \equiv a (\mathrm{mod}\, p)$.

Окрім того, $x_1 \neq -x_1$, бо інакше конгруенція $2x_1 \equiv 0 (\mathrm{mod}\, p)$ мала б більше ніж один розв'язок, а це неможливо, оскільки $(2, p) = (x_1, p) = 1$. Чкркз те, що

конгруенція (2.65) не може мати більше, ніж два розв'язки $[5]$, то інших розв'язків немає.

Властивість 2. Зведена система лишків за модулем p складається з $\frac{p-1}{2}$ квадратичних лишків, які конгруентні з числами

$$1^2, 2^2, 3^2, ..., \left(\frac{p-1}{2}\right)^2 \qquad (2.66)$$

і $\frac{p-1}{2}$ квадратичних нелишків.

Дійсно, серед лишків зведеної системи лишків за модулем p квадратичними лишками є ті і тільки ті, які конгруентні з квадратами чисел зведеної системи лишків:

$$-\frac{p-1}{2}, ..., -2, -1, 1, 2, ..., \frac{p-1}{2},$$

тобто числами (2.66).

Зауважимо, що числа (2.66) не конгруентні за модулем p, оскільки з конгруенції

$$k^2 = l^2 \pmod p, \quad 0 < k < l \le \frac{p-1}{2}$$

випливало б, що конгруенція другого степеня $x^2 \equiv l^2 \pmod p$ мала б чотири розв'язки: $-l, l, -k, k$, що неможливо.

Приклад 2.6.2. Вказати всі квадратичні лишки і нелишки за модулем 17.

Розв'язання. В прикладі 2.6.1. ми знайшли квадрати всіх чисел із зведеної системи чисел за модулем 17. Таким чином, ми вказали всі квадратичні лишки за модулем 17. Це числа:

1, 2, 4, 8, 9, 13, 15, 16.

Решта чисел із зведеної системи лишків за модулем 17, тобто числа

$$3,\quad 5,\quad 6,\quad 7,\quad 10,\quad 11,\quad 12,\quad 14,$$

за властивістю 2, є квадратичними нелишками за модулем 17.

Властивість 3. *Якщо* $a-$ квадратичний лишок за модулем p, то

$$a^{\frac{p-1}{2}} \equiv 1 \pmod{p}, \qquad (2.67)$$

якщо $a-$ квадратичний нелишок за модулем p, то

$$a^{\frac{p-1}{2}} \equiv -1 \pmod{p}. \qquad (2.68)$$

Дійсно, за теоремою Ферма

$$a^{p-1} \equiv 1 \pmod{p},$$

звідки, застосувавши формулу для різниці квадратів, маємо

$$\left(a^{\frac{p-1}{2}} - 1\right)\left(a^{\frac{p-1}{2}} + 1\right) \equiv 0 \pmod{p}.$$

Зауважимо, що два множники, які знаходяться ліворуч в останній конгруенції, не можуть одночасно ділитись на p. Якби це було так, то справджувалась би конгруенція

$$\left(a^{\frac{p-1}{2}} - 1\right) - \left(a^{\frac{p-1}{2}} + 1\right) \equiv 2 \pmod{p},$$

що неможливо, оскільки $(2, p) = 1$. Отже, справедливе одне з двох співвідношень (2.67) або (2.68).

Покажемо, що квадратичний лишок справджує конгруенцію (2.67). Дійсно, для квадратичного лишка a, за визначенням, справджується конгруенція

$$x^2 \equiv a \pmod{p}$$

і

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

Тому квадратичний лишок справджує конгруенцію (2.67). Кількість квадратичних лишків дорівнює $\frac{p-1}{2}$, оскільки конгруенція (2.67) не може мати більше ніж $\frac{p-1}{2}$ розв'язків$[5]$.

З попередніх міркувань робимо висновок, що всі квадратичні нелишки справджують конгруенцію (2.68) і їх кількість також дорівнює $\frac{p-1}{2}$.

2.6.2. Символ Лежандра

Нехай $(a, p) = 1$. Введемо *символ Лежандра*

$$\left(\frac{a}{p}\right) \overset{df}{=} a^{\frac{p-1}{2}} (\mathrm{mod}\, p). \qquad (2.69)$$

З властивості 3 випливає, що, за умови $(a, p) = 1$, маємо

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

Подальші властивості символу Лежандра дозволяють встановити можливість розв'язальності конгруенції

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

а не спосіб розв'язання цієї конгруенції.

Властивості символу Лежандра.

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

2. $\left(\frac{1}{p}\right) = 1.$

3. $\left(\frac{-1}{p}\right) = (-1)^{\frac{p-1}{2}} = \begin{cases} 1 & якщо \quad p = 4m+1, \\ -1 & якщо \quad p = 4m+3. \end{cases}$

4. $\left(\frac{a_1 \cdot a_2 \cdots a_k}{p}\right) = \left(\frac{a_1}{p}\right) \cdot \left(\frac{a_2}{p}\right) \cdots \left(\frac{a_r}{p}\right).$

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

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

$$= \begin{cases} 1, & якщо \quad p = 8m+1 \quad або \quad p = 8m+7, \\ -1, якщо & p = 8m+3 \quad або \quad p = \quad 8m+5. \end{cases}$$

7. *Квадратичний закон взаємності*.

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

Властивості 1-3 пропонуємо довести самостійно.

Властивість 4 також майже очевидна. Дійсно

$$\left(\frac{a_1 \cdot a_2 \cdots a_k}{p}\right) = \left(a_1 \cdot a_2 \cdots a_k\right)^{\frac{p-1}{2}} = a_1^{\frac{p-1}{2}} \cdot a_2^{\frac{p-1}{2}} \cdots a_k^{\frac{p-1}{2}} =$$

$$= \left(\frac{a_1}{p}\right) \cdot \left(\frac{a_2}{p}\right) \cdots \left(\frac{a_r}{p}\right).$$

Властивість 5 – це наслідок властивості 4 та визначення квадратичного лишку.

Властивості 6,7 доводяться складно і ми обмежимось їх практичним застосуванням. Доведення цих властивостей можна знайти,наприклад, в $[5]$.

2.6.3. Символ Якобі

Нехай P – довільне непарне число, яке більше ніж одиниця і для якого заданий розклад на прості множники

$$P = p_1 \cdot p_2 \cdots p_k,$$

серед яких можуть бути й однакові. Нехай, до того ж, $(a, P) = 1$.

Символом Якобі називається добуток

$$\left(\frac{a}{P}\right) = \left(\frac{a}{p_1}\right) \cdot \left(\frac{a}{p_2}\right) \cdots \left(\frac{a}{p_k}\right), \qquad (2.70)$$

де $\left(\frac{a}{p_i}\right)$, $i = \overline{1,k}$ – символи Лежандра.

Зокрема, якщо $P = p$ – просте , то $\left(\frac{a}{p}\right)$ – символ Лежандра.

Властивості символу Лежандра дають можливість встановити аналогічні властивості символу Якобі, на доведенні яких ми зупинятись не будемо, відсилаючи читача(слухача) до відповідної літератури $[3,5]$.

Властивості символу Якобі

1. Якщо $a \equiv b \pmod P$, то $\left(\frac{a}{P}\right) = \left(\frac{b}{P}\right)$.
2. $\left(\frac{1}{P}\right) = 1$.
3. $\left(\frac{-1}{P}\right) = (-1)^{\frac{P-1}{2}}$.

4. $\left(\frac{a_1 \cdot a_2 \cdots a_k}{P}\right) = \left(\frac{a_1}{P}\right) \cdot \left(\frac{a_2}{P}\right) \cdots \left(\frac{a_r}{P}\right)$.

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

6. *Квадратичний закон взаємності*.

Якщо $P > 1, \quad Q > 1, \quad (P,Q) = 1,$ то

$$\left(\frac{Q}{P}\right) = (-1)^{\frac{P-1}{2} \cdot \frac{Q-1}{2}} \left(\frac{P}{Q}\right).$$

Приклад 2.6.3. Обчислити символ Якобі $\left(\frac{219}{1915}\right)$, використовуючи властивості 1-6.

Розв'язання. Переконаємось спочатку, що $(219,1915) = 1,$ використовуючи алгоритм Евкліда. Маємо

$$1915 = 219 \cdot 8 + 163,$$
$$219 = 163 \cdot 1 + 56,$$
$$163 = 56 \cdot 2 + 51,$$
$$51 = 5 \cdot 10 + 1,$$
$$5 = 5 \cdot 1.$$

Далі обчислюємо

$$\left(\frac{219}{1915}\right) = \left(\frac{219}{383 \cdot 5}\right) = \left(\frac{219}{383}\right) \cdot \left(\frac{219}{5}\right) =$$

$$= (-1)^{\frac{219-1}{2} \cdot \frac{383-1}{2}} \left(\frac{383}{219}\right) \cdot \left(\frac{4}{5}\right) = -\left(\frac{383}{219}\right) \cdot \left(\frac{2^2}{5}\right) =$$

$$= -\left(\frac{383}{219}\right) = -\left(\frac{219 \cdot 1 + 164}{219}\right) = -\left(\frac{164}{219}\right) =$$

$$= -\left(\frac{4 \cdot 41}{219}\right) = -\left(\frac{4}{219}\right) \cdot \left(\frac{41}{219}\right) = -\left(\frac{41}{219}\right) =$$

$$= -(-1)^{\frac{41-1}{2} \cdot \frac{219-1}{2}} \left(\frac{219}{41}\right) = -\left(\frac{219}{41}\right) = -\left(\frac{41 \cdot 5 + 14}{41}\right) =$$

$$= = -\left(\frac{14}{41}\right) = -\left(\frac{2}{41}\right)\cdot\left(\frac{7}{41}\right) = -(-1)^{\frac{41^2-1}{8}}(-1)^{\frac{7-1}{2}\cdot\frac{41-1}{2}}\left(\frac{41}{7}\right) =$$

$$= -\left(\frac{42-1}{7}\right) = -\left(\frac{-1}{7}\right) = -(-1)^{\frac{7-1}{2}} = -(-1) = 1.$$

З визначення символу Лежандра випливає: якщо $a-$ квадратичний лишок за модулем p, то $\left(\frac{a}{p}\right)=1$, і навпаки, якщо $\left(\frac{a}{p}\right)=1$, то $a-$ квадратичний лишок за модулем p, тобто рівність $\left(\frac{a}{p}\right)=1$ є критерієм того, що $a-$ квадратичний лишок, або, що конгруенція $x^2 \equiv a(\mathrm{mod}\, p)$ має розв'язок.

Однак для символу Якобі аналогічне твердження не справджується. Справджується тільки наступне твердження: якщо $a-$квадратичний лишок за модулем P і $(a,P)=1$, то $\left(\frac{a}{P}\right)=1$.

Протилежне твердження, взагалі кажучи, невірне, що показує наступний приклад.

Приклад 2.6.4. Число $a=2$ не є квадратичним лишком за модулем $P=15$, бо воно не є квадратичним лишком ні за модулем 3, ні за модулем $5[3]$.

Дійсно, за властивістю 6 символу Лежандра маємо

$$\left(\frac{2}{3}\right)=(-1)^{\frac{3^2-1}{8}}=-1, \quad \left(\frac{2}{5}\right)=(-1)^{\frac{5^2-1}{8}}=-1,$$

проте

$$\left(\frac{2}{15}\right)=\left(\frac{2}{3}\right)\cdot\left(\frac{2}{5}\right)=(-1)\cdot(-1)=1.$$

А це означає, що рівність $\left(\frac{2}{15}\right)=1$ виконується для квадратичного нелишка за модулем $P=15.$ Число $a=2$ називається *псевдоквадратом* за модулем 15

Цей приклад породжує

Визначення 2.6.2. Нехай $a\in\mathbb{Z}_n^*$, де $\mathbb{Z}_n^*$ – зведена система лишків за модулем n (тобто $(a,n)=1$). Якщо a – не є квадратичним лишком за модулем n, проте символ Якобі $\left(\frac{a}{n}\right)=1$, то число a називається *псевдоквадратом* за модулем n.

Псевдоквадрати використовуються при ймовірнісному криптуванні для створення відкритого ключа, про що ми поговоримо згодом.

2.6.4. Частинні випадки знаходження розв'язків квадратичних конгруенцій

1. Добування квадратного кореня за простим модулем.

Випадок 1. Знайти розв'язок конгруенції (2.64)

$$x^2\equiv a\pmod p,$$

якщо $p=4m+3$ і $\left(\frac{a}{p}\right)=1.$

Розв'язання. Маємо

$$a^{\frac{p-1}{2}}=a^{2m+1}\equiv 1\pmod p\Rightarrow a^{2m+1}\cdot a\equiv$$

$$\equiv a\pmod p\Rightarrow a^{2m+2}\equiv a\pmod p,$$

тобто

$$\left(a^{m+1}\right)^2\equiv a\pmod p$$

і розв'язками квадратичної конгруенції (2.64) є пара лишків:

$$x \equiv \pm a^{m+1} \pmod{p}. \qquad (2.71)$$

Приклад 2.6.5. Переконавшись, що $a = 2-$ квадратичний лишок за модулем $p = 311$, знайти розв'язок квадратичної конгруенції

$$x^2 \equiv 2 \pmod{311}. \qquad (2.72)$$

Розв'язання.

а) переконаємось, що $a = 2-$ квадратичний лишок за модулем 311.

Маємо

$$\left(\frac{2}{311}\right) = (-1)^{\frac{311^2-1}{8}} = 1.$$

б) оскільки $311 = 4 \cdot 77 + 3$, то $m = 77$ і розв'язком конгруенції (2.72) за формулою (2.71) є лишки:

$$x \equiv \pm 2^{78} \pmod{311} \equiv \pm 66 \pmod{311}.$$

Випадок 2. Знайти розв'язок конгруенції (2.64)

$$x^2 \equiv a \pmod{p},$$

якщо $p = 8m + 5$ і $\left(\frac{a}{p}\right) = 1.$

Розв'язання .Оскільки $\left(\frac{a}{p}\right) = 1$, то

$$a^{4m+2} \equiv 1 \pmod{p} \Rightarrow a^{2m+1} \equiv \pm 1 \pmod{p} \Rightarrow a^{2m+2} \equiv \pm a \pmod{p}.$$

Зауважимо, що

$$\left(\frac{2}{p}\right) = \left(\frac{2}{8m+5}\right) = (-1)^{\frac{(8m+5)^2-1}{8}} = (-1)^{8m^2+10m+3} = -1.$$

Тому

$$2^{4m+2} \equiv -1 \pmod{p}.$$

Отже для $s=0,$ або $s=1$ справджуються конгруенції

$$a^{2m+2}\cdot 2^{(4m+2)s}\equiv a\pmod p,$$

або

$$\left(a^{m+1}\cdot 2^{(2m+1)s}\right)^2\equiv a\pmod p.$$

Тому розв'язок конгруенції (2.64) в цьому випадку – це пара лишків:

$$x\equiv\pm a^{m+1}\cdot 2^{(2m+1)s}\pmod p,\quad s=0,1.\ (2.73)$$

Приклад 2.6.6. Переконавшись, що $a=3-$ квадратичний лишок за модулем $p=277,$ знайти розв'язок квадратичної конгруенції

$$x^2\equiv 2\pmod{277}.\qquad(2.74)$$

Розв'язання.

а) $\left(\dfrac{3}{277}\right)=(-1)^{\frac{3-1}{2}\cdot\frac{277-1}{2}}\left(\dfrac{277}{3}\right)=\left(\dfrac{9\cdot 23+1}{3}\right)=\left(\dfrac{1}{3}\right)=1.$

б) за формулою (2.73) з урахуванням $277=8\cdot 34+5$ отримуємо розв'язок конгруенції (2.74)

$$x\equiv\pm 3^{35}\cdot 2^{69\cdot s}\pmod{277},\quad s=0,1.$$

Покладемо $s=0.$ Маємо

$$x\equiv\pm 3^{35}\equiv 130\pmod{277}.$$

Легко переконатись, що $(\pm 130)^2\equiv 3\pmod{277},$ тобто що це $-$розв'язки конгруенції (2.74).

Приклад 2.6.7. Розв'яжемо конгруенцію

$$x^2\equiv 5\pmod{29},\qquad(2.75)$$

перевіривши, що $5-$ квадратичний лишок за модулем $p=29.$

Розв'язання. Дійсно

$$\left(\frac{5}{29}\right)=(-1)^{\frac{5-1}{2}\cdot\frac{29-1}{2}}\left(\frac{29}{5}\right)=\left(\frac{29}{5}\right)=\left(\frac{4}{5}\right)=\left(\frac{2^2}{5}\right)=1.$$

Отже $5-$ квадратичний лишок за $\bmod 29$; Оскільки $29=8\cdot 3+5,$ то $m=3$ і за формулою (2.73) маємо

$$x\equiv\pm 5^4\cdot 2^{7s}\,(\bmod 29),\quad s=1.$$

Легко підрахувати, що $x\equiv\pm 11(\bmod 29).$

Перевірка підтверджує, що розв'язок знайдено правильно.

Випадок 3. Знайти розв'язок конгруенції (2.64)

$$x^2\equiv a(\bmod p),$$

якщо $p=8m+1$ і $\left(\frac{a}{p}\right)=1.$

Розв'язання $[1,2]$. Нехай $p=2^l h+1,$ де $l\geq 3$ і $h-$ непарне. За теоремою Ферма маємо

$$a^{2^{l-1}h}\equiv 1(\bmod p)\Rightarrow a^{2^{l-2}h}\equiv\pm 1(\bmod p).\qquad(2.76)$$

Виберемо довільний квадратичний нелишок b за модулем $p.$ Тоді, за критерієм квадратичного нелишку за простим модулем (властивість 3), маємо

$$b^{2^{l-1}h}\equiv -1(\bmod p).\qquad(2.77)$$

З конгруенцій (2.76) і (2.77) випливає, що знайдеться деяке ціле s_1, яке дорівнює 0 або $h,$ для якого справджуються конгруенції:

$$a^{2^{l-2}h}b^{s_1 2^{l-1}}\equiv 1(\bmod p)\Rightarrow a^{2^{l-3}h}b^{s_1 2^{l-2}}\equiv\pm 1(\bmod p).$$

Використавши знову конгруенцію (2.77), з останньої конгруенції отримуємо для деякого цілого невід'ємного s_2

$$a^{2^{l-3}h}b^{s_2 2^{l-2}}\equiv 1(\bmod p)\Rightarrow a^{2^{l-4}h}b^{s_2 2^{l-3}}\equiv\pm 1(\bmod p).$$

Проробивши подібну процедуру $l-3$ рази, прийдемо до конгруенцій:

$$a^h b^{2s_{l-1}} \equiv 1(\mathrm{mod}\, p) \Rightarrow a^{h+1} b^{2s_{l-1}} \equiv a(\mathrm{mod}\, p),$$

звідки остаточно отримуємо

$$x \equiv \pm a^{\frac{h+1}{2}} b^{s_{l-1}} (\mathrm{mod}\, p). \qquad (2.78)$$

Отже задача добування кореня за простим модулем $p = 8m+1$ розв'язана і її розв'язок дається формулою (2.78). Зауважимо, що (2.78) містить довільний нелишок b за модулем p. Вибір нелишка за модулем простого числа описаний, наприклад, в $[1]$.

Приклад 2.6.8. Переконавшись, що $a = 2-$ квадратичний лишок за модулем 97, розв'язати конгруенцію

$$x^2 \equiv 2(\mathrm{mod}\, 97).$$

Розв'язання.

а) $\left(\frac{2}{97}\right) = (-1)^{\frac{97^2-1}{8}} = 1;$

б) $97 = 8 \cdot 12 + 1 = 2^5 \cdot 3 + 1;$

в) за квадратичний нелишок b візьмемо, наприклад, 5. Дійсно,

$$\left(\frac{5}{97}\right) = (-1)^{\frac{5-1}{2}\cdot\frac{97-1}{2}} \left(\frac{97}{5}\right) = \left(\frac{97}{5}\right) = \left(\frac{2}{5}\right) = (-1)^{\frac{25-1}{8}} = -1;$$

г) дотримуючись загального підходу, отримуємо послідовно

$$2^{48} \equiv 1(\mathrm{mod}\, 97), \quad 2^{24} \equiv -1(\mathrm{mod}\, 97),$$

$$5^{48} \equiv -1(\mathrm{mod}\, 97), \quad 2^{24} \cdot 5^{48} \equiv 1(mod\, 97),$$

$$2^{12} \cdot 5^{24} \equiv -1(\mathrm{mod}\, 97), \quad 2^{12} \cdot 5^{72} \equiv 1(\mathrm{mod}\, 97),$$

$$2^6 \cdot 5^{36} \equiv -1(\mathrm{mod}\, 97), \quad 2^6 \cdot 5^{36+48} \equiv 12^{12} \cdot 5^{24} \equiv -1(\mathrm{mod}\, 97),$$

$$2^3\cdot 5^{42}\equiv -1(\mathrm{mod}\,97),\quad 2^3\cdot 5^{42+48}\equiv 1(\mathrm{mod}\,97),$$

$$2^4\cdot 5^{90}\equiv 2(\mathrm{mod}\,97)\Rightarrow\quad x\equiv\pm 2^2\cdot 5^{45}(\mathrm{mod}\,97)\equiv\pm 14(\mathrm{mod}\,97).$$

Перевіркою переконуємось, що розв'язки $x=\pm 14$ справджують конгруенцію $x^2\equiv 2(\mathrm{mod}\,97)$.

Добування квадратного кореня з числа a за модулем $n=p\cdot q$, де p,q – прості непарні і $(a,n)=1$.

Щоб розв'язати задачу добування квадратного кореня за модулем $n=p\cdot q$, де p,q – прості непарні і $(a,n)=1$, доведемо наступну теорему.

Теорема 2.6.1. Нехай $n=p\cdot q$ – добуток двох простих непарних чисел. Припустимо, що число a – взаємно просте з n ($(a,n)=1$) і числа a_1,a_2 справджують конгруенції:

$$a_1\equiv a(\mathrm{mod}\,p),\quad a_2\equiv a(\mathrm{mod}\,q).$$

Тоді справджуються наступні твердження:

1. Якщо ціле число x справджує конгруенцію

$$x^2\equiv a(\mathrm{mod}\,n), \qquad (2.79)$$

тоді лишки

$$x_1\equiv x(\mathrm{mod}\,p),\quad x_2\equiv x(\mathrm{mod}\,q) \qquad (2.80)$$

справджують конгруенції

$$x_1^2\equiv a_1(\mathrm{mod}\,p),\quad x_2^2\equiv a_2(\mathrm{mod}\,q). \qquad (2.81)$$

Навпаки, якщо x_1,x_2 справджують конгруенції (2.81) і визначені конгруенціями (2.80), то x_1,x_2 справджують конгруенцію (2.79).

2. x є квадратичним лишком за модулем n тоді і тільки тоді, коли x є квадратичним лишком за кожним із модулів p і q.

Якщо x є квадратичним лишком за модулем n, то конгруенція (2.79) має в $\mathbb{Z}_n^*$ рівно чотири розв'язки.

Доведення. Твердження 1 випливає із загальної теорії многочленних конгруенцій за складним модулем .

Твердження 2 – це наслідок твердження 1.

Твердження 3 випливає також із твердження 2.5.1.

Приклад 2.6.9. Розв'язати квадратичну конгруенцію

$$x^2 \equiv 58 \pmod{77}. \qquad (2.82)$$

Розв'язання. Оскільки $77 = 7 \cdot 11$, то знайдемо спершу $a_1 \equiv 58 \pmod 7$, $a_2 \equiv 58 \pmod{11}$. Маємо $a_1 \equiv 2 \pmod 7$, $a_2 \equiv 3 \pmod{11}$. За теоремою 2.6.1 і твердженням 2.5.1. квадратична конгруенція (2.82) еквівалентна системі конгруенцій

$$\begin{cases} x_1^2 \equiv 2 \pmod 7, \\ x_2^2 \equiv 3 \pmod{11}. \end{cases} \qquad (2.83)$$

Кожна квадратична конгруенція системи (2.83) має два розв'язки, які знаходяться за формулою (2.71), оскільки $7 = 4 \cdot 1 + 3$, $11 = 4 \cdot 2 + 3$ (випадок 1, $p = 4m + 3$). Знайдемо ці розв'язки.

$$x_1 \equiv \pm 2^2 \pmod 7 \equiv \pm 4 \pmod 7,$$

$$x_2 \equiv \pm 3^3 \pmod{11} \equiv \pm 5 \pmod{11}.$$

За твердженням 2.5.1. знаходимо $4 = 2 \cdot 2$ розв'язки системи конгруенцій (2.83), які отримаємо, використовуючи китайську теорему про лишки. Маємо

$$\overline{x}_i = M_1 \cdot M_1' \cdot b_1 + M_2 \cdot M_2' \cdot b_2, \quad i = 1, 2, 3, 4,$$

де

$$M_1 = 11,\ M_1' = 2,\ M_2 = 7,\ M_2' = 8,$$

$$b_1 = \pm 4 \pmod 7,\ b_2 = \pm 5 \pmod{11}.$$

Отже отримуємо

$$\overline{x}_1 \equiv 11\cdot 2\cdot 4 + 7\cdot 8\cdot 5 = 368 \equiv 60 \pmod{77},$$

$$\overline{x}_2 \equiv 11\cdot 2\cdot 4 + 7\cdot 8\cdot 6 = 424 \equiv 39 \pmod{77},$$

$$\overline{x}_3 \equiv 11\cdot 2\cdot 3 + 7\cdot 8\cdot 5 = 346 \equiv 38 \pmod{77},$$

$$\overline{x}_4 \equiv 11\cdot 2\cdot 3 + 7\cdot 8\cdot 6 = 402 \equiv 17 \pmod{77},$$

Враховуючи,що $60 \equiv -17 \pmod{77}$, $39 \equiv -38 \pmod{77}$, дістанемо дві пари розв'язків конгруенції

$$\overline{x}_{1,4} \equiv \pm 17 \pmod{77} \quad \overline{x}_{2,3} \equiv \pm 38 \pmod{77}.$$

Зауважимо, що число 77, як добуток чисел вигляду $4m+3$ є числом Блюма.

Наступна теорема дозволяє факторизувати число n, знаючи хоча б один квадратний корінь з числа a за модулем n.

Теорема 2.6.2. Нехай x, x' – два квадратні корені з числа a, $n = p\cdot q$, де p, q – різні, прості непарні числа, жодне з яких не ділиться на a. Припустимо, що

$$x \neq x' \pmod n. \qquad (2.84)$$

Тоді $(x+x', n)$ (найбільший спільний дільник чисел $x+x'$ і n) дорівнює або p, або q.

Доведення. За умовою $x^2 \equiv (x')^2 = a \pmod n$, звідки отримуємо

$$x^2 - (x') \equiv 0 \pmod n \Rightarrow (x+x')(x-x') \equiv 0 \pmod n.$$

З умови (2.84) випливає, що $x - x' \neq 0 \pmod n$, $x + x' \neq 0 \pmod n$, тому найбільший спільний дільник чисел $x+x'$ і n не дорівнює ні 1, ні n, а дорівнює p або q.

2.6.5. Застосування квадратичних лишків до ймовірнісно гокриптування.

Продемонструємо застосування квадратичних лишків, символів Лежандра, Якобі на прикладі ймовірнісного криптування [3]. Ідея ймовірнісного криптування базується на розпізнаванні квадратичних лишків та псевдоквадратів.

Генерування ключів у ймовірнісному криптуванні відбувається наступним чином. Вибирають великі прості числа p і q та обчислюють їх добуток $n = p \cdot q$. Вибирають випадковий псевдоквадрат a за алгоритмом, який опишемо згодом. Формуємо ключі.

Відкритий ключ: n, a;

Таємний ключ: p, q.

Шифрування. Двійкове повідомлення $M = m_1 m_2 \cdots m_i \cdots m_l$, де $m_i \in \{0,1\}$, $i = \overline{1,l}$ перетворюють у криптотекст $C = c_1 c_2 \cdots c_i \cdots c_l$, де $\left(\frac{c_i}{n}\right) = 1$, $(c_i, n) = 1$. Елементи c_i генерують за допомогою такої ймовірнісної процедури:

- вибирають випадковий елемент $r_i \in \mathbb{Z}_n$, $(r_i, n) = 1$, $i = \overline{1,l}$;
- для $m_i = 0$ покладають $c_i \equiv r_i^2 \pmod{n}$;
- для $m_i = 1$ покладають $c_i \equiv a r_i^2 \pmod{n}$.

Очевидно, що бітовому повідомленню $m_i = 0$ у криптотексті відповідатиме квадратичний лишок c_i, а бітовому повідомленню $m_i = 1$ відповідає елемент c_i, який є добутком квадратичного лишку на псевдоквадрат a [3].

Отже, повідомлення M однозначно визначається криптотекстом C, незалежно від випадкових виборів елементів r_i алгоритмом шифрування.

Дешифрування вимагає уміння відрізняти квадратичні лишки від псевдоквадратів. Для цього можна використати, наприклад, теореми 2.6.1, 2.6.2.

Вибір випадкового псевдоквадрату. Вибирають два випадкові нелишки $a_1 \in \mathbb{Z}_p^*$, $a_2 \in \mathbb{Z}_q^*$. Випадковий нелишок a за модулем n визначають із системи:

$$\begin{cases} a \equiv a_1 \pmod{p}, \\ a \equiv a_2 \pmod{q}, \end{cases}$$

яка розв'язується за алгоритмом китайської теореми про лишки. a – псевдоквадрат, бо

$$\left(\frac{a}{n}\right) = \left(\frac{a}{p}\right) \cdot \left(\frac{a}{q}\right) = \left(\frac{a_1}{p}\right) \cdot \left(\frac{a_2}{q}\right) = (-1) \cdot (-1) = 1.$$

Зауважимо, що a – випадковий елемент, тобто розподілений на множині псевдоквадратів за модулем n рівномірно.

Приклад 2.6.10 .Зашифрувати українське повідомлення «є».

Розв'язання. Оскільки літера «є» має номер 7 в українській абетці, то двійковим еквівалентом нашого повідомлення є 111. Через те, що українська абетка містить 33 літери, то для запису довільної літери потрібно користуватись шестирозрядними двійковими числами. Отже двійковий еквівалент повідомлення «є» – це число 000111.

Відкритий ключ: $n = 77, \quad a = 24;$

Таємний ключ: $p = 7 \quad q = 11.$

Вияснимо, звідки з'явився псевдоквадрат $a=24$. Використовуючи запропонований вище алгоритм, з урахуванням властивостей символу Лежандра, маємо

$$\left(\frac{3}{7}\right)=(-1)^{\frac{3-1}{2}\cdot\frac{7-1}{2}}\left(\frac{7}{3}\right)=-\left(\frac{7}{3}\right)=-\left(\frac{1}{3}\right)=-1,$$

$$\left(\frac{2}{11}\right)=(-1)^{\frac{121-1}{8}}=(-1)^{15}=-1.$$

А це означає, що $a_1\equiv 3(\mathrm{mod}\,7)$, $a_2\equiv 2(\mathrm{mod}11)$ – квадратичні нелишки за модулями $p=7$ та $q=11$ відповідно. Тоді псевдоквадрат a знайдемо з системи конгруенцій:

$$\begin{cases} a\equiv 3(\mathrm{mod}\,7), \\ a\equiv 2(\mathrm{mod}11). \end{cases}$$

Для розв'язання цієї системи використаємо алгоритм китайської теореми про лишки. Маємо

$$M_1=11,\quad M_2=7,\quad M_1^*=2,\quad M_2^*=8.$$

Тому

$$a=11\cdot 2\cdot 3+7\cdot 8\cdot 2=178\equiv 24(\mathrm{mod}\,77).$$

Зрозуміло, що

$$\left(\frac{24}{77}\right)=\left(\frac{24}{7}\right)\cdot\left(\frac{24}{11}\right)=\left(\frac{3}{7}\right)\cdot\left(\frac{2}{11}\right)=(-1)\cdot(-1)=1.$$

Отже, за теоремою 2.6.1., $a=24(\mathrm{mod}\,77)$ – псевдоквадрат.

Шифрування опишемо таблицею, в якій числа r_i, $i=\overline{1,6}$ виберемо довільно (однак $r_i\in\mathbb{Z}_{77}^*$).

i	1	2	3	4	5	6
r_i	19	41	23	19	41	23
c_i	53	64	67	40	73	20

Компоненти c_i криптотексту нашого повідомлення утворені за алгоритмом шифрування, який описаний вище. Шифрування завершено, отримали криптотекст $C = 53\ 64\ 67\ 40\ 73\ 20$.

Розшифрування. Маючи таємний ключ $p = 7,\quad q = 11,$ перевіряємо, що $53, 64, 67$ – квадратичні лишки за модулем $n = 77.$ Дійсно,

$$\left(\frac{67}{7}\right) = \left(\frac{4}{7}\right) = 1,\ \left(\frac{67}{11}\right) = \left(\frac{1}{11}\right) = 1,$$

$$\left(\frac{53}{7}\right) = \left(\frac{4}{7}\right) = 1,\ \left(\frac{53}{11}\right) = \left(\frac{9}{11}\right) = 1.$$

64 – повний квадрат, тому 64 – також квадратичний лишок.

Перевіримо, що числа $40, 73, 20$ – псевдоквадрати. Дійсно,

$$\left(\frac{40}{7}\right) = \left(\frac{5}{7}\right) = \left(\frac{7}{5}\right) = \left(\frac{2}{5}\right) = (-1)^{\frac{25-1}{8}} = (-1)^3 = -1,$$

$$\left(\frac{73}{7}\right) = \left(\frac{3}{7}\right) = (-1)^{\frac{3-1}{2}\cdot\frac{7-1}{2}} = (-1)^3 = -1,$$

$$\left(\frac{20}{7}\right) = \left(\frac{6}{7}\right) = \left(\frac{2}{7}\right)\cdot\left(\frac{3}{7}\right) = -(-1)^{\frac{49-1}{8}} = -(-1)^6 = -1,$$

тобто маємо

$$c_1 = 53 \to m_1 = 0,\ c_2 = 64 \to m_2 = 0\ c_3 = 67 \to m_3 = 0,$$

$$c_4 = 40 \to m_4 = 1,\quad c_5 = 73 \to m_5 = 1,\quad c_6 = 20 \to m_6 = 1.$$

Отже, криптотекст $C = 53\ 64\ 67\ 40\ 73\ 20$ переходить в двійковий еквівалент повідомлення «є» $-000\ 111$.

2.7. Первісні корені та індекси.

2.7.1. Показники та їх властивості.

Нехай $n-$ціле додатне число, більше за одиницю і $(a,n)=1$. Тоді, за теоремою Ейлера, для вказаного a існує число $\varphi(n)$ таке, що

$$a^{\varphi(n)} \equiv 1(\mathrm{mod}\, n). \qquad (2.85)$$

Проте, можливо, існує й число $\delta < \varphi(n)$ таке, що

$$a^{\delta} \equiv 1(\mathrm{mod}\, n). \qquad (2.86)$$

Визначення 2.7.1. Найменше додатне число δ, для якого справджується конгруенція (2.86), називається *показником числа a за модулем n* і позначається $P_n(a)$.

Визначення 2.7.2. В тому випадку, коли $P_n(a)=\varphi(n)$, число a називається *первісним коренем за модулем n* і позначається g, тобто

$$P_n(g)=\varphi(n). \qquad (2.87)$$

Приклад 2.7.1. Знайти показник числа $a=5$ за модулем $n=12$.

Розв'язання. Оскільки $\varphi(12)=\varphi(3)\cdot\varphi(4)=2\cdot(2^2-2)=4$, то або $P_{12}(5)=2$, або $P_{12}(5)=4$. Перевіримо припущення, що $P_{12}(5)=2$. Дійсно, $5^2=25\equiv 1(\mathrm{mod}12)$. Отже показник числа $a=5$ за модулем $n=12$ дорівнює 2.

Приклад 2.7.2. Перевірити, що первісним коренем за модулем $n=10$ є число $g=3$.

Розв'язання. Оскільки $\varphi(10)=\varphi(2)\cdot\varphi(5)=4$, то перевіримо, як і в попередньому прикладі, показники 2 і 4. Маємо

$$3^2 \equiv 9(mod10), \quad 3^4=81\equiv 1(mod10).$$

Отже, найменший показник числа $a=3$ за модулем $n=10$ – це $P_{10}(3)=\varphi(10)=4$ і тому, використовуючи (2.87), можна стверджувати, що $g=3$ – первісний корінь за модулем $n=10$.

Властивості показників

1. Якщо $a\equiv b(\bmod n)$, то $P_n(a)=P_n(b)$.
2. $a^{\delta}\equiv 1(\bmod n)$ тоді і тільки тоді, коли $P_n(a)\,|\,\delta$.
3. $P_n(a)\,|\,\varphi(n)$.
4. $1\le P_n(a)\le\varphi(n)$.
5. $a^{\delta}\equiv a^{\eta}(\bmod n)$ тоді і тільки тоді, коли $\delta\equiv\eta(\bmod P_n(a))$.
6. Числа $a^0,a^1,...,a^{P_n(a)-1}$ належать різним класам лишків за модулем n.
7. Числа $g^0,g^1,...,g^{\varphi(n)-1}$ утворюють зведену систему лишків за модулем n.
8. Кількість натуральних чисел показника k, що не перевищують n, дорівнює або 0, або $\varphi(k)$. Зокрема, кількість класів лишків показника k за простим модулем p дорівнює $\varphi(k)$.
9. $P_n(a^m)=\dfrac{P_n(a)}{(m,P_n(a))}$.
10. $P_{p_1^{\alpha_1}\cdots p_s^{\alpha_s}}(a)=\left[P_{p_1^{\alpha_1}}(a),...,P_{p_s^{\alpha_s}}(a)\right]$.
11. Якщо $P_n(a)=\gamma_1\cdot\gamma_2$, то $P_n(a^{\gamma_1})=\gamma_2$.
12. Якщо $P_{p^k}(a)=\gamma$, $P_{p^{k+1}}(a)=\{\gamma,\gamma\cdot p\}$. (або γ або $\gamma\cdot p$)

Доведемо кілька властивостей показників.

1. Нехай $P_n(a)=\gamma_1, \quad P_n(b)=\gamma_2$. Тоді

$$a^{\gamma_1} \equiv a^{\gamma_2} \pmod n.$$

Оскільки $a^{\gamma_1} \equiv 1 \pmod n$, то й $b^{\gamma_1} \equiv 1 \pmod n$ і отже $\gamma_2 \le \gamma_1$. Аналогічно, з конгруенції

$$a^{\gamma_2} \equiv b^{\gamma_2} \pmod n$$

прийдемо до нерівності $\gamma_1 \le \gamma_2$. Отже, $\gamma_1 = \gamma_2$.

5.

- Нехай $\delta \equiv \eta \pmod{P_n(a)}$. Тоді

$$\delta = \eta + P_n(a)\cdot t, \quad t \in \mathbb{Z}, \quad t > 0.$$

Тому $a^{\delta} = a^{\eta + P(a)_n \cdot t} = a^{\eta} \cdot \left(a^{P(a)_n}\right)^t \equiv a^{\eta} \pmod n.$

- Нехай $a^{\delta} \equiv a^{\eta} \pmod n$. Маємо

$$\delta = P_n(a)\cdot q_1 + r_1, \quad \eta = P_n(a)\cdot q_2 + r_2,$$
$$a^{P_n(a)\cdot q_1 + r_1} \equiv a^{P_n(a)\cdot q_2 + r_2} \pmod n,$$

або

$$\left(a^{P_n(a)}\right)^{q_1} \cdot a^{r_1} \equiv \left(a^{P_n(a)}\right)^{q_2} \cdot a^{r_2} \pmod n,$$

звідки отримуємо $a^{r_1} \equiv a^{r_2} \pmod n$ і, за властивістю 6, дістанемо $r_1 = r_2$. Отже

$$\delta = P_n(a)\cdot q_1, \quad \eta = P_n(a)\cdot q_2$$

і остаточно отримуємо

$$\delta \equiv \eta \pmod{P_n(a)}.$$

6. Потрібно показати, що всі числа $a^0, a^1, \ldots, a^{P_n(a)-1}$ – не конгруентні один з одним за модулем n. Припустимо протилежне, тобто,що

$$a^s \equiv a^t \pmod n, \quad s > t.$$

Оскільки $(a,n)=1,$ то

$$a^{s-t}\equiv 1(\bmod n),$$

тобто існує число $s-t<\delta$, для якого виконується (2.86). А цей факт заперечує визначення показника $\delta=P_n(a)$.

Доведення інших властивостей показників можна знайти, наприклад, в $[5,8]$.

Приклад 2.7.3. Обчислити $P_{4000}(81)$.

Розв'язання. Використовуючи властивості показників, маємо

$$P_{4000}(81)=P_{4000}(3^4)=\frac{P_{4000}(3)}{(4,P_{4000}(3))}.$$

$$P_{4000}(3)=P_{2^5\cdot 5^3}(3)=\left[P_{2^5}(3),P_{5^3}(3)\right].$$

Знайдемо $P_{2^5}(3)$. Почнемо з $P_2(3)=1$. Оскільки $3^1\neq 1(\bmod 2^2)$, то за властивістю 12 маємо $P_{2^2}(3)=1\cdot 2=2$. Можна переконатись, що $P_{2^3}(3)=2$. Оскільки $P_{2^4}(3)\neq 2$, то $P_{2^4}(3)=2\cdot 2=2^2$. Аналогічно перевіримо, що $P_{2^5}(3)=2^3$.

Знайдемо $P_{5^3}(3)$. Почнемо з $P_5(3)=4$. Оскільки $3^4\neq 1(\bmod 5^2)$, то $P_{5^2}(3)=4\cdot 5=20$.

Аналогічно $P_{5^3}(3)=4\cdot 5^2$.

Тому , за властивістю 10, маємо

$$P_{4000}(3)=\left[P_{2^5}(3),P_{5^3}(3)\right]=\left[2^3,4\cdot 5^2\right]=2^3\cdot 5^2=200.$$

Отже

$$P_{4000}(81)=\frac{P_{4000}(3)}{(4,P_{4000}(3))}=\frac{200}{(4,200)}=\frac{200}{4}=50.$$

2.7.2. Первісні корені.

Вкажемо деякі способи відшукання первісних коренів за модулем n.

Теорема 2.7.1. Нехай $\varphi(n)=q_1^{\alpha_1}\cdot q_2^{\alpha_2}\cdots q_k^{\alpha_k}$, де $q_1,q_2,...,q_k$ – прості числа. Для того, щоб число g таке, що $(g,n)=1$, було первісним коренем за модулем n необхідно і досить, щоб g не справджувало жодній з конгруенцій:

$$g^{\frac{\varphi(n)}{q_1}}\equiv 1(\bmod n),\quad g^{\frac{\varphi(n)}{q_2}}\equiv 1(\bmod n),\quad ...,\quad g^{\frac{\varphi(n)}{q_k}}\equiv 1(\bmod n).\ (2.88)$$

Доведення. Дійсно, якщо g – первісний корінь за модулем n, то $P_n(g)=\varphi(n)$ і g не належить жодному з менших показників.

Навпаки, нехай g не справджує жодній з конгруенцій (2.88). Тоді, якби показник $P_n(g)$ первісного кореня був меншим від $\varphi(n)$, то позначаючи буквою q один з простих дільників $\dfrac{\varphi(n)}{P_n(g)}$, ми отримаємо:

$$\frac{\varphi(n)}{P_n(g)\cdot u}=q\cdot u,\quad \frac{\varphi(n)}{q}=P_n(g)\cdot u.$$

Тому справджується конгруенція $g^{\frac{\varphi(n)}{q}}\equiv 1(\bmod n)$, що заперечує наше припущення. Отже $P_n(g)=\varphi(n)$ і g – первісний корінь за модулем n.

Приклад 2.7.4. Знайти первісний корінь за модулем 41.

Розв'язання. Маємо $\varphi(41)=40=2^3\cdot 5$. Отже,

$$\frac{\varphi(41)}{2}=\frac{40}{2}=20,\quad \frac{\varphi(41)}{5}=\frac{40}{5}=8.$$

Перевіримо, чи числа $2,3,4,5,6$ справджують конгруенції (2.88). Маємо

$$2^8\equiv 10(\mathrm{mod}\,41),\quad 2^{20}\equiv 1(\mathrm{mod}\,41),$$
$$3^8\equiv 1(\mathrm{mod}\,41),$$
$$4^8\equiv 18(\mathrm{mod}\,41),\quad 4^{20}\equiv 1(\mathrm{mod}\,41),$$
$$5^8\equiv 18(\mathrm{mod}\,41),\quad 5^{20}\equiv 1(\mathrm{mod}\,41),$$
$$6^8\equiv 10(\mathrm{mod}\,41),\quad 6^{20}\equiv 40(\mathrm{mod}\,41).$$

Отже для чисел $2,3,4,5$ хоча б для одного простого дільника $\varphi(41)=40$ справджуються конгруенції (2.88), а для $g=6$ – не справджуються, тому $g=6$ – найменший первісний корінь за модулем 41.

Теорема 2.7.2. Нехай $\varphi(p)=p-1=q_1^{\alpha_1}\cdot q_2^{\alpha_2}\cdots q_k^{\alpha_k}$ – канонічний розклад числа $p-1$ в добуток простих. Розглянемо конгруенцію

$$x^{\frac{p-1}{q_i}}\equiv 1(\mathrm{mod}\,p),\quad i=\overline{1,k}. \qquad (2.89)$$

Як відомо [5], існує число a_i, $i=\overline{1,k}$, яке не справджує конгруенцію (2.89), тобто

$$a^{\frac{p-1}{q_i}}\neq 1(\mathrm{mod}\,p),\quad i=\overline{1,k}.$$

Тоді первісний корінь g можна подати у вигляді

$$g=b_1\cdot b_2\cdots b_k, \qquad (2.90)$$

де $b_i=a_i^{\frac{p-1}{q_i^{\alpha_i}}}$, $i=\overline{1,k}$.

Доведення цієї теореми не наводимо і відішлемо читача до монографії [5].

Приклад 2.7.5.Знайти первісний корінь за модулем 17.

*Розв'язання.*Спочатку знайдемо число a, яке не справджує конгруенцію

$$x^{\frac{16}{2}} = x^8 \equiv 1(\mathrm{mod}17).$$

Перевірку почнемо з числа $a = 2.$

$$2^8 \equiv 1(\mathrm{mod}17),$$

Отже $a = 2$ не є шуканим числом,яке справджує (2.89). Перевіримо $a = 3.$

$$3^8 \equiv 16(\mathrm{mod}17).$$

Тому, за теоремою 2.7.2. отримуємо

$$g = b = 3^{\frac{16}{2^4}} = 3^1 = 3.$$

Іноді , в застосуваннях, використовують *інше визначеня первісного кореня.*

Нагадаємо, що $\mathbb{Z}_n^*$ позначає мультиплікативну групу елементів кільця $\mathbb{Z}_n = \{0,1,2,...,\mathrm{n}-1\}$, яка складається з елементів цього кільця $x \in \mathbb{Z}_n$, що є взаємно простими з n, тобто $(x,n) = 1.$ Зауважимо, що кожний елемент $x \in \mathbb{Z}_n^*$ має обернений елемент x^{-1} (інверсія елемента x), який легко знайти, використовуючи, наприклад, алгоритм Евкліда.

Дамо наступне визначення первісного кореня g для простого $p[4,6].$

Визначення 2.7.3. Ціле число g називається *первісним коренем за модулем p,* якщо лишок $g(\mathrm{mod}\, p)$ є твірним елементом групи $\mathbb{Z}_n^*$.

Слід зауважити, що первісний корінь за непростим модулем n може й не існувати. Легко перевірити, що не

існує первісного кореня за модулем $n=15$. Більш того, справедлива

Теорема 2.7.3.[5] Якщо n – непарне складене число, що містить хоча б два прості множники, то не існує первісного кореня за модулем n.

Відомо[5], що первісні корені існують тільки за модулями: $2, 4, p^{\alpha}, 2p^{\alpha}$, $\alpha \in \mathbb{N}$, де $p \neq 2$ – просте число.

2.7.3. Індекси (дискретні логарифми). Таблиці індексів.

Нехай $a \in \mathbb{Z}$, $(a, p)=1$, g – первісний корінь за модулем p.

Визначення 2.7.4. *Індексом числа* a за модулем p за основою g називається таке ціле додатне число γ, для якого справджується конгруенція

$$g^{\gamma} \equiv a \pmod{p}.$$

Індекс числа a за модулем p за основою g ще називають *дискретним логарифмом* і позначають $\gamma = ind(a, g, p)$.

Приклад 2.7.6. Знайти $ind(7, 2, 11)$.

Розв'язання. В таблиці простих чисел, яка є, наприклад, в[5,8], іноді вказані ще й первісні корені за простими модулями. Тому знайдемо в таблиці найменший первісний корінь за модулем $p=11$, а саме $g=2$. Порахуємо всі його степені:

$$2^0 \equiv 1 \pmod{11};\ 2^1 \equiv 2 \pmod{11};$$

$$2^2 \equiv 4 \pmod{11};\ 2^3 \equiv 8 \pmod{11};$$

$$2^4 \equiv 5(\mathrm{mod}11); 2^5 \equiv 10(\mathrm{mod}11);$$

$$2^6 \equiv 9(\mathrm{mod}11);\ 2^7 \equiv 7(\mathrm{mod}11);$$

Отже, за визначенням 2.7.4, $ind(7,2,11) = 7.$

Зауважимо, що степені $g^0, g^1, ..., g^{p-2}$ первісного кореня g утворюють зведену систему лишків за модулем p. Тому, перебираючи степені первісного кореня $g = 2$ за модулем $p = 11$, обов'язково натрапимо на будь-яке число із зведеної системи лишків за модулем $p = 11$, зокрема й на число $a = 7$. Як бачимо, $2^7 \equiv 7(\mathrm{mod}11)$, тому й $ind(7,2,11) = 7.$

Властивості індексів.

1. Якщо $\gamma = ind(a, g, p)$ і $\gamma' = ind(a, g, p)$, то $\gamma \equiv \gamma'(\mathrm{mod}\, p-1).$
2. Якщо $b \equiv a(\mathrm{mod}\, p)$, то $ind(\mathrm{b}, g, p) \equiv ind(a, g, p)(\mathrm{mod}\, p-1).$
3. $ind(a_1 \cdot a_2, g, p) = ind(a_1, g, p) + ind(a_2, g, p).$
4. $ind(a^n, g, p) = n \cdot ind(a, g, p).$

Властивість 1 випливає з властивості 5 показників. Властивість 2 нескладно доовести самостійно.

Доведемо властивість 3. Нехай $\gamma_1 = ind(a_1, g, p)$ $\gamma_2 = ind(a_2, g, p).$ А це означає, що $a_1 = g^{\gamma_1}$, $a_2 = g^{\gamma_2}$. Тоді

$$g^{\gamma_1} \cdot g^{\gamma_2} = a_1 \cdot a_2 = g^{\gamma_1+\gamma_2}$$

і отримуємо

$$\gamma_1 = ind(a_1 \cdot a_2, g, p) = \gamma_1 + \gamma_2 \equiv$$

$$\equiv ind(a_1, g, p) + ind(a_2, g, p)(\mathrm{mod}\, p-1).$$

Властивість 4 – це наслідок властивості 3.

Таблиця індексів.

Таблиця індексів в теорії чисел відіграє таку ж роль, як і таблиця логарифмів в алгебрі. Таблиці індексів за модулями простих чисел , менших за 100, наведені в кожному підручник або збірнику задач з теорії чисел(наприклад, $[5,8]$).

Покажемо, як користуватись таблицями індексів на прикладі числа $p=29$. Спочатку навчимось користуватись таблицею, яка для $p=29$ розміщена ліворуч. Знайдемо за цією таблицею $ind(2,2,29)$. На перетині стовпця з номером 2 і рядка з номером 0 (0 десятків) знайдемо $ind(2,29)=1$. А це означає, що $g^1 \equiv 2 \pmod{29}$, тобто $g=2$ – найменший первісний корінь за модулем $p=29$. Таким самим способом знайдемо $ind(25,2,29)$. Цей індекс знаходиться на перетині рядка з номером 2 (є 2 десятки в числі 25) і стовпця з номером 5(є 5 одиниць в числі 25). Отже маємо $ind(25,2,29)=16$. А це означає, що $2^{16} \equiv 25 \pmod{29}$.

Покажемо далі, як знайти індекс числа, якого нема в таблиці ліворуч, наприклад числа $a=345$. Використаємо для цього властивість 2 індексів, тобто знайдемо лишок числа 345 за модулем $p=29$. Маємо

$$345 \equiv 26 \pmod{29},$$

тому, за властивістю індексів 2, отримаємо

$$ind(345,2,29)=ind(26,2,29)=19.$$

Зауважимо, що на перетині рядка з номером 2 і стовпця з номером 6 є число 19.

Таблиця, яка знаходиться праворуч числа $p=29$ дозволяє знаходити число a за заданим його індексом $\gamma = ind(a, g, 29)$. Знайдемо, наприклад, число a, якому відповідає індекс $\gamma = ind(a, 2, 29) = 23$. На перетині рядка з номером 2 і стовпця з номером 3 знаходимо число 10, тобто $a = 10$. А це означає, що

$$2^{23} \equiv 10 \pmod{29}.$$

Знайдемо далі число з індексом, якого нема в правій таблиці для простого $p=29$, наприклад, для індекса $\gamma = ind(a, 2, 29) = 47$. Використавши властивість 1 індексів, маємо $47 \equiv 19 \pmod{28}$ і відчитавши число, яке знаходиться на перетині стрічки з номером 1 та стовпця з номером 9, отримаємо $a \equiv 26 \pmod{29}$.

2.7.4. Застосування таблиці індексів.

- Розв'язування двочленних конгруенцій

$$x^n \equiv a \pmod{m}. \qquad (2.91)$$

Нехай $(n, \varphi(m)) = d$. Конгруенція (2.91) розв'язальна тоді і тільки тоді,коли

$$d \mid inda, \qquad (2.92)$$

і в цьому випадку конгруенція (2.91) має d розв'язків.

Приклад 2.7.7. Розв'язати конгруенцію

$$x^8 \equiv 23 \pmod{41},$$

або довести її несумісність.

Розв'язання. Маємо $(8, \varphi(41)) = (8, 40) = 8$. Отже, в цьому випадку $d = 8$, а за таблицею індексів знаходимо

$ind\,23 = 36\,(\mathrm{mod}\,40)$ і 8 не ділить 36. Тому конгруенція $x^8 \equiv 23\,(\mathrm{mod}\,41)$ не має розв'язків.

Приклад 2.7.8. Розв'язати конгруенцію $x^{12} \equiv 37\,(\mathrm{mod}\,41)$.

Розв'язання.. $(12, \varphi(41)) = (12, 40) = 4$. Отже в цій конгруенції $d = 4$ і, за таблицею індексів, $ind\,37 = 32\,(\mathrm{mod}\,40)$. Оскільки $4 \mid 32$, то конгруенція – розв'язальна і має 4 розв'язки. Знайдемо їх. Візьмемо дискретний логарифм від обидвох частин конгруенції $x^{12} \equiv 37\,(\mathrm{mod}\,41)$, використовуючи властивості індексів (чи дискретних логарифмів). Матимемо

$$12\,ind\,(x, 6, 41) = ind\,(37, 6, 41) \equiv 32\,(\mathrm{mod}\,40),$$

або, після скорочення конгруенції на 4 (див. властивості конгруенцій), отримаємо

$$3\,ind\,(x, 6, 41) \equiv 8\,(\mathrm{mod}\,10),$$

звідки маємо

$$3z \equiv 8\,(\mathrm{mod}\,10).$$

Неважко встановити методом підбору, що $z \equiv 6\,(\mathrm{mod}\,10)$ – розв'язок цієї лінійної конгруенції. Отже

$$ind\,(x, 6, 41) \equiv 6\,(\mathrm{mod}\,40).$$

Далі, використовуючи праву таблицю індексів за модулем $p = 41$, за даним індексом $\gamma = 6$, знайдемо чотири числа x таких, що $x^{12} \equiv 37\,(\mathrm{mod}\,41)$:

$$x \equiv 39\,(\mathrm{mod}\,41);\ \ x \equiv 18\,(\mathrm{mod}\,41);$$

$$x \equiv 2\,(\mathrm{mod}\,41);\ \ x \equiv 23\,(\mathrm{mod}\,41).$$

Для розв'язування задач на знаходження показників та первісних коренів корисними є наступні рекомендації: [5]

- В зведеній системі лишків за модулем p число лишків степені n дорівнює

$$\frac{p-1}{d},\ \text{де}\ d=(n,p-1). \qquad (2.93)$$

Приклад 2.7.9. Знайти всі лишки степені 12 за модулем 41.

Розв'язання. Оскільки $(12,40)=4$, то, за формулою (2.93), кількість таких лишків дорівнює $\frac{40}{4}=10$. В таблиці індексів легко знайти лишки степені 12, тобто такі числа $a\in\mathbb{Z}_{41}^{*}$, для яких справджується конгруенція

$$x^{12}\equiv a\pmod{41}.$$

Це будуть числа, індекси яких кратні 4, тобто числа

$$1,4,10,16,18,23,25,31,37,40.$$

Для одного з цих лишків, а саме для $a=37$, й розв'язана конгруенція прикладу 2.7.8.

- Показник $\delta=P_p(a)$ визначається рівністю

$$\delta=\frac{p-1}{(inda,p-1)}. \qquad (2.94)$$

- Число a є первісним коренем за модулем p тоді і тільки тоді, коли виконується рівність

$$(inda,p-1)=1. \qquad (2.95)$$

- В зведеній системі лишків за модулем p кількість чисел k показника δ визначена рівністю

$$k=\varphi(\delta). \qquad (2.96)$$

Зокрема, кількість первісних коренів за модулем p визначена рівністю

$$l = \varphi(p-1), \qquad (2.97)$$

де $\varphi(x)$ – функція Ейлера

Приклад 2.7.10. Знайти всі числа показника $\delta = 10$ за модулем 41.

Розв'язання

- Кількість таких чисел визначиться формулою (2.96) і дорівнює

$$k = \varphi(10) = \varphi(5)\cdot\varphi(2) = 4.$$

- Самі ж числа показника $\delta = 10$ знайдемо в таблиці індексів, використовуючи рівність (2.94), яка набуває вигляду

$$(inda, 40) = \frac{40}{10} = 4.$$

Цими числами є наступні чотири числа:

$$4, 23, 25, 31.$$

Приклад2.7.11. Знайти всі первісні корені за модулем 41.

Розв'язання.

- Кількість первісних коренів визначиться формулою (2.97) і дорівнює

$$l = \varphi(40) = \varphi(8)\cdot\varphi(5) = \left(2^3 - 2^2\right)(5-1) = 16.$$

- Знайдемо ці корені в таблиці індексів, користуючись при цьому рівністю (2.95), яка набуває вигляду

$$(inda, 40) = 1.$$

Отже первісними коренями за модулем 41 є числа:

$$6, 7, 11, 12, 13, 15, 17, 19, 22, 24, 26, 28, 29, 30, 34, 35.$$

2.7.5. Алгоритм Сільвера-Поліга-Хелмана.

Алгоритм С-П-Х $[3,10]$ застосовують для відшукання дискретного логарифму при великих p, тобто для знаходженню невідомого x з конгруенції

$$g^x \equiv y \pmod p, \quad 0 \le x < p-1,$$

де g – первісний корінь за простим модулем p, а ціле число y вважається відомим. Таке число x, як випливає з *визначення 2.7*.4, є *дискретним логарифмом* числа y за модулем p за основою g і позначається $x = ind(y, g, p)$.

Опишемо алгоритм С-П-Х.

- Спочатку для кожного простого дільника q числа $p-1$ знайдемо корені q – го степеня з одиниці:

$$r_{q,j} = g^{\frac{j(p-1)}{q}}, \quad j = \overline{0, q-1}.$$

Ця таблиця $r_{q,j}$ є основою обчислення дискретного логарифму числа $y \in F_p^*$,

- Нехай $p-1 = \prod_q q^\alpha$ – подання числа $p-1$ у вигляді добутку простих.

Досить знайти $x \pmod{q^\alpha}$ для кожного простого q, що ділить $p-1$.

Тоді число x однозначно визначиться, якщо застосувати китайську теорему про лишки.

- Отже, зафіксуємо просте число q і покажемо, як знайти $x \pmod{q^\alpha}$. Спершу, подамо число x у вигляді

$$x = x_0 + x_1 q + x_2 q^2 + \cdots x_{\alpha-1} q^{\alpha-1}, \quad 0 \le x_i < q.$$

Для того, щоб знайти x_0, обрахуємо $y^{\frac{p-1}{q}}$. По-перше, $y^{\frac{p-1}{q}}$ – це корінь з одиниці $q-$го порядку, оскільки $y^{p-1} \equiv 1 (\mathrm{mod}\, p)$ за теоремою Ферма.

По-друге, з рівності $g^x \equiv y (\mathrm{mod}\, p)$ випливає, що

$$y^{\frac{p-1}{q}} \equiv g^{x\cdot\frac{p-1}{q}} \equiv g^{x_0\cdot\frac{p-1}{q}} = r_{q,x_0}.$$

Порівнюючи $y^{\frac{p-1}{q}}$ з $r_{q,j}$, $j = \overline{0, q-1}$, надамо x_0 те значення j, при якому

$$y^{\frac{p-1}{q}} = r_{q,j}.$$

Щоб знайти x_1, позначимо $y_1 = yg^{-x_0}$. Тоді y_1 має дискретний логарифм $x - x_0 = x_1 q + x_2 q^2 + \cdots x_{\alpha-1} q^{\alpha-1} (\mathrm{mod}\, q^\alpha)$. Дійсно,

$$g^{x-x_0} = g^x \cdot g^{-x_0} = yg^{-x_0}.$$

Оскільки y_1 – це $q-$й степінь, то $y_1^{\frac{p-1}{q}} \equiv 1 (\mathrm{mod}\, p)$ і

$$y_1^{\frac{p-1}{q^2}} = g^{(x-x_0)\frac{p-1}{q^2}} = g^{\left(x_1 + x_2 q + \cdots x_{\alpha-1} q^{\alpha-1}\right)\frac{p-1}{q}} = g^{x_1\frac{p-1}{q}} = r_{q,x_1}.$$

Порівнюючи $y_1^{\frac{p-1}{q^2}}$ з $r_{q,j}$, $0 \le j < q-1$, покладемо x_1 тому значенню j, при якому $y_1^{\frac{p-1}{q^2}} = r_{q,j}$.

Продовжуючи цей процес за аналогією, отримаємо решта значень

$$x_2, x_3, \ldots, x_{\alpha-1}.$$

А саме, для кожного $i = \overline{1, \alpha-1}$ покладемо

$$y_i = yg^{-x_0 - x_1 q - x_2 q^2 - \cdots - x_{i-1} q^{i-1}}.$$

Оскільки $g^x \equiv y \left(\mathrm{mod}\, q^\alpha\right)$, то

$$g^{x-x_0-x_1p-x_2p^2-\cdots-x_{i-1}p^{i-1}} = g^x \cdot g^{-x_0-x_1q-x_2q^2-\cdots-x_{i-1}q^{i-1}} =$$

$$= y \cdot g^{-x_0-x_1q-x_2q^2-\cdots-x_{i-1}q^{i-1}} =$$

$$y_i \equiv g^{x_iq^i+x_{i+1}q^{i+1}+\cdots x_{\alpha-1}q^{\alpha-1}} \left(\mathrm{mod}\, p\right).$$

і дискретний логарифм y_i, $i = \overline{1, \alpha-1}$ за модулем q^α дорівнює

$$x_iq^i + x_{i+1}q^{i+1} + \cdots x_{\alpha-1}q^{\alpha-1}.$$

Оскільки y_i є $q^i -$ степенем, то $y_i^{\frac{p-1}{q^i}} \equiv 1 \left(\mathrm{mod}\, p\right)$ і

$$y_i^{\frac{p-1}{q^{i+1}}} = g^{(x_i+x_{i+1}q+\cdots)\frac{p=1}{q}} = g^{x_i\frac{p-1}{q}} = r_{q,x_i}.$$

Тому покладемо x_i тому значенню j, при якому

$$y_i^{\frac{p-1}{q^{i+1}}} = r_{q,j}.$$

Таким чином, $x \left(\mathrm{mod}\, q^\alpha\right)$ знайдено.

• Повторимо цей процес для кожного простого дільника $q_l \mid p-1$ і прийдемо до скінченої системи лінійних конгруенцій

$$\begin{cases} x \equiv b_1 \left(\mathrm{mod}\, q_1^{\alpha_1}\right), \\ x \equiv b_2 \left(\mathrm{mod}\, q_2^{\alpha_2}\right), \\ \ldots\ldots\ldots\ldots\ldots\ldots \\ x \equiv b_s \left(\mathrm{mod}\, q_s^{\alpha_s}\right), \end{cases}$$

яку розв'яжемо, використовуючи китайську теорему про лишки.

Розв'язок цієї системи й є дискретним логарифмом числа y за модулем p і за основою g.

Зауважимо, що алгоритм, запропонований Сільвером і Хелманом, гарно працює, тобто є ефективним, якщо прості дільники числа $p-1-$ невеликі, оскільки для складання таблиці $\left\{r_{q,j}\right\}$ і порівняння елементів $y_i^{\frac{p-1}{q^i}}$ з її елементами знадобиться багато часу, якщо прості дільники числа $p-1-$ великі.

Приклад 2.7.12. Використовуючи алгоритм Сільвера-Поліга-Хелмана, знайти $ind\left(34,2,101\right)$.

Розв'язання. Маємо $101-1=100=2^2\cdot 5^2$. Тому простими множниками числа $p-1$ в цьому випадку є $q_1=2$ і $q_2=5$.

- Знайдемо первісні корені $2-$го та $5-$го порядків відповідно, тобто складемо визначальну таблицю $\left\{r_{q_i,j_i}\right\}$, $i=1,2$.

$$r_{2,0}=1;\quad r_{2,1}=-1;$$

$$r_{5,0}=2^{0\cdot\frac{100}{5}}\equiv 1\left(\mathrm{mod}101\right);\quad r_{5,1}=2^{1\cdot\frac{100}{5}}=2^{20}\equiv 95\left(\mathrm{mod}101\right);$$

$$r_{5,2}=2^{2\cdot\frac{100}{5}}=2^{40}\equiv 36\left(\mathrm{mod}101\right);$$

$$r_{5,3}=2^{3\cdot\frac{100}{5}}=2^{60}\equiv 87\left(\mathrm{mod}101\right);$$

$$r_{5,4}=2^{4\cdot\frac{100}{5}}=2^{80}\equiv 84\left(\mathrm{mod}101\right).$$

- Знайдемо $x\left(\mathrm{mod}\,2^2\right)=x\left(\mathrm{mod}\,4\right)$. Для цього подамо x у вигляді

$$x=x_0+x_1\cdot 2.$$

Знайдемо x_0 за правилом, описаним в алгоритмі С-П-Х. Маємо $34^{\frac{100}{2}} = 34^{50} \equiv -1 \pmod{101}$, отже $x_0 = 1$, оскільки $34^{\frac{100}{2}} = r_{2,1}$.

Знайдемо x_1. Маємо $y_1 = 34 \cdot 2^{-1} = 17$, отже $17^{\frac{100}{4}} = 17^{25} \equiv -1 \pmod{101}$. Тому $x_1 = 1$, так як $17^{\frac{100}{4}} = r_{2,1}$. Отже $x \pmod{2^2} = 1 + 1 \cdot 2 = 3$.

- Знайдемо $x \pmod{5^2} = x_0 + x_1 \cdot 5$. Для визначення x_0 маємо $34^{\frac{100}{5}} \equiv 95 \pmod{101}$, отже $x_0 = 1$, оскільки $34^{\frac{100}{5}} = r_{5,1}$. Для визначення x_1 маємо $\left(34 \cdot 2^{-1}\right)^{\frac{100}{25}} = 17^4 \equiv 95 \pmod{101}$, отже $x_1 = 1$, оскільки $\left(\frac{34}{2}\right)^{\frac{199}{5^2}} = r_{5,1}$. Тому дістанемо $x \pmod{5^2} = 1 + 1 \cdot 5 = 6$.

- Остаточно для знаходження дискретного логарифма $x \pmod{100}$ розв'яжемо систему лінійних конгруенцій

$$\begin{cases} x \equiv 3 \pmod{4}, \\ x \equiv 6 \pmod{25}, \end{cases}$$

використовуючи КТЛ. Маємо

$$M_1 = 25; \quad M_1' = 1; \quad M_2 = 4; \quad M_2' = 19.$$

Тоді $x = 25 \cdot 1 \cdot 3 + 4 \cdot 19 \cdot 6 = 531 \equiv 31 \pmod{100}$. Отже $ind\,(34, 2, 101) = 31$, в чому неважко переконатись безпосередньою перевіркою.

Дещо важчим є наступний

Приклад 2.7.13. Знайти $ind(7,5,577)$.

Розв'язання.

- $577-1=576=2^6\cdot 3^2$.
- $r_{2,0}=1;\quad r_{2,1}=-1;$

$$r_{3,0}=1;\ r_{3,1}=5^{\frac{576}{3}}=5^{192}\equiv 363(\bmod 577);$$

$$r_{3,2}=5^{2\cdot\frac{576}{3}}=5^{192\cdot 2}\equiv 213(\bmod 577).$$

- Знаходимо

$$x(\bmod 2^6)=x_0+x_1\cdot 2+x_2\cdot 2^2+x_3\cdot 2^3+x_4\cdot 2^4+x_5\cdot 2^5.$$

Визначимо x_0. $7^{\frac{576}{2}}=7^{288}\equiv -1(\bmod 577)$, тому $x_0(r_{2,1})=1(\bmod 577)$.

Визначимо x_1:

$\left(7\cdot 5^{-1}\right)^{\frac{576}{2^2}}=(7\cdot 231)^{144}=(463)^{144}=1(\bmod 577)$, тому $x_1=r_{2,0}=0$. Зауважимо, що $5^{-1}\in F_{577}^{*}$ можна знайти, застосовуючи узагальнений алгоритм Евкліда.

Визначимо x_2:

$\left(7\cdot 5^{-1}\right)^{\frac{576}{2^3}}=(5\cdot 231)^{72}=(-114)^{72}=-1(\bmod 577)$, отже $x_2=r_{2,1}=1$.

Визначимо x_3:

$\left(7\cdot 5^{-(1+1\cdot 2^2)}\right)^{\frac{576}{2^4}}=\left(7\cdot 5^{-5}\right)^{36}=(7\cdot 113)^{36}=214^{36}=1(\bmod 577)$,

отже $x_3=r_{2,0}=0$. Тут 5^{-5} також можна знайти, застосувавши узагальнений алгоритм Евкліда.

Визначимо $x_4 : \left(7\cdot 5^{-5}\right)^{\frac{576}{2^5}} = (214)^{18} \equiv 1 \pmod{577}$, отже $x_4 = r_{2,0} = 0.$

Визначимо $x_5 : \left(7\cdot 5^{-5}\right)^{\frac{576}{2^6}} = (214)^{9} \equiv -1 \pmod{577}$, отже $x_5 = r_{2,1} = 1.$

Тому

$$x \pmod{2^6} = 1 + 0\cdot 2 + 1\cdot 2^2 + 0\cdot 2^3 + 0\cdot 2^4 + 1\cdot 2^5 = 37.$$

- Знаходимо $x \pmod{3^2} = x_0 + x_1 \cdot 3.$

Визначимо $x_0 : 7^{\frac{576}{3}} = 7^{192} = 213 \pmod{577}$, отже $x_0 = r_{3,2} = 2.$

Визначимо $x_1 : \left(7\cdot 5^{-2}\right)^{\frac{576}{3^2}} = (7\cdot 277)^{64} = 208^{64} = 213,$ отже $x_1 = r_{3,2} = 2.$

Таким чином, $x \pmod{3^2} = 2 + 2\cdot 3 = 8.$

- Розв'язуємо систему конгруенцій

$$\begin{cases} x \equiv 37 \pmod{64}, \\ x \equiv 8 \pmod{9}. \end{cases}$$

Тут

$$M_1 = 9; \quad M_1' = 57; \quad M_2 = 64; \quad M_2' = 1.$$

Тодіотримуємо розв'язок системи

$$x = 9\cdot 57\cdot 37 + 64\cdot 1\cdot 8 = 19493 \equiv 485 \pmod{576}.$$

Отже $ind\,(7,5,577) = 485.$ Можна перевірити, що дискретний логарифм знайдено вірно, тобто $5^{485} \equiv 7 \pmod{577}.$

Однією з криптосистем, яка передбачає відомим первісний корінь за великим модулем є криптосистема Ель-Гамаля.

2.7.6. Криптосистеми Ель-Гамаля.

Генерування ключів. Вибирають велике просте число p і число g, $1 < g < p-1$, яке має в мультиплікативній групі $\mathbb{Z}_p^*$ великий порядок. В ідеальному випадку g – первісний корінь за модулем p. Числа p і q не є таємницею і перебувають в загальному користуванні. Кожен абонент вибирає собі випадкове число a у проміжку від 1 до $p-1$ і обчислює $h \equiv g^a \pmod p$.

Відкритий ключ: p, g, h;

Таємний ключ: a.

Шифрування відбувається блоками. Кожен блок M вважаємо елементом з $\mathbb{Z}_p^*$. Повідомлення $M \in \mathbb{Z}_p^*$ перетворюють в криптотекст $C \in \mathbb{Z}_p^* \times \mathbb{Z}_p^*$ таким чином:

- Вибирають випадкове число r таке, що $1 \le r \le p-1$;
- Обчислюють $C = (c_1, c_2)$, де

$$c_1 \equiv g^r \pmod p, \quad c_2 \equiv Mh^r \pmod p.$$

Дешифрування. $D(C) = c_2 \left(c_1^a\right)^{-1} \pmod p$.

Приклад 2.7.14. Нехай $p = 43, \quad g = 3, \quad a = 6.$

Розв'язання. Обчислимо $h \equiv 3^6 \pmod{43} = 41.$

Отже маємо *відкритий ключ:* 43, 3, 41.

Припустимо, що шифрується числова інформація і потрібно зашифрувати повідомлення $M = 7$. Виберемо випадкове число r, наприклад, $r = 10$. Тоді

$$c_1 \equiv 3^{10} \pmod{43} = 10, \quad c_2 \equiv \left(7 \cdot 41^{10}\right) \pmod{43} = 30.$$

Отримуємо криптотекст $C=(10,30)$.

Дешифруємо криптотекст $C=(10,30)$, тобто перевіримо справедливість конгруенції

$$D(10,30)\equiv 30\cdot\left(10^6\right)^{-1}(\bmod 43)=7.$$

Дійсно, легко перевірити, що $10^6\equiv 35(\bmod 43)$. Знайдемо обернений елемент до числа 35 в групі $\mathbb{Z}_{43}^*$, використавши алгоритм Евкліда. Маємо

$$43=35\cdot 1+8,$$
$$35=8\cdot 4+3,$$
$$8=3\cdot 2+2,$$
$$3=2\cdot 1+1.$$

Повертаючись знизу вгору, отримаємо

$$1=3-2=2-(8-3\cdot 2)=-8+3\cdot 3=-8+(35-8\cdot 4)\cdot 3=$$
$$=35\cdot 3-8\cdot 13=35\cdot 3-(43-35)\cdot 13=35\cdot 16-43\cdot 13.$$

Отже оберненим елементом до елемента 35 за $\bmod 43$ є елемент 16. Далі перевіримо, що $30\cdot 16(\bmod 43)=7$, тобто приходимо до вихідного шифрованого повідомлення.

Піднесення до степеня за $\bmod p$ виконується за допомогою бінарного методу. Вибір великого простого p можна знайти, наприклад, в [3]. За число g найкраще вибрати первісний корінь за $\bmod p$, що є,взагалі кажучи, нелегкою задачею.

Розкриття системи Ель-Гамаля еквівалентна наступній задачі:

Задано: $p,g,x.y\in\mathbb{N}$, де $1<g<p-1$, $x\equiv g^a(\bmod p)$, $y\equiv g^b(\bmod p)$ для деяких a і b.

Обчислити $z\equiv g^{ab}(\bmod p)$.

Очевидно, що розкриття системи Ель-Гамаля зводиться до задачі дискретного логарифмування, яку можна, зокрема, розв'язувати, використовуючи алгоритм Сільвера-Поліга-Хелмана. Проте, під час розкриття криптосистеми Ель-Гамаля слід виключити той варіант, коли число $p-1$ має невеликі прості дільники, інакше суперник може скористатись алгоритмом Сільвера-Поліга-Хелмана.

Розділ 3. Еліптичні криві

3.1. *Елементарні відомості про еліптичні криві.*

Асиметричними криптосистемами, які базуються на еліптичних кривих над скінченими полями, займається розділ криптографії, що називається еліптичним криптуванням.

Хоча еліптичні криві досліджувались більш як сотні років, інтерес до них виявляли тільки вузькі спеціалісти з теорії чисел та алгебраїчної геометрії. Проте в 1986 році одночасно і незалежно один від одного американські математики Н. Кобліц та В. Міллер запропонували використати еліптичні криві для побудови криптосистем з відкритим ключем $[9,13]$.

3.1.1. Основні визначення.

Визначення 3.1.1. Еліптичною кривою E над полем F називається сукупність точок, координати яких справджують кубічне рівняння

$$y^2 + a_{11}xy + a_{01}y = x^3 + a_{20}x^2 + a_{10}x + a_{00}, \qquad (3.1)$$

де $a_{00}, a_{10}, a_{20}, a_{01}, a_{11} \in F$ або

$$f(x,y) = y^2 + a_{11}xy + a_{01}y - x^3 - a_{20}x^2 - a_{10}x - a_{00} = 0 \qquad (3.2)$$

Визначення 3.1.2. Еліптична крива E називається *сингулярною*, якщо на E існує хоча б одна *особлива точка*, тобто точка, в якій виконуються умови:

$$\frac{\partial f}{\partial x} = 0, \quad \frac{\partial f}{\partial y} = 0. \qquad (3.3)$$

В іншому випадку крива E називається *несингулярною.*

Несингулярні еліптичні криві є гладкими, тобто не мають точок звороту і самоперетинів, і в довільній їх точці можна провести дотичну. Саме ці еліптичні криві використовують в криптографії.

Слід зауважити,що в залежності від характеристики поля, з допомогою заміни змінних, рівняння (3.1), що визначає еліптичну криву, зводиться до різних канонічних форм, а саме:

1. якщо характеристика поля F не дорівнює 2 або 3, то приходимо до форми Вейєрштрасса

$$y^2 = x^3 + ax + b; \qquad (3.4)$$

2. якщо характеристика поля F дорівнює 3 ,то еліптична крива (3.1) має канонічну форму

$$y^2 = x^3 + ax^2 + bx + c; \qquad (3.5)$$

3. якщо характеристика поля дорівнює 2, то рівняння (3.1) набуває однієї з двох форм:

- $y^2 + y = x^3 + ax + b;$ – суперсингулярна крива (3.6)
- $y^2 + xy = x^3 + ax + b$ – несуперсингулярна крива (3.7)

3.1.2.Умова несингулярності еліптичної кривої.

Розглянемо еліптичну криву в формі Вейєрштрасса (3.4) над полем дійсних чисел $\mathbb{R}$, що дозволяє будувати її графік. Оскільки з (3.4) маємо

$$y = \pm\sqrt{x^3 + ax + b},$$

то графік кривої – симетричний відносно осі абсцис, а абсциси точок перетину цього графіка з віссю абсцис – це корені рівняння

$$x^3 + ax + b = 0. \qquad (3.8)$$

Дискримінант кубічного рівняння (3.8) дорівнює

$$D = \left(\frac{a}{3}\right)^3 + \left(\frac{b}{2}\right)^2.$$

При цьому

• якщо $D<0,$ то рівняння (3.8) має три різні дійсні корені α,β,γ. Типовий графік еліптичної кривої в цьому випадку $-$це крива , яка складається з двох частин (Рис.1);

• $D=0.$ В цьому випадку рівняння (3.8) має два дійсні корені α,β,β, два з яких однакові. Тоді точка $(\beta;0)-$ особлива, а крива $(3.4)-$сингулярна(рис.2);

• якщо $D>0,$ то алгебраїчне рівняння (3.8) має один дійсний корінь і два комплексно спряжені. Графік еліптичної кривої в цьому випадку зображений на рис. 3.

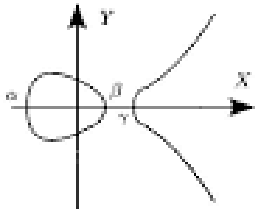

Рис. 1 D<0

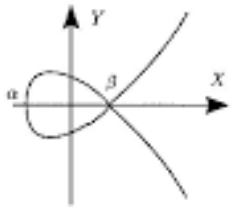

Рис. 2 D=0

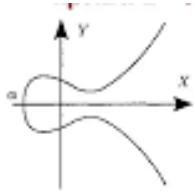

Рис. 3 D>0

Всі попередні викладки переносяться й на еліптичні криві над скінченими полями. Тому для скінчених полів характеристики p, що не дорівнює 2 і 3 еліптична крива є несингулярною за умови, $D\neq 0.$ Отже умовою несингулярності еліптичної кривої в цьому випадку є умова

$$4a^3+27b^2\neq 0\left(\mathrm{mod}\ p^n\right). \qquad (3.9)$$

3.1.3. Операція додавання і побудова групи точок еліптичної кривої.

Симетрія кривої відносно осі Ox дає наочне визначення точки, оберненої до заданої точки еліптичної кривої.

Визначення 3.1.3. Оберненою до точки $P(x;y)$ несингулярної еліптичної кривої вважається точка з координатами $(x;-y)$, яку прийнято позначати $-P(x;-y)$.

Таке визначення буде виправдане трохи згодом.

Важливими властивостями несингулярних еліптичних кривих є наступні:

- довільна пряма, яка проходить через дві різні точки еліптичної кривої, перетинає цю криву в єдиній точці;
- дотична до еліптичної кривої в довільній точці, окрім точки перегину, перетинає цю криву ще в одній точці.

Ці властивості несингулярної еліптичної кривої дозволяють задати на ній операцію, яка називається операцією додавання точок кривої і яка описується наступним визначенням.

Визначення 3.1.4. Сумою двох точок P і Q еліптичної кривої називається точка $R = P + Q$, яка є оберненою до третьої точки перетину еліптичної кривої і прямої, що проходить через точки P і Q (Рис.4).

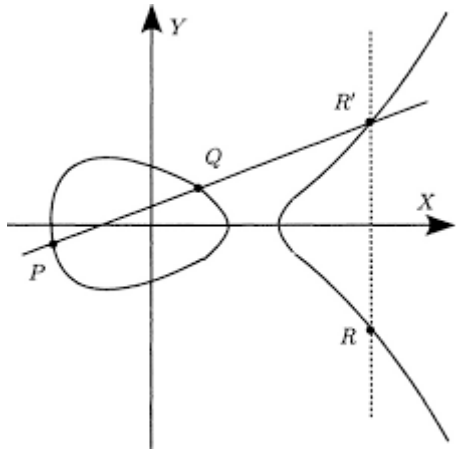

Рис.4

Якщо ж точки P і Q співпадають, тобто $P = Q$, то операція додавання $P + P = 2P = R$ – рівносильна подвоєнню точки P, тобто $R = 2P$ (Рис.5).

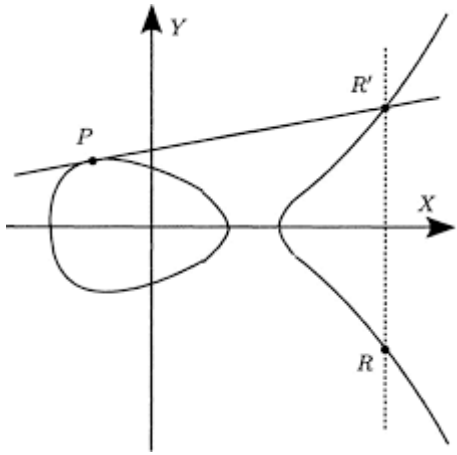

Рис.5

Зауважимо, що у випадку $P = Q$ січна PQ стає дотичною до кривої в точці P і, таким чином, геометрично

подвоєна точка $2P$ – це точка обернена до точки перетину цієї дотичної з кривою.

Рисунки наочно демонструють операції додавання точок та подвоєння точки.

Далі слід вияснити, як визначити координати точки $R = P + Q = (x_3; y_3)$ через координати доданків $P(x_1; y_1)$ і $Q(x_2; y_2)$ [9]. Тут маємо два випадки:

- $P \neq \pm Q$

Напишемо рівняння січної PQ з кутовим коефіцієнтом

$$\lambda = \frac{y_2 - y_1}{x_2 - x_1}.$$

Маємо

$$y = y_1 + \lambda(x - x_1).$$

Підставимо останнє рівняння в рівняння еліптичної кривої (3.4) і прийдемо до рівності

$$\left[y_1 + \lambda(x - x_1)\right]^2 = x^3 + ax + b.$$

Піднімемо вираз ліворуч в останній рівності до квадрату і прийдемо до кубічного рівняння

$$x^3 + \lambda^2 x^2 + x\left(2\lambda^2 x_1 + 2\lambda y_1 - a\right) - 2\lambda x_1 y_1 - b = 0.$$

За теоремою Вієта для кубічного рівняннядля коренів x_1, x_2, x_3 цього рівняння отримуємо

$$x_1 + x_2 + x_3 = \lambda^2,$$

звідки

$$x_3 = \lambda^2 - x_1 - x_2.$$

Підставивши x_3 в рівняння січної PQ, знаходимо ординату точки $-R$, яку позначимо y_3^*.

$$y_3^* = y_1 + \lambda(x_3 - x_1).$$

Оскільки точка $R(x_3; y_3)$ – симетрична до точки $-R(x_3; -y_3)$ відносно осі абсцис, то остаточно отримуємо координати точки $R = P + Q$

$$\begin{aligned} x_3 &= \lambda^2 - x_1 - x_2, \\ y_3 &= \lambda(x_1 - x_3) - y_1, \end{aligned} \quad \lambda = \frac{y_2 - y_1}{x_2 - x_1}. \qquad (3.10)$$

2.Знайдемо далі координати подвійної точки $R(x_3; y_3) = 2P(x_1; y_1)$. Розглянувши рівняння еліптичної кривої (3.4), як неявне, знайдемо похідну докривоїв довільній її точці. Маємо

$$y^2 = x^3 + ax + b \Rightarrow 2ydy = (3x^2 + a)dx \Rightarrow \frac{dy}{dx} = \frac{3x^2 + a}{2y}.$$

Оскільки в точці $P(x_1; y_1)$ кутовий коефіцієнт дотичної дорівнює похідній в цій точці, то

$$\lambda = \left.\frac{dy}{dx}\right|_{\substack{x=x_1 \\ y=y_1}} = \frac{3x_1^2 + a}{2y_1}.$$

Отже тепер можна записати координати подвійної точки $R(x_3; y_3)$ через координати точки $P(x_1; y_1)$

$$\begin{aligned} x_3 &= \lambda^2 - 2x_1, \\ y_3 &= \lambda(x_1 - x_3) - y_1, \end{aligned} \quad \lambda = \frac{3x_1^2 + a}{2y_1}. \qquad (3.11)$$

Формули додавання і подвоєння точок еліптичної кривої справедливі для усіх полів, зокрема й для полів характеристики 2 і 3. В доданій таблиці вказані подібні формули для операцій додавання та подвоєнняі в цих полях.

Щоб побудувати групу точок еліптичної кривої, нам знадобиться ще нейтральний (нульовий) елемент цієї групи $O(x; \infty)$, для якого приймемо

$$P + (-P) = O$$

для довільної точки еліптичної кривої P. Введення нейтрального елемента виправдовують такі міркування. Пряма, що проходить через точки P і $-P$ перпендикулярно до осі абсцис повинна мати третю точку перетину цього перпендикуляра з еліптичною кривою. Тому можна прийняти, що ця третя точка йде до нескінченості вздовж осі ординат. Таку точку вважають точкою еліптичної кривої, називають *нескінченно віддаленою точкою* і позначають $O(x;\infty)$.

Видатний французький вчений А.Пуанкаре довів, що множина точок еліптичної кривої разом з нескінченно віддаленою точкою утворює комутативну групу відносно операції додавання точок.

Оскільки ми розглядаємо еліптичні криві над скінченими полями, то дамо наступне

Визначення 3.1.5. Групою точок еліптичної кривої над скінченим полем $GF(p)$ називається множина точок, координати яких належать цьому полю і справджують конгруенцію $y^2 = x^3 + ax^2 + b \pmod p$, якщо $p \neq 2,3,\ \ a,b \in GF(p)$, і для дискримінанта D кубічного многочлена $x^3 + ax^2 + b$ виконується умова несингулярності (3.9). До групи точок еліптичної кривої належить нескінченно віддалена точка $O(x;\infty)$.

Група точок еліптичної кривої $y^2 = x^3 + ax^2 + b \pmod p$ позначається $E_p(a,b)$.

3.1.4.Відшукання точок еліптичної кривої над скінченим полем

Шукати точки еліптичної кривої $y^2 = x^3 + ax^2 + b$ над скінченим полем $GF(p)$ пропонуємо за такою схемою:

- знайти всі квадратичні лишки за модулем p і квадрати для них;
- обчислити $x^3 + ax^2 + b$ для кожного $x \in GF(p)$;
- якщо для деякого конкретного значення $x \in GL(p)$ $x^3 + ax^2 + b = A$ виявиться квадратичним лишком, то розв'язати квадратне рівняння $y^2 = A$ і отримати дві точки еліптичної кривої $\left(x; \sqrt{A}\right)$ і$\left(x; p - \sqrt{A}\right)$;
- якщо ж при деякому $x \in GL(p)$ $x^3 + ax^2 + b = A$ виявиться квадратичним нелишком, то точки з такою абсцисою на еліптичній кривій немає.
- якщо для деякого $x \in GL(p)$ $x^3 + ax^2 + b = 0,$ то такій абсцисі відповідає одна точка $(x;0)$.

Приклад 3.1.1. Знайти всі точки еліптичної кривої $y^2 = x^3 + 3x + 5$ для $p = 17$.

- знайдемо квадратичні лишки: $1, 2, 4, 8, 9, 13, 15, 16$ і квадрати: $2 = 6^2$, $8 = 5^2$, $13 = 8^2$, $15 = 7^2$.
- використовуючи запропоновані вище рекомендації, знайдемо точки еліптичної кривої:

$$(1,3),(1,14),(2,6),(2,11),(4,8),(4,9),(5,3),(5,14),(6,1),$$
$$(6,16),(9,8),(9,9),(10,7)(10,10),(11,3),(11,14),(12,1),$$
$$(12,16),(15,5),(15,12),(16,1),(16,16),O.(x;\infty)$$

3.1.5. Число елементів групи точок еліптичної кривої.

Визначення 3.1.6. Число елементів групи точок еліптичної кривої $E_p(a,b)$ над полем $GL(p)$ називається *порядком цієї групи і позначається* N_E.

Межі порядку групи точок еліптичної кривої над полем $GL(q)$, де $q = p^n$, визначаються теоремою Хассе.

Теорема Хассе. Порядок N_E групи точок еліптичної кривої над скінченим полем $GL(q)$, $q = p^n$ визначений нерівністю

$$q+1-2\sqrt{q} \le N_E \le q+1+2\sqrt{q}. \qquad (3.12)$$

З нерівності (3.12) випливає, що число точок еліптичної кривої перевищує загальне число елементів поля на величину меншого порядку, ніж $O\left(\sqrt{q}\right)$.

У випадку простого скінченого поля $GL(p)$ для порядку N_E еліптичної кривої $y^2 = x^3 + ax^2 + b$ є точна формула на мові символу Лежандра для квадратичних лишків [5]

$$N_E = p+1+\sum_{x=0}^{p-1}\left(\frac{f(x)}{p}\right), \qquad (3.13)$$

де $\left(\frac{f(x)}{p}\right)$ – символ Лежандра, тобто $\left(\frac{f(x)}{p}\right) = \pm 1$ в залежності від того, чи є $f(x) \equiv x^3 + ax^2 + b$ квадратичним лишком, чи нелишком за модулем p.

Приклад 3.1.2. Перевірити за формулою (3.13), що число точок N_E еліптичної кривої $y^2 = x^3 + 3x + 5$ над полем $GF(17)$ дорівнює 23. .

3.1.6. Порядок точки еліптичної кривої.

Визначення 3.1.7. Порядком точки $P \in E_p$ називається *найменше натуральне число* n, *для якого* $nP = O$.

Якщо точка $P(x;y)$ еліптичної кривої над скінченим полем має порядок n, то справедливі наступні твердження:

- множина $\{O,P,2P,...,(n-1)P\}$ утворює циклічну підгрупу в $E_p(a,b)$;
- порядок довільної точки еліптичної кривої є дільником числа точок еліптичної кривої N_E;
- якщо $n=N_E$, то точка порядку n є твірним елементом групи E_p;
- при належному виборі параметрів a і b можна досягти того, щоб число точок еліптичної кривої було просте число, і тоді кожна точка еліптичної кривої, окрім точки O, є твірним елементом групи E_p.

Слід зауважити, що арифметика еліптичних кривих не містить прямих формул для обчислення кратного mP для заданої точки P. Проте цю операцію виконують з використанням операцій додавання, віднімання і подвоєння точки. Аналогічно, як для піднесення до степеня за модулем, ми використовували подання степеня в двійковій системі, так і для відшукання кратної точки mP подамо число m в двійковій системі

$$m=b_t b_{t-1}...b_0, \text{ де } b_i\in\{0,1\},\quad i=\overline{0,t},\quad (3.14)$$

потім обчислимо точки $2P,4P,...,2^tP$ і підрахуємо суму точок 2^iP, для яких $b_i=1$.

Приклад 1.3.3. Знайти $13P(1;3)$ для еліптичної кривої $E_{17}(3,5)$.

Розв'язання. $13_{10}=1101_2$. Отже $13P=8P+4P+P$.

Знайдемо координати точки $2P$ за формулами (3.11)

$$\lambda = \frac{3+3}{2\cdot 3} = 1,$$

$$x_3 = 1-2 = -1 \equiv 16 \pmod{17},$$

$$y_3 = 1-16-3 = -18 \equiv 16 \pmod{17}.$$

Отже $2P = (16;16)$. Знайдемо знову за формулами (3.11) координати точки $4P$

$$\lambda = \frac{3\cdot(-1)^2+3}{2\cdot(-1)} = -\frac{6}{2} = -3 \equiv 14 \pmod{17},$$

$$x_3 = 14^2 - 32 = 164 \equiv 11 \pmod{17},$$

$$y_3 = 14(16-11)-16 = 54 \equiv 3 \pmod{17}.$$

Отже $4P = (11;3)$. Аналогічно знайдемо точку $8P$

$$\lambda = \frac{3\cdot 11^2+3}{6} = 61 \equiv 10 \pmod{17},$$

$$x_3 = 100-22 = 78 \equiv 10 \pmod{17},\ y_3 = 10(11-10)-3 = 7.$$

Тому $8P = (10;7)$.

Знайдемо координати суми точок $8P+4P=12P$ за формулами (3.10)

$$\lambda = \frac{7-3}{10-11} = -4 \equiv 13 \pmod{17},\ x_3 = 13^2 - 21 = 148 \equiv 12 \pmod{17},$$

$$y_3 = 13(11-12)-3 = -16 \equiv 1 \pmod{17}.$$

Отже координати точки $12P = (12;1)$. Знайдемо координати точки $13P = 12P + P$ за формулами (3.10)

$$\lambda = \frac{1-3}{12-1} = \frac{2}{-11} = \frac{2\cdot 3}{-11\cdot 3} = 6,\ x_3 = 36-13 = 23 \equiv 6 \pmod{17},$$

$$y_3 = 6(1-6)-3 = -33 \equiv 1 \pmod{17}.$$

І остаточно маємо точку $13P = (6;1)$.

Приклад 1.3.4. Знайти порядок точки $P(1;3)$ еліптичної кривої $E_7(2,6)$.

Розв'язання. Знайдемо координати точки $2P$ за формулами (3.11). Маємо

$$\lambda = \frac{3\cdot 1+2}{6} = \frac{5\cdot 6}{6\cdot 6} = 30 \equiv 2 \pmod 7,\ x_3 = 4-2-2 = 2,$$

$$y_3 = 2(1-2)-3 = -5 \equiv 2 \pmod 7.$$

Отже координати точки $2P = (2;2)$. Знайдемо координати точки $4P$ за формулами (3.11). Маємо

$$\lambda = \frac{3\cdot 4+2}{4} \equiv 0 \pmod 7,\ x_3 = -4 \equiv 3 \pmod 7,$$

$$y_3 = -2 \equiv 5 \pmod 7.$$

Отже $4P = (3;5)$. Аналогічно знайдемо координати точки $8P$. Маємо

$$\lambda = \frac{3\cdot 9+2}{10} = \frac{8}{3} = \frac{8\cdot 5}{3\cdot 5} = 40 \equiv 5 \pmod 7,$$

$$x_3 = 25-6 = 19 \equiv 5 \pmod 7,\ y_3 = 5(3-5)-5 = -15 \equiv 6 \pmod 7.$$

Тому $8P = (5;6)$. Знайдемо координати точки $3P = 2P + P = (2;2)+(1;3)$ за формулами (3.10). Маємо

$$\lambda = \frac{1}{-1} = -1 \equiv 6 \pmod 7,\ x_3 = 36-3 = 33 \equiv 5 \pmod 7,$$

$$y_3 = 6(2-5)-2 = -20 \equiv 1 \pmod 7.$$

Отже $3P = (5;1)$.

Знайдемо $11P = 8P + 3P = (5;6)+(5;1) = (5;6)+(5;-6)$. Оскільки ці точки лежать на вертикальній прямій $x = 5$ симетрично відносно осі абсцис, то їх сума дорівнює нескінченно віддаленій точці $O(x;\infty)$. Отже $11P = O$ і

порядок точки $P(1;3)$ в групі точок еліптичної кривої $E_7(2,6)$ дорівнює 11.

Приклад 3.1.5. Показати, що точка $P(1;11)$ еліптичної кривої $E_{23}(1,4)$ має порядок 29.

Вказівка: використати формули додавання і подвоєння точок, а також подання числа 29 у вигляді (3.14).

Операція множення на еліптичній кривій – це аналог операції піднесення до степеня в скінченому полі. Тому в еліптичній криптографії в ролі прямої задачі маємо задачу скалярного множення точок кривої, тобто обчислення $Q = mP$ для відомих m і P. Обернена задача за традицією називається дискретним логарифмуванням на еліптичній кривій і полягає у відшуканні для заданих точок P і Q еліптичної кривої такого числа m, що $Q = mP$. Стійкість шифрування на еліптичних кривих визначається складністю розв'язання задачі дискретного логарифмування на групі точок цих кривих.

Якщо порядок N_E групи точок кривої – добуток малих простих чисел, то дискретне логарифмування можна ефективно провести з допомогою алгоритму Поліа-Хеллмана.

3.1.7. Вибір еліптичної кривої і базової точки.

Зазвичай для криптування використовують еліптичні криві над простим полем і полем характеристики 2.

Генерація еліптичної кривої здійснюється за наступними кроками:

- вибір характеристики поля Галуа;
- вибір коефіцієнтів еліптичної кривої;
- обчислення порядку N_E групи точок кривої;
- вибір базової точки $G(x;y)$ кривої;

- визначення порядку базової точки кривої (кофактор $h = \frac{N_E}{n} < 4$, де n – порядок базової точки, в ідеальному варіанті $h = 1$).

В системах Даффі-Хелмана і Ель-Гамаля для вибору еліптичної кривої

використовують випадковий вибір, який полягає в наступному:

- вибираємо скінчене поле $GF\left(p^n\right)$ для великого $p > 3$;
- використовуємо криву у формі Вейєрштраса $y^2 = x^3 + ax + b$;
- задаємо довільну трійку чисел $x, y, a \in GF\left(p\right)$, обчислюємо $b = y^2 - \left(x^3 + ax\right)$ і перевіряємо умову несингулярності $4a^3 + 27b^2 \neq 0 \left(\mathrm{mod}\, p\right)$;
- якщо умова несингулярності виконується, то крива підібрана і точка $P\left(x; y\right)$ – точка цієї кривої, якщо ж умова несингулярності не виконується, то вибираємо іншу випадкову трійку чисел $x, y, a \in GF\left(p\right)$ і т.д.

Одна з гарантій того, що вибрана точка $G\left(x; y\right)$ еліптичної кривої згенерує групу точок еліптичної кривої – це такий вибір кривої і поля, для яких кількість точок N_E кривої є просте число. В цьому випадку довільна точка еліптичної кривої буде *твірним елементом* групи точок цієї кривої.

Таким чином, набір параметрів для задач криптування у випадку полів характеристики $p \neq 2, 3$ і еліптичних кривих у формі Вейєрштраса $\left(3.4\right)$ – наступний: $p, a, b, G, n, h,$ а для полів $GF\left(2^m\right)$ характеристики 2 трохи інший, а саме:

$m, f, a, b, G, n, h.$ Існує 15 еліптичних кривих, які рекомендовані *NIST* (США). Федеральні стандарти обробки інформації $(FIPS)$ рекомендують 10 скінчених полів де p має довжину 192, 224, 256, 384, 521 біт і поля $GF\left(2^m\right)$, де m має довжину 163, 233, 409, 571 біт.

Наприклад, одна з цих кривих наступна

$$y^2 = x^3 + 3176890812513255034763174764138276932727469559 27\,x + \\ +790528966078787587181205720257185354321006519 34.$$

3.2.Криптосистеми на еліптичних кривих.

3.2.1.Створення спільного ключа на еліптичній кривій

Криптоалгоритми на еліптичних кривих будуються аналогічно, як в простих скінчених полях. Піднесення до степеня за великим модулем в еліптичному криптуванні замінений на добуток точки кривої на число з вибраного поля. Суть переходу до еліптичних кривих полягає в заміні відносно повільної операції піднесення до степеня за модулем в алгоритмі RSA на швидшу операцію скалярного множення на еліптичній кривій $[9,10,12,13]$.

Розглянемо приклад створення спільного ключа на еліптичній кривій користувачами A і B. Опишемо цей алгоритм.

- вибираємо просте число $p \neq 2,3$ і відповідно поле $GF(p)$;
- формуємо еліптичну криву $E_p(a,b): y^2 = x^3 + ax + b$;
- вибираємо на кривій $E_p(a,b)$ базову точку $G(x;y)$ порядку n, тобто таку, що $nG = O$, де $n < N_E$.

Формування спільного ключа

1. Аліса обирає число $k_A < n$ і генерує відкритий ключ $Y_A = k_A G.$

2. Боб обирає число $k_B < n$ і генерує відкритий ключ $Y_B = k_B G.$

3. Аліса генерує таємний ключ $K = k_A Y_B$, а Боб – таємний ключ $k_B Y_A$.

Отже маємо

Відкритий ключ; $E_p(a,b), G.$

Таємний ключ Аліси k_A,

Таємний ключ Боба k_B,

Спільний таємний ключ K.

Коректність

Дійсно ключ K – спільний через те,що

$$k_A Y_B = k_A (k_B G) = k_B k_A G = k_B Y_A = K.$$

Приклад 3.2.1. Сформувати спільний ключ K для Аліси і Боба , якщо

- $p = 47;$
- $E_{47}(3,5): y^2 = x^3 + 3x + 5;$
- точка $G(5;45)$ порядку 61, тобто $61G = O.$

Розв'язання.

Формування спільного ключа

1. Аліса обирає число $k_A = 11 < n = 61$ і генерує відкритий ключ $Y_A = 11G = (14,21).$

2. Боб обирає число $k_B = 17 < n = 61$ і генерує відкритий ключ $Y_B = 17G = (34;5).$

3. Аліса генерує таємний ключ $K = k_A Y_B = 11(34;5) = (9,3)$, а Боб – таємний ключ $k_B Y_A = 17(14;21) = (13;19)$.

Отже маємо:

Відкритий ключ; $E_p(3,5): y^2 = x^3 + 3x + 5.$

Відкритий ключ Аліси $Y_A = (14;21);;$

Відкритий ключ Боба $Y_B = (34;5);$

Таємний ключ Аліси $k_A = 11;$

Таємний ключ Боба $k_B = 17;$

Спільний таємний ключ $K = (13;19).$

Здійснення атаки на цю схему полягає у знаходженні таємних ключів k_A і k_B Аліси і Боба із співвідношень $Y_A = k_A G$ та $Y_B = k_B G$, тобто у розв'язанні задачі дискретного логарифмування на еліптичній кривій, що є важкою задачею. Однак, протокол Деффі-Хеллмана не є захищений від суперника, який має доступ до каналу зв'язку і може підмінити відкриті точки Y_A та Y_B.

3.2.2.Криптосистема Ель-Гамаля над групою точок еліптичної кривої.

Спершу користувачі узгоджують параметри криптосистеми:

- поле $GF(q)$, де $q = p^n$;
- рівняння еліптичної кривої $E(a,b): y^2 = x^3 + ax^2 + b;$
- базову точку $G(x;y)$ вибираємо, як при створенні спільного ключа.

Нехай Аліса хоче послати Бобу повідомлення M, якому відповідає точка еліптичної кривої $M(x;y)$.

- Аліса має таємний ключ k_A і відкритий ключ $Y_A = k_A G$;
- Боб має таємний ключ k_B і відкритий ключ $Y_B = k_B G$;

Шифрування

- Аліса обирає випадкове ціле число k і обчислює точки kG і kY_B;
- Аліса обчислює точку $R = M + kY_B$;
- криптотекст, що відповідає повідомленню M – це пара точок $(kG; R)$;

Аліса надсилає криптотекст $(kG; R)$ Бобу.

Дешифрування

- Боб обчислює $k_B \cdot kG$;
- Боб знаходить різницю $R - k_B \cdot kG = M$.

Коректність

$$R - k_B \cdot kG = M + kY_B - k \cdot k_B G = M + k \cdot k_B G - k \cdot k_B G = M.$$

Приклад 3.2.2. Вибравши еліптичну криву $E_{47}(3,5)$, зашифрувати повідомлення $M(1;3)$ і дешифрувати його.

Розв'язання.

1. Генерація ключа отримувача

Покладемо базову точку $G(5;2)$, таємний ключ отримувача $k_B = 3$. Знайдемо відкритий ключ отримувача $Y_B = 3G$. Оскільки $3G = 2G + G$, то обчислимо спочатку $2G$, а потім $2G + G$ за формулами (3.11) і (3.10). Маємо:

$$2G: \lambda = \frac{3(25+1)}{4} = \frac{3 \cdot 26 \cdot 12}{4 \cdot 12} \equiv \frac{43}{1} (\mathrm{mod}\, 47) = 43;$$

$$x = 43^2 - 10 \equiv 6 (\mathrm{mod}\, 47);\ y = 43(5-6) - 2 \equiv 2 (\mathrm{mod}\, 47).$$

$$2G + G: \lambda = \frac{2-3}{1} = 0;\ x = -11 \equiv 36 (\mathrm{mod}\, 47);$$

$$y = -2 \equiv 45 (\mathrm{mod}\, 47).$$

Отже відкритий ключ отримувача $Y_B = (36;45)$.

2. *Шифрування*

• обираємо випадкове число $k = 5$ і обчислюємо за формулами (3.10), (3.11) точки $5G$ і $5Y_B$. Маємо:

$$5G = 3G + 2G = (36;45) + (6;2):$$

$$\lambda = \frac{43}{30} = \frac{43 \cdot 11}{30 \cdot 11} \equiv 3 \pmod{47};$$

$$x = 9 - 42 \equiv 14 \pmod{47}; \quad y = 3(6-14) - 2 \equiv 21 \pmod{47}.$$

Зауважимо, що обернений елемент 11 до числа 30 за mod47 можна знайти, наприклад, використовуючи алгоритм Евкліда в $\mathbb{Z}$.

Отже $5G = (14;21)$.

$5Y_B = 15G = 10G + 5G$. Для $10G$ за формулами (3.11) маємо

$$\lambda = \frac{3(14^2+1)}{42} = \frac{197 \cdot 37}{14 \cdot 37} = 333 \equiv 4 \pmod{47};$$

$$x = 16 - 28 \equiv 35 \pmod{47}; \; y = 4(14-35) - 21 \equiv 36 \pmod{47}.$$

Отже $10G = (35;36)$. Для $15G = (35;36) + (13;21)$ за формулами (3.10) маємо:

$$\lambda = \frac{15}{21} = \frac{5}{7} = \frac{5 \cdot 27}{7 \cdot 27} \equiv 41 \pmod{47}; \; x = 41^2 - 49 \equiv 34 \pmod{47};$$

$$y = 41(14-34) - 21 \equiv 5 \pmod{47}.$$

Отже $5Y_B = (34;5)$.

• обчислюємо точку $M + 5Y_B = (1;3) + (34;5)$. Маємо:

$$\lambda = \frac{2}{33} = \frac{2 \cdot 10}{33 \cdot 10} = 20; \; x = 20^2 - 35 \equiv 36 \,(mod\, 47);$$

$$y = 20(1-36) - 3 \equiv 2 \,(mod\, 47).$$

Отже $R=(36;2)$.

• надсилаємо криптотекст $((14;21),\ (36;2))$ отримувачу.

Дешифрування

• отримувач обчислює $3(14;21)$. Маємо (див. обчислення $5Y_B$) для $2Y_B$

$$\lambda\equiv 4(\bmod 47);\quad x=35(\bmod 47);\quad y=36(\bmod 47).$$

Для $3Y_B=2Y_B+Y_B$ маємо

$$\lambda=41(\bmod 47);\quad x=34(\bmod 47);\quad y=5(\bmod 47).$$

Тому $3(14;21)=(34;5)$.

• обчислюємо різницю $R-3\cdot(14;21)=(36;2)-(34;5)=(36;2)+(34;-5)$ за формулами (3.10):

$$\lambda=\frac{-7}{-2}=\frac{7\cdot 24}{2\cdot 24}\equiv 27(\bmod 47);\ x=27^2-70\equiv 1(\bmod 47);$$

$$y=27(36-1)-2\equiv 3(\bmod 47).$$

Отже $R-3\cdot 5G=(3;1)=M$, тобто отримувач розшифрував вихідне повідомлення $M=(1;3)$.

Додаток 1

Зразок тестових завдань

1. Розшифрувати, використовуючи шифр підстановки:

$$\text{ЕЛОС,ключ } K = \begin{pmatrix} 1 & 2 & 3 & 4 \\ 4 & 1 & 2 & 3 \end{pmatrix}:$$

2. Обчислити $\frac{\overline{2}}{\overline{3}} + \overline{3}$: в полі $F_7 = Z/7Z$:

3. Обчислити $\overline{4}^{-1} \cdot \overline{3}$ в полі $F_5 = Z/5Z$:

4. Яким може бути порядок підгрупи порядку $n = 15$?

5. Знайти Інверсію числа 25 відносно числа 33.

6. Рошифрувати словоГЗЇЬ, яке зашифрованелінійним шифром $ax \pmod{33}$ з ключем $a = 2$.

7. Яким словом є зашифроване з допомогою афінного шифру 3-го порядку з ключем $A = \begin{pmatrix} 1 & 2 & 3 \\ 1 & 4 & 7 \\ 3 & 6 & 10 \end{pmatrix}$ словоЩПВ?

8. Знайти функцію Ейлера $\varphi(p \cdot q)$, якщо p і q – прості числа.

9. Яка з трьох конгруенцій вірна?

а) $431 \equiv 27(101)$;

б) $1002 \equiv 63(134)$;

в) $95 \equiv 20 \pmod{37}$.

10. Обчислити $3^{13} \pmod{13}$.

11. Обчислити $2^{104} \pmod{101}$

12. Які значення x справджують конгруенцію $3^x \equiv 5 \pmod{7}$:

13. Чи справджується рівність $x^2+1=(x+1)(x-1)$ над полем $F_2 = Z/2Z$?

14. Переконатись, що многочлен x^3+x+1 є незвідним над $F_2 = Z/2Z$.

15. Знайти квадратичні нелишки за модулем 11.

16. Знайти квадратичні лишки за модулем 13.

17. Яке з чисел є показником числа $a=7$ за модулем $n=11$?

а)3; б)7; в)5.

18. Яке з чисел є первісним коренем за модулем $n=11$?

а) $g=3$; б)g=2; в)g=6 .

19. Які з точок належать еліптичній кривій $E_{17}(3,5)$?

а) $M_1(1;3)$; б) $M_2(10;7)$; в) $M_3(4;7)$.

20. На еліптичній кривій $E_{17}(3,5)$ знайти суму точок $P(11;3)$ і $Q(10;7)$.

21. На еліптичній кривій $E_{23}(1,4)$ знайти точку $2(7;3)$.

22. Знайти таємний ключ в криптосистемі RSA, якщо $p=7;\quad q=23;\quad e=13$.

23. Використовуючивластивостіфункції Лежандра, обчислити $\left(\frac{65}{11}\right)$.

24. Використовуючи символ Лежандра,з'ясувати, чи розв'язальна квадратична конгруенція $x^2 \equiv 11(\mathrm{mod}13)$.

Додаток 2

Зразок розрахункових завдань

1. Для підстановки $\sigma = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 & 7 & 8 & 9 & 10 \\ 3 & 4 & 8 & 7 & 5 & 10 & 2 & 1 & 9 & 6 \end{pmatrix}$ виконати наступні завдання:

- подати підстановку σ у вигляді добутку циклів і транспозицій і встановити парність чи непарність підстановки;
- знайти число інверсій у підстановці σ і встановити парність чи непарність на мові інверсій;
- знайти σ^k, де $k = 101$.

2. Використовуючи шифр підстановки, розшифрувати задане слово, якщо заданий ключ K має період $l = 4$

$$\text{ІОВДРЖБАНЯЕН } K = \begin{pmatrix} 1 & 2 & 3 & 4 \\ 3 & 1 & 4 & 2 \end{pmatrix}, l = 4.$$

3. Написати таблиці додавання і множення в кільці $17\mathbb{Z}/85\mathbb{Z}$. Знайти одиницю в цьому кільці та переконатись, що $17\mathbb{Z}/85\mathbb{Z}$ – поле. Знайти протилежні та оберненіелементи до елементів кільця $17\mathbb{Z}/85\mathbb{Z}$.

4. Знайти:

- всі нетривіальні підгрупи групи коренів з одиниці для $\sqrt[28]{1}$;
- всі первісні корені для $\sqrt[28]{1}$.

5. Використовуючи алгоритм Евкліда для чисел $a=1261,\quad b=1067;\ c=419,$ знайти:

- найбільший спільний дільник $d=(a,b)$;
- цілі числа u і v, для яких справджується рівність:
$$a\cdot u+b\cdot v=d;$$
- інверсію c відносно a.

6. Використовуючи алгоритм Евкліда для многочленів $P(x)=x^8+2x^5+x^3+x^2+1,\ Q(x)=2x^6+x^5+2x^3+2x^2+2$ в F_3, знайти:

- найбільший спільний дільник $D=(P(x),Q(x))$;
- многочлени $U(x)$ і $V(x)$, для яких справджується рівність:
$$P(x)\cdot U(x)+Q(x)\cdot V(x)=D(x).$$

7. Переконавшись, що $P(X)=X^3+X^2+1$ – незвідний многочлен над $F_2=\mathbb{Z}/2\mathbb{Z}$, знайти елемент $\dfrac{X^2+X}{X^2+X+1}$ в полі $F_2[X]/P(X)F_2[X]$.

8. Розв'язати рівняння $\varphi(x)=8$.

9. Використовуючи теореми Ейлера і Ферма, знайти найменший додатний лишок числа $a=2^{10000}$ за модулем $m=176$.

10. Знайти всі розв'язки лінійної конгруенції $388x \equiv 8(\mathrm{mod}1636)$;

11. Розв'язати систему конгруенцій, використовуючи китайську теорему про лишки

$$\begin{cases} x \equiv 4(\mathrm{mod}13), \\ x \equiv 3(\mathrm{mod}17), \\ x \equiv 10(\mathrm{mod}15). \end{cases}$$

12. Використовуючи властивості символу Лежандра вияснити, чи розв'язальна конгруенція $x^2 \equiv 10(\mathrm{mod}163)$. В разі позитивної відповіді розв'язати її.

13. Використовуючи властивості символу Лежандра вияснити, чи розв'язальна конгруенція $x^2 \equiv 3(\mathrm{mod}349)$. В разі позитивної відповіді розв'язати її.

14. Знайти показник $P_{1575}(169)$.

15. Використовуючи таблиці індексів, знайти:

- всі первісні корені за модулем 41;
- всі числа показника 10 за модулем 41;

16. Використовуючи лінійний шифр $ax(\mathrm{mod}33)$ з ключем $a = 13$ розшифрувати приказку

ЩАУГНОАЦЇСІЩИВЯЩІБЮҐ

17. Розшифрувати криптотекст, використовуючи ключ A

ДХБЮСУ $A = \begin{pmatrix} 1 & 5 \\ 15 & 4 \end{pmatrix}$

18. Розшифрувати слово,

ЛЄСАИЯ

використовуючи афінний шифр 3-го порядку з ключем

$$A=\begin{pmatrix}4 & 1 & 1\\ 6 & 2 & 1\\ 8 & 2 & 7\end{pmatrix};$$

19. Використовуючи криптосистему RSA, виконати наступні завдання для заданих $p=17,\quad q=11,\quad M=7$:

- записати відкритий ключ;
- записати таємний ключ;
- зашифрувати повідомлення М;
- розшифрувати повідомлення М.

20. Знайти точку $17(37;44)$ еліптичної кривої $E_{47}(3,5)\colon y^2=x^3+3x+5(\mathrm{mod}\,47)$.

Додаток 3

Канонічні рівняння еліптичних кривих і арифметичні операції для точок кривої

Тип поля і варіанти кривих	Канонічне рівняння кривої	Формули додавання $(x;y)=(x_1;y_1)+(x_2;y_2)$ $(x_1;y_1)\neq(x_2;y_2)$	Формули подвоєння $(x;y)=2(x_1;y_1)$
Поле характеристики $p\neq 2,3$	$y^2=x^3+ax^2+b$	$\lambda=\frac{y_2-y_1}{x_2-x_1};$ $x=\lambda^2-x_1-x_2;$ $y=\lambda(x_1-x)-y_1$	$\lambda=\frac{3x_1^2+a}{2y_1};$ $x=\lambda^2-2x_1;$ $y=\lambda(x_1-x)-y_1$
Поле характеристики $p=3$	$y^2=x^3+ax^2+bx+c$	$\lambda=\frac{y_2-y_1}{x_2-x_1};$ $x=\lambda^2-x_1-x_2-a;$ $y=\lambda(x_1-x)-y_1$	$\lambda=\frac{ax_1-b}{y_1};$ $x=\lambda^2-x_1-a;$ $y=\lambda(x_1-x)-y_1$
Поле характеристики $p=2$ супер-сингулярна крива	$y^2+ax=x^3+ax+b$	$\lambda=\frac{y_2+y_1}{x_2+x_1};$ $x=\lambda^2+x_1+x_2;$ $y=\lambda(x_1+x)+y_1+a$	$x=\frac{x_1^4+b^2}{a^2};$ $y=\frac{x_1^2+b}{a}(x_1+x)+y_1+a$
Поле характеристики $p=2$ несупер-сингулярна крива	$y^2+axy=x^3+bx^2+c$	$\lambda=\frac{y_2+y_1}{x_2+x_1};$ $x=\lambda^2+\lambda x_1+x_2+b$ $y=\lambda(x_1+x)+y_1+x$	$x=x_1^2+\frac{y_1^2}{x_1^2}+x_1+\frac{x_1}{y_1}+b$ $y=x_1^2+\frac{x_1^2+y_1}{x_1}x+x$

Додаток 4

Таблиці індексів

p=3, p-1=2, g=2

N	0	1	2	3	4	5	6	7	8	9
0		0	1							

I	0	1	2	3	4	5	6	7	8	9
0	1	2								

p=5, p-1=2^2, g=2

N	0	1	2	3	4	5	6	7	8	9
0		0	1	3	2					

I	0	1	2	3	4	5	6	7	8	9
0	1	2	4	3						

p=7, p-1=2·3, g=3

N	0	1	2	3	4	5	6	7	8	9
0		0	2	1	4	5	3			

I	0	1	2	3	4	5	6	7	8	9
0	1	3	2	6	4	5				

p=11, p-1=2·5, g=2

N	0	1	2	3	4	5	6	7	8	9
0		0	1	8	2	4	9	7	3	6
1	5									

I	0	1	2	3	4	5	6	7	8	9
0	1	2	4	8	5	10	9	7	3	6
1										

p=13, p-1=2^2·3, g=2

N	0	1	2	3	4	5	6	7	8	9
0		0	1	4	2	9	5	11	3	8
1	10	7	6							

I	0	1	2	3	4	5	6	7	8	9
0	1	2	4	8	3	6	12	11	9	5
1	10	7								

p=17, p-1=2^2·3, g=2

N	0	1	2	3	4	5	6	7	8	9
0		0	14	1	12	5	15	11	10	2
1	3	7	13	4	9	6	8			

I	0	1	2	3	4	5	6	7	8	9
0	l	3	9	10	13	5	15	11	16	14
1	8	7	4	12	2	6				

p=19, p-1=2·3², g=2

N	0	1	2	3	4	5	6	7	8	9
0		0	1	13	2	16	14	6	3	8
1	17	12	15	5	7	11	4	10	9	

I	0	1	2	3	4	5	6	7	8	9
0	1	2	4	8	16	13	7	14	9	18
1	17	15	11	3	6	12	5	10		

p=23, p-1=2·11, g=5

N	0	1	2	3	4	5	6	7	8	9	10
0		0	2	16	4	1	18	19	6	10	
1	3	9	20	14	21	17	8	7	12	15	
2	5	13	11								

I	0	1	2	3	4	5	6	7	8	9	10
0	1	5	2	10	4	20	8	17	16	11	
1	9	22	18	21	13	19	3	15	6	7	
2	12	14									

p=29, p-1=2²·7, g=2

N	0	1	2	3	4	5	6	7	8	9	10
0		0	1	5	2	22	6	12	3	10	
1	23	25	7	18	13	27	4	21	11	9	
2	24	17	26	20	8	16	19	15	14		

I	0	1	2	3	4	5	6	7	8	9	10
0	1	2	4	8	16	3	6	12	24	19	
1	9	18	7	14	28	27	25	21	13	26	
2	23	17	5	10	20	11	22	15			

p=31, p-1=2·3·5, g=3

N	0	1	2	3	4	5	6	7	8	9	10
0		0	24	1	18	20	25	28	12	2	
1	14	23	19	11	22	21	6	7	26	4	
2	8	29	17	27	13	10	5	3	16	9	
3	15										

I	0	1	2	3	4	5	6	7	8	9	10
0	1	3	9	27	19	26	6	17	20	9	
1	25	13	8	24	10	30	8	22	4	12	
2	5	15	14	11	2	6	18	23	7	21	

p=37, p-1=22·32, g=2

N	0	1	2	3	4	5	6	7	8	9	10
0		0	1	26	2	23	27	32	3	16	
1	24	30	28	11	33	13	4	7	17	35	
2	25	22	31	15	29	10	12	6	34	21	
3	14	9	5	20	8	19	18				

I	0	1	2	3	4	5	6	7	8	9	10
0	1	2	4	8	16	32	7	17	34	31	
1	25	13	26	15	30	23	9	18	36	35	
2	33	29	21	5	10	20	3	6	12	24	
3	11	22	7	14	28	19					

p=41, p-1=23·5, g=6

N	0	1	2	3	4	5	6	7	8	9
0		0	27	1	12	25	28	35	39	2
1	10	30	13	32	20	26	24	38	29	19
2	37	36	15	16	40	8	17	3	5	41
3	11	34	9	31	23	18	14	7	4	33
4	22	6	21							

I	0	1	2	3	4	5	6	7	8	9
0	1	6	36	11	25	27	39	29	10	19
1	32	28	4	24	21	3	18	26	33	34
2	40	35	5	30	16	14	2	12	31	22
3	9	13	37	17	20	38	23	15	8	7

p=43, p-1=2·3·7, g=3

N	0	1	2	3	4	5	6	7	8	9
0		0	27	I	12	25	28	35	39	2
1	10	30	13	32	20	26	24	38	29	19
2	37	36	15	16	40	8	17	3	5	41
3	11	34	9	31	23	18	14	7	4	33
4	22	6	21							

I	0	1	2	3	4	5	6	7	8	9
0	1	3	9	27	38	28	41	37	25	32
1	10	30	4	12	36	22	23	26	35	19
2	14	42	40	34	16	5	15	2	6	18
3	11	33	13	39	31	7	21	20	17	8
4	24	29								

p=47, p-1=2·23, g=5

N	0	1	2	3	4	5	6	7	8	9
0		0	18	20	36	1	38	32	8	40
1	19	7	10	11	4	21	26	16	12	45
2	37	6	25	5	28	2	29	14	22	35
3	39	3	44	27	34	33	30	42	17	31
4	36	15	24	13	43	41	23			

I	0	1	2	3	4	5	6	7	8	9
0	1	5	25	31	14	23	21	11	8	40
1	12	13	18	43	27	41	17	38	2	10
2	3	15	28	46	42	22	16	33	24	26
3	36	39	7	35	34	29	4	20	6	30
4	9	45	37	44	32	19				

p=53, p-1=22·13, g=2

N	0	1	2	3	4	5	6	7	8	9
0		0	1	17	2	47	18	14	3	34
1	48	6	19	24	15	12	4	10	35	37
2	49	31	7	39	20	42	25	51	16	46
3	13	33	5	23	11	9	36	30	38	41
4	50	45	32	22	8	29	40	44	21	28
5	43	27	26							

I	0	1	2	3	4	5	6	7	8	9
0	1	2	4	8	16	32	11	22	44	35
1	17	34	15	30	7	14	28	3	6	12
2	24	48	43	33	13	26	52	51	49	45
3	37	21	42	31	9	18	36	19	38	23
4	46	39	25	50	47	41	29	5	10	20
5	40	27								

p=59, p-1=2·29, g=2

N	0	1	2	3	4	5	6	7	8	9
0		0	1	50	2	6	51	18	3	42
1	7	25	52	45	19	56	4	40	43	38
2	8	10	26	15	53	12	46	34	20	28
3	57	49	5	17	41	24	44	55	39	37
4	9	14	11	33	27	48	16	23	54	36
5	13	32	47	22	35	31	21	30	29	

I	0	1	2	3	4	5	6	7	8	9
0	1	2	4	8	16	32	5	10	20	40
1	21	42	25	50	41	23	46	33	7	14
2	28	56	53	47	35	11	22	44	29	58
3	57	55	51	43	27	54	49	39	19	38
4	17	34	9	18	36	13	26	52	45	31
5	3	6	12	24	48	37	15	30		

p=61, p-1=22·3·5, g=2

N	0	1	2	3	4	5	6	7	8	9
0		0	1	6	2	22	7	49	3	12
1	23	15	8	40	50	28	4	47	13	26
2	24	55	16	57	9	44	41	18	51	35
3	29	59	5	21	48	11	14	39	27	46
4	25	54	56	43	17	34	58	20	10	38
5	45	53	42	33	19	37	52	32	36	31
6	30									

I	0	1	2	3	4	5	6	7	8	9
0	1	2	4	8	16	32	3	6	12	24
1	48	35	9	18	36	11	22	44	27	54
2	47	33	5	10	20	40	19	38	15	30
3	60	59	57	53	45	29	58	55	49	37
4	13	26	52	43	25	50	39	17	34	7
5	14	28	56	51	41	21	42	23	46	31

p=67, p-1=2·3·11, g=2

N	0	1	2	3	4	5	6	7	8	9
0		0	1	39	2	15	40	23	3	12
1	16	59	41	19	24	54	4	64	13	10
2	17	62	60	28	42	30	20	51	25	44
3	55	47	5	32	65	38	14	22	11	58
4	18	53	63	9	61	27	29	50	43	46
5	31	37	21	57	52	8	26	49	45	36
6	56	7	48	35	6	34	33			

I	0	1	2	3	4	5	6	7	8	9
0	1	2	4	8	16	32	64	61	55	43
1	19	38	9	18	36	5	10	20	40	13
2	26	52	37	7	14	28	56	45	23	46
3	25	50	33	66	65	63	59	51	35	3
4	6	12	24	48	29	58	49	31	62	57
5	47	27	54	41	15	30	60	53	39	11
6	22	44	21	42	17	34				

p=71, p-1=2·5·7, g=7

N	0	1	2	3	4	5	6	7	8	9
0		0	6	26	12	28	32	1	18	52
1	34	31	38	39	7	54	24	49	58	16
2	40	27	37	15	44	56	45	8	13	68
3	60	11	30	57	55	29	64	20	22	65
4	46	25	33	48	43	10	21	9	50	2
5	62	5	51	23	14	59	19	42	4	3
6	66	69	17	53	36	67	63	47	61	41
7	35									

I	0	1	2	3	4	5	6	7	8	9
0	1	5	25	52	41	59	3	15	2	10
1	50	31	9	45	6	30	4	20	27	62
2	18	17	12	60	8	40	54	51	36	34
3	24	47	16	7	35	29	72	68	48	21
4	32	14	70	58	71	63	23	42	64	28
5	67	43	69	53	46	11	55	56	61	13
6	65	33	19	22	37	39	49	26	57	66
7	38	44								

p=73, p-1=23·32, g=5

N	0	1	2	3	4	5	6	7	8	9
0		0	8	6	16	1	14	33	24	12
1	9	55	22	59	41	7	32	21	20	62
2	17	39	63	46	30	2	67	18	49	35
3	15	11	40	61	29	34	28	64	70	65
4	25	4	47	51	71	13	54	31	38	66
5	10	27	3	53	26	56	57	68	43	5
6	23	58	19	45	48	60	69	50	37	52
7	42	44	36							

I	0	1	2	3	4	5	6	7	8	9
0	1	5	25	52	41	59	3	15	2	10
1	50	31	9	45	6	30	4	20	27	62
2	18	17	12	60	8	40	54	51	36	34
3	24	47	16	7	35	29	72	68	48	21
4	32	14	70	58	71	63	23	42	64	28
5	67	43	69	53	46	11	55	56	61	13
6	65	33	19	22	37	39	49	26	57	66
7	38	44								

p=79, p-1=2·3·13, g=3

N	0	1	2	3	4	5	6	7	8	9
0		0	4	1	8	62	5	53	12	2
1	66	68	9	34	57	63	16	21	6	32
2	70	54	72	26	13	46	38	3	61	11
3	67	56	20	69	25	37	10	19	36	35
4	74	75	58	49	76	64	30	59	17	28
5	50	22	42	77	7	52	65	33	15	31
6	71	45	60	55	24	18	73	48	29	27
7	41	51	14	44	23	47	40	43	39	

I	0	1	2	3	4	5	6	7	8	9
0	1	3	9	27	2	6	18	54	4	12
1	36	29	8	24	72	58	16	48	65	37
2	32	17	51	74	64	34	23	69	49	68
3	46	59	19	57	13	39	38	35	26	78
4	76	70	52	77	73	61	25	75	67	43
5	50	71	55	7	21	63	31	14	42	47
6	62	28	5	15	45	56	10	30	11	33
7	20	60	22	66	40	41	44	53		

p=83, p-1=2·41, g=2

N	0	1	2	3	4	5	6	7	8	9
0		0	1	72	2	27	73	8	3	62
1	28	24	74	77	9	17	4	56	63	47
2	29	80	25	60	75	54	78	52	10	12
3	18	38	5	14	57	35	64	20	48	67
4	30	40	81	71	26	7	61	23	76	16
5	55	46	79	59	53	51	11	37	13	34
6	19	66	39	70	6	22	15	45	58	50
7	36	33	65	69	21	44	49	32	68	43
8	31	42	41							

I	0	1	2	3	4	5	6	7	8	9
0	1	2	4	8	16	32	64	45	7	14
1	28	56	29	58	33	66	49	15	30	60
2	37	74	65	47	11	22	44	5	10	20
3	40	80	77	71	59	35	70	57	31	62
4	41	82	81	79	75	67	51	19	38	76
5	69	55	27	54	25	50	17	34	68	53
6	23	46	9	18	36	72	61	39	78	73
7	63	43	3	6	12	24	48	13	26	52
8	21	42								

p=89, p-1=23·11, g=3

N	0	1	2	3	4	5	6	7	8	9
0		0	16	1	32	70	17	81	48	2
1	86	84	33	23	9	71	64	6	18	35
2	14	82	12	57	49	52	39	3	25	59
3	87	31	80	85	22	63	34	11	51	24
4	30	21	10	29	28	72	73	54	65	74
5	68	7	55	78	19	66	41	36	75	43
6	15	69	47	83	8	5	13	56	38	58
7	79	62	50	20	27	53	67	77	40	42
8	46	4	37	61	26	76	45	60	44	

I	0	1	2	3	4	5	6	7	8	9
0	1	3	9	27	81	65	17	51	64	14
1	42	37	22	66	20	60	2	6	18	54
2	73	41	34	13	39	28	84	74	44	43
3	40	31	4	12	36	19	57	82	68	26
4	78	56	79	59	88	86	80	62	8	24
5	72	38	25	75	47	52	67	23	69	29
6	87	83	71	35	16	48	55	76	50	61
7	5	15	45	46	49	58	85	77	53	70
8	32	7	21	63	11	33	10	30		

p=97, p-1=2^5·3, g=5

N	0	1	2	3	4	5	6	7	8	9
0		0	34	70	68	1	8	31	6	44
1	35	86	42	25	65	71	40	89	78	81
2	69	5	24	77	76	2	59	18	3	13
3	9	46	74	60	27	32	16	91	19	95
4	7	85	39	4	58	45	15	84	14	62
5	36	63	93	10	52	87	37	55	47	67
6	43	64	80	75	12	26	94	57	61	51
7	66	11	50	28	29	72	53	21	33	30
8	41	88	23	17	73	90	38	83	92	54
9	79	56	49	20	22	82	48			

I	0	1	2	3	4	5	6	7	8	9
0	1	5	25	28	43	21	8	40	6	30
1	53	71	64	29	48	46	36	83	27	38
2	93	77	94	82	22	13	65	34	73	74
3	79	7	35	78	2	10	50	56	86	42
4	16	80	12	60	9	45	31	58	96	92
5	72	69	54	76	89	57	91	67	44	26
6	33	68	49	51	61	14	70	59	4	20
7	3	15	75	84	32	63	24	23	18	90
8	62	19	95	87	47	41	11	55	81	17
9	85	37	88	52	66	39				

Додаток 5

Таблиця простих чисел $p < 4070$ та їх найменших первісних коренів g

p	g	p	g	p	g	p	g	p	g	p	g	p	g
2	1	179	2	419	2	661	2	947	2	1229	2	1523	2
3	2	181	2	421	2	673	5	953	3	1231	3	1531	2
5	2	191	19	431	7	677	2	967	5	1237	2	1543	5
7	3	193	5	433	5	683	5	971	6	1249	7	1549	2
11	2	197	2	439	15	691	3	977	3	1259	2	1553	3
13	2	199	3	443	2	701	2	983	5	1277	2	1559	19
17	3	211	2	449	3	709	2	991	6	1279	3	1567	3
19	2	223	3	457	13	719	11	997	7	1283	2	1571	2
23	5	227	2	461	2	727	5	1009	11	1289	6	1579	3
29	2	229	6	463	3	733	6	1013	3	1291	2	1583	5
31	3	233	3	467	2	739	3	1019	2	1297	10	1597	11
37	2	239	7	479	13	743	5	1021	10	1301	2	1601	3
41	6	241	7	487	3	751	3	1031	14	1303	6	1607	5
43	3	251	6	491	2	757	2	1033	5	1307	2	1609	7
47	5	257	3	499	7	761	6	1039	3	1319	13	1613	3
53	2	263	5	503	5	769	11	1049	3	1321	13	1619	2
59	2	269	2	509	2	773	2	1051	7	1327	3	1621	2
61	2	271	6	521	3	787	2	1061	2	1361	3	1627	3
67	2	277	5	523	2	797	2	1063	3	1367	5	1637	2
71	7	281	3	541	2	809	3	1069	6	1373	2	1657	11
73	5	283	3	547	2	811	3	1087	3	1381	2	1663	3
79	3	293	2	557	2	821	2	1091	2	1399	13	1667	2
83	2	307	5	563	2	823	3	1093	5	1409	3	1669	2
89	3	311	17	569	3	827	2	1097	3	1423	3	1693	2
97	5	313	10	571	3	829	2	1103	5	1427	2	1697	3
101	2	317	2	577	5	839	11	1109	2	1429	6	1699	3
103	5	331	3	587	2	853	2	1117	2	1433	3	1709	3
107	2	337	10	593	3	857	3	1123	2	1439	7	1721	3
109	6	347	2	599	7	859	2	1129	11	1447	3	1723	3

113	3	349	2	601	7	863	5	1151	17	1451	2	1733	2
127	3	353	3	607	3	877	2	1153	5	1453	2	1741	2
131	2	359	7	613	2	881	3	1163	5	1459	5	1747	2
137	3	367	6	617	3	883	2	1171	2	1471	6	1753	7
139	2	373	2	619	2	887	5	1181	7	1481	3	1759	6
149	2	379	2	631	3	907	2	1187	2	1483	2	1777	5
151	6	383	5	641	3	911	17	1193	3	1487	5	1783	10
157	5	389	2	643	11	919	7	1201	11	1489	14	1787	2
163	2	397	5	647	5	929	3	1213	2	1493	2	1789	6
167	5	401	3	653	2	937	5	1217	3	1499	2	1801	11
173	2	409	21	659	2	941	2	1223	5	1511	11	1811	6

Література

1. А. И. Кострикин. *Введение в алгебру.* М., Наука, 1994.

2. В. І. Андрійчук, Б.В. Забавський.*Алгебра і теорія чисел.* Університетська математика: основні курси. ВНТЛ, Львів, 1998.

3. Вербіцький О.В.Вступ до криптології / О.В.Вербіцький. –Львів.: ВНТЛ, 1998. –246с.

4. Ленг С. Алгебра / С. Ленг. –М. Мир, 1968. –564с.

5. И.М. ВиноградовОсновы теории чисел/И.М. Виноградов. –Москва.: Наука,1965. –172 с.

6. Я.В.РадыноЭлементы алгебры для студентов-аналитиков / Я.В.Радыно, А.Я.Радыно, Е.М.Радыно. – Гродно.:ГрГУим.Я.Купалы, 2013. – 196 с.

7. В.А.Фільштинський Математичні основи криптографії. Конспект лекцій/ В.А.Фільштинський, А.В. Бережний. – Суми.: Сумський державний університет, 2011. –138 с.

8. ДезаЕ.И.Сборник задач по теории чисел. Учебноепособие/ ДезаЕ.И., Котова Л.В. –М. Книжныйдом, ЛИБРОКОМ, 2012. –224 с.

9. М.В.Захарченко Асиметричні методи шифрування в телекомунікація. Навчальнийпосібник/ М.В.Захарченко, О.В. Онацький, Л.Г.Йова, Т.М. Шинкарук. –Одеса:2011. –184 с.

10. Коблиц Н. Курс теории чисел и криптографии /Коблиц И.. – Москва.: Наука, Изд-во ТВП, 2001. –260 с.

11. Хинчин А.Я. Цепные дроби/А.Я.Хинчин . – Москва.: URSS. 2003. –112 с.

12. Нечаев В.И. Элементы криптографии/Москва.: Высшая школа, 1999. –109 с.

13. Яценко В.В. Введение в криптографию/Москва.: МЦНМО, 1998. –272 с.

14. Нестеренко Ю.В.Алгоритмічні проблеми теорії чисел/МЦНМО. М.1998. 87-114.

15. Ємець В. Сучасна криптографія/ В.Ємець, А.Мельник, Р.Попович. –Львів.:БАК, 2003. – 144 с.

16. Остапов С.ЕОснови криптографії/ С.Е. Остапов, Л.О.Валь. – Чернівці.: Книги XXL, 2008. – 188 с.

17. Фергусон Н.Практическаякриптография/ Н.Фергусон, Брюс Шнайер. – М.: Вильямс, 2005. – 424 с.

18. Ю.С.Харин,В.И. Берник, Г.В.Матвеев Математические основы криптологииУчебн. Пособие – Мн. БГУ, 1999, 319 с.

19. Смарт Н. Алгоритмы возведення в степень / Криптография. –Москва.:2005. –528с.