МІНІСТЕРСТВО ОСВІТИ І НАУКИ УКРАЇНИ
НАЦІОНАЛЬНИЙ ГІРНИЧИЙ УНІВЕРСИТЕТ

Г.В. Кузнецов
С.О. Сушко
Л.Я. Фомичова
А.В. Корабльов

ФАКУЛЬТЕТ ІНФОРМАЦІЙНИХ ТЕХНОЛОГІЙ
Кафедра електроніки та обчислювальної техніки

СПЕЦІАЛЬНІ РОЗДІЛИ МАТЕМАТИКИ

Розділ «Теорія чисел»
(теоретичні відомості, тестові завдання, приклади)

Навчальний посібник

для студентів напрямів підготовки:
6.170101 Безпека інформаційних і комунікаційних систем,
6.170102 Системи технічного захисту інформації,
6.170103 Управління інформаційною безпекою
з галузі знань 1701 Інформаційна безпека

Дніпропетровськ
НГУ
2010

УДК 511.17
ББК 22.131
С33

Рекомендовано вченою радою університету як навчальний посібник для студентів напрямів підготовки 6.170101 Безпека інформаційних і комунікаційних систем, 6.170102 Системи технічного захисту інформації, 6.170103 Управління інформаційною безпекою з галузі знань 1701 Інформаційна безпека (протокол № 2 від 17.02.2010).

Рецензенти:

І.В. Жуковицький, д-р техн. наук, професор (Дніпропетровський національний університет залізничного транспорту ім. акад. В. Лазаряна, завідувач кафедри ЕОМ);

О.М. Петренко, д-р техн. наук, професор (Дніпропетровський національний університет, декан фізико-технічного факультету).

Спеціальні розділи математики. Розділ «Теорія чисел» (теоретичні
Т33 відомості, тестові завдання, приклади) [Текст]: Навч. посібник / Г.В. Кузнецов, С.О. Сушко, Л.Я. Фомичова, А.В. Корабльов. – Д.: Національний гірничий університет, 2010. – 86 с.

Викладено короткі теоретичні відомості та розглянуто задачі з усіх основних тем теорії чисел. Особливу увагу приділено типовим задачам, які подаються з докладними розв'язаннями і забезпечують ефективність самостійної роботи студентів над теоретичним та практичним матеріалом. Наведено велику кількість тестових завдань, що дасть змогу студенту самостійно підготуватися до модульного контролю.

Для студентів спеціальностей з інформаційної безпеки.

УДК 511.17
ББК 22.131

ЗМІСТ

ВСТУП

Мета викладання дисципліни «Спеціальні розділи математики» студентам напрямів 6.170101, 6.170102, 6.170103 – допомогти оволодіти математичним апаратом та здобути спеціальну математичну освіту, аби у майбутньому вони могли кваліфіковано вибрати той чи інший криптографічний засіб для захисту інформації, використовувати математичну мову як інструмент досягнення лаконічності та точності тверджень. Важливим елементом при цьому є самостійна робота студента – неперервна складова виконання поточних домашніх завдань і циклічної роботи з виконання індивідуальних модульних завдань. Результативність самостійної роботи забезпечується ефективною системою контролю, яка включає опитування студентів за змістом лекцій, перевірку виконання домашніх завдань, розв'язування задач біля дошки, захист індивідуальних модульних робіт.

У зв'язку з переходом до кредитно-модульної системи навчання вся дисципліна «Спеціальні розділи математики» розділена на 2 модулі, кожен з яких завершується написанням модульної контрольної роботи.

Кафедра вищої математики разом з кафедрою електроніки та обчислювальної техніки в рамках кредитно-модульної системи розробили цей посібник за навчальним матеріалом другого модуля дисципліни. У посібнику наведено стислі теоретичні відомості, тестові завдання для перевірки теоретичних знань, задачі для аудиторної та домашньої роботи.

Призначенням навчального посібника є підвищення ефективності самостійної роботи студентів під час підготовки до модульного контролю за результатами теоретичних та практичних занять з дисципліни «Спеціальні розділи математики».

1. ЕЛЕМЕНТИ ТЕОРІЇ ЧИСЕЛ (ТЕОРЕТИЧНІ ВІДОМОСТІ)

1.1. Подільність

Множину Z ***цілих чисел*** утворюють натуральні числа $N = \{1;2;3...\}$, число 0 і цілі від'ємні числа $\{...,-3;-2;-1\}$, тобто $Z = \{...,-3;-2;-1;0;1;2;3,...\}$. Якщо a і b – цілі числа, то $a+b$, $a-b$, ab обов'язково належать множині Z, тоді як результат ділення $\frac{a}{b}$ (при $b \neq 0$) не обов'язково належить Z. Якщо частка $\frac{a}{b} \in Z$, то це означає, що існує ціле число $q \in Z$, для якого $a = bq$ (це скорочено записують $a:b$ або $b|a$). Ділення числа a на число b націлі інколи виражають синонімами: a кратно b або b – ***дільник*** числа a (при цьому число q називають ***часткою*** ділення).

Теорема про ділення цілих чисел з остачею. Для будь-яких цілих чисел a і b можна в єдиний спосіб підібрати такі цілі числа q і r, для яких справедлива рівність

$$a = bq + r, \quad \text{де } 0 \le r < |b| .$$

У такому випадку число q називають ***неповною часткою***, а r ***остачею від ділення***. У подальшому будемо розглядати лише додатні дільники чисел.

Очевидно, якщо при діленні чисел a_1 і a_2 на число b утворюються остачі r_1 і r_2 відповідно, то:

1) остача від ділення суми $a_1 + a_2$ на b дорівнює остачі від ділення $r_1 + r_2$ на b;

2) остача від ділення добутку $a_1 a_2$ на b дорівнює остачі від ділення $r_1 r_2$ на b;

3) остача від ділення степеня a_1^n на b дорівнює остачі від ділення r_1^n на b (тут $n \in N$).

Будь-яке число, на яке діляться числа a і b, називається їх спільним дільником. ***Найбільший спільний дільник*** чисел a і b позначається НСД(a,b) або $d(a,b)$, або (a,b). Наприклад, НСД$(18,45) = 9$.

Числа a і b називаються ***взаємно простими***, якщо НСД$(a,b) = 1$. Так, числа 20 і 11 – взаємно прості, оскільки НСД$(20,11) = 1$. У разі, коли задано більше ніж два числа і кожні два з них взаємно прості, то такі числа називають ***попарно взаємно простими.*** Наприклад, 8, 9, 7 і 55 – попарно взаємно прості.

Властивості НСД чисел:

1^0 якщо $a = bq$, то НСД$(a,b) = b$;
2^0 якщо $a = bq + r$, то НСД$(a,b) =$ НСД(b,r);
3^0 НСД$(am,bm) = m \cdot$ НСД(a,b);
4^0 якщо НСД$(a,b) = 1$, то НСД$(ac,b) =$ НСД(c,b);
5^0 якщо НСД$(a,b) = 1$ та $(ac) \vdots b$, то $c \vdots b$.

Будь-яке ціле число, яке ділиться без остачі на числа a і b, називається їх спільним кратним. Найменше додатне кратне чисел a і b називають їх ***найменшим спільним кратним*** (НСК) та позначають НСК(a,b). Так, наприклад, НСК$(16,6) = 48$.

НСД(a,b) і НСК(a,b) чисел зв'язані формулою:

$$ab = \text{НСД}(a,b) \cdot \text{НСК}(a,b).$$

1.2. Алгоритм Евкліда для пошуку НСД чисел

Найбільший спільний дільник можна визначити за ***алгоритмом Евкліда***, основна перевага якого полягає в тому, що алгоритм не потребує попереднього розкладання чисел на множники. Розглянемо суть алгоритму.

Нехай a і b – цілі додатні числа і $a > b$. Складемо ряд рівностей:

$$\begin{aligned}
&a = bq_1 + r_1, && 0 < r_1 < b,\\
&b = r_1 q_2 + r_2, && 0 < r_2 < r_1,\\
&r_1 = r_2 q_3 + r_3, && 0 < r_3 < r_2, \qquad (1.1)\\
&\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\\
&r_{n-3} = r_{n-2} q_{n-1} + r_{n-1}, && 0 < r_{n-1} < r_{n-2},\\
&r_{n-2} = r_{n-1} q_n, && r_n = 0.
\end{aligned}$$

Остання рівність неминуча, бо ряд $b, r_1, r_2, r_3, \ldots$ спадних цілих чисел не може містити більше ніж b додатних чисел.

Із формул (1.1) випливає, що $(a,b) = (b,r_1) = (r_1,r_2) = \ldots = (r_{n-2},r_{n-1}) = (r_{n-1},0) = r_{n-1}$. А відтак найбільшим спільним дільником буде остання остача r_{n-1}, що не дорівнює нулю, отримана при діленні чисел.

Тепер запишемо порядок дій для пошуку НСД чисел: 1) розділити більше число на менше; 2) якщо є остача, то розділити менше число на остачу; 3) якщо знову утвориться остача, то розділити першу остачу на другу. Так продовжуємо доти, поки в остачі не дістанемо нуль. Тоді НСД буде дорівнювати останній, відмінній від нуля остачі у процесі ділення.

Теорема про зображення НСД чисел у вигляді їх лінійної комбінації. Якщо НСД(a,b) – найбільший спільний дільник натуральних чисел a і b, то існують такі цілі числа α і β, що

$$\alpha a + \beta b = \text{НСД}(a,b).$$

Зокрема, якщо $(a,b) = 1$, то $\alpha a + \beta b = 1$.

1.3. Прості числа. Решето Ератосфена. Розподіл простих чисел

Натуральне число p називають ***простим***, якщо воно має рівно два натуральних дільники, а саме: одиницю і самого себе. Так, простими числами будуть 2, 3, 5, 7, 11, 13, 17, 19, 23, 29, 31, ... (таблицю простих чисел наведено в додатку А). Натуральне число називають ***складеним***, якщо воно має принаймні один інший додатний цілий дільник, відмінний від одиниці і самого себе.

Згідно з означенням множина натуральних чисел розбивається на три підмножини: 1) прості числа, 2) складені числа і 3) число 1, що не відносять, а ні до простих, а ні до складених чисел.

Властивості простих чисел:

1^0 для будь-якого цілого числа $n>1$ **найменший, відмінний** від одиниці додатний дільник завжди є простим числом, бо у протилежному випадку, можливо, було б вибрати дільник ще менший;

2^0 найбільший простий дільник, відмінний від 1, будь-якого складеного числа n не перевищує $\sqrt{n}$;

3^0 простих чисел безліч;

4^0 якщо добуток натуральних чисел ab ділиться на просте число p, то принаймні одне з чисел a або b ділиться на p;

5^0 якщо НСД$(a,b)=1$, то арифметична прогресія $an+b$, $n\in N$, містить нескінченно багато простих чисел (***теорема Діріхле***). Так, при $a=4$ існує нескінченно багато простих чисел вигляду $4n+1$ і $4n+3$, при $a=3$ існує нескінченно багато простих чисел вигляду $3n+1$ і $3n+2$.

Два простих числа, різниця між якими дорівнює 2, наприклад, 3 і 5, 8004119 і 8004121, називають простими ***числами-близнюками***.

Важлива проблема щодо простих чисел – це знайти функцію від змінного n, яка б при всіх натуральних значеннях n давала б прості числа (принаймні не всі). Деякі результати з цього питання наведені у табл. 1.

Решето Ератосфена – найпростіша процедура отримання послідовності простих чисел. Покажемо, як за допомогою решета визначити всі додатні прості числа, менші за число n. Виписуємо всі натуральні числа від 2 до n. Перше просте число цього ряду, яке більше за 1, є 2. Отже викреслюємо з ряду (як складені) усі числа, кратні 2, крім його самого:

$$2,3,\cancel{4},5,\cancel{6},7,\cancel{8},9,\cancel{10},11,\cancel{12},13,...,n.$$

Тепер перше не викреслене число після двійки – це 3, і воно просте. З ним, як і з числом 2, виконуємо аналогічну процедуру, тобто викреслюємо за числом 3 всі числа, що кратні 3:

$$2,3,\cancel{4},5,\cancel{6},7,\cancel{8},\cancel{9},\cancel{10},11,\cancel{12},13,...,n.$$

Якщо аналогічними діями викреслені всі числа, кратні простим числам, які не перевищують $\sqrt{n}$, то всі не викреслені числа будуть простими.

Одне з найскладніших завдань теорії чисел – визначення кількості простих чисел серед перших n чисел натурального ряду. Позначимо через $\pi(x)$ кількість простих чисел, що не перевищують дійсного числа $x>1$. Множина простих чисел нескінченна, тому з ростом x значення функції $\pi(x)$ також зростають. Наприклад, $\pi(10)=4$, $\pi(100)=25$, $\pi(1000)=168$.

ТАБЛИЦЯ 1

Прості числа, побудовані за поліноміальними, експоненціальними та прайморіальною формулами

Спосіб побудови простих чисел	Формули	Зв'язок значення n і простоти побудованого числа	Примітка
Поліноміальний	Ейлера: $m=n^2+n+17$	m – просте при $0\le n\le 15$.	Доведено, що не існує многочлена від однієї змінної, значення якого були б простими числами при всіх цілих значеннях змінної n.
	$m=n^2+n+41$	m – просте при $0\le n\le 39$.	
	Лежандра: $m=2n^2+29$	m – просте при $0\le n\le 28$.	
	Скотта: $m=n^2-79n+1601$	m – просте при $0\le n\le 79$.	
Експоненціальний	$M_n=2^n-1$ – числа Марсенна	M_n – обов'язково складені числа, коли n є парним ($n\ge 4$) або непарним і складеним; при простих $n=2;3;5;7;13;17;19;...$ числа M_n є простими, а при простих $n=11;23;29;...$ числа M_n – складені.	При $n=43112609$ число M_n є простим і містить 12978189 десяткових знаків, це поки найбільше з усіх відомих простих чисел. На 2009-й рік відомо 47 простих чисел Марсенна.
	$F_n=2^{2^n}+1$ – числа Ферма	F_n – прості при $n=0,1,2,3,4$, при всіх інших n числа F_n – складені.	Всі дільники числа Ферма мають вигляд $m2^n+1$, $m-const$.
Прайморіальний	$m=p_n^{\#}\pm 1$	$p_n^{\#}+1$ – просте при $n=1,2,3,4,5,11,75,...$ $p_n^{\#}-1$ – просте при $n=2,3,5,6,13,24,66,...$ ***Прайморіал*** $p_n^{\#}$ простого числа p – це добуток перших n простих чисел. $p_n^{\#}=\prod_{k=1}^{n}p_k$; де p_k – k-те просте число.	Поки знайдено 22 простих числа вигляду $p_n^{\#}+1$ та 18 простих чисел вигляду $p_n^{\#}-1$. Найбільше з цих чисел $392113^{\#}+1$ складається з 169966 десяткових знаків.

Проте в міру зростання x послідовність простих чисел стає все більш рідкою, крім того, прості числа розподілені у натуральному ряді нерівномірно. Відношення $\frac{\pi(x)}{x}$ називають ***щільністю розподілу простих чисел***. Відзначимо деякі оцінки щільності розподілу простих чисел:

1) оцінка Ейлера $\frac{\pi(x)}{x} \approx \frac{1}{\frac{1}{3}+\frac{1}{4}+\frac{1}{5}+\ldots+\frac{1}{x}}$, де $x > 50$;

2) оцінка Чебишева $0{,}89\frac{x}{\ln x} < \pi(x) < 1{,}11\frac{x}{\ln x}$;

3) оцінки Біхама і Шаміра: $\pi(x) > \frac{x}{\ln x}$ для $x \geq 17$, $\pi(x) < \frac{x}{\ln x - 4}$ для $x \geq 55$.

Згідно з ***постулатом Бертрана*** при $n \geq 2$ в інтервалі $(n; 2n)$ завжди можна знайти принаймні одне просте число. Цей постулат уперше дістав своє математичне обґрунтування ще у 1850 р. У наш час найкращий в цьому напрямку результат гарантує наявність простого числа в інтервалі $(n; n + n^{107/200})$.

1.4. Основна теорема арифметики

Основна теорема арифметики. Для будь-якого цілого числа $a \neq 1$ існує єдиний ***канонічний розклад на прості множники*** (із точністю до перестановки множників), тобто

$$a = p_1^{k_1} p_2^{k_2} \cdot \ldots \cdot p_n^{k_n},$$

де $p_1, p_2, \ldots, p_n$ – різні прості числа, а $k_1, k_2, \ldots, k_n$ – натуральні числа, що називаються ***кратностями простих множників***.

Наслідки: нехай $a = p_1^{k_1} p_2^{k_2} \cdot \ldots \cdot p_n^{k_n}$ і $b = p_1^{t_1} p_2^{t_2} \cdot \ldots \cdot p_n^{t_n}$. Тоді

1. Число a ділиться на число b тоді і тільки тоді, коли $0 \leq t_1 \leq k_1$, $0 \leq t_2 \leq k_2, \ldots, 0 \leq t_n \leq k_n$.
2. $\text{НСД}(a,b) = p_1^{m_1} p_2^{m_2} \cdot \ldots \cdot p_n^{m_n}$, де $m_i = \min\{k_i; t_i\}$, $i = 1,2,\ldots n$,
   $\text{НСК}(a,b) = p_1^{s_1} p_2^{s_2} \cdot \ldots \cdot p_n^{s_n}$, де $s_i = \max\{k_i; t_i\}$, $i = 1,2,\ldots n$
   (деякі показники k_i і t_i можуть дорівнювати нулю).
3. Число a тоді і тільки тоді буде точним l-м степенем деякого цілого числа, коли всі показники $k_1, k_2, \ldots, k_n$ діляться на число l.
4. Кількість всіх дільників числа a
   $$\tau(a) = (k_1 + 1)(k_2 + 1)\ldots(k_n + 1).$$

5. Сума $S(a)$ всіх дільників числа m
   $$S(a) = \frac{p_1^{k_1+1} - 1}{p_1 - 1} \cdot \frac{p_2^{k_2+1} - 1}{p_2 - 1} \cdot \ldots \cdot \frac{p_n^{k_n+1} - 1}{p_n - 1}.$$
6. Числа a і b, відмінні від 0 і ± 1, взаємно прості тоді і тільки тоді, коли їх канонічний розклад не містить однакових простих множників.

1.5. Порівняння. Їх властивості

Нехай $m > 1$ – ціле додатне число, яке назвемо ***модулем***. Два цілих числа називаються ***порівняними за модулем*** m, якщо їх різниця $a - b$ ділиться без остачі на число m. Таке співвідношення між числами a і b називають ***порівнянням*** (***конгруенцією***) чисел та записують як

$$a \equiv b (\text{mod } m).$$

Про число b кажуть, що це ***лишок числа*** a ***за модулем*** m. Інколи порівняння скорочено записують як $a \equiv b(m)$, $a \overset{m}{\equiv} b$, а коли зрозуміло, за яким модулем записано порівняння, то $a \equiv b$. Запис $a \equiv b \bmod m$ (без дужок) означає лишок числа a, що дорівнює деякому цілому числу від 0 до $m-1$, саму операцію визначення числа b у такому разі називають ***зведенням числа*** a ***за модулем*** m. Наприклад, $77 \equiv 45(\text{mod } 8)$, $19 \equiv 4 \bmod 5$, $102 \equiv 0(\text{mod } 3)$.

Якщо $a \equiv b(\text{mod } m)$, то остачі від ділення a і b на m однакові, тобто із $a = mq_1 + r$ і $b = mq_2 + r$, де $0 \leq r < m$, випливає $a = b + mt$, $t = 0, \pm 1, \pm 2, \ldots$.

Властивості порівнянь:

1^0 $a \equiv a(\text{mod } m)$;

2^0 якщо $a \equiv b(\text{mod } m)$, то $b \equiv a(\text{mod } m)$;

3^0 якщо $a \equiv b(\text{mod } m)$ і $c \equiv b(\text{mod } m)$, то $a \equiv c(\text{mod } m)$;

4^0 якщо $a \equiv b(\text{mod } m)$, то $\text{НСД}(a,m) = \text{НСД}(b,m)$;

5^0 якщо $a \equiv b(\text{mod } m)$, $c \equiv d(\text{mod } m)$, то $a \pm c \equiv b \pm d(\text{mod } m)$ і $ac \equiv bd(\text{mod } m)$;

6^0 будь-який доданок лівої та правої частин порівняння можна переносити з протилежним знаком в іншу частину, тобто:
1) якщо $a \equiv b + c(\text{mod } m)$, то $a - c \equiv b(\text{mod } m)$ або $a - b \equiv c(\text{mod } m)$;
2) якщо $a + b \equiv c(\text{mod } m)$, то $a \equiv c - b(\text{mod } m)$;

7^0 якщо $\text{НСД}(k,m) = 1$ і $ak \equiv bk(\text{mod } m)$, то $a \equiv b(\text{mod } m)$;

8^0 якщо $\text{НСД}(k,m) = d$, $ak \equiv bk(\text{mod } m)$, то $a \equiv b(\text{mod } \frac{m}{d})$;

9^0 якщо $a \equiv b(\mathrm{mod}\, m)$ і $f(x) = c_n x^n + c_1 x^{n-1} + ... + c_1 x + c_0$ – многочлен із цілими коефіцієнтами, то $f(a) \equiv f(b)(\mathrm{mod}\, m)$;

10^0 якщо $a \equiv b(\mathrm{mod}\, m_1)$, $a \equiv b(\mathrm{mod}\, m_2)$ і $m = \mathrm{НСК}(m_1, m_2)$, то $a \equiv b(\mathrm{mod}\, m)$;

11^0 якщо $a \equiv b(\mathrm{mod}\, m)$ і $m : n$, то $a \equiv b(\mathrm{mod}\, n)$.

1.6. Класи лишків за модулем. Кільце Z_m лишків за модулем

На множині цілих чисел визначимо бінарне відношення, поклавши $a \sim b$, якщо $a \equiv b(\mathrm{mod}\, m)$. Таке бінарне відношення є відношенням еквівалентності, оскільки воно рефлексивне, симетричне і транзитивне.

Відношення «$\equiv(\mathrm{mod}\, m)$» розбиває множину всіх цілих чисел на непересічні класи еквівалентності $\bar{0}, \bar{1}, \bar{2}, ..., \overline{m-1}$, які називаються класами лишків за модулем m, а будь-яке число класу – лишком класу (представником класу). ***Клас лишків $\bar{a}$ за модулем m***, що містить число a, – це множина всіх чисел x, які порівняні з числом a за модулем m, тобто задовольняють умову $x \equiv a(\mathrm{mod}\, m)$. Отже,

$$\bar{0} = \{..., -2m, -m, 0, m, 2m...\},$$
$$\bar{1} = \{..., -2m+1, -m+1, 1, m+1, 2m+1...\},$$
$$.....$$
$$\overline{m-1} = \{..., -m-1, -1, m-1, 2m-1, 3m-1...\}.$$

Наприклад, за модулем 10 число 73 належить до класу $\bar{3}$, а число (-16) – до класу $\bar{4}$, бо $73 \equiv 13(\mathrm{mod}\, 10)$, $-16 \equiv 4(\mathrm{mod}\, 10)$.

Усім числам класу відповідає одна й та сама остача r від ділення на модуль, тому ми одержимо всі числа класу, коли у виразі $r + mt$ змінна t пробігатиме всі цілі числа. Лишок, обчислений при $t = 0$, дорівнює самій остачі r і називається ***найменшим невід'ємним лишком***.

Властивості класів лишків за модулем:

1^0 усі лишки одного й того ж класу порівняні один з одним за модулем m, на відміну від лишків різних класів;

2^0 кожен клас лишків містить нескінченну множину чисел. Кількість класів за модулем m скінчена і дорівнює m. Кожне ціле число можна порівняти за модулем m тільки з одним із чисел $0, 1, 2, ..., m-1$;

3^0 якщо два класи мають принаймні одне спільне число, то вони збігаються;

4^0 усі лишки одного класу $\bar{a}$ за модулем m мають із числом m однаковий найбільший спільний дільник.

Повною системою лишків за модулем m називається будь-яка система з m чисел, узятих по одному з кожного класу лишків за цим модулем. Очевидно, для будь-якого модуля m повну систему лишків утворюють числа $\{0, 1, 2, ..., m-1\}$. Класи лишків за модулем m, представники яких є взаємно простими з числом m, називаються ***зведеними***, а будь-яка система чисел, узятих по одному з кожного зведеного класу, – ***зведеною системою лишків***. Таким чином, зведена система лишків складається з тих чисел повної системи, що є взаємно простими з модулем (звичайно, їх вибирають із повної системи найменших невід'ємних лишків). Якщо модуль m – просте число, то у зведену систему лишків входить уся множина чисел $\{0, 1, 2, ..., m-1\}$.

Позначимо через $Z_m = \{0, 1, 2, ..., m-1\}$ множину чисел повної системи найменших невід'ємних лишків за модулем m, що еквівалентно заданню множини класів лишків $\bar{0}, \bar{1}, \bar{2}, ..., \overline{m-1}$ за цим модулем. На цій множині введемо дві операції, які відповідно назвемо ***додаванням*** та ***множенням класів лишків за модулем*** і позначимо їх «$+$» та «$\cdot$». Для цих операцій покладемо

$$\bar{a} + \bar{b} = \overline{a+b}, \quad \text{якщо } a + b < m$$
$$\bar{a} + \bar{b} = \overline{a+b-m}, \text{ якщо } a + b \geq m$$

тобто $a + b \equiv (a+b)(\mathrm{mod}\, m)$;

$$\bar{a} \cdot \bar{b} = \bar{r}, \text{ де } a \cdot b = mq + r,\ 0 \leq r < m$$

тобто $a \cdot b \equiv (ab)(\mathrm{mod}\, m)$.

Клас лишків $\overline{-a}$ назвемо ***протилежним до класу*** $\bar{a}$. Очевидно, $\overline{-a} = \overline{m-a}$.

Така множина класів лишків $Z_m = \{0, 1, 2, ..., m-1\}$ за модулем m із введеними операціями додавання та множення класів утворює скінченне комутативне ***кільце лишків за модулем m***.

1.7. Функція Ейлера

Кількість класів лишків, представники яких є взаємно простими з модулем m, дорівнює кількості цілих чисел, що не перевищують m та взаємно прості з m. Далі дамо два еквівалентних означення функції Ейлера, яка саме й визначає цю кількість класів лишків.

Означення 1. ***Функцією Ейлера*** $\varphi(m)$ називають кількість класів за модулем m, представники яких взаємно прості із цим модулем.

Означення 2. ***Функцією Ейлера*** $\varphi(m)$ називають кількість натуральних чисел, що не перевищують числа m і є взаємно простими з m.

Наприклад, $\varphi(24)=8$, бо 8 чисел 1,5,7,11,13,17,19,23 є взаємно простими з числом 24.

Властивості функції Ейлера:

1^0 властивість мультиплікативності: якщо числа m_1 і m_2 взаємно прості, тобто $\text{НСД}(m_1,m_2)=1$, то $\varphi(m_1m_2)=\varphi(m_1)\varphi(m_2)$;

2^0 якщо $p-$ просте число і $\alpha>0$, то $\varphi(p^\alpha)=p^\alpha-p^{\alpha-1}=p^\alpha\left(1-\frac{1}{p}\right)$,

зокрема $\varphi(p)=p-1$;

3^0 якщо $m=p_1^{\alpha_1}p_2^{\alpha_2}\cdot\ldots\cdot p_n^{\alpha_n}$, де всі p_i – прості числа, то

$$\varphi(m)=m\left(1-\frac{1}{p_1}\right)\left(1-\frac{1}{p_2}\right)\ldots\left(1-\frac{1}{p_n}\right)$$

або скорочено

$$\varphi(m)=m\prod_{i=1}^{n}\left(1-\frac{1}{p_i}\right).$$

1.8. Теореми Ейлера і Ферма. Псевдопрості числа. Числа Кармайкла

Теорема Ейлера. Для будь-якого модуля m і будь-якого $a\geq 1$, що є взаємно простим із числом m, справедливе порівняння

$$a^{\varphi(m)}\equiv 1(\text{mod } m).$$

Окремий випадок теореми Ейлера – це теорема Ферма, яка враховує, що для простого p функція Ейлера визначається за формулою $\varphi(p)=p-1$.

Теорема Ферма. Для будь-якого простого p і будь-якого $a\geq 1$, що не ділиться на p, справедливе порівняння

$$a^{p-1}\equiv 1(\text{mod } p)\ .$$

Якщо при деякому a порівняння порушується, то можна стверджувати, що модуль порівняння – складене число (число a у такому разі називають ***свідком непростоти*** модуля). Тому теорему Ферма можна розглядати як метод тестування чисел на простоту, при якому немає потреби розкладати число на множники. Сформулюємо тест у вигляді теореми.

Теорема (***тест на розкладність***). Якщо n – непарне натуральне число і знайдеться таке ціле число a з проміжку $(1;n-1)$, що $a^{n-1}\not\equiv 1(\text{mod } n)$, то $n-$ складене число.

На жаль, ми не можемо впевнено стверджувати, що число n – просте, навіть у разі, коли теорема Ферма виконується для всіх чисел $1<a<n-1$. Це пов'язано з існуванням так званих псевдопростих чисел Ферма. Непарне число n, яке задовольняє умові $a^{n-1}\equiv 1(\text{mod } n)$ і $\text{НСД}(a,n)=1$, але не є простим, називається ***псевдопростим числом Ферма за основою*** a. Наприклад, має

місце порівняння $2^{341-1}\equiv 1(\text{mod}341)$, проте $341=11\cdot 31$, і тому число 341 – псевдопросте число Ферма за основою $a=2$.

Непарне натуральне складене число n називається ***числом Кармайкла***, якщо $a^{n-1}\equiv 1(\text{mod } n)$ для всіх цілих чисел a, що є взаємно простими з модулем n. Умови, які має задовольняти число, щоб бути кармайкловим, визначає теорема ***Корселта***: непарне ціле число n є числом Кармайкла, якщо для кожного його простого дільника виконуються дві умови: 1) число n не ділиться на p^2; 2) число $n-1$ ділиться на $p-1$.

Приклад кармайклового числа: $n=3\cdot 11\cdot 17=561$ (для будь-якого цілого a з умовою $\text{НСД}(a,561)=1$ виконується $a^{560}\equiv 1(\text{mod}561)$. Псевдопростих чисел і чисел Кармайкла значно менше, ніж простих. Так, в інтервалі $[1;10^9]$ міститься 50847544 простих, 5597 псевдопростих за основою 2 та 646 чисел Кармайкла.

1.9. Визначення обернених елементів (ділення за модулем)

Нехай $Z_m=\{0,1,2,\ldots,m-1\}$ – кільце лишків за модулем m. Елемент кільця $a^{-1}\in Z_m$ називається ***оберненим*** до елемента $a\in Z_m$ у кільці Z_m, а число a називається ***оборотним***, якщо виконується порівняння $aa^{-1}=1(\text{mod } m)$. Множина елементів в Z_m, для яких в Z_m існують обернені елементи, утворює мультиплікативну групу, яку позначають Z_m^*.

Теорема. У кільці лишків $Z_m=\{0,1,2,\ldots,m-1\}$ за модулем m обернені елементи існують тільки для тих ненульових елементів кільця, що є взаємно простими з модулем m.

У разі простого модуля p будь-який ненульовий елемент кільця лишків матиме обернений елемент (для простого модуля кільце Z_p є скінченним полем).

Розглянемо два методи пошуку обернених елементів у кільці лишків.

1. ***За допомогою алгоритму Евкліда***: якщо елемент a кільця лишків Z_m має обернений, то $\text{НСД}(a,m)=1$. Алгоритм Евкліда дає нам такі числа α та β, що $\alpha a+\beta m=1$, а це еквівалентно тотожності $\alpha a\equiv 1(\text{mod } m)$ у Z_m, тобто $\alpha=a^{-1}$. Таким чином, число α у виразі $\alpha a+\beta m=1$ дорівнює оберненому елементу a^{-1}.

2. ***За допомогою теореми Ейлера***: $a^{-1}\equiv a^{\varphi(m)-1}(\text{mod } m)$.

1.10. Порівняння першого степеня

Загальний вид ***порівняння першого степеня (лінійного порівняння)*** такий:

$$ax\equiv b(\text{mod } m),$$

де a і b – цілі задані числа (степінь порівняння збігається із степенем невідомого x). ***Розв'язком (коренем)*** порівняння $ax \equiv b(\mathrm{mod}\, m)$ називається таке ціле число x_0, при якому добуток ax_0 стає порівняним з числом b за модулем m. Якщо число x_0 задовольняє порівняння, то увесь клас лишків $\overline{x_0}$ за модулем m, представником якого є число x_0, також задовольнятиме порівняння і тому клас $\overline{x_0}$ вважається розв'язком порівняння.

ТАБЛИЦЯ 2

Умови існування розв'язків порівнянь першого степеня

$d = \text{НСД}(a,m) = 1$, тобто числа a і m взаємно прості	Коефіцієнт b не ділиться на $d = \text{НСД}(a,m)$	Коефіцієнт b ділиться на $d = \text{НСД}(a,m)$
Тільки один розв'язок $x = x_0(\mathrm{mod}\, m)$	Немає розв'язків	Існує рівно d розв'язків: $x_0,\ x_0 + \frac{m}{d},\ x_0 + 2\frac{m}{d},\ldots,\ x_0 + (d-1)\frac{m}{d}$, де x_0 – розв'язок порівняння $\frac{a}{d}x \equiv \frac{b}{d}(\mathrm{mod}\, \frac{m}{d})$

Способи розв'язування порівнянь $ax \equiv b(\mathrm{mod}\, m)$:

1. ***Випробування лишків повної системи*** за модулем m. Оскільки кількість класів за даним модулем скінченна, то можна вибрати будь-яку повну систему лишків $x_1, x_2, \ldots, x_m$ за модулем m, обчислити $ax_1, ax_2, \ldots, ax_m$ та підібрати те значення x, при якому $ax - b$ ділиться на m. Таке число x буде розв'язком порівняння.

2. ***За допомогою теореми Ейлера*** $a^{\varphi(m)} \equiv 1(\mathrm{mod}\, m)$, де $\text{НСД}(a;m) = 1$. Почленно множимо обидві частини порівняння на $a^{\varphi(m)-1}$:

$$aa^{\varphi(m)-1}x \equiv ba^{\varphi(m)-1}(\mathrm{mod}\, m) \Rightarrow \quad a^{\varphi(m)}x \equiv ba^{\varphi(m)-1}(\mathrm{mod}\, m) \Rightarrow$$

$$x \equiv ba^{\varphi(m)-1}(\mathrm{mod}\, m).$$

При великому m розв'язування порівнянь методом випробувань та за теоремою Ейлера досить нелегка обчислювана задача.

3. ***Заміна даного порівняння еквівалентними на основі теореми***: якщо $\text{НСД}(a;m) = 1$ і $(b + km) \vdots a$, то розв'язком порівняння є $x \equiv \frac{b+km}{a}(\mathrm{mod}\, m)$.

За цією теоремою порівняння $ax \equiv b(\mathrm{mod}\, m)$ послідовно замінюємо еквівалентними порівняннями: $ax \equiv b \pm m(\mathrm{mod}\, m)$, $ax \equiv b \pm 2m(\mathrm{mod}\, m)$, $ax \equiv b \pm 3m(\mathrm{mod}\, m)$, ..., поки не дістанемо порівняння, в якому ліву та праву частини можна скоротити на a. При цьому кількість випробувань буде не більша за a.

4. ***За допомогою алгоритму Евкліда***: коли $\text{НСД}(a, m) = 1$ за алгоритмом визначаємо обернений елемент a^{-1} до елемента a за модулем m. Помноживши обидві частини порівняння на a^{-1}, дістаємо x: $a^{-1}ax \equiv a^{-1}b(\mathrm{mod}\, m) \Rightarrow$ $\Rightarrow x \equiv a^{-1}b(\mathrm{mod}\, m)$.

Порівняння $ax \equiv b(\mathrm{mod}\, m)$ являє собою інакше записане алгебраїчне рівняння першого ступеня з двома невідомими $ax - b = my$ або $ax - my = b$. Тому розв'язувати такі рівняння можна як звичайне алгебраїчне порівняння.

1.11. Система порівнянь першого степеня. Китайська теорема про остачі

Система порівнянь першого степеня складається з n порівнянь з одним і тим самим невідомим, але з різними модулями:

$$\begin{cases} a_1x \equiv b_1(\mathrm{mod}\, m_1); \\ a_2x \equiv b_2(\mathrm{mod}\, m_2); \\ \ldots\ldots\ldots\ldots\ldots\ldots \\ a_nx \equiv b_n(\mathrm{mod}\, m_n), \end{cases}$$

де $\text{НСД}(a_1, m_1) = 1$, $\text{НСД}(a_2, m_2) = 1, \ldots, \text{НСД}(a_n, m_n) = 1$, $M = \text{НСК}(m_1, m_2, \ldots, m_n)$.

Розв'язком системи порівнянь буде клас лишків за модулем M, представники якого задовольняють усі порівняння системи.

Якщо окремо розв'язати кожне порівняння системи, то її можна переписати у вигляді:

$$\begin{cases} x \equiv c_1(\mathrm{mod}\, m_1); \\ x \equiv c_2(\mathrm{mod}\, m_2); \\ \ldots\ldots\ldots\ldots\ldots\ldots \\ x \equiv c_n(\mathrm{mod}\, m_n). \end{cases} \qquad (1.2)$$

Коли хоч одне з порівнянь у системі не має розв'язків, то вся система вважається несумісною.

Теорема про сумісність системи порівнянь. Якщо $d = \text{НСД}(m_1, m_2)$ є найбільшим спільним дільником чисел m_1 і m_2, а $M = \text{НСК}(m_1, m_2)$ – їх найменшим спільним кратним, то система двох порівнянь

$$\begin{cases} x \equiv c_1(\mathrm{mod}\, m_1); \\ x \equiv c_2(\mathrm{mod}\, m_2) \end{cases}$$

має розв'язок $x \equiv x_0(\mathrm{mod}\, M)$ тільки за умови, що $c_2 \equiv c_1(\mathrm{mod}\, d)$. Зокрема, якщо числа m_1 і m_2 взаємно прості, тобто $d = 1$, то система завжди має єдиний розв'язок за модулем m_1m_2.

Китайська теорема про остачі. Нехай у системі порівнянь (1.2) модулі $m_1, m_2, ..., m_n$ – попарно взаємно прості числа, $M = \text{НСК}(m_1, m_2, ..., m_n)$ – найменше спільне кратне модулів, а числа $y_1, y_2, ..., y_n$ є розв'язками порівнянь $\frac{M}{m_1} y_1 \equiv 1 (\text{mod } m_1)$, $\frac{M}{m_2} y_2 \equiv 1 (\text{mod } m_2)$, ... , $\frac{M}{m_n} y_n \equiv 1 (\text{mod } m_n)$.

Тоді система (1.2) має єдиний розв'язок $x \equiv x_0 (\text{mod } M)$, де

$$x_0 = \frac{M}{m_1} y_1 c_1 + \frac{M}{m_2} y_2 c_2 + ... + \frac{M}{m_n} y_n c_n .$$

1.12. Псевдовипадкові числові послідовності

Псевдовипадкова послідовність чисел – це послідовність чисел, отримана за допомогою арифметичного алгоритму (***генератора псевдовипадкової послідовності***), який притаманний весь комплекс частотних властивостей, що вважається типовим для послідовності реалізацій випадкової величини із заданим законом розподілу. Псевдовипадкові послідовності широко розповсюджені в криптографії. Наведемо деякі генератори псевдовипадових послідовностей чисел.

1. ***Лінійний конгруентний генератор*** будує послідовність псевдовипадкових чисел $\{x_i\}$ за законом $x_{i+1} = a \cdot x_i + b (\text{mod } m)$, $i = 0,1,...$, де $x_0 \geq 0$ – початкове значення (ключ), $a \geq 0$, $b \geq 0$, $m > x_0$, $m > a$, $m > b$. Послідовність періодична, має максимальний період довжини m за таких умов:

- $\text{НСД}(b, m) = 1$;
- число $a - 1$ ділиться націло на кожний простий дільник модуля m;
- $(a-1) \vdots 4$, якщо модуль $m \vdots 4$.

Наприклад, лінійний конгруентний генератор $x_{i+1} = 7x_i + 7 (\text{mod } 10)$ при $x_0 = 7$ будує послідовність $7,6,9,0,7,6,9,0,...$, довжина періоду якої дорівнює 4.

2. ***Квадратичний генератор*** працює за рівнянням $x_{i+1} = (a_2 x_i^2 + a_1 x_i + b) (\text{mod } m)$. У цьому разі максимальний період послідовності не перевищує числа m і досягається, коли:

- $\text{НСД}(b, m) = 1$;
- a_1 і a_2 діляться націло на кожний простий дільник модуля m;
- $a_2 = (a_1 - 1) (\text{mod } 2)$, якщо $m \vdots 2$, або $a_2 = (a_1 - 1) (\text{mod } 4)$, якщо $m \vdots 4$, або $a_2 \neq 3b (\text{mod } 9)$, якщо $m \vdots 9$.

3. ***Адитивний генератор Фібоначчі***, рівняння роботи якого $x_{i+1} = (x_i + x_{i-1}) (\text{mod } m)$, де m – парне число.

4. ***Інверсивний конгруентний генератор***, рівняння роботи якого $x_{i+1} = a \cdot x_i^{-1} + b (\text{mod } p)$, де p – просте число, $x_i^{-1} x_i \equiv 1 (\text{mod } p)$ (припускається, що $0^{-1} = 0$).

5. ***Генератор BBS*** (абревіатура утворена від імен його авторів – Л. Блюма, М. Блюма та М. Шуба). Робота цього генератора будується за принципами:

- вибираються прості числа p і q з властивістю $p \equiv 3 (\text{mod } 4)$, $q \equiv 3 (\text{mod } 4)$ та обчислюється $n = pq$;
- вибирається інше ціле число x з умов, що $\text{НСД}(x, n) = 1$;
- обчислюється число $x_0 \equiv x^2 (\text{mod } n)$ (початкове значення генератора);
- формується послідовність чисел за законом $x_i \equiv x_{i-1}^2 \text{ mod } n$;
- шуканою псевдовипадковою послідовністю буде послідовність $b_1, b_2, ..., b_m$, де $b_i \equiv x_{i-1} \text{ mod } 2$.

1.13. Афінні шифри

Нехай n – кількість букв абетки, нумерація яких починається з нуля. Кожну букву тексту, що шифрується, замінимо її номером в абетці (номери букв української абетки, наведеної у додатку Б). Цим самим абетка ототожниться з кільцем лишків Z_n за модулем n. Тоді можна збудувати шифри, наведені в табл. 3.

ТАБЛИЦЯ 3

Афінні шифри

Назва шифру	Рівняння шифрування	Рівняння дешифрування
Шифр зсуву	Кожна буква x замінюється на $y = (x + k) \text{mod } n$, де ключ $0 < k < n$	Кожна буква y замінюється на $x = (y + k') \text{mod } n$, де ключ $k' = k - n$
Лінійний шифр	Кожна буква x замінюється на $y = (kx) \text{mod } n$, де ключ $0 < k < n$, $\text{НСД}(k, n) = 1$	Кожна буква y замінюється на $x = (k'y) \text{mod } n$, де ключ $k' = k^{-1} \text{mod } n$
Афінний шифр	Кожна буква x замінюється на $y = (kx + t) \text{mod } n$, де ключі $0 \leq t < n$, $0 < k < n$, $\text{НСД}(k, n) = 1$	Кожна буква y замінюється на $x = (k'y + t') \text{mod } n$, де $k' = k^{-1} \text{mod } n$; $t' = (-k't) \text{mod } n$

1.14. Шифр Хілла

Абетку відкритого тексту, як і раніше, ототожнимо з кільцем лишків Z_n за модулем n (n – кількість букв абетки, нумерація яких починається з нуля.).

Текст, що має шифруватися, спершу розіб'ємо на блоки довжиною l – так звані l-грами. Далі ці l-грами запишемо у стовпці матриці X.

У методі Хілла рівняння шифрування має вигляд $Y = AX \bmod n$, де A – невироджена квадратна матриця над Z_n порядку l, а рівняння дешифрування записується як $X = A^{-1}Y \bmod n$, де $A^{-1} = A \bmod n$ – обернена матриця до матриці A. Це можливо тільки за умови, що найбільший спільний дільник НСД$(\det A, n) = 1$, де $\det A \neq 0$ – визначник матриці A.

1.15. Основи криптосистеми RSA

Шифрування за допомогою системи RSA здійснюється таким чином:

1. Отримувач повідомлень генерує закритий ключ – числа p q d та відкритий ключ – пару чисел n і e. Для цього він:
   - вибирає два простих великих числа p і q;
   - обчислює добуток $n = pq$;
   - вибирає непарне число e, яке має бути взаємно простим із числом $\varphi(n)$ і $0 < e < \varphi(n)$, де $\varphi(n) = \varphi(p)\varphi(q) = (p-1)(q-1)$ – значення функції Ейлера;
   - визначає число d з умови $de \equiv 1 (\bmod (\varphi(n))$.

Числа n і e повідомляються відправнику повідомлень.

2. Відправник повідомлень шифрує останні за допомогою ***рівняння шифрування*** $y \equiv x^e (\bmod n)$ (якщо потрібно, повідомлення розбивають на послідовності символів, довжиною менше за $\log_2 n$ розрядів). Шифроване повідомлення відправник відсилає отримувачу.

3. Отримувач дешифрує шифрований текст за допомогою закритого ключа d на основі ***рівняння дешифрування*** $x \equiv y^d (\bmod n)$.

Доведемо, що коли за цією схемою зашифрувати повідомлення x і отримати шифроване повідомлення $y \equiv x^e (\bmod n)$, то після дешифрування $x \equiv y^d (\bmod n)$ дістанемо саме вихідне повідомлення x. Дійсно, якщо НСД$(x, p) = p$, то число x ділиться на p і $x \equiv 0 (\bmod p)$, якщо ж НСД$(x, p) = 1$, то за теоремою Ферма $x^{p-1} \equiv 1 (\bmod p)$ або $x^{p-1} - 1 \equiv 0 (\bmod p)$. Перемножимо обидві частини порівнянь: $x(x^{p-1} - 1) \equiv 0 (\bmod p)$, звідки для будь-якого x виконується порівняння $x^p - x \equiv 0 (\bmod p)$ або $x^p \equiv x (\bmod p)$. Оскільки $ed \equiv 1 (\bmod \varphi(n))$, то існує таке ціле число t, що $ed = t\varphi(n) + 1$. Врахувавши порівняння $x^p \equiv x (\bmod p)$, дістаємо:

$$y^d (\bmod p) \equiv (x^e)^d (\bmod p) \equiv x^{ed} (\bmod p) \equiv x^{t\varphi(n)+1} (\bmod p) \equiv$$
$$\equiv x^{t(p-1)(q-1)+1} (\bmod p) \equiv x^{tp(q-1)} x^{-tq+t+1} (\bmod p) \equiv$$
$$\equiv (x^p)^{t(q-1)} x^{-tq+t+1} (\bmod p) \equiv x^{t(q-1)} x^{-tq+t+1} (\bmod p) \equiv x (\bmod p).$$

Аналогічно можна довести, що $y^d \equiv x (\bmod q)$.

p, q – різні прості числа і $n = pq$, а відтак за властивостями лишків та згідно з китайською теоремою про остачу дістанемо $x \equiv y^d (\bmod n)$.

Таким чином, для розшифровки повідомлення, отриманого за допомогою RSA, неодмінно потрібен закритий ключ d. Супротивник може дізнатися його значення в двох випадках: 1) якщо відомий розклад числа $n = pq$ на прості множники; 2) при відомому значенні функції Ейлера $\varphi(n)$ у порівнянні $ed \equiv 1 (\bmod \varphi(n))$. Тоді $\varphi(n) = (p-1)(q-1) = pq - (p+q) + 1$ і $(p-q)^2 = (p+q)^2 - 4pq$, і значення p та q визначаються з системи:

$$\begin{cases} \varphi(n) = n - (p+q) + 1; \\ (p-q)^2 = (p+q)^2 - 4n. \end{cases}$$

1.16. Квадратні порівняння. Критерій Ейлера. Символ Лежандра

Двочленне порівняння

$$x^2 \equiv a (\bmod m),$$

де НСД$(a, m) = 1$, називається ***квадратним порівнянням*** за модулем m. Якщо це порівняння має розв'язки, то число a називається ***квадратичним лишком за модулем*** m, у протилежному випадку – ***квадратичним нелишком за модулем*** m. Якщо a – квадратичний лишок за модулем m, то у цьому разі x називають ***квадратним коренем з числа*** a ***за модулем*** m. Наприклад, $\pm 4 (\bmod 13)$ – квадратні корені з числа 3 за модулем 13, оскільки ці числа задовольняють порівняння $x^2 \equiv 3 (\bmod 13)$, а число 3 є квадратичним лишком за модулем 13.

Теорема про кількість коренів квадратного порівняння. Якщо a – квадратичний лишок за простим модулем p, то порівняння $x^2 \equiv a (\bmod p)$ завжди має два корені.

Існування коренів квадратного порівняння $x^2 \equiv a (\bmod p)$ за простим модулем можна встановити за допомогою критерія Ейлера або використовуючи символ Лежандра.

1. ***Критерій Ейлера***: число a, взаємно просте з числом $p > 2$, буде квадратичним лишком за модулем p тоді і тільки тоді, коли $a^{\frac{p-1}{2}} \equiv 1 (\bmod p)$, і буде квадратичним нелишком за модулем p тоді і тільки тоді, коли $a^{\frac{p-1}{2}} \equiv -1 (\bmod p)$.

Є сенс застосовувати критерій при невеликому модулі p.

2. ***Символ Лежандра*** $L(a;p)$ – арифметична функція, визначена для простих непарних p і будь-яких цілих a за правилом:

$$L(a;p)=\begin{cases}+1, \text{ якщо } a-\text{квадратичний лишок за модулем } p;\\ -1, \text{ якщо } a-\text{квадратичний нелишок за модулем } p;\\ 0, \text{ якщо } a \text{ ділиться на число } p.\end{cases}$$

Значення символу Лежандра обчислюється за формулою $L(a;p)=a^{\frac{p-1}{2}} \pmod p$, яка випливає з критерію Ейлера, але на практиці для обчислень широко використовують його властивості.

Властивості символу Лежандра:

1^0. Якщо $a=b(\bmod p)$, то $L(a;p)=L(b;p)$.

2^0. $L(a^2;p)=1$, зокрема $L(1;p)=1$.

3^0. $L(-1;p)=(-1)^{\frac{p-1}{2}}$; $L(2;p)=(-1)^{\frac{p^2-1}{8}}$.

4^0. $L(ab...s;p)=L(a;p)L(b;p)...L(s;p)$.

5^0. $L(a^n;p)=\big(L(a;p)\big)^n$.

6^0. $L(q;p)=(-1)^{\frac{p-1}{2}\cdot\frac{q-1}{2}}L(p;q)$, де $p\neq q$ – прості непарні числа (***квадратичний закон взаємності***).

7^0. $L(p;q)L(q;p)=(-1)^{\frac{p-1}{2}\cdot\frac{q-1}{2}}$.

Алгоритм обчислення символу Лежандра $L(a;p)$:

1. Якщо $a=1$, то $L(a;p)=1$.

2. Якщо a – парне, то $L(a;p)=(-1)^{\frac{p^2-1}{8}}L\left(\frac{a}{2};p\right)$.

3. Якщо a – непарне, то $L(a;p)=(-1)^{\frac{(a-1)(p-1)}{4}}L(p(\bmod a);a)$.

За допомогою символу Лежандра зручно з'ясовувати існування квадратних коренів з числа a за простим великим модулем.

1.17. Добування квадратних коренів за простим модулем

Способи добування квадратних коренів за простим модулем, тобто розв'язання порівнянь $x^2\equiv a(\bmod p)$, де a – квадратичний лишок за простим непарним числом p, НСД$(a,p)=1$:

1) випробування лишків $1,2,...,p-1$ повної системи за модулем p;

2) якщо модуль $p=4k+3$, де k – ціле, то $x\equiv\pm a^{k+1}(\bmod p)$;

3) якщо модуль $p=8k+5$, де k – ціле, і $a^{2k+1}\equiv 1(\bmod p)$, то $x\equiv\pm a^{k+1}(\bmod p)$;

4) якщо модуль $p=8k+5$, де k – ціле, і $a^{2k+1}\equiv -1(\bmod p)$, то $x\equiv\pm 2^{2k+1}a^{k+1}(\bmod p)$;

5) якщо модуль $p=4k+1$, де k – ціле, то готової формули для розв'язання квадратних порівнянь не існує, проте Шенксом була запропонована апроксимаційна процедура, яка залежить від максимального степеня s двійки у розкладі числа $p-1=2^s t$, де $t-$ і $s\geq 2$.

1.18. Добування квадратних коренів за модулем $n=pq$, де p,q – прості числа

Порівняння $x^2\equiv a(\bmod n)$, $n=pq$, де p і q – прості різні числа, НСД$(a,n)=1$, еквівалентно системі порівнянь

$$\begin{cases}x^2\equiv a(\bmod p),\\ x^2\equiv a(\bmod q).\end{cases}$$

Очевидно, число a є квадратичним лишком за модулем n тоді і тільки тоді, коли воно є квадратичним лишком за кожним із модулів p і q. Отже, аби здобути квадратні корені з числа a за модулем $n=pq$, потрібно:

1) перевірити, чи буде число a квадратичним лишком за простими модулями p і q;

2) у разі стверджувальної відповіді розв'язати кожне порівняння системи окремо;

3) якщо x_1, $p-x_1$ і x_2, $q-x_2$ – відповідно розв'язки першого і другого порівнянь системи, то комбінувати здобуті розв'язки між собою у системи:

$$\begin{cases}x=x_1 \bmod p;\\ x=x_2 \bmod q.\end{cases}\quad\begin{cases}x=p-x_1 \bmod p;\\ x=q-x_2 \bmod q.\end{cases}\quad\begin{cases}x=x_1 \bmod p;\\ x=q-x_2 \bmod q.\end{cases}\quad\begin{cases}x=p-x_1 \bmod p;\\ x=x_2 \bmod q.\end{cases}$$

Розв'язки цих систем – це квадратні корені x з числа a за модулем $n=pq$. У розглядуваному випадку кожен квадратичний лишок a має чотири різних корені.

Розглянемо зручний ***спосіб визначення коренів з числа a за модулем*** $n=pq$, ***який базується на використанні лінійної комбінації для***

НСД $(p,q)=1$. Припустимо, що вже знайдено розв'язок x_1 порівняння $x^2 \equiv a \bmod p$ і розв'язок x_2 порівняння $x^2 \equiv a \bmod q$. За алгоритмом Евкліда знаходимо такі числа u і v, для яких $up+vq=1$. Покажемо, що тоді число $x = upx_2 + vqx_1$ є коренем з числа a за модулем $n = pq$. Взявши до уваги, що $x_2^2 = a + kq$ та $x_1^2 = a + tp$, де $k,t \in Z$, піднесемо x до квадрату:

$$x^2 = u^2p^2x_2^2 + 2uvpqx_1x_2 + v^2q^2x_1^2 = u^2p^2(a+kq) + 2uvnx_1x_2 + \\ + v^2q^2(a+tp) \equiv a(u^2p^2 + v^2q^2) \bmod n.$$

Оскільки $up+vq=1$, то $u^2p^2 + v^2q^2 \equiv 1 \bmod n \Rightarrow x = upx_2 + vqx_1$ – корінь порівняння $x^2 \equiv a \bmod n$. Решту розв'язків отримуємо, підставивши замість x_1 і x_2 у вираз $x = upx_2 + vqx_1$ інші розв'язки порівнянь за простими модулями p і q:

$$x = (upx_2 - vqx_1) \bmod n;$$
$$x = (-upx_2 - vqx_1) \bmod n;$$
$$x = (-upx_2 + vqx_1) \bmod n.$$

1.19. Первісні корені. Дискретні логарифми

Первісний корінь за модулем m – це таке ціле число g, для якого $НСД(g,m)=1$, $g^{\varphi(m)} \equiv 1 (\bmod m)$, але $g^{\gamma} \not\equiv 1 (\bmod m)$, де γ – цілі числа з відрізка $[1;\varphi(m)-1]$, $\varphi(m)$ – функція Ейлера.

Первісні корені існують не для всіх модулів m, а тільки для модулів вигляду $2, 4, p^{\alpha}, 2p^{\alpha}$, де $p \geq 3$ – просте, $\alpha \geq 1$ – ціле.

Критерій для пошуку первісних коренів за простим модулем: якщо $p-1 = p_1^{\alpha_1} p_2^{\alpha_2} \ldots p_k^{\alpha_k}$ – канонічний розклад числа $p-1$ і

$$g^{\frac{p-1}{p_1}} \not\equiv 1 (\bmod p),\ g^{\frac{p-1}{p_2}} \not\equiv 1 (\bmod p), \ldots,\ g^{\frac{p-1}{p_k}} \not\equiv 1 (\bmod p),$$

то g – первісний корінь за простим модулем p.

Алгоритм визначення найменшого первісного кореня за простим модулем p:

1. Знайти всі різні прості дільники числа $p-1$ (позначимо їх $p_1, p_2, \ldots, p_k$).
2. Послідовно перевіряти, чи задовольняють числа $g \in \{1,2,3,\ldots,p-1\}$ порівняння $g^{\frac{p-1}{p_1}} \equiv 1 (\bmod p)$, $g^{\frac{p-1}{p_2}} \equiv 1 (\bmod p), \ldots,$ $g^{\frac{p-1}{p_k}} \equiv 1 (\bmod p)$.

Перше з чисел, яке не задовольняє жодне з порівнянь, буде шуканим первісним коренем.

Степені первісного кореня $g^0 = 1, g, g^2, \ldots, g^{\varphi(m)-1}$ не порівняні між собою за модулем m і утворюють зведену систему лишків за модулем m. Таким чином, для кожного числа a, взаємно простого з числом m, знайдеться показник γ $(0 \leq \gamma \leq \varphi(m)-1)$, для якого виконується порівняння $a \equiv g^{\gamma} (\bmod m)$. За аналогією з поняттям логарифмів у звичайній алгебрі показник γ називають дискретним логарифмом. Наведемо строге означення.

Дискретним логарифмом (індексом) числа a ***за модулем*** m ***і основою*** g називається показник γ у порівнянні

$$g^{\gamma} \equiv a (\bmod m),$$

де $НСД(a,m)=1$, g – фіксований первісний корінь за модулем m.

Скорочено це позначають $\gamma = ind_g a$, а якщо основа g фіксована, то $\gamma = ind\, a$. Наприклад, оскільки $5^4 \equiv 16 (\bmod 21)$, то $ind_5 16 = 4$.

Згідно з означенням дискретного логарифма $g^{ind_g a} \equiv a (\bmod m)$.

Обчислення дискретного логарифма, очевидно, є оберненою задачею до задачі піднесення до степеня за модулем.

Якщо за основу вибрати не первісний корінь за модулем m, то дискретні логарифми будуть існувати не для всіх чисел, взаємно простих із модулем. Наступна теорема встановлює, що будь-яке число, взаємно просте з модулем, має безліч дискретних логарифмів.

Теорема: якщо g – будь-який первісний корінь за модулем m, то для кожного числа a з умовою $НСД(a,m)=1$ існує єдиний дискретний логарифм γ за основою g, для якого $g^{\gamma} \equiv a (\bmod m))$, причому $0 \leq \gamma \leq \varphi(m)-1$. Будь-який інший дискретний логарифм γ' числа a задовольняє порівняння $\gamma' \equiv \gamma (\bmod \varphi(m))$, тобто дискретні логарифми числа a утворюють клас лишків за модулем $\varphi(m)$.

Теорема про логарифмування та потенціювання порівнянь. Якщо g – первісний корінь за модулем m, $НСД(a,m)=1$, то порівняння

$$b \equiv a (\bmod m) \qquad (1.3)$$

має місце тоді і тільки тоді, коли

$$ind_g b \equiv ind_g a (\bmod \varphi(m)). \qquad (1.4)$$

Перехід від порівняння (1.3) до порівняння (1.4) називають ***логарифмуванням (індексуванням) порівняння*** (1.3), а перехід від (1.4) до (1.3) – ***потенціюванням***.

1.20. Властивості дискретних логарифмів

Операції з дискретними логарифмами виконуються за правилами, що схожі на правила логарифмування. Нехай g – первісний корінь за модулем m, НСД$(a,m)=1$, НСД$(b,m)=1$. Тоді

$1^0\ ind_g(ab)\equiv ind_g a+ind_g b\ (\mathrm{mod}\varphi(m))$;

$2^0\ ind_g a^n\equiv n\cdot ind_g a\ (\mathrm{mod}\varphi(m))$;

$3^0\ ind_g\left(ab^{-1}\right)\equiv ind_g a-ind_g b\ (\mathrm{mod}\varphi(m))$, де ab^{-1} – розв'язок порівняння $ax\equiv b(\mathrm{mod}\varphi(m))$;

$4^0\ ind_g 1\equiv 0\ (\mathrm{mod}\varphi(m))$;

$5^0\ ind_g g\equiv 1\ (\mathrm{mod}\varphi(m))$;

$6^0\ ind_g(-1)\equiv ind_g(m-1)\equiv\frac{1}{2}\varphi(m)\ (\mathrm{mod}\varphi(m))$.

1.21. Дискретні логарифми за простим модулем

Первісні корені існують за будь-яким простим модулем p, тому, взявши за основу будь-який із них, дістанемо систему дискретних логарифмів, у якій кожне число, що не ділиться на p, матиме свої дискретні логарифми. Згідно з наведеною теоремою вони являтимуть собою невід'ємні числа деякого класу лишків за модулем $p-1$.

Властивості дискретних логарифмів за простим модулем:

1^0 якщо $a\equiv b(\mathrm{mod}\,p)$, то $ind_g a\equiv ind_g b\ (\mathrm{mod}\ (p-1))$;

$2^0\ ind_g(ab)\equiv ind_g a+ind_g b\ (\mathrm{mod}\ (p-1))$;

$3^0\ ind_g a^n\equiv n\cdot ind_g a\ (\mathrm{mod}\ (p-1))$;

$4^0\ ind_g\left(ab^{-1}\right)\equiv ind_g a-ind_g b\ (\mathrm{mod}\ (p-1))$;

$5^0\ ind_g 1\equiv 0\ (\mathrm{mod}\ (p-1))$;

$6^0\ ind_g g\equiv 1\ (\mathrm{mod}\ (p-1))$;

$7^0\ ind_g(-1)\equiv ind_g(p-1)\equiv\frac{1}{2}(p-1)\ (\mathrm{mod}\ (p-1))$.

Таблиці дискретних логарифмів чисел від 1 до $p-1$ складені для простих невеликих модулів p.

1.22. Розв'язання двочленних порівнянь за допомогою дискретних логарифмів

Розглянемо двочленні порівняння степеня n

$$x^n\equiv a(\mathrm{mod}\,m),\qquad(1.5)$$

де $m=p^\alpha$ або $m=2p^\alpha$, тут $p>2$ – просте непарне число, $\alpha\geq 1$, НСД$(a,m)=1$. Позначимо НСД$(n,\varphi(m))=d$.

За таких умов порівняння має розв'язки (і число a є ***лишком степеня*** n ***за модулем*** m) тоді і тільки тоді, коли дискретний логарифм $ind\,a$ кратний числу d, причому кількість розв'язків дорівнює d. Дійсно, за модулем $m=p^\alpha$ або $m=2p^\alpha$ існують первісні корені, а відтак злогарифмуємо порівняння (1.5)

$$n\cdot ind\,x\equiv ind\,a(\mathrm{mod}\varphi(m)).\qquad(1.6)$$

Порівняння (1.6) можна розв'язати відносно $ind\,x$ тоді і тільки тоді, коли $ind\,a$ кратний d. У випадку розв'язності порівняння, ми визначимо d непорівняних за модулем $\varphi(m)$ значень $ind\,x$, яким буде відповідати d непорівняних за модулем m значень x.

Дискретні логарифми можна застосовувати й для розв'язання ***двочленних показникових порівнянь*** вигляду $a^x\equiv b(\mathrm{mod}\,m)$. Якщо за модулем m існують первісні корені, то, злогарифмувавши показникове порівняння, дістанемо

$$x\cdot ind\,a\equiv ind\,b(\mathrm{mod}\varphi(m)),$$

звідки вже можна визначити x за стандартними процедурами.

2. АУДИТОРНІ ПРАКТИЧНІ ЗАНЯТТЯ

2.1. Подільність чисел. Алгоритм Евкліда для пошуку НСД чисел. Прості числа. Решето Ератосфена. Розподіл простих чисел

Тестові завдання для перевірки теоретичних знань

1. Якщо n – парне, то яке з нижченаведених чисел буде непарним?

а) $3n+2$; **б)** $8n+5$; **в)** $7n$; **г)** n^2; **д)** n^3.

2. Якщо число n – парне, то яке з наступних тверджень обов'язково виконується для числа $a=\frac{3n}{2}$?

а) a – парне; **б)** a – непарне; **в)** a ділиться на 3;
г) a ділиться на 6; **д)** усі попередні твердження неправильні.

3. Яке з нижченаведених чисел не може бути цілим за умови, що k – парне, а m і n – непарні?

а) k/m; **б)** m/n; **в)** km/n; **г)** mn/k; **д)** kn/m.

4. Якщо $\frac{2\cdot3\cdot5\cdot7\cdot11\cdot13}{77\cdot n}$ – ціле число, то число n може дорівнювати ....

а) 22; **б)** 26; **в)** 35; **г)** 54; **д)** 60.

5. Натуральне число n при діленні на 6 дає остачу 3. Яке з нижченаведених чисел може не ділитися на 6?

а) $n+3$; **б)** $n-3$; **в)** $3n$; **г)** $2n$; **д)** $4n$.

6. Якщо числа m і n при діленні на 8 дають остачі 1 і 3 відповідно, то якому з наведених чисел не може дорівнювати сума $m+n$?

а) 78; **б)** 68; **в)** 44; **г)** 36; **д)** 92.

7. Які з чисел $A=mnkp$, $B=m+2n+3k+4p$, $C=m+3n+5k+7p$ обов'язково будуть парними, якщо m,n,k,p – натуральні числа і їх сума парна?

а) всі; **б)** A та B; **в)** B та C; **г)** A та C; **д)** тільки одне з них.

8. Які з чисел $A=mnkp$, $B=m+2n+3k+4p$, $C=m+3n+5k+7p$ обов'язково будуть парними, якщо m,n,k,p – натуральні числа і їх сума непарна?

а) всі; **б)** A та B; **в)** B та C; **г)** A та C; **д)** тільки одне з них.

9. Яке з нижченаведених чисел не може бути найбільшим спільним дільником двох натуральних чисел m і n?

а) 1; **б)** $m+n$; **в)** n; **г)** m; **д)** $m-n$.

10. Нехай НСД$(a,b)=6$. Якому з поданих далі чисел може дорівнювати НСД$(8a,8b)$?

а) тільки 48; **б)** 48 або 24; **в)** 48, 24, 12; **г)** 48, 24, 12, 6; **д)** 48 або 6.

11. При діленні числа n на 17 частка дорівнює x та остача 5, а якщо n ділити на 23, то частка буде дорівнювати y та остача 14. Якою рівністю зв'язані між собою x і y?

а) $23x+17y=19$; **б)** $17x-23y=9$; **в)** $17x+23y=19$;
г) $14x+5y=6$; **д)** $5x-14y=-6$.

12. Про деяке натуральне число n є шість тверджень: «Число n ділиться на 4», «Число n ділиться на 6», «Число n ділиться на 8», «Число n ділиться на 9», «Число n ділиться на 12», «Число n ділиться на 24». Рівно два з цих тверджень хибні. Які?

а) про подільність на 24 і на 12; **б)** про подільність на 24 і на 9;
в) про подільність на 12 і на 9; **г)** про подільність на 9 і на 8;
д) про подільність на 24 і на 8.

13. Якщо m і n – прості числа, то яке з нижченаведених чисел не може бути їх сумою?

а) 5; **б)** 9; **в)** 13; **г)** 16; **д)** 23.

14. Яке з наведених чисел належить до чисел Ферма і є простим?

а) $2^{2^7}+1$; **б)** $2^{2^3}+1$; **в)** $2^{2^4}-1$; **г)** 2^{2^3}; **д)** $2^{23}-1$.

15. Які з наведених чисел Марсенна будуть складеними?

а) 2^8-1; **б)** 2^7-1; **в)** $2^{15}-1$; **г)** 2^5-1.

16. Які твердження *правильні*?

а) числа-близнюки – це всі натуральні числа m і n, для яких $m-n=2$;
б) простих чисел нескінченно багато;
в) простих чисел Марсенна нескінченно багато;
г) існують многочлени, числові значення яких при будь-якому цілому аргументі є прості числа.

17. Чотиризначне число буде простим, якщо воно не має дільників, окрім 1, менших, ніж ...

а) 25; **б)** 50; **в)** 75; **г)** 99; **д)** 100.

Завдання для аудиторної роботи

Приклад 1. Визначити неповну частку q та остачу r від ділення числа a на число b, якщо: а) $a=89$, $b=24$; б) $a=-89$, $b=24$; в) $a=89$, $b=-24$; г) $a=-89$, $b=-24$.

Розв'язання: а) $89=24\cdot 3+17 \Rightarrow q=3;\ r=17;$

б) $-89=24\cdot(-4)+7 \Rightarrow q=-4;\ r=7;$

в) $89=(-24)\cdot(-3)+17 \Rightarrow q=-3;\ r=17;$

г) $-89=(-24)\cdot 4+17 \Rightarrow q=4;\ r=7.$

Приклад 2. Довести, що коли a і b діляться на ціле m, то й сума $a+b$ ділиться на m.

Доведення. За визначенням подільності існують такі числа $k,l\in Z$, що $a=km$, $b=lm$. Тоді $a+b=km+lm=(k+l)m$, де $k,l\in Z$, тобто сума $a+b$ ділиться на m.

Приклад 3. Довести, що коли число a ділиться на два взаємно простих числа m і n, то це число ділиться на їх добуток mn.

Доведення. За визначенням подільності існують такі числа $k,l\in Z$, що $a=km$, $a=ln$. Звідси $km=ln$ або $l=\frac{km}{n}$. Оскільки дріб $\frac{m}{n}$ нескоротний через взаємну простоту чисел m і n, то число $l\in Z$ тільки за умови, що $k\vdots n$. Тоді $k=nt$, де $t\in Z$. Отже, $a=km=ntm=(mn)t$, $t\in Z$, тобто число a ділиться на добуток mn.

Приклад 4. На скільки відсотків треба збільшити число n, яке при діленні на 8 дає остачу 2, щоб воно стало ділитися на 8 без остачі?

Розв'язання. Згідно з теоремою про подільність з остачею $n=8q+2$. Якщо число збільшити на 6, то воно стане ділиться на 8 вже без остачі: $m=8q+2+6=8(q+1)$. У відсотках величина збільшення числа на 6 складає $\frac{600}{n}\%$.

Приклад 5. Яке найбільше ціле число при діленні з остачею на 19 дає частку 20?

Розв'язання. Згідно з теоремою про подільність з остачею маємо $n=20\cdot 19+r$, де $1\le r<19$. Очевидно, число n буде найбільшим за умови, що $r=18$, а отже, $n=20\cdot 19+18=398$.

Приклад 6. Розв'язати систему рівнянь $\begin{cases}\text{НСК}(a,b)=540,\\ ab=16200.\end{cases}$

Розв'язання. $\text{НСД}(a,b)=\frac{ab}{\text{НСК}(a,b)}=\frac{16200}{540}=30$, тоді $a=30m$, $b=30n$, де m,n – взаємно прості числа. $\text{НСК}(a,b)=30mn=540 \Rightarrow mn=18$. Унаслідок взаємної простоти чисел $m=1$, $n=18$ або $m=2$, $n=9$ або навпаки. Відповідно при цих m,n визначаємо a та b: (30;540), (60;270), (540;30), (270;60).

Приклад 7. Довести, що для будь-яких натуральних чисел a і b виконується нерівність $a+b\le\text{НСД}(a,b)+\text{НСК}(a,b)$.

Доведення. Позначимо $d=\text{НСД}(a,b)$, $m=\text{НСК}(a,b)$. Тоді $ab=dm$ і нерівність, яку доводимо, можна переписати у вигляді $d+\frac{ab}{d}\ge a+b$ або $d^2-(a+b)d+ab\ge 0$, звідки, врахувавши теорему Вієта, дістаємо $(d-a)(d-b)\ge 0$. Оскільки завжди $d\le a$ і $d\le b$, то отримана нерівність завжди виконується.

Приклад 8. При яких натуральних n число $p=n^2-6n+8$ є простим?

Розв'язання: $p=n^2-6n+8=(n-2)(n-4)$. Аби добуток давав просте число, один з множників $n-2$ або $n-4$ неодмінно повинен дорівнювати 1. Якщо $n-2=1$, то $n=3$ і тоді $n-4=3-4=-1\notin N$. Якщо $n-4=1$, то $n=5$, а другий множник просте число 3. Отже, число p – просте при $n=5$.

Приклад 9. Знайти границю, яку не може перевищити найбільший простий дільник числа 5050656.

Розв'язання. Найбільший простий дільник будь-якого складеного числа n не перевищує $\sqrt{n}$, тобто для заданого числа це $\sqrt{5050656}\approx 2247$.

Приклад 10. За алгоритмом Евкліда визначити найбільший спільний дільник чисел: а) 1234 і 54; б) 353 і 124.

Розв'язання:

а) $1234\,|\,54$ $\quad 108\quad 22$ $\quad 154$ $\quad 108$ $\quad 46$; $\quad 54\,|\,46$ $\quad 46\quad 1$ $\quad 8$; $\quad 46\,|\,8$ $\quad 40\quad 5$ $\quad 6$; $\quad 8\,|\,6$ $\quad 6\quad 1$ $\quad 2$; $\quad 6\,|\,2$ $\quad 6\quad 3$ $\quad 0$ $\Rightarrow$ НСД(1234, 54)=2.

б) $\begin{array}{r|l} 353 & 124 \\ \hline 248 & 2 \\ \hline 105 & \end{array}$ $\begin{array}{r|l} 124 & 105 \\ \hline 105 & 1 \\ \hline 19 & \end{array}$ $\begin{array}{r|l} 105 & 19 \\ \hline 95 & 5 \\ \hline 10 & \end{array}$ $\begin{array}{r|l} 19 & 10 \\ \hline 10 & 1 \\ \hline 9 & \end{array}$ $\begin{array}{r|l} 10 & 9 \\ \hline 9 & 1 \\ \hline 1 & \end{array}$ $\begin{array}{r|l} 9 & 1 \\ \hline 9 & 9 \\ \hline 0 & \end{array}$ $\Rightarrow$

$\Rightarrow$ НСД(353, 124)=1, тому дані числа взаємно прості.

Приклад 11. Довести, що НСД$(3n+1, 2n+1)=1$.

Розв'язання: $\begin{array}{r|l} 3n+1 & 2n+1 \\ \hline 2n+1 & 1 \\ \hline n & \end{array}$ $\begin{array}{r|l} 2n+1 & n \\ \hline 2n & 2 \\ \hline 1 & \end{array}$ $\begin{array}{r|l} n & 1 \\ \hline n & n \\ \hline 0 & \end{array}$ $\Rightarrow$

$\Rightarrow$ НСД $(3n+1, 2n+1)=1$.

Приклад 12. Для взаємно простих чисел 211 та 79 знайти такі цілі числа α і β, щоб виконувалась умова $211\alpha+79\beta=1$.

Розв'язання. За алгоритмом Евкліда:

$211=79\cdot 2+53$; $79=53\cdot 1+26$; $53=26\cdot 2+1 \Rightarrow$

$\Rightarrow 1=53-26\cdot 2=53-2\cdot(79-53)=53\cdot 3-2\cdot 79=3\cdot(211-2\cdot 79)-2\cdot 79=$

$=3\cdot 211-8\cdot 79 \Rightarrow 211\cdot 3+79\cdot(-8)=1 \Rightarrow \alpha=3;\ \beta=-8$.

Приклад 13. Для чисел 7123 та 5984 знайти такі цілі числа α і β, щоб виконувалась умова $7123\alpha+5984\beta=$НСД(7123, 5984).

Розв'язання. За алгоритмом Евкліда:

$7123=5984\cdot 1+1139$; $5984=1139\cdot 5+289$; $1139=289\cdot 3+272$; $289=272\cdot 1+17$;

$272=17\cdot 16 \Rightarrow$ НСД(7123, 5984)$=17$.

$17=289-272=289-(1139-289\cdot 3)=289\cdot 4-1139=(5984-1139\cdot 5)\cdot 4-1139=$

$=5984\cdot 4-1139\cdot 21=5984\cdot 4-(7123-5984)\cdot 21=7123\cdot(-21)+5984\cdot 25 \Rightarrow$

$\Rightarrow \alpha=-21;\ \beta=25$.

Приклад 14. Довести, що простих чисел нескінченно багато.

Доведення. Розглянемо число $N=p^{\#}+1=2\cdot 3\cdot 5\cdot\ldots\cdot p+1$, де $p^{\#}=2\cdot 3\cdot 5\cdot\ldots\cdot p$ – добуток усіх простих чисел, не більших за просте число p. Число N не ділиться ані на 2, ані на 3, … , ані на p, оскільки перший доданок ділиться на всі ці числа, а одиниця – не ділиться. Отже, або N ділиться на прості числа, більші за p, або N є новим простим числом, тобто послідовність простих чисел нескінченна.

Приклад 15. З'ясувати, які з чисел 509, 1841, 1079 прості, а які складені.

Розв'язання. Найбільший простий дільник числа n не перевищує $\sqrt{n}$. Тоді:

а) $\sqrt{509}\approx 23$, жодне з простих чисел 2,3,5,7,11,13,17,19,23 не є дільником числа 509, тобто число 509 просте;

б) $\sqrt{1841}\approx 43$, потрібно перевірити подільність числа 1841 на прості числа 2,3,5,7,11,13,17,19,23,29,31,37,41,43. Виявляється, що $1841=7\cdot 263$, тобто число складене;

в) $\sqrt{1079}\approx 33$, потрібно перевірити подільність числа 1079 на прості числа 2,3,5,7,11,13,17,19,23,29,31. Оскільки $1079=13\cdot 83$, то це також складене число.

Приклад 16. Які числа з відрізку [731;800] будуть простими?

Розв'язання. Застосуємо решето Ератосфена, для чого виписуємо всі цілі числа з даного відрізка. Границя, яку не може перевищити найбільший простий дільник будь-якого числа з відрізка [731;800], – це $\sqrt{800}\approx 28$. Отже, викреслюємо всі числа з відрізка, що кратні 2,3,5,7,11,13, 17, 19, 23. Числа, що кратні 2, – це парні, числа, що кратні 3, – це кожне третє число, починаючи з першого числа 732, що ділиться на 3. На 5 діляться числа з п'ятого та десятого стовпців. Перше число на відрізку, що ділиться на 7, – це 735, тому викреслюємо його і кожне сьоме число за ним. Аналогічно перше число на відрізку, що ділиться на 11, – це 737, отже, викреслюємо 737 і кожне одинадцяте число за ним і т.д., поки не проаналізуємо числа, кратні 23. Залишені не викреслені числа (у прямокутній рамці) будуть простими. Це 733, 739, 743, 751, 757, 761, 769, 773, 787, 797.

~~731~~[17]	~~732~~[2;3]	[733]	~~734~~	~~735~~[5;7]	~~736~~[23]	~~737~~[11]	~~738~~	[739]	~~740~~
~~741~~[13;19]	~~742~~	[743]	~~744~~	~~745~~	~~746~~	~~747~~	~~748~~	~~749~~	~~750~~
[751]	~~752~~	~~753~~	~~754~~	~~755~~	~~756~~	[757]	~~758~~	~~759~~	~~760~~
[761]	~~762~~	~~763~~	~~764~~	~~765~~	~~766~~	~~767~~	~~768~~	[769]	~~770~~
~~771~~	~~772~~	[773]	~~774~~	~~775~~	~~776~~	~~777~~	~~778~~	~~779~~	~~780~~
~~781~~	~~782~~	~~783~~	~~784~~	~~785~~	~~786~~	[787]	~~788~~	~~789~~	~~790~~
~~791~~	~~792~~	~~793~~	~~794~~	~~795~~	~~796~~	[797]	~~798~~	~~799~~	~~800~~

Приклад 17. Довести, що всі числа Марсенна $M_n=2^n-1$ є складеними за умови, що $n-$ непарне і складене.

Доведення. Нехай $n=ab$, $a,b\geq 3$. Застосуємо формулу:

$a^n-b^n=(a-b)(a^{n-1}+a^{n-2}b+\ldots+ab^{n-2}+b^{n-1})$.

Тоді $2^{ab}-1=(2^a)^b-1=(2^a-1)(2^{a(b-1)}+2^{a(b-2)}+\ldots+2^a+1)$, тобто числа 2^n-1 при складеному непарному n будуть складеними.

Приклад 18. Скільки цифр у числі Марсенна $M_{11213}=2^{11213}-1$?

Розв'язання. Загальна формула чисел Марсенна $M_n=2^n-1$, отже, кількість цифр у чисел 2^n і M_n+1 збігається. $\lg 2^n=n\lg 2=n\cdot 0{,}30103$. При $n=11213$ дістаємо $\lg 2^{11213}=11213\cdot\lg 2=3375$. Отже, число $2^{11213}-1$ містить 3376 цифр.

Приклад 19. Нехай $n>m$ – натуральні числа, а r – остача від ділення n на m. Показати, що остача від ділення чисел Марсенна $M_n=2^n-1$ на $M_m=2^m-1$ дорівнює числу Марсенна з множини $M_r=2^r-1$.

$$\begin{array}{l|l} 2^n-1 & 2^m-1 \\ \hline 2^n-2^{n-m} & 2^{n-m}+2^{n-2m}+2^{n-3m}+\ldots+2^{n-qm} \\ \hline 2^{n-m}-1 & \\ 2^{n-m}-2^{n-2m} & \\ \hline 2^{n-2m}-1 & \\ 2^{n-2m}-2^{n-3m} & \\ \hline 2^{n-3m}-1 & \\ \ldots\ldots\ldots\ldots & \\ \hline 2^{n-qm}-1=2^r-1. & \end{array}$$

Розв'язання. Нехай $n=qm+r$, де q – неповна частка. Розділивши M_n на M_m, визначаємо частку $M_r=2^r-1$.

Приклад 20. Довести, що число, обчислене за прайморіальною формулою $n=p^{\#}+1$ не має дільників, менших або таких, що дорівнюють p.

Доведення. Припустимо супротивне, тобто що $q\le p$ – простий дільник числа $p^{\#}+1$. Оскільки $p^{\#}$ – добуток усіх простих чисел, не більших за p, то $p^{\#}$ має ділитися на q. Звідси q ділить різницю $(p^{\#}+1)-p^{\#}=1$, тобто $q=1$, що суперечить його простоті. Дістаємо: число $p^{\#}+1$ не може мати дільників, менших або таких, що дорівнюють p.

Приклад 21. Чи існують такі натуральні числа m, n, p при яких $2^m\cdot 3^4\cdot 26^n=39^p$?

Розв'язання: $2^m\cdot 3^4\cdot 2^n\cdot 13^n=3^p\cdot 13^p \Rightarrow 2^{m+n}\cdot 3^4\cdot 13^n=3^p\cdot 13^p$. Унаслідок єдиності розкладу чисел на прості множники маємо:

$$\begin{cases} m+n=0, \\ p=4, \\ n=p \end{cases} \Rightarrow \begin{cases} m=-4, \\ p=4, \\ n=4. \end{cases}$$

$m=-4\notin N$, отже, натуральних чисел, що задовольняють рівність, не існує.

Приклад 22. Застосувавши канонічний розклад чисел на прості множники, визначити НСД(7560, 1008) і НСК(7560, 1008).

Розв'язання:

7560 | 2	1008 | 2
3780 | 2	504 | 2
1890 | 2	252 | 2
945 | 3	126 | 2
315 | 3	63 | 3
105 | 3	21 | 3
35 | 5	7 | 7
7 | 7	1 | 1
1 | 1	

$7560=2^3\cdot 3^3\cdot 5\cdot 7$;

$1008=2^4\cdot 3^3\cdot 5^0\cdot 7$;

НСД(7560, 1008)$=2^3\cdot 3^2\cdot 7=504$;

НСК(7560, 1008)$=2^4\cdot 3^3\cdot 5\cdot 7=15120$.

Приклад 23. Знайти кількість та суму всіх дільників числа 1008.

Розв'язання. $1008=2^4\cdot 3^3\cdot 7$. Кількість усіх дільників числа $a=p_1^{k_1}p_2^{k_2}\cdot\ldots\cdot p_n^{k_n}$, розкладеного на прості множники, визначиться як $\tau(a)=(k_1+1)(k_2+1)\ldots(k_n+1)=(4+1)(3+1)(1+1)=40$, а сума $S(a)$ всіх цих дільників буде

$$S(a)=\frac{p_1^{k_1+1}-1}{p_1-1}\cdot\frac{p_2^{k_2+1}-1}{p_2-1}\cdot\ldots\cdot\frac{p_n^{k_n+1}-1}{p_n-1}=\frac{2^5-1}{2-1}\cdot\frac{3^4-1}{3-1}\cdot\frac{7^2-1}{7-1}=31\cdot 40\cdot 8=9\,920.$$

Приклад 24. Обчислити значення функції $\pi(x)$ при $x=38$ за допомогою решета Ератосфена та наближеної формули $\pi(x)\approx\frac{x}{\ln x}$. Знайти відносну похибку, допущену при використанні наближеної формули.

Розв'язання. За допомогою решета Ератосфена визначаємо всі прості числа, менші за 38: 2,3,5,7,11,13,17,19,23,29,31,37. Таких чисел 12, тобто $\pi(38)=12$. За наближеною формулою $\pi(38)\approx\frac{38}{\ln 38}\approx 10$. Відносна похибка $\Delta=\frac{12-10}{12}\cdot 100\%=16{,}7\%$.

Завдання для домашньої роботи

1. Визначити неповну частку q та остачу r від ділення числа a на число b, якщо: а) $a=83$, $b=13$; б) $a=-83$, $b=13$; в) $a=83$, $b=-13$; г) $a=-83$, $b=-13$.

2. Натуральне число N при діленні на 9 дає остачу 5. Це число збільшили у 12 разів. На скільки відсотків при цьому зміниться остача?

3. Довести, що коли цілі a і b діляться на ціле число m, то й різниця $a-b$ ділиться на m.

4. Якщо сума декількох доданків ділиться на число m і відомо, що всі доданки, крім одного, діляться на m, то і цей доданок ділиться на m. Довести це.

5. Довести, що коли число pA ділиться на q, де p і q – взаємно прості, то й число A ділиться на q.

6. Яке найменше ціле число при діленні з остачею на 19 дає частку 20?

7. Довести, що коли $a=bq+r$, то НСД$(a,b)=$ НСД(b,r).

(*Доведення*: позначимо $d_1=$НСД(a,b), $d_2=$НСД(b,r). Тоді $a\vdots d_1$ і $b\vdots d_1$, тобто існують такі натуральні числа m і n, що $a=d_1m$, $b=d_1n$. Звідси $d_1m=d_1nq+r \Rightarrow r=d_1m-d_1nq=d_1(m-nq)$, тобто $r\vdots d_1 \Rightarrow d_1\le d_2$. Аналогічно можна довести, що $d_2\le d_1$. Рівність $d_1=d_2$ одразу випливає з останніх двох нерівностей).

8. Довести, що НСД$(a,b,c)=$НСД(НСД(a,b), c).

(*Доведення*: позначимо $d_1=$НСД(a,b), $d_2=$НСД(d_1,c). Очевидно, $a\vdots d_2$, $b\vdots d_2$, тобто d_2 – спільний дільник чисел a,b і c. Нехай d' – якийсь інший спільний дільник цих чисел. Тоді $d_1\vdots d'$, а звідси і $d_2\vdots d'$, тобто d_2-НСД(a,b,c).

9. Розв'язати системи рівнянь: а) $\begin{cases} НСК(m,n)=180, \\ НСД(m,n)=12; \end{cases}$ б) $\begin{cases} m+n=20, \\ НСД(m,n)=5. \end{cases}$

(*Відповідь*: а) (12;180),(36;60),(180;12),(60;36); б) (15;5),(5;15)).

10. Знайти НСД$((n+1)!+1,\ n!+1)$, де $n\in N$.

(*Розв'язання*: використовуємо співвідношення

$$(n+1)!-n!\cdot n=n!\cdot(n+1)-n!\cdot n=n!\cdot(n+1-n)=n!\,.$$

$$\begin{array}{r|l} (n+1)!+1 & n!+1 \\ \hline n!\cdot n+n & n \\ \hline n!-n+1 & \end{array} \qquad \begin{array}{r|l} n!+1 & n!-n+1 \\ \hline n!-n+1 & 1 \\ \hline n & \end{array} \qquad \begin{array}{r|l} n!-n+1 & n \\ \hline n!-n & (n-1)!-1 \\ \hline 1 & \end{array}$$

$n\vdots 1=n \Rightarrow$ НСД$((n+1)!+1,\ n!+1)=1$).

11. Знайти НСД$(30n+2,\ 12n+1)$, $n\in N$.

12. Довести, що коли n ділиться на m, то число Марсенна M_n ділиться на число Марсенна M_m.

13. Довести, що число, яке більше 4 і знаходиться між числами-близнюками, обов'язково ділиться на 6.

14. Для взаємно простих чисел 137 та 113 знайти такі цілі числа α і β, щоб виконувалась умова $137\alpha+113\beta=1$.

(*Відповідь*: $\alpha=33,\beta=-40$).

15. Для чисел 1173 та 323 знайти такі цілі числа α і β, щоб виконувалась умова $1173\alpha+323\beta=$НСД$(1173,\ 323)$.

(*Відповідь*: $\alpha=8,\ \beta=-29$).

16. Визначити кількість цифр числа Марсенна $M_{127}=2^{127}-1$.

(*Відповідь*: 39 цифр).

17. Розкласти на множники $7^{\#}-1$, $13^{\#}+1$.

18. Чи існують 2009 послідовних натуральних чисел, серед яких немає жодного простого?

(*Розв'язання.* Число $n!$ ділиться на кожне з чисел $2,3,\ldots,n$. Тому при натуральних k, для яких $2\le k\le 2009$, число $2009!+k$ буде ділитись на k. Отже, при всіх $k=2,3,\ldots,2009$ число $2009!+k$ ділитися на k, тобто всі ці 2009 чисел є складеними).

19. Обчислити значення функції $\pi(x)$ при $x=50$ та $x=100$ за допомогою решета Ератосфена і наближеної формули $\pi(x)\approx\dfrac{x}{\ln x}$. Знайти відносну похибку, допущену при використанні наближеної формули.

(*Відповідь*: $\pi(50)=15$, $\pi(100)=25$, $\pi(50)\approx\dfrac{50}{\ln 50}\approx 13$, $\pi(100)\approx\dfrac{100}{\ln 100}\approx 22$, $\Delta(50)=13{,}3\%$, $\Delta(100)=12\%$).

20. Відомо, що будь-яке непарне просте число можна зобразити як $4n+1$ або як $4n+3$, $n\in N$. Нехай $\pi_1(x)$ і $\pi_2(x)$ – кількості додатних простих чисел вигляду $4n+1$ і $4n+3$ відповідно, що не перевищують додатного дійсного числа x. Обчислити відношення $\dfrac{\pi_1(1000)}{\pi_2(1000)}$.

2.2. Порівняння. Їх властивості. Класи лишків за модулем. Кільце Z_m лишків за модулем

Тестові завдання для перевірки теоретичних знань

1. Яке з нижченаведених тверджень *неправильне*, якщо $x \equiv y(\mathrm{mod}\, z)$?

а) $x - y = zn$, де $n \in N$; **б)** $y \equiv x(\mathrm{mod}\, z)$; **в)** $y - x \equiv 0(\mathrm{mod}\, z)$;
г) $x = y - zn$, де $n \in N$; **д)** $z \equiv y(\mathrm{mod}\, x)$;
е) числа x та y дають однакову остачу при діленні на 34.

2. Записати порівняння, які випливають з того, що вираз $y+8$ кратний 17.

а) $y+8 \equiv 0(\mathrm{mod}17)$; **б)** $y+17 \equiv 0(\mathrm{mod}8)$; **в)** $y \equiv -8(\mathrm{mod}17)$;
г) $y \equiv -17(\mathrm{mod}8)$; **д)** $y \equiv 9(\mathrm{mod}17)$; **е)** $y \equiv -1(\mathrm{mod}8)$.

3. Визначити кількість правильних порівнянь серед записаних нижче, які випливатимуть з того факту, що число a при діленні на 12 дає остачу 7.
$a \equiv 7(\mathrm{mod}12)$, $a \equiv 1(\mathrm{mod}2)$, $a \equiv 1(\mathrm{mod}3)$, $a \equiv 1(\mathrm{mod}4)$, $a \equiv 1(\mathrm{mod}6)$
а) 0; **б)** 1; **в)** 2; **г)** 3; **д)** 4; **е)** 5.

4. При діленні числа x на число y утворюється частка t та остача z. Як записати це за допомогою порівняння?

а) $x \equiv y(\mathrm{mod}\, z)$; **б)** $y \equiv z(\mathrm{mod}\, x)$; **в)** $z \equiv y(\mathrm{mod}\, t)$; **г)** $x \equiv z(\mathrm{mod}\, y)$;
д) $x \equiv y(\mathrm{mod}\, t)$; **е)** $y \equiv t(\mathrm{mod}\, z)$; **ж)** $x \equiv z(\mathrm{mod}\, t)$; **и)** $x \equiv t(\mathrm{mod}\, y)$.

5. Яке порівняння *не* випливає з порівняння $a \equiv b(\mathrm{mod}\, n)$?

а) $b \equiv a(\mathrm{mod}\, n)$; **б)** $a \equiv b(\mathrm{mod}\, m)$, де $m \vdots n$; **в)** $a^2 \equiv b^2(\mathrm{mod}\, n)$;
г) $a^2 \equiv b^2(\mathrm{mod}\, n^2)$; **д)** $a - b \equiv 0(\mathrm{mod}\, n)$; **е)** $ac \equiv dc(\mathrm{mod}\, n)$.

6. Які з чисел $75, 73, 59, 52, -13$ порівняні з числом 27 за модулями 8 і 14?

а) за модулем 8 числа 59, 73, за модулем 14 числа 75 і -13;
б) за модулем 8 числа 75, -13, за модулем 14 числа 59 і 73;
в) усі числа не порівняні;
г) за модулем 8 числа 52, -13, за модулем 14 числа 59 і 73;
д) за модулем 8 числа 75, -13 і 59, за модулем 14 – жодне.

7. За умови, що $a \equiv 4(\mathrm{mod}5)$, $b \equiv 3(\mathrm{mod}5)$, заповнити порожні клітини у порівняннях: $a+b \equiv \square(\mathrm{mod}5)$, $a-b \equiv \square(\mathrm{mod}5)$, $ab \equiv \square(\mathrm{mod}5)$, $3a+8b \equiv \square(\mathrm{mod}5)$, $8a+3b \equiv \square(\mathrm{mod}5)$.

8. Яка пара з чисел 185, 254, 116, 42 порівняна між собою за модулем 6?

а) 185, 116; **б)** 116, 254; **в)** 254, 185;
г) 42, 254; **д)** 185, 42.

9. З яким найменшим натуральним числом порівняне число $n = 7 \cdot 19 \cdot 41 \cdot 53 \cdot 1724$ за модулем 11?

а) 2; **б)** 6; **в)** 9; **г)** 4; **д)** 10; **е)** 5.

10. Якщо a – парне число, то яке з наведених порівнянь може бути *правильним*?

а) $a \equiv 1(\mathrm{mod}6)$; **б)** $a \equiv 3(\mathrm{mod}6)$; **в)** $a \equiv 4(\mathrm{mod}6)$;
г) $a \equiv 5(\mathrm{mod}6)$; **д)** $a \equiv 7(\mathrm{mod}6)$.

11. Заповнити порожні клітини у порівняннях, виходячи з умови, записаної у першому стовпці таблиці.

Число a непарне і кратне 3	$a \equiv \square(\mathrm{mod}6)$
Число a парне і при діленні на 3 дає остачу 1	$a \equiv \square(\mathrm{mod}6)$
Число a кратне 6	$a \equiv \square(\mathrm{mod}6)$

12. Заповніть порожні клітини таблиці, кожного разу вибираючи найменше додатне число з усіх можливих.

Порівняння	a	n	b
$a \equiv b \mathrm{mod}\, n$	119	14	
$a \equiv b \mathrm{mod}\, n$	48		3
$a \equiv b \mathrm{mod}\, n$		7	4

13. У якому стовпці таблиці всі лишки обчислені *правильно*?

а	б	в	г
$6819 \equiv 1 \mathrm{mod}14$	$6164 \equiv 8 \mathrm{mod}13$	$5267 \equiv 4 \mathrm{mod}19$	$3152 \equiv 0 \mathrm{mod}4$
$3152 \equiv 2 \mathrm{mod}4$	$5267 \equiv 4 \mathrm{mod}19$	$542 \equiv 3 \mathrm{mod}11$	$6164 \equiv 2 \mathrm{mod}13$
$542 \equiv 3 \mathrm{mod}11$	$3152 \equiv 0 \mathrm{mod}4$	$6164 \equiv 2 \mathrm{mod}13$	$542 \equiv 6 \mathrm{mod}11$

14. Обчислити найменші невід'ємні лишки чисел 277, -387, -159, 356, -490, 1111 за модулем 11 та записати їх за зростанням.

а) 0, 2, 4, 5, 6, 9; **б)** 1, 3, 4, 5, 7, 9; **в)** 0, 2, 5, 6, 7, 9; **г)** 2, 4, 5, 6, 9, 11.

15. За якої умови із порівняння $xt \equiv yt(\mathrm{mod}\, m)$ після скорочення t випливає $x \equiv y(\mathrm{mod}\, m)$?

а) якщо $\mathrm{НСК}(m,t) = t$; **б)** якщо $\mathrm{НСК}(m,t) = m$; **в)** якщо $\mathrm{НСД}(m,t) = 1$;
г) якщо $\mathrm{НСД}(m,t) = m$; **д)** якщо $\mathrm{НСД}(m,t) = t$; **е)** умови не існує.

16. З яких чисел складається клас лишків $\bar{a}$ за модулем m ?

а) кратних НСД(a,m); **б)** не порівняних з числом a за модулем m;

в) кратних числу a; **г)** порівняних з числом a за модулем m.

17. Нижче записані декілька представників класів лишків за модулем 9. У яких випадках у класи потрапили не свої представники?

а) $\bar{0}=\{...-9,9,19,27,...\}$; **б)** $\bar{2}=\{...-16,2,11,20,29,38,...\}$;

в) $\bar{5}=\{...-4,14,23,32,...\}$; **г)** $\bar{7}=\{...-11,-2,16,25,34,...\}$.

18. Яке число слід замінити, щоб сукупність чисел 9, 2, 16, 20, 27, 39, 46, 86 стала повною системою лишків за модулем 8? Якщо чисел два, то вказати найбільше.

а) 9; **б)** 2; **в)** 16; **г)** 20; **д)** 27; **е)** 39; **є)** 46; **ж)** 86.

19. Повну систему лишків за модулем 6 утворює сукупність чисел 12, 25, 2, 33, 28, 65. Які з цих чисел входять до зведеної системи лишків за цим модулем?

а) 12, 33; **б)** 25, 33; **в)** 12,65;

г) 25, 65; **д)** 2, 28.

20. Які з чисел слід замінити, щоб сукупність чисел 18, 22, 44, 12, 28, 32, 51, 25, 47 за модулем 9 входила у зведену систему лишків за цим модулем?

а) 28,47,12; **б)** 28,47,22; **в)** 18,12,51;

г) 32,25,47; **д)** 51,47,22; **е)** 47,22,32.

Завдання для аудиторної роботи

Приклад 1. Звести дані числа за вказаним модулем: а) $55(\mathrm{mod}17)$; б) $654321(\mathrm{mod}12)$; в) $-55(\mathrm{mod}17)$.

Розв'язання: а) знаходимо остачу від ділення числа 55 на модуль: $55=17\cdot3+4 \Rightarrow 55\equiv4\,\mathrm{mod}17$; б) $654321=54526\cdot12+9\Rightarrow 654321\equiv9\,\mathrm{mod}12$; в) $-55\equiv-4\,\mathrm{mod}17\equiv13\,\mathrm{mod}17$.

Приклад 2. Обчислити: а) $8^{31}(\mathrm{mod}55)$; б) $13^{14}-18^{13}(\mathrm{mod}7)$; в) $9^{2009}+2007\cdot2008\cdot2009(\mathrm{mod}8)$.

Розв'язання: а) $8^{31}(\mathrm{mod}55)\equiv(8^2)^{15}\cdot8(\mathrm{mod}55)\equiv(64)^{15}\cdot8(\mathrm{mod}55)\equiv$
$\equiv9^{15}\cdot8(\mathrm{mod}55)\equiv(9^3)^5\cdot8(\mathrm{mod}55)\equiv(729)^5\cdot8(\mathrm{mod}55)\equiv14^5\cdot8(\mathrm{mod}55)\equiv$
$\equiv(14^2)^2\cdot14\cdot8(\mathrm{mod}55)\equiv196^2\cdot112(\mathrm{mod}55)\equiv31^2\cdot2(\mathrm{mod}55)\equiv961\cdot2(\mathrm{mod}55)\equiv$
$\equiv26\cdot2(\mathrm{mod}55)\equiv52(\mathrm{mod}55)$ (тут ураховано, що $64\equiv9\,\mathrm{mod}\,55$, $112\equiv2\,\mathrm{mod}\,55$, $9^3=729\equiv14\,\mathrm{mod}\,55$, $14^2=196\equiv31\,\mathrm{mod}\,55$, $31^2=961\equiv26\,\mathrm{mod}\,55$);

б) $13^{14}-18^{13}(\mathrm{mod}7)\equiv6^{14}-4^{13}\equiv(6^2)^7-(4^3)^4\cdot4\equiv(36)^7-(64)^4\cdot4\equiv(1)^7-(1)^4\cdot4\equiv$
$\equiv1-4\equiv-3\equiv4\,\mathrm{mod}7$;

в) $9^{2009}+2007\cdot2008\cdot2009(\mathrm{mod}8)\equiv1^{2009}+7\cdot8\cdot9\equiv1+0=1$.

Приклад 3. Знайти остачу від ділення числа $7\cdot5^6+21$ на 29.

Розв'язання: $7\cdot5^6+21(\mathrm{mod}29)\equiv7\cdot(5^3)^2+21(\mathrm{mod}29)\equiv$
$\equiv7\cdot125^2+21(\mathrm{mod}29)\equiv7\cdot9^2+21(\mathrm{mod}29)\equiv588(\mathrm{mod}29)\equiv8\,\mathrm{mod}29$.

Приклад 4. Знайти останню цифру у десятковому записі числа 2^{2009}.

Розв'язання. Остання цифра у десятковому записі будь-якого числа збігається з остачею від ділення даного числа на 10. Тому
$2^{2009}(\mathrm{mod}10)\equiv(2^{10})^{200}\cdot2^9(\mathrm{mod}10)\equiv(1024)^{200}\cdot512(\mathrm{mod}10)\equiv4^{200}\cdot2(\mathrm{mod}10)\equiv$
$\equiv(4^4)^{50}\cdot2(\mathrm{mod}10)\equiv256^{50}\cdot2(\mathrm{mod}10)\equiv6^{50}\cdot2(\mathrm{mod}10)\equiv(6^4)^{12}\cdot36\cdot2(\mathrm{mod}10)\equiv$
$\equiv1296^{12}\cdot2(\mathrm{mod}10)\equiv6^{12}\cdot2(\mathrm{mod}10)\equiv1296^3\cdot2(\mathrm{mod}10)\equiv6^3\cdot2(\mathrm{mod}10)\equiv432(\mathrm{mod}10)\equiv2$.

Приклад 5. Довести, що десятковий запис чисел Ферма $F_n=2^{2^n}+1$, де $n\in N$, $n\neq1$, закінчується цифрою 7.

Доведення. За математичною індукцією $2^{2^2}=16\equiv6(\mathrm{mod}10)$, $2^{2^3}=256\equiv6(\mathrm{mod}10)$. Припустимо, що й $2^{2^n}\equiv6(\mathrm{mod}10)$. Піднесемо до квадрата $2^{2^{n+1}}\equiv36\equiv6(\mathrm{mod}10)$. Тоді $F_n\equiv2^{2^{n+1}}+1\equiv7(\mathrm{mod}10)$.

Приклад 6. Довести, що квадрат будь-якого непарного числа порівняний з 1 за модулем 8.

Доведення. Будь-яке непарне число можна записати як $4n\pm1$, $n\in N, n=0$. Тоді $(4n\pm1)^2=16n^2\pm8n+1\equiv1(\mathrm{mod}8)$.

Приклад 7. Довести, що непарне число вигляду $4n+3$, $n\in N$, не може дорівнювати сумі квадратів двох цілих чисел.

Доведення. Нехай x і y – два цілих числа. Якщо вони одночасно парні або непарні, то x^2+y^2 – парне число і не може дорівнювати непарному числу. Коли ж парність чисел різна, наприклад, x – парне, y – непарне, то $x^2:4$, тобто $x^2\equiv0(\mathrm{mod}4)$. З попереднього прикладу 6 випливає, що $y^2\equiv1(\mathrm{mod}8)$, а тоді за властивістю порівнянь $y^2\equiv1(\mathrm{mod}4)$.

Тоді $+\begin{cases}x^2\equiv0(\mathrm{mod}4),\\ y^2\equiv1(\mathrm{mod}4)\end{cases}$

$x^2+y^2\equiv1(\mathrm{mod}4)$.

Приклад 8. Довести, що коли $\frac{5a+3b}{17}$ – ціле число, то й вираз $\frac{5a+b}{17}$ також є цілим числом.

Д о в е д е н н я. Якщо $\frac{5a+3b}{17}$ – ціле число, то чисельник кратний знаменнику і тоді $5a+3b\equiv 0(\mathrm{mod}17) \Rightarrow 5a\equiv 0(\mathrm{mod}17)(*)$ і $3b\equiv 0(\mathrm{mod}17)$. Оскільки $3\not\equiv 0(\mathrm{mod}17)$, то $b\equiv 0(\mathrm{mod}17)(**)$. Додаємо почленно порівняння (*) і (**): $5a+b\equiv 0(\mathrm{mod}17) \Rightarrow (5a+b)\vdots 17$.

Приклад 9. Довести, що $(2+7)^5\equiv 2^5+7^5(\mathrm{mod}5)$, не виконуючи додавання чисел в дужках.

Д о в е д е н н я. За формулою бінома Ньютона:

$$(2+7)^5=2^5+5\cdot 2^4\cdot 7+10\cdot 2^3\cdot 7^2+10\cdot 2^2\cdot 7^3+5\cdot 2\cdot 7^4+7^5(\mathrm{mod}5).$$

Доданки $5\cdot 2^4\cdot 7$, $10\cdot 2^3\cdot 7^2$, $10\cdot 2^2\cdot 7^3$, $5\cdot 2\cdot 7^4$ кратні 5, тому

$$5\cdot 2^4\cdot 7+10\cdot 2^3\cdot 7^2+10\cdot 2^2\cdot 7^3+5\cdot 2\cdot 7^4\equiv 0(\mathrm{mod}5).$$

Отже, $(2+7)^5\equiv 2^5+7^5(\mathrm{mod}5)$.

Приклад 10. Вивести критерій подільності чисел на 3.

Р о з в' я з а н н я. Будь-яке число $a=\overline{a_n a_{n-1}...a_1 a_0}$, десятковий запис якого містить цифри $a_n, a_{n-1},..., a_1, a_0$, можна записати у вигляді: $a=a_n 10^n+a_{n-1}10^{n-1}+...+a_1 10+a_0$, де $0\le a_i\le 9, i=1,2,...,n$. Оскільки $10\equiv 1(\mathrm{mod}3)$ і $10^k\equiv 1(\mathrm{mod}3)$, то $a\equiv a_n+a_{n-1}+...+a_1+a_0(\mathrm{mod}3)$. Звідси випливає, що $a\equiv 0(\mathrm{mod}3)$, тільки якщо $a_n+a_{n-1}+...+a_1+a_0\equiv 0(\mathrm{mod}3)$, а це означає, що сума цифр числа має ділитися на 3.

Приклад 11. Перемножити матриці $\begin{pmatrix}12 & 10\\ -5 & 16\end{pmatrix}\cdot\begin{pmatrix}2 & -4\\ 10 & 11\end{pmatrix}\mathrm{mod}7$.

Р о з в' я з а н н я. Знаходимо добуток матриць за стандартним правилом та зводимо результат за модулем.

$$\begin{pmatrix}12 & 10\\ -5 & 16\end{pmatrix}\cdot\begin{pmatrix}2 & -4\\ 10 & 11\end{pmatrix}\mathrm{mod}7\equiv\begin{pmatrix}12\cdot 2+10\cdot 10 & 12\cdot(-4)+10\cdot 11\\ -5\cdot 2+16\cdot 10 & -5\cdot(-4)+16\cdot 11\end{pmatrix}\mathrm{mod}7\equiv$$

$$\equiv\begin{pmatrix}124 & 62\\ 150 & 196\end{pmatrix}\mathrm{mod}7\equiv\begin{pmatrix}5 & 6\\ 3 & 0\end{pmatrix}\mathrm{mod}7.$$

Приклад 12. Побудувати повну систему найменших додатних лишків за модулем 9 і зведену систему лишків за модулем 9.

Р о з в' я з а н н я. Повну систему лишків за модулем m утворюють числа $\{0,1,2,...,m-1\}$, отже, $\{0,1,2,3,4,5,6,7,8\}$ – повна система найменших додатних

лишків за модулем 9. Лишки, які будуть взаємно простими з модулем 9, утворюють зведену систему лишків, тобто це $\{1,2,4,5,7,8\}$.

Приклад 13. Розподілити числа від -30 до 20 на класи лишків за модулем 7.

Р о з в' я з а н н я. У першому рядку таблиці записані класи лишків за модулем 7, а у відповідних стовпцях – їх представники.

$\bar{0}$	$\bar{1}$	$\bar{2}$	$\bar{3}$	$\bar{4}$	$\bar{5}$	$\bar{6}$
-28	-27	-26	-25	-24	-30	-29
-21	-20	-19	-18	-17	-23	-22
-14	-13	-12	-11	-10	-16	-15
-7	-6	-5	-4	-3	-9	-8
0	1	2	3	4	-2	-1
7	8	9	10	11	5	6
14	15	16	17	18	12	13
					19	20

Приклад 14. На множині Z_5 визначити операції додавання та множення класів лишків за модулем.

Р о з в' я з а н н я. Операції над класами лишків задамо за допомогою таблиць Келі, у першому рядку і першому стовпці яких запишемо представників класів, а результат додавання та множення – на перетині відповідних рядів таблиці.

+	0	1	2	3	4
0	0	1	2	3	4
1	1	2	3	4	0
2	2	3	4	0	1
3	3	4	0	1	2
4	4	0	1	2	3

·	0	1	2	3	4
0	0	0	0	0	0
1	0	1	2	3	4
2	0	2	4	1	3
3	0	3	1	4	2
4	0	4	3	2	1

Завдання для домашньої роботи

1. Які з чисел $75, 73, 59, 52, -13$ порівняні з числом 29 за модулем 8 ?

2. Які з чисел $75, 73, 59, 52, -13$ порівняні з числом 29 за модулем 14 ?

3. Чи можна сукупність чисел 9, 2, 16, 20, 27, 39,46, 85 вважати за повну систему лишків за модулем $\dot{8}$?

4. Парні числа a і b, не кратні 6, при діленні на 6 дають різні остачі. Довести, що $a+b\equiv 0(\mathrm{mod}\,6)$.

5. Обчислити: а) $56785678(\mathrm{mod}\,9)$ і $-56785678(\mathrm{mod}\,9)$; б) $8^{100}+11^{100}(\mathrm{mod}\,19)$; в) $5^{21}(\mathrm{mod}\,77)$; г) $1979^{1980}(\mathrm{mod}\,7)$; д) $13^{14}-19^{19}(\mathrm{mod}\,5)$; е) $3^{19}+5^{48}(\mathrm{mod}\,23)$. (*Відповідь*: а) $7(\mathrm{mod}\,9)$; $2(\mathrm{mod}\,9)$; б) $3(\mathrm{mod}\,19)$; в) $27(\mathrm{mod}\,77)$; г) $1(\mathrm{mod}\,7)$; д) $0(\mathrm{mod}\,5)$; е) $10(\mathrm{mod}\,23)$).

6. Знайти остачу від ділення числа: а) $17\cdot 14^9+5$ на 45; б) $9^{2005}+2005$ на 10. (*Відповідь*: а) 33; б) 4).

7. Довести, що а) $\left(2^{70}+3^{70}\right)\vdots 13$; б) $\left(177^{99}+643^{44}+1994^{88}\right)\vdots 10$.

8. Знайти дві останні цифри у десятковому записі числа 9^{9^9}.
(*Вказівка*: дві останні цифри у десятковому записі числа збігаються з остачею від ділення даного числа на 100).

9. Довести, що всі числа вигляду $2^{4^n}-5$, $n\in N$, закінчуються цифрою 1.

10. Довести, що квадрат будь-якого парного числа, не кратного 4, порівняний з числом 4 за модулем 32.

11. Довести, що квадрат будь-якого числа, не кратного числам 2 і 3, порівняний з одиницею за модулем 6.

12. Вивести критерій подільності чисел на 11.
(*Розв'язання*: нехай $a=a_n10^n+a_{n-1}10^{n-1}+\ldots+a_110+a_0$, де $0\le a_i\le 9$, $i=1,2,\ldots,n$. Оскільки $10\equiv -1(\mathrm{mod}\,11)$, то $10^k\equiv(-1)^k(\mathrm{mod}\,11)$ або $10^k\equiv 1(\mathrm{mod}\,11)$ при парному k та $10^k\equiv -1(\mathrm{mod}\,11)$ при непарному k. Тоді $a\equiv a_n(-1)^n+a_{n-1}(-1)^{n-1}+\ldots+a_2-a_1+a_0(\mathrm{mod}\,11)\Rightarrow$ альтернативна сума цифр числа має ділитися на 11, наприклад, $3443\vdots 11$, бо $3-4+4-3=0$).

13. Перемножити матриці: а) $\begin{pmatrix}3&5\\8&6\end{pmatrix}\cdot\begin{pmatrix}10&4\\2&8\end{pmatrix}\mathrm{mod}17$;
б) $\begin{pmatrix}4&12\\-6&-10\end{pmatrix}\cdot\begin{pmatrix}-5&3\\-8&12\end{pmatrix}\mathrm{mod}15$; в) $\begin{pmatrix}15&21\\11&0\end{pmatrix}\cdot\begin{pmatrix}3&28\\6&1\end{pmatrix}\mathrm{mod}34$.
(*Відповідь*: а) $\begin{pmatrix}6&1\\7&12\end{pmatrix}\mathrm{mod}17$; б) $\begin{pmatrix}4&6\\5&12\end{pmatrix}\mathrm{mod}15$; в) $\begin{pmatrix}1&33\\33&1\end{pmatrix}\mathrm{mod}34$.

14. Побудувати повну систему найменших додатних лишків за модулем 10 і зведену систему лишків за модулем 10.

15. Розподілити числа від -40 до 30 на класи лишків за модулем 8.

2.3. Функція Ейлера. Теореми Ейлера і Ферма. Псевдопрості числа. Числа Кармайкла

Тестові завдання для перевірки теоретичних знань

1. Якщо значення функції Ейлера $\varphi(m)=12$, то скільки натуральних чисел, менших за число m, будуть взаємно простими з числом m?
а) 24; **б)** 13; **в)** 12; **г)** 11; **д)** 8; **е)** 6.

2. Скільки існує класів лишків за модулем m, представники яких є взаємно простими з модулем ?
а) $m-1$; **б)** m; **в)** $\varphi(m)$; **г)** $m!$; **д)** $\varphi(m)+1$; **е)** $\varphi(m)-1$.

3. Для функції Ейлера $\varphi(m_1m_2)=\varphi(m_1)\varphi(m_2)$ тільки за умови, що...
а) НСД$(m_1,m_2)=1$; **б)** НСК$(m_1,m_2)=m_1$; **в)** $m_1>m_2$;
г) $m_2>m_1$; **д)** m_1m_2 – точний квадрат.

4. Якщо значення функції Ейлера обчислюється за формулою $\varphi(m)=m-1$, то обов'язково аргумент m – ...
а) просте число; **б)** складене число; **в)** псевдопросте число;
г) число Кармайкла; **д)** точний квадрат.

5. В яких випадках значення функції Ейлера обчислено *неправильно*?
а) $\varphi(7)=7-1$; **б)** $\varphi(6)=6-1$; **в)** $\varphi(11)=11-1$;
г) $\varphi(9)=9\left(1-\frac{1}{3}\right)$; **д)** $\varphi(4)=(4-1)^2$; **е)** $\varphi(4^2)=4\left(1-\frac{1}{4}\right)$.

6. Для яких m значення $\varphi(m)$ непарне?
а) 0; **б)** 1 і 2; **в)** тільки 2; **г)** тільки 1; **д)** $m+1$; **е)** $m-1$.

7. З яким твердженням Ви *не* згодні?
а) якщо $a>1$ і НСД$(a;m)=1$, то $a^{\varphi(m)}\equiv 1(\mathrm{mod}\,m)$;
б) якщо число p – просте і число a не ділиться на p, то $a^{p-1}\equiv 1(\mathrm{mod}\,p)$;
в) якщо $a^{n-1}\equiv 1(\mathrm{mod}\,n)$, $a\in(1;n-1)$ і НСД$(a;n)=1$, то n – просте;
г) якщо $a^{n-1}\not\equiv 1(\mathrm{mod}\,n)$ і $a\in(1;n-1)$, то n – просте.

8. Якій умові мають задовольняти натуральні числа a і m, щоб виконувалось порівняння $a^{\varphi(m)} \equiv 1 (\mathrm{mod}\, m)$?

а) НСК$(a,m)=a$; **б)** НСК$(a,m)=m$; **в)** $a^{\varphi(m)} > m$;
г) НСД$(a,\varphi(m))=1$; **д)** НСД$(a,m)=1$.

9. Якій умові мають задовольняти натуральні числа a і p, щоб виконувалось порівняння $a^{p-1} \equiv 1 (\mathrm{mod}\, p)$?

а) НСК$(a,p)=a$; **б)** p – складене; **в)** p – просте;
г) $a \not\vdots p$; **д)** $(a-1) \vdots p$; **е)** НСД$(a,p)=p$.

10. Яке з нижченаведених порівнянь є *правильним* записом теореми Ферма?

а) $2^{16} \equiv 1 (\mathrm{mod}\, 17)$; **б)** $2^{17} \equiv 1 (\mathrm{mod}\, 18)$; **в)** $2^{18} \equiv 1 (\mathrm{mod}\, 17)$;
г) $2^{17} \equiv 1 (\mathrm{mod}\, 17)$; **д)** $2^{16} \equiv 17 (\mathrm{mod}\, 17)$; **е)** $2^{17} \equiv 1 (\mathrm{mod}\, 16)$.

11. Яке з нижченаведених порівнянь є *правильним* записом теореми Ейлера?

а) $36^8 \equiv 1 (\mathrm{mod}\, 15)$; **б)** $37^8 \equiv 1 (\mathrm{mod}\, 15)$; **в)** $37^9 \equiv 1 (\mathrm{mod}\, 15)$;
г) $37^{14} \equiv 1 (\mathrm{mod}\, 15)$; **д)** $37^{15} \equiv 1 (\mathrm{mod}\, 15)$; **е)** $37^8 \equiv 37 (\mathrm{mod}\, 15)$.

12. Яким буде натуральне непарне складене число n, для якого існує таке число a, що виконуються умови $a^{n-1} \equiv 1 (\mathrm{mod}\, n)$ і НСД$(a,n)=1$?

а) числом Кармайкла; **б)** числом Ейлера; **в)** простим числом;
г) псевдопростим числом Ферма; **д)** інша відповідь.

13. За яких умов число n буде числом Кармайкла?

а) n – складене; **б)** n – просте; **в)** $(n-1) \not\vdots (p-1)$; **г)** $(n-1) \vdots (p-1)$;
д) $n \vdots p^2$; **е)** $n \not\vdots p^2$, де p – будь-який простий дільник числа n.

Завдання для аудиторної роботи

Приклад 1. Користуючись означенням, обчислити значення функції Ейлера $\varphi(45)$.

Р о з в ' я з а н н я. Виписуємо натуральні числа від 1 до 45 та викреслюємо ті з них, що мають спільні дільники з числом 45, які не дорівнюють одиниці, тобто числа, що діляться на 3 і 5. Залишені числа

1, 2, 4, 7, 8, 11, 13, 14, 16, 17, 19, 22, 23, 26, 28, 29, 31, 32, 34, 37, 38, 41, 43, 44

утворюють зведену систему лишків за модулем 45. Їх кількість 24, отже, $\varphi(45)=24$.

Приклад 2. Обчислити значення функції Ейлера а)$\varphi(180)$; б)$\varphi(1875)$; в) $\varphi(387)$; г)$\varphi(512)$.

Р о з в ' я з а н н я. Для того, щоб обчислити значення функції Ейлера, числа повинні бути розкладені на прості множники.

а) $\varphi(180)=\varphi(2^2\cdot 3^2\cdot 5)=180\cdot\left(1-\frac{1}{2}\right)\left(1-\frac{1}{3}\right)\left(1-\frac{1}{5}\right)=48$;

б) $\varphi(1875)=\varphi(3\cdot 5^4)=1875\cdot\left(1-\frac{1}{3}\right)\left(1-\frac{1}{5}\right)=1000$;

в) $\varphi(387)=\varphi(3^2\cdot 43)$. НСД$(3,43)=1 \Rightarrow \varphi(387)=\varphi(3^2)\varphi(43)=$
$=3^2\left(1-\frac{1}{3}\right)(43-1)=252$;

г) $\varphi(512)=\varphi(2^9)=2^9\left(1-\frac{1}{2}\right)=256$.

Приклад 3. Скільки існує натуральних чисел, взаємно простих з числом 160 і не перевищуючих його?

Р о з в ' я з а н н я. За означенням функції Ейлера кількість натуральних чисел, що не перевищують числа 160 і є взаємно простими з ним, дорівнює 64, тобто:

$$\varphi(160)=\varphi(2^5\cdot 5)=160\cdot\left(1-\frac{1}{2}\right)\left(1-\frac{1}{5}\right)=64.$$

Приклад 4. Розв'язати рівняння: а) $\varphi(10^x)=400$; б) $\varphi(21x)=120$; в) $\varphi(x)=16$.

Р о з в ' я з а н н я:

а) $\varphi(10^x)=\varphi(2^x\cdot 5^x)=10^x\left(1-\frac{1}{2}\right)\left(1-\frac{1}{5}\right)=10^x\cdot\frac{2}{5}$;

$$10^x\cdot\frac{2}{5}=400;\ 10^x=1000;\ x=3.$$

б) для простого x маємо

$$\varphi(21x)=\varphi(3\cdot 7\cdot x)=\varphi(3)\varphi(7)\varphi(x)=2\cdot 6\cdot(x-1)=$$
$$=12(x-1);\ 12(x-1)=120;\ x=11.$$

Якщо x – складене число, тобто $x=p_1^{\alpha_1}p_2^{\alpha_2}\cdot\ldots\cdot p_n^{\alpha_n}$, то прості числа p_i можуть вибиратися тільки з ряду 2,3,5,7,11. $\varphi(22)=\varphi(11\cdot 2)=\varphi(11)\varphi(2)=10\cdot 1=10$. Перевіряємо $\varphi(21\cdot 22)=12\cdot 10=120$. Отже, $x_1=11$, $x_2=22$;

в) число x може бути складеним $x=p_1^{\alpha_1}p_2^{\alpha_2}\cdot\ldots\cdot p_n^{\alpha_n}$. Тоді

$$\varphi(x)=x\left(1-\frac{1}{p_1}\right)\left(1-\frac{1}{p_2}\right)\cdot\ldots\cdot\left(1-\frac{1}{p_n}\right)=16.$$

Отже, p_i можуть бути простими числами з ряду $2,3,5,7,11,13,17$. Перебором установлюємо, що підходять лише такі значення x:

$$x=17, \quad \text{бо} \quad \varphi(17)=17-1=16;$$
$$x=17\cdot 2=34, \quad \text{бо} \quad \varphi(34)=\varphi(2)\varphi(17)=1\cdot 16=16;$$
$$x=5\cdot 2^3=40, \quad \text{бо} \quad \varphi(40)=40\left(1-\frac{1}{2}\right)\left(1-\frac{1}{5}\right)=16;$$
$$x=3\cdot 2^4=48, \quad \text{бо} \quad \varphi(48)=48\left(1-\frac{1}{2}\right)\left(1-\frac{1}{3}\right)=16.$$

Приклад 5. Знайти α і β, якщо $\varphi(3^\alpha\cdot 7^\beta)=108$.

Р о з в ' я з а н н я: $\varphi(3^\alpha\cdot 7^\beta)=3^\alpha\cdot 7^\beta\left(1-\frac{1}{3}\right)\left(1-\frac{1}{7}\right)=108 \Rightarrow$

$$\Rightarrow 3^{\alpha-1}\cdot 7^{\beta-1}\cdot 2\cdot 6=108 \Rightarrow 3^{\alpha-1}\cdot 7^{\beta-1}=9 \Rightarrow 3^{\alpha-1}\cdot 7^{\beta-1}=3^2\cdot 7^0 \Rightarrow$$
$$\Rightarrow \alpha-1=2,\ \beta-1=0 \Rightarrow \alpha=3,\ \beta=1.$$

Приклад 6. Знайти число n, якщо $\varphi(n)=48$, $n=2^\alpha\cdot 3^\beta\cdot 5^\gamma\cdot 7^\delta$.

Р о з в ' я з а н н я:

$$\varphi(2^\alpha\cdot 3^\beta\cdot 5^\gamma\cdot 7^\delta)=2^\alpha\cdot 3^\beta\cdot 5^\gamma\cdot 7^\delta\left(1-\frac{1}{2}\right)\left(1-\frac{1}{3}\right)\left(1-\frac{1}{5}\right)\left(1-\frac{1}{7}\right)=48 \Rightarrow$$

$$\Rightarrow 2^\alpha\cdot 3^\beta\cdot 5^\gamma\cdot 7^\delta\cdot\frac{1}{2}\cdot\frac{2}{3}\cdot\frac{4}{5}\cdot\frac{6}{7}=2^4\cdot 3 \Rightarrow 2^{\alpha+3}\cdot 3^\beta\cdot 5^{\gamma-1}\cdot 7^{\delta-1}=2^4\cdot 3 \Rightarrow$$
$$\Rightarrow \alpha+3=4,\ \beta=1,\ \gamma-1=0,\ \delta-1=0 \Rightarrow \alpha=1,\ \beta=1,\ \gamma=1,\ \delta=1 \Rightarrow$$
$$\Rightarrow n=2\cdot 3\cdot 5\cdot 7=210.$$

Приклад 7. Довести, що $\varphi(20p\pm 4)=2\varphi(5p\pm 1)$, де p – просте число.

Д о в е д е н н я: $\varphi(20p\pm 4)=\varphi(4(5p\pm 1)=\varphi(4)\varphi(5p\pm 1)=2\varphi(5p\pm 1)$.

Приклад 8. Розкласти на два прості множники p і q число $n=pq=256\ 999$, беручи до уваги значення функції Ейлера $\varphi(n)=255\ 664$.

Р о з в ' я з а н н я: $\varphi(n)=\varphi(pq)=\varphi(p)\varphi(q)=(p-1)(q-1)=pq-(p+q)+1$, тоді множники p і q визначаємо із системи

$$\begin{cases} pq=256\,999, \\ pq-(p+q)+1=255\,664. \end{cases}$$

Звідси числа p і q є розв'язками рівнянь

$$p^2-1336p+256\ 999=0; \qquad q=256\ 999/p, \quad \text{тобто} \quad p=1103,\ q=233.$$

Приклад 9. За умови, що число a не ділиться на просте число p, обчислити значення $a^k \pmod p$.

Р о з в ' я з а н н я. Розділимо показник k на $(p-1)$ з остачею:

$$k=(p-1)q+r,\ 0<r<p-1,\ q>0.$$

Тоді $a^k\equiv a^{(p-1)q+r}(\text{mod } p)=(a^{p-1})^q a^r(\text{mod } p)=1^q a^r(\text{mod } p)=a^r(\text{mod } p)$.

Приклад 10. На основі приклада 9 обчислити $3^{123456}(\text{mod } 11)$.

Р о з в ' я з а н н я. Розділимо показник 123456 на $(11-1)$ з остачею.

$$123456=12345\cdot 10+6 \Rightarrow 3^{123456}(\text{mod } 11)\equiv 3^6(\text{mod } 11)\equiv (3^3)^2(\text{mod } 11)\equiv$$
$$\equiv 27^2(\text{mod } 11)\equiv 5^2(\text{mod } 11)=3.$$

Приклад 11. Обчислити за допомогою теореми Ейлера $347^{64}(\text{mod } 85)$.

Р о з в ' я з а н н я. Умови теореми Ейлера виконуються:

$$\text{НСД}(347,85)=1,\ \varphi(85)=\varphi(17\cdot 5)=\varphi(17)\cdot\varphi(5)=16\cdot 4=64.$$

Тоді $347^{64}(\text{mod } 85)\equiv 347^{\varphi(85)}(\text{mod } 85)\equiv 1(\text{mod } 85)$.

Приклад 12. Довести, що при $\text{НСД}(a,35)=1$ справедливе порівняння $a^{10}-a^6-a^4+1\equiv 0(\text{mod } 35)$.

Р о з в ' я з а н н я. Згідно з теоремою Ферма

$$a^4\equiv 1(\text{mod } 5) \text{ і } a^6\equiv 1(\text{mod } 7) \Rightarrow$$
$$\Rightarrow a^4-1=5t_1 \text{ і } a^6-1=7t_2, \text{ де } t_1=0,\pm 1,\pm 2,\ldots,\ t_2=0,\pm 1,\pm 2,\ldots \Rightarrow$$
$$\Rightarrow (a^4-1)(a^6-1)=35t_1t_2 \Rightarrow$$
$$\Rightarrow a^{10}-a^6-a^4+1=35t_1t_2 \text{ або } a^{10}-a^6-a^4+1=35t, \text{ де } t=0,\pm 1,\pm 2,\ldots \Rightarrow$$
$$\Rightarrow a^{10}-a^6-a^4+1\equiv 0(\text{mod } 35).$$

Приклад 13. За допомогою теореми Ферма довести, що для будь-якого цілого n число $n^3+(n+1)^3+(n+2)^3$ ділиться на 9.

Д о в е д е н н я. За теоремою Ферма $n^{3-1}\equiv 1(\text{mod } 3)$, звідки $n^3\equiv n(\text{mod } 3)$. Знаходимо:

$$(n+1)^3(\text{mod } 3)\equiv n^3+3n^2+3n+1(\text{mod } 3)\equiv n^3+1(\text{mod } 3)\equiv n+1(\text{mod } 3);$$
$$(n+2)^3(\text{mod } 3)\equiv n^3+6n^2+12n+8(\text{mod } 3)\equiv n^3+8(\text{mod } 3)\equiv n+8(\text{mod } 3).$$
$$n^3+(n+1)^3+(n+2)^3(\text{mod } 3)\equiv n+n+1+n+8(\text{mod } 3)\equiv 3n+9(\text{mod } 3)\equiv$$
$$\equiv 9n+27(\text{mod } 9)\equiv 0(\text{mod } 9).$$

Приклад 14. За допомогою теореми Ферма довести, що коли p – просте і $a_1,a_2,\ldots,a_n$ – цілі, то $(a_1+a_2+\ldots+a_n)^p\equiv a_1^{\,p}+a_2^{\,p}+\ldots+a_n^{\,p}(\text{mod } p)$.

Д о в е д е н н я. За теоремою Ферма

$$a_1^{\,p-1}\equiv 1(\text{mod } p) \text{ або } a_1^{\,p}\equiv a_1(\text{mod } p). \text{ Аналогічно}$$
$$a_2^{\,p}\equiv a_2(\text{mod } p),$$
$$\ldots\ldots\ldots\ldots$$
$$a_n^{\,p}\equiv a_n(\text{mod } p).$$

Сумуючи почленно ці порівняння, дістанемо

$$a_1^p + a_2^p + \ldots + a_n^p \equiv a_1 + a_2 + \ldots + a_n (\mathrm{mod}\, p).$$

З іншого боку, за теоремою Ферма буде правильним і порівняння

$$(a_1 + a_2 + \ldots + a_n)^p \equiv a_1 + a_2 + \ldots + a_n (\mathrm{mod}\, p).$$

Тоді згідно з першою властивістю порівнянь

$$(a_1 + a_2 + \ldots + a_n)^p \equiv a_1^p + a_2^p + \ldots + a_n^p (\mathrm{mod}\, p).$$

Приклад 15. Яке з чисел 645 і 567 є псевдопростим за основою 2?

Розв'язання: $2^{p-1} (\mathrm{mod}\, p) \equiv 2^{644} (\mathrm{mod}\, 645) \equiv (2^{20})^{32} \cdot 2^4 (\mathrm{mod}\, 645) \equiv$
$\equiv 451^{32} \cdot 2^4 (\mathrm{mod}\, 645) \equiv 226^{16} \cdot 2^4 (\mathrm{mod}\, 645) \equiv 121^8 \cdot 2^4 (\mathrm{mod}\, 645) \equiv 451^4 \cdot 2^4 (\mathrm{mod}\, 645) \equiv$
$\equiv 121 \cdot 16 (\mathrm{mod}\, 645) \equiv 1 (\mathrm{mod}\, 645)$. Оскільки при цьому $645 = 5 \cdot 129$, то 645 – псевдопросте число за основою 2.

Аналогічно $2^{566} (\mathrm{mod}\, 567) \equiv (2^{20})^{28} \cdot 2^6 (\mathrm{mod}\, 567) \equiv 193^{28} \cdot 2^6 (\mathrm{mod}\, 567) \equiv$
$\equiv (193^4)^7 \cdot 2^6 (\mathrm{mod}\, 567) \equiv 445^7 \cdot 2^6 (\mathrm{mod}\, 567) \equiv 142^3 \cdot 445 \cdot 64 (\mathrm{mod}\, 567) \equiv 445 \,\mathrm{mod}\, 567$..

Отже, 567 – складене число.

Приклад 16. Знайти всі основи a, за якими число 15 є псевдопростим числом Ферма.

Розв'язання. Якщо ціле непарне число a належить інтервалу $(1; n-1)$ та є взаємно простим з числом n і $a^{n-1} \equiv 1 (\mathrm{mod}\, n)$, то n – псевдопросте число за основою a. Із чисел від 1 до 14 взаємно простими з числом 15 будуть 7, 11 і 13. Далі обчислюємо:

$$7^{14} (\mathrm{mod}\, 15) \equiv 49^7 (\mathrm{mod}\, 15) \equiv 4^7 (\mathrm{mod}\, 15) \equiv 16^3 \cdot 4 (\mathrm{mod}\, 15) \equiv 4 (\mathrm{mod}\, 15);$$

$$11^{14} (\mathrm{mod}\, 15) \equiv 121^7 (\mathrm{mod}\, 15) \equiv 1 (\mathrm{mod}\, 15);$$

$$13^{14} (\mathrm{mod}\, 15) \equiv 169^7 (\mathrm{mod}\, 15) \equiv 4^7 (\mathrm{mod}\, 15) \equiv 4 (\mathrm{mod}\, 15).$$

Число 15 є псевдопростим числом Ферма тільки за основою 11.

Приклад 17. Розкласти число 29 341 на множники та показати, що воно кармайклове.

Розв'язання: $29\,341 = 13 \cdot 37 \cdot 61$. Умови, які має задовольняти число, щоб бути кармайкловим, такі: 1) число n не ділиться на p^2; 2) число $n-1$ ділиться на $p-1$, де p – простий дільник числа.

$p = 13 \Rightarrow n \vdots p^2 = 29\,341 \not\vdots 169$; $(n-1) : (p-1) = 29\,340 : 12 = 2445$;

$p = 37 \Rightarrow n \vdots p^2 = 29\,341 \not\vdots 1369$; $(n-1) : (p-1) = 29\,340 : 36 = 815$;

$p = 61 \Rightarrow n \vdots p^2 = 29\,341 \not\vdots 3721$; $(n-1) : (p-1) = 29\,340 : 60 = 489$.

Обидві потрібні умови виконуються, 29 341 – кармайклове число.

Завдання для домашньої роботи

1. Довести, що $\varphi(p^\alpha) = p^\alpha - p^{\alpha-1}$, де p – просте число.

2. Обчислити $\varphi(155)$, $\varphi(1296)$, $\varphi(625)$, $\varphi(865)$, $\varphi(231)$, $\varphi(729)$.
(*Відповідь*: $\varphi(155) = 120$, $\varphi(1296) = 432$, $\varphi(625) = 500$, $\varphi(865) = 688$, $\varphi(231) = 120$, $\varphi(729) = 486$0).

3. Перевірити рівність $\varphi(240) = \varphi(160)$.

4. Скільки існує натуральних чисел, взаємно простих з числом 324 і менших за це число?
(*Відповідь*: 48).

5. Скільки існує натуральних чисел, менших за 120 і взаємно простих з числом 160?
(*Відповідь*: 108).

6. Довести, що $\varphi(22n \pm 2) = \varphi(11n \pm 1)$, $n \in N$.
(*Вказівка*: $\varphi(22n \pm 2) = \varphi(2)\varphi(11n \pm 1)$).

7. Розв'язати рівняння: а) $\varphi(6^x) = 72$; б) $\varphi(4x) = 8$; в) $\varphi(3x) = 24$.
(*Відповідь*: а) $x = 3$; б) $x = 5$ або $x = 6$; в) $x = 13$, $x = 26$, $x = 28$.
Вказівка: якщо x – просте, то $\varphi(3x) = \varphi(3)\varphi(x) = 2 \cdot (x-1) = 24 \Rightarrow x = 13$; при складеному $x = p_1^{\alpha_1} \cdot p_2^{\alpha_2} \cdot \ldots \cdot p_n^{\alpha_n}$ обчислюємо

$$\varphi(x) = p_1^{\alpha_1} \cdot p_2^{\alpha_2} \cdot \ldots \cdot p_n^{\alpha_n} \left(1 - \frac{1}{p_1}\right)\left(1 - \frac{1}{p_2}\right) \ldots \left(1 - \frac{1}{p_n}\right) = 12, \text{ де } p = 2,3,5,7,11,13.$$

Далі з множини значень $x = 13 \cdot 2$, $x = 3 \cdot 7$, $x = 4 \cdot 7$, $x = 21 \cdot 2$, $x = 2^2 \cdot 3^2$ безпосередньо перевіркою вибрати ті значення x, для яких $\varphi(3x) = 24$).

8. Знайти α і β, якщо: а) $\varphi(5^\alpha \cdot 7^\beta) = 4200$; б) $\varphi(2^\alpha \cdot 11^\beta) = 440$.
(*Відповідь*: а) $\alpha = 2$, $\beta = 3$; б) $\alpha = 3$, $\beta = 2$).

9. Знайти число n, якщо $\varphi(n) = 320$, $n = 2^\alpha \cdot 3^\beta \cdot 5^\gamma$.
(*Відповідь*: $n = 1200$).

10. Розкласти на два прості множники p і q число $n = pq = 137\,438\,953\,471$, беручи до уваги значення функції Ейлера $\varphi(n) = 136\,822\,635\,072$.
(*Відповідь*: $p = 616\,318\,177$, $q = 223$).

11. Довести, використавши теорему Ферма, що $2^{70} + 3^{70}$ ділиться на 13.

12. На основі теореми Ферма довести, що

$$1^{18}+2^{18}+3^{18}+4^{18}+5^{18}+6^{18}\equiv -1(\mathrm{mod}\,7).$$

(*Вказівка*: за теоремою Ферма $a^6\equiv 1(\mathrm{mod}\,7)$, де $a=2,3,4,5,6$. Після піднесення кожного з цих порівнянь до куба, додати їх почленно).

13. За допомогою теореми Ферма обчислити $3^{102}(\mathrm{mod}101)$.
(*Відповідь*: 9. *Вказівка*: використати $3^{102}=9\cdot 3^{100}$).

14. Знайти, використавши теорему Ейлера, остачу від ділення 527^{144} на 65.
(*Відповідь*: 1).

15. Обчислити за допомогою теореми Ферма $17^{356740}(\mathrm{mod}193)$.
(*Відповідь*: 145).

16. Обчислити за допомогою теореми Ейлера $199^{72}(\mathrm{mod}144)$.
(*Відповідь*: 1).

17. На основі теореми Ейлера довести , що $3^{100}\equiv 1(\mathrm{mod}1000)$.
(*Відповідь*: $3^{100}\equiv 1(\mathrm{mod}1000)$. *Вказівка*: за теоремою Ейлера $3^4\equiv 1(\mathrm{mod}8)$ і $3^{100}\equiv 1(\mathrm{mod}125)$. Перше з порівнянь піднести до 25 степеня та застосувати властивості порівнянь).

18. Застосувавши теорему Ферма, довести, що $(73^{12}-1)\vdots 105$.
(*Вказівка*: $105=3\cdot 5\cdot 7$, застосувати теорему Ферма для модулів 3,5,7).

19. Знайти всі основи a, за якими число 21 є псевдопростим числом Ферма.
(*Відповідь*: 13).

20. Серед чисел 15125, 11687, 294409 знайти число Кармайкла.
(*Відповідь*: 294409).

2.4. Визначення обернених елементів. Порівняння першого степеня. Система порівнянь першого степеня. Китайська теорема про остачі

Тестові завдання для перевірки теоретичних знань

1. Для двох елементів a і b кільця лишків за модулем m виконується порівняння: $ab\equiv 1(\mathrm{mod}\,m)$. Яким елементом є елемент b для елемента a?

а) $b=\sqrt{a}(\mathrm{mod}\,m)$; **б)** $b=a^{-1}(\mathrm{mod}\,m)$;
в) b – дільник числа a; **г)** b – взаємно просте число з a.

2. Виписати всі елементи кільця лишків за модулем 24, для яких існують обернені елементи.

а) $\{1,5,7,8,11,13,16,17,19,23\}$; **б)** $\{1,5,7,11,13,17,19,23\}$;
в) $\{2,3,4,6,8,9,12,14,15,16,18,20,21,22\}$; **г)** $\{1,3,6,9,12,18,24\}$.

3. Вибрати серед запропонованих чисел таке значення модуля m, щоб у кільці лишків за цим модулем усі ненульові елементи мали обернені.

а) 20; **б)** 21; **в)** 22; **г)** 23; **д)** 24.

4. Яке з наведених порівнянь має найбільшу кількість розв'язків?

а) $13x\equiv 185(\mathrm{mod}\,98)$; **б)** $18x\equiv 81(\mathrm{mod}\,45)$; **в)** $15x\equiv 150(\mathrm{mod}\,75)$;
г) $13x\equiv 91(\mathrm{mod}\,26)$; **д)** $13x\equiv 75(\mathrm{mod}\,26)$; **е)** $18x\equiv 81(\mathrm{mod}\,37)$.

5. Яке з наведених порівнянь не має розв'язків?

а) $8x\equiv 5(\mathrm{mod}\,4)$; **б)** $5x\equiv 8(\mathrm{mod}\,4)$; **в)** $3x=5(\mathrm{mod}\,4)$; **г)** $3x\equiv 0(\mathrm{mod}\,4)$.

6. Яке з наведених порівнянь має один розв'язок?

а) $7x\equiv 14(\mathrm{mod}\,7)$; **б)** $2x\equiv 31(\mathrm{mod}\,10)$;
в) $7x=6(\mathrm{mod}\,8)$; **г)** $5x\equiv 43(\mathrm{mod}\,10)$.

7. Яке з наведених порівнянь має нескінченно багато розв'язків?

а) $6x\equiv 7(\mathrm{mod}\,9)$; **б)** $19x\equiv 4(\mathrm{mod}\,11)$; **в)** $7x=8(\mathrm{mod}\,6)$; **г)** $18x\equiv 36(\mathrm{mod}\,6)$.

8. Яка з наведених систем порівнянь не має розв'язків?

а) $\begin{cases}x\equiv 21(\mathrm{mod}\,45),\\ x\equiv 3(\mathrm{mod}\,18);\end{cases}$ **б)** $\begin{cases}x\equiv 21(\mathrm{mod}\,36),\\ x\equiv 3(\mathrm{mod}\,18);\end{cases}$ **в)** $\begin{cases}x\equiv 25(\mathrm{mod}\,45),\\ x\equiv 5(\mathrm{mod}\,35);\end{cases}$ **г)** $\begin{cases}x\equiv 25(\mathrm{mod}\,35),\\ x\equiv 2(\mathrm{mod}\,21).\end{cases}$

Завдання для аудиторної роботи

Приклад 1. Знайти обернений елемент для елемента 79 у кільці Z_{211}.

Р о з в ' я з а н н я. Застосуємо алгоритм Евкліда:

211 | 79	79 | 53	53 | 26	26 | 1
158 | 2	53 | 1	52 | 2	26 | 26
53	26	1	0

$\Rightarrow$ НСД(211, 79)=1.

Отже, обернений елемент до елемента 79 у кільці Z_{211} існує.

$1=53-2\cdot 26=53-2\cdot(79-53)=3\cdot 53-2\cdot 79=3\cdot(211-2\cdot 79)-2\cdot 79=3\cdot 211-8\cdot 79.$

Алгоритм дав нам рівність $3\cdot 211-8\cdot 79=1$, що еквівалентно тотожності $-8\cdot 79\equiv 1(\mathrm{mod}\,211)$. Таким чином, $79^{-1}(\mathrm{mod}\,211)\equiv -8(\mathrm{mod}\,211)\equiv 203(\mathrm{mod}\,211)$.

Приклад 2. Знайти обернений елемент для елемента 5 у кільці Z_{11}.

Р о з в ' я з а н н я. Оскільки модуль невеликий і НСД(11,5)=1, то можна застосувати теорему Ейлера: $a^{-1} \equiv a^{\varphi(m)-1} (\mathrm{mod}\, m)$.

$5^{-1} \equiv 5^{\varphi(11)-1} (\mathrm{mod}\, 11) \equiv 5^{10-1} (\mathrm{mod}\, 11) \equiv 5^9 (\mathrm{mod}\, 11) \equiv (5^3)^3 (\mathrm{mod}\, 11) \equiv (125)^3 (\mathrm{mod}\, 11) \equiv$
$\equiv 4^3 (\mathrm{mod}\, 11) \equiv 64 (\mathrm{mod}\, 11) \equiv 9 (\mathrm{mod}\, 11)$.

Приклад 3. Знайти обернену матрицю A^{-1} для матриці $A = \begin{pmatrix} 5 & 15 \\ 5 & 3 \end{pmatrix}$ у кільці лишків Z_{17}.

Р о з в ' я з а н н я: $A^{-1} = (\det A)^{-1} \begin{pmatrix} A_{11} & A_{21} \\ A_{12} & A_{22} \end{pmatrix} (\mathrm{mod}\, n)$;

$$\det A = \begin{vmatrix} 5 & 15 \\ 5 & 3 \end{vmatrix} (\mathrm{mod}\, 17) \equiv 15 - 75 \equiv -60 (\mathrm{mod}\, 17) \equiv 8 (\mathrm{mod}\, 17).$$

НСД$(\det A, n)$ = НСД$(8,17) = 1$, тому обернена матриця в кільці Z_{17} існує.

$$(\det A)^{-1} (\mathrm{mod}\, 17) \equiv 8^{-1} (\mathrm{mod}\, 17) = 15 (\mathrm{mod}\, 17).$$

Обчислюємо алгебраїчні доповнення елементів матриці:

$$A_{11} \equiv 3 (\mathrm{mod}\, 17);\ A_{12} \equiv -5 (\mathrm{mod}\, 17) \equiv 12 (\mathrm{mod}\, 17);$$
$$A_{21} \equiv -15 (\mathrm{mod}\, 17) \equiv 2 (\mathrm{mod}\, 17);\ A_{22} \equiv 5 (\mathrm{mod}\, 17).$$

$$A^{-1} = 15 \begin{pmatrix} 3 & 2 \\ 12 & 5 \end{pmatrix} (\mathrm{mod}\, 17) = \begin{pmatrix} 45 & 30 \\ 180 & 75 \end{pmatrix} (\mathrm{mod}\, 17) \equiv \begin{pmatrix} 11 & 13 \\ 10 & 7 \end{pmatrix} (\mathrm{mod}\, 17).$$

Приклад 4. Довести, що $(p-1)! + 1 \equiv 0 (\mathrm{mod}\, p)$, де p – просте число (теорема Вільсона).

Д о в е д е н н я. $Z_p = \{1,2,...,p-1\}$ – зведена система лишків за модулем p. Для кожного лишка x цієї системи існує єдиний обернений елемент x^{-1} із цієї ж системи, для якого $x^{-1} x \equiv 1 (\mathrm{mod}\, p)$. Відзначимо, що порівняння $xx \equiv 1 (\mathrm{mod}\, p)$ виконується тільки для двох чисел: $x = 1$ і $x = p-1$. Решта елементів $x \in \{2,3,...,p-2\}$ не збігається із своїми оберненими елементами $x^{-1} \in \{2,3,...,p-2\}$, тобто для них $x^{-1} x \equiv 1 (\mathrm{mod}\, p)$ і $x \neq x^{-1}$. А отже, буде правильним порівняння $2 \cdot 3 \cdot ... \cdot (p-2) \equiv 1 \mathrm{mod}\, p$. Помноживши обидві частини останнього порівняння на $1 \cdot (p-1)$, дістанемо

$1 \cdot 2 \cdot 3 \cdot ... \cdot (p-2)(p-1) \equiv (p-1) \mathrm{mod}\, p$ або $(p-1)! \equiv p-1 \mathrm{mod}\, p$.

Врахувавши, що $p \equiv 0 \mathrm{mod}\, p$, приходимо до порівняння $(p-1)! + 1 \equiv 0 (\mathrm{mod}\, p)$, що й треба було довести.

Приклад 5. Знайти розв'язки системи рівнянь $\begin{cases} x + 2z = 1, \\ y + 2z = 2, \\ 2x + z = 1 \end{cases}$ у кільці Z_5.

Р о з в ' я з а н н я. За методом Крамера:

$$\Delta = \begin{vmatrix} 1 & 0 & 2 \\ 0 & 1 & 2 \\ 2 & 0 & 1 \end{vmatrix} (\mathrm{mod}\, 5) \equiv 1 - 4 (\mathrm{mod}\, 5) \equiv -3 (\mathrm{mod}\, 5) \equiv 2 (\mathrm{mod}\, 5);\ 2^{-1} (\mathrm{mod}\, 5) = 3 (\mathrm{mod}\, 5);$$

$$\Delta_1 = \begin{vmatrix} 1 & 0 & 2 \\ 2 & 1 & 2 \\ 1 & 0 & 1 \end{vmatrix} (\mathrm{mod}\, 5) \equiv 1 - 2 (\mathrm{mod}\, 5) \equiv -1 (\mathrm{mod}\, 5) \equiv 4 (\mathrm{mod}\, 5);$$

$$\Delta_2 = \begin{vmatrix} 1 & 1 & 2 \\ 0 & 2 & 2 \\ 2 & 1 & 1 \end{vmatrix} (\mathrm{mod}\, 5) \equiv 2 + 4 - 8 - 2 (\mathrm{mod}\, 5) \equiv -4 (\mathrm{mod}\, 5) \equiv 1 (\mathrm{mod}\, 5);$$

$$\Delta_3 = \begin{vmatrix} 1 & 0 & 1 \\ 0 & 1 & 2 \\ 2 & 0 & 1 \end{vmatrix} (\mathrm{mod}\, 5) \equiv 1 - 2 (\mathrm{mod}\, 5) \equiv -1 (\mathrm{mod}\, 5) \equiv 4 (\mathrm{mod}\, 5).$$

$x = \Delta_1 \cdot \Delta^{-1} \equiv 4 \cdot 3 (\mathrm{mod}\, 5) \equiv 12 (\mathrm{mod}\, 5) \equiv 2 (\mathrm{mod}\, 5);$

$y = \Delta_2 \cdot \Delta^{-1} \equiv 1 \cdot 3 (\mathrm{mod}\, 5) \equiv 3 (\mathrm{mod}\, 5);$

$z = \Delta_3 \cdot \Delta^{-1} \equiv 4 \cdot 3 (\mathrm{mod}\, 5) \equiv 12 (\mathrm{mod}\, 5) \equiv 2 (\mathrm{mod}\, 5).$

Цю систему рівнянь можна було розв'язати і за допомогою оберненої матриці $X = A^{-1} B$, зводячи всі результати за модулем 5.

Приклад 6. Випробовуючи лишки повної системи за модулем 7, розв'язати порівняння $2x \equiv 38 (\mathrm{mod}\, 7)$.

Р о з в ' я з а н н я. Оскільки $38 \equiv 3 (\mathrm{mod}\, 7)$, то $2x \equiv 3 (\mathrm{mod}\, 7)$.
НСД$(2,7) = 1$, порівняння має єдиний розв'язок. По черзі перевіримо лишки повної системи за модулем 7, а саме – числа 0,1,2,3,4,5,6:

$1) x = 0 \Rightarrow 0 \not\equiv 3 (\mathrm{mod}\, 7)$ $\quad 2) x = 1 \Rightarrow 2 \not\equiv 3 (\mathrm{mod}\, 7);$
$3) x = 2 \Rightarrow 4 \not\equiv 3 (\mathrm{mod}\, 7);$ $\quad 4) x = 3 \Rightarrow 6 \not\equiv 3 (\mathrm{mod}\, 7);$
$5) x = 4 \Rightarrow 8 \not\equiv 3 (\mathrm{mod}\, 7);$ $\quad 6) x = 5 \Rightarrow 10 \equiv 3 (\mathrm{mod}\, 7) \Rightarrow x \equiv 5 (\mathrm{mod}\, 7).$

Приклад 7. Розв'язати порівняння $4x - 5 \equiv 0 (\mathrm{mod}\, 197)$, використовуючи еквівалентні перетворення.

Р о з в ' я з а н н я. За умовою $4x \equiv 5 (\mathrm{mod}\, 197)$; $a = 4$; $b = 5$; $m = 197$. Число a невелике, тому перебором встановлюємо, що $(b + km) \vdots a$ при $k = 3$, тобто $(5 + 3 \cdot 197) : 4 = 596 : 4 = 149$. Розв'язком порівняння є

$$x \equiv \frac{596}{4} (\mathrm{mod}\, 197) \equiv 149 (\mathrm{mod}\, 197).$$

Приклад 8. Розв'язати порівняння $5x \equiv 8 (\mathrm{mod}\, 14)$ за допомогою теореми Ейлера.

Р о з в ' я з а н н я: $a=5$; $b=8$; $m=14$; НСД$(5,14)=1$. Обчислюємо функцію Ейлера $\varphi(14)=\varphi(2\cdot 7)=\varphi(2)\cdot\varphi(7)=(2-1)(7-1)=6$.

$$x \equiv b \cdot a^{\varphi(m)-1} (\mathrm{mod}\, m) \equiv 8 \cdot 5^{6-1} (\mathrm{mod}\, 14) \equiv 25000 (\mathrm{mod}\, 14) \equiv 10 (\mathrm{mod}\, 14) \Rightarrow$$
$$\Rightarrow x \equiv 10 (\mathrm{mod}\, 14).$$

Приклад 9. Розв'язати порівняння $1081x \equiv 118 (\mathrm{mod}\, 2924)$ за допомогою алгоритму Евкліда.

Р о з в ' я з а н н я:

2924	1081	1081	762	762	319	319	124
2162	2	762	1	638	2	248	2
762		319		124		71	

124	71	71	53	53	18	18	17
71	2	53	1	36	2	17	1
53		18		17		1	

$\Rightarrow$ НСД$(1081, 2924)=1$.

$$1=18-17=18-(53-2\cdot 18)=3\cdot 18-53=3(71-53)-53=3\cdot 71-4\cdot 53=$$
$$=3\cdot 71-4(124-71)=7\cdot 71-4\cdot 124=7(319-2\cdot 124)-4\cdot 124=7\cdot 319-18\cdot 124=$$
$$=7\cdot 319-18(762-2\cdot 319)=43\cdot 319-18\cdot 762=43\cdot(1081-762)-18\cdot 762=$$
$$=43\cdot 1081-61\cdot 762=43\cdot 1081-61(2924-2\cdot 1081)=165\cdot 1081-61\cdot 2924,$$

тобто $1=165\cdot 1081-61\cdot 2924$. Звідси $1081^{-1} (\mathrm{mod}\, 2924) \equiv 165 (\mathrm{mod}\, 2924)$.

$$x \equiv 118\cdot 1081^{-1} (\mathrm{mod}\, 2924) \equiv 118\cdot 165 (\mathrm{mod}\, 2924) \equiv 19470 \equiv 1926 (\mathrm{mod}\, 2924).$$

Приклад 10. Розв'язати порівняння $196x \equiv 77 (\mathrm{mod}\, 91)$.

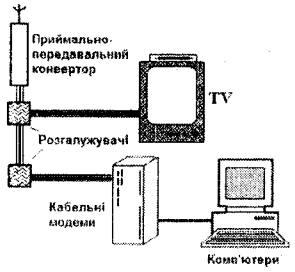
Р о з в ' я з а н н я. Оскільки $196 \equiv 14 (\mathrm{mod}\, 91)$, то $14x \equiv 77 (\mathrm{mod}\, 91)$. $a=14$, $b=77$, $m=91$. Визначаємо $d=$НСД$(14,91)=7$. Число $b=77$ ділиться на $d=7$, тому дане порівняння має 7 розв'язків. Діємо за планом: 1) скорочуємо обидві частини і модуль заданого порівняння на $d=7$, отримаємо $2x \equiv 11 (\mathrm{mod}\, 13)$; 2) знаходимо розв'язок x_0 цього порівняння у будь-який спосіб. Наприклад, за допомогою теореми Ейлера $\varphi(13)=13-1=12$, і тоді

$$x_0 \equiv 11\cdot 2^{\varphi(13)-1} (\mathrm{mod}\, 13) \equiv 11\cdot 2^{11} (\mathrm{mod}\, 13) \equiv 22528 \equiv 12 (\mathrm{mod}\, 13);$$

3) усі корені вихідного порівняння визначаємо за формулою $x = x_0 + \frac{mk}{d}$, де $k=0,1,2,\ldots,d-1$, тобто $x = 12 + \frac{91k}{7} = 12+13k$, $k=0,1,2,3,4,5,6$. Підставивши k,

отримаємо сім коренів порівняння: $12 (\mathrm{mod}\, 91)$, $25 (\mathrm{mod}\, 91)$, $38 (\mathrm{mod}\, 91)$, $51 (\mathrm{mod}\, 91)$, $64 (\mathrm{mod}\, 91)$, $77 (\mathrm{mod}\, 91)$, $90 (\mathrm{mod}\, 91)$.

Приклад 11. На рисунку наведено приклад організації бездротового доступу до мережі INTERNET та передачі телевізійних сигналів за допомогою *MMDS* мережі на базі приймально-передавального конвертора *SIDK*. Робота одного TV-каналу потребує смуги частот шириною 5 МГц, а для доступу до INTERNET на кожен модем потрібно виділити смугу частот шириною 7 МГц. Скільки TV-каналів і кабельних модемів можна підключити до конвертора, якщо конвертор передбачає використання частотного діапазону шириною 283 Мгц? Бажано, щоб кількості каналів для TV та для кабельних модемів були майже однаковими.



Р о з в ' я з а н н я. Нехай конвертор забезпечує n каналів TV та m каналів для модемів, $n,m \in N$. Тоді $5n+7m=283$. Це рівняння еквівалентне порівнянню $5n \equiv 283 (\mathrm{mod}\, 7)$ або після зведення $5n \equiv 3 (\mathrm{mod}\, 7)$. Перебором встановлюємо, що $n = 2 \bmod 7$ або $n = 2+7k$, $k=0,\pm 1,\pm 2,\ldots$ $n \approx m$ при $k=3$. Отже, $n=23$, $m=24$.

Приклад 12. Розв'язати систему порівнянь $\begin{cases} x \equiv 12 (\mathrm{mod}\, 20), \\ x \equiv 6 (\mathrm{mod}\, 7) \end{cases}$ за допомогою підстановки.

Р о з в ' я з а н н я. Система має розв'язки, бо НСД$(m_1,m_2)=$ НСД$(20,7)=1$. З першого порівняння визначаємо невідоме $x=12+20t$, $t=0,\pm 1,\pm 2,\ldots$ і підставляємо цей вираз у друге порівняння: $12+20t \equiv 6 (\mathrm{mod}\, 7)$. Тоді $20t \equiv -6 (\mathrm{mod}\, 7)$. Звівши 20 та -6 за модулем 7, дістанемо $6t \equiv 1 (\mathrm{mod}\, 7)$, звідки визначаємо випробуванням лишків повної системи, що $t \equiv 6 (\mathrm{mod}\, 7) \Rightarrow$ $\Rightarrow t = 6+7k$, $k=0,\pm 1,\pm 2,\ldots$ Підставимо це значення t у вираз для x:
$x = 12+20t = 12+20(6+7k) = 132+140k \Rightarrow x \equiv 132 \bmod 140$.

Приклад 13. Розв'язати систему порівнянь $\begin{cases} x \equiv 8 (\mathrm{mod}\, 18), \\ x \equiv 2 (\mathrm{mod}\, 7), \\ x \equiv 3 (\mathrm{mod}\, 5) \end{cases}$ за допомогою китайської теореми про остачі.

Р о з в ' я з а н н я. Модулі порівнянь попарно взаємно прості, бо НСД(18,7) = НСД(18,5) = НСД(7,5) = 1. Обчислюємо найменше спільне кратне модулів $M = 18\cdot 7\cdot 5 = 630$. Згідно з китайською теоремою про остачі складаємо допоміжні порівняння $\frac{M}{m_i} y_i \equiv 1 (\mathrm{mod}\, m_i)$, $i=1,2,3$ та розв'язуємо їх:

$$\frac{630}{18}y_1 \equiv 1(\mathrm{mod}\,18) \Rightarrow 35y_1 \equiv 1(\mathrm{mod}\,18) \Rightarrow 17y_1 \equiv 1(\mathrm{mod}\,18) \Rightarrow y_1 \equiv 17(\mathrm{mod}\,18);$$

$$\frac{630}{7}y_2 \equiv 1(\mathrm{mod}\,7) \Rightarrow 90y_2 \equiv 1(\mathrm{mod}\,7) \Rightarrow 6y_2 \equiv 1(\mathrm{mod}\,7) \Rightarrow y_2 \equiv 6(\mathrm{mod}\,7);$$

$$\frac{630}{5}y_3 \equiv 1(\mathrm{mod}\,5) \Rightarrow 126y_3 \equiv 1(\mathrm{mod}\,5) \Rightarrow y_3 \equiv 1(\mathrm{mod}\,5).$$

Визначимо

$$x_0 = \frac{M}{m_1}y_1c_1 + \frac{M}{m_2}y_2c_2 + \frac{M}{m_3}y_3c_3,$$

Де $c_1 = 8$, $c_2 = 2$, $c_3 = 3$ – праві частини порівнянь системи.

$x_0 = 35\cdot 17\cdot 8 + 90\cdot 6\cdot 2 + 126\cdot 1\cdot 3 = 6218$. Тоді $x \equiv 6218(\mathrm{mod}\,630) \equiv 548(\mathrm{mod}\,630)$.

Приклад 14. За допомогою китайської теореми про остачі обчислити $2^{6754}(\mathrm{mod}\,1155)$.

Р о з в ' я з а н н я. Розкладаємо модуль на прості множники: $1155 = 3\cdot 5\cdot 7\cdot 11$. Застосовуємо теорему Ферма до кожного з цих простих множників: $a^{p-1} \equiv 1(\mathrm{mod}\,p)$, де p – просте, НСД$(a,p) = 1$.

$$2^{6754}(\mathrm{mod}\,3) \equiv (2^2)^{3377}(\mathrm{mod}\,3) \equiv (1)^{3377}(\mathrm{mod}\,3) \equiv 1\,\mathrm{mod}\,3;$$
$$2^{6754}(\mathrm{mod}\,5) \equiv (2^4)^{1688}\cdot 4(\mathrm{mod}\,5) \equiv (1)^{1688}\cdot 4(\mathrm{mod}\,5) \equiv 4\,\mathrm{mod}\,5;$$
$$2^{6754}(\mathrm{mod}\,7) \equiv (2^6)^{1125}\cdot 2^4(\mathrm{mod}\,7) \equiv (1)^{1125}\cdot 16(\mathrm{mod}\,7) \equiv 2\,\mathrm{mod}\,7;$$
$$2^{6754}(\mathrm{mod}\,11) \equiv (2^{10})^{675}\cdot 2^4(\mathrm{mod}\,11) \equiv (1)^{1125}\cdot 16(\mathrm{mod}\,11) \equiv 5\,\mathrm{mod}\,11.$$

Тоді розв'язком системи $\begin{cases} x \equiv 1(\mathrm{mod}\,3), \\ x \equiv 4(\mathrm{mod}\,5), \\ x \equiv 2(\mathrm{mod}\,7), \\ x \equiv 5(\mathrm{mod}\,11) \end{cases}$ буде лишок $2^{6754}(\mathrm{mod}\,1155)$.

$$\frac{1155}{3}y_1 \equiv 1(\mathrm{mod}\,3) \Rightarrow 385y_1 \equiv 1(\mathrm{mod}\,3) \Rightarrow y_1 \equiv 1(\mathrm{mod}\,3);$$

$$\frac{1155}{5}y_2 \equiv 1(\mathrm{mod}\,5) \Rightarrow 231y_2 \equiv 1(\mathrm{mod}\,5) \Rightarrow y_2 \equiv 1(\mathrm{mod}\,5);$$

$$\frac{1155}{7}y_3 \equiv 1(\mathrm{mod}\,7) \Rightarrow 165y_3 \equiv 1(\mathrm{mod}\,7) \Rightarrow 4y_3 \equiv 1(\mathrm{mod}\,7) \Rightarrow y_3 \equiv 2(\mathrm{mod}\,7);$$

$$\frac{1155}{11}y_4 \equiv 1(\mathrm{mod}\,11) \Rightarrow 105y_4 \equiv 1(\mathrm{mod}\,11) \Rightarrow 6y_4 \equiv 1(\mathrm{mod}\,11) \Rightarrow y_4 \equiv 2(\mathrm{mod}\,11);$$

$$x_0 = 385\cdot 1\cdot 1 + 231\cdot 1\cdot 4 + 165\cdot 2\cdot 2 + 105\cdot 2\cdot 5 = 3019 \Rightarrow$$
$$\Rightarrow 2^{6754}(\mathrm{mod}\,1155) \equiv 3019(\mathrm{mod}\,1155) \equiv 709\,\mathrm{mod}\,1155.$$

Приклад 15. Праворуч від числа 428 приписати такі три цифри, щоб отримане число ділилось без остачі на 8, 7 і 3.

Р о з в ' я з а н н я. Після приписування праворуч від числа 428 трьох цифр отримуємо нове число $428\cdot 10^3 + x$. За умовою дістанемо систему:

$$\begin{cases} 428\cdot 10^3 + x \equiv 0\,\mathrm{mod}\,3, \\ 428\cdot 10^3 + x \equiv 0\,\mathrm{mod}\,7, \\ 428\cdot 10^3 + x \equiv 0\,\mathrm{mod}\,8 \end{cases} \text{ або } \begin{cases} x \equiv -428\cdot 10^3\,\mathrm{mod}\,3, \\ x \equiv -428\cdot 10^3\,\mathrm{mod}\,7, \\ x \equiv -428\cdot 10^3\,\mathrm{mod}\,8. \end{cases}$$

Модулі порівнянь взаємно прості, тому система має один розв'язок за модулем $M = \mathrm{НОК}(3,7,8)=168$. Отже, $x \equiv -428\cdot 10^3(\mathrm{mod}\,168)$. Зводимо за модулем 168:

$x \equiv 76\cdot 10^3(\mathrm{mod}\,168) = 64\,\mathrm{mod}\,168$ або $x = 64 + 168\,t$, де $t = 0,1,2,...$

Таким чином, праворуч від числа 428 можна приписати такі цифри 064, 232, 400, 568, 728, 896,...

Завдання для домашньої роботи

1. Указати всі елементи кільця лишків за модулем 21, для яких існують обернені елементи.

(*Відповідь*: 1,2,4,5,8,10,11,13,16,17,19,20).

2. Знайти обернений елемент до: а) елемента 113 у кільці Z_{137}; б) елемента 56 у кільці Z_{109}; в) елемента 111 у кільці Z_{131}; г) елемента 323 у кільці Z_{1173}.

(*Відповідь*: а) $97\,\mathrm{mod}\,137$; б) $37\,\mathrm{mod}\,109$; в) $72\,\mathrm{mod}\,131$; г) не існує).

3. Знайти обернену матрицю A^{-1} для матриці а) $A = \begin{pmatrix} 7 & 8 \\ 26 & 21 \end{pmatrix}$ у кільці лишків Z_{34}; б) $A = \begin{pmatrix} 2 & 14 & 3 \\ 4 & 15 & 5 \\ 0 & 16 & 0 \end{pmatrix}$ у кільці лишків Z_{27}.

(*Відповідь*: а) $\begin{pmatrix} 3 & 28 \\ 6 & 1 \end{pmatrix}\mathrm{mod}\,34$; б) $\begin{pmatrix} 11 & 15 & 5 \\ 0 & 0 & 22 \\ 2 & 26 & 11 \end{pmatrix}\mathrm{mod}\,27$).

4. Знайти розв'язки системи рівнянь $\begin{cases} 3x + y + 2z = 1, \\ x + 2y + 3z = 1, \\ 4x + 3y + 2z = 1 \end{cases}$

а) у кільці Z_5; б) у кільці Z_7.

(*Відповідь*: а) несумісна; б) $x = 2$; $y = 6$, $z = 5$).

5. Розв'язати порівняння: а) $5x \equiv 7 (\mathrm{mod}\, 8)$; б) $2x \equiv 13 (\mathrm{mod}\, 15)$; в) $29x \equiv 35 (\mathrm{mod}\, 123)$; г) $111x \equiv 49 (\mathrm{mod}\, 179)$; д) $73x \equiv 39 (\mathrm{mod}\, 28)$; е) $18x \equiv 12 (\mathrm{mod}\, 30)$; ж) $12x \equiv 16 (\mathrm{mod}\, 28)$; и) $17x \equiv 15 (\mathrm{mod}\, 34)$.

(*Відповідь*: а) $x \equiv 3 (\mathrm{mod}\, 8)$; б) $x \equiv 14 (\mathrm{mod}\, 15)$; в) $x \equiv 103 (\mathrm{mod}\, 123)$; г) $x \equiv 123 (\mathrm{mod}\, 179)$; д) $x \equiv 27 (\mathrm{mod}\, 28)$; е) $x_1 \equiv 4 (\mathrm{mod}\, 30)$, $x_2 \equiv 9 (\mathrm{mod}\, 30)$, $x_3 \equiv 14 (\mathrm{mod}\, 30)$, $x_4 \equiv 19 (\mathrm{mod}\, 30)$, $x_5 \equiv 24 (\mathrm{mod}\, 30)$, $x_6 \equiv 29 (\mathrm{mod}\, 30)$; ж) $x_1 \equiv 6 (\mathrm{mod}\, 28)$, $x_2 \equiv 13 (\mathrm{mod}\, 28)$, $x_3 \equiv 20 (\mathrm{mod}\, 28)$, $x_4 \equiv 27 (\mathrm{mod}\, 28)$; и) $\varnothing$).

6. Розв'язати системи порівнянь: а) $\begin{cases} x \equiv 100 (\mathrm{mod}\, 211), \\ x \equiv 10 (\mathrm{mod}\, 79); \end{cases}$ б) $\begin{cases} x \equiv 13 (\mathrm{mod}\, 17), \\ x \equiv 7 (\mathrm{mod}\, 23); \end{cases}$

в) $\begin{cases} 4x \equiv 3 (\mathrm{mod}\, 25), \\ 3x \equiv 8 (\mathrm{mod}\, 20); \end{cases}$ г) $\begin{cases} x \equiv 11 (\mathrm{mod}\, 12), \\ x \equiv 4 (\mathrm{mod}\, 7), \\ x \equiv 4 (\mathrm{mod}\, 5); \end{cases}$ д) $\begin{cases} x \equiv 2 (\mathrm{mod}\, 9), \\ x \equiv 10 (\mathrm{mod}\, 11), \\ x \equiv 6 (\mathrm{mod}\, 13); \end{cases}$ е) $\begin{cases} x \equiv 5 (\mathrm{mod}\, 9), \\ x \equiv 5 (\mathrm{mod}\, 7), \\ x \equiv 3 (\mathrm{mod}\, 10). \end{cases}$

(*Відповідь*: а) $9806 (\mathrm{mod}\, 16\,669)$; б) $30 (\mathrm{mod}\, 391)$; в) $\varnothing$; г) $179 (\mathrm{mod}\, 420)$; д) $461 (\mathrm{mod}\, 1287)$; е) $383 (\mathrm{mod}\, 630)$).

7. За допомогою китайської теореми про остачі знайти остачу від ділення числа: а) $2^{45\,632}$ на 12155; б) $2^{54\,632}$ на 12155.

8. Праворуч від числа 25 приписати таке найменше тризначне число, щоб отримане п'ятизначне число ділилось без остачі на 8, 6 і 3. У відповідь запишіть це п'ятизначне число.

(*Відповідь*: 25104).

2.5. Афінні шифри. Основи криптосистеми RSA

Тестові завдання для перевірки теоретичних знань

1. Записати 8 перших членів лінійної конгруентної послідовності, побудованої за допомогою генератора $x_{i+1} \equiv 3x_i + 2 (\mathrm{mod}\, 7)$ при $x_0 = 15$.

а) 15,8,1,3,7,8,1,3; **б)** 15,5,6,7,0,0,0,0; **в)** 15,6,2,7,0,3,6,5; **г)** 15,5,3,4,0,2,1,5.

2. За яких умов період лінійної конгруентної послідовності, отриманої за допомогою генератора $x_{i+1} = ax_i + b (\mathrm{mod}\, 12)$, $i = 0,1,\ldots$ буде дорівнювати 12?

а) $\mathrm{НСД}(b,12) \neq 1$; **б)** $\mathrm{НСД}(b,12) = 1$; **в)** $(a-1) \not\vdots 4$; **г)** $(a-1) \vdots 4$;
д) $(a-1) \not\vdots 3$; **е)** $(a-1) \vdots 3$; **ж)** $(a-2) \not\vdots 6$; **и)** $(a-2) \vdots 6$.

3. Рівняння роботи квадратичного генератора має вигляд

$$x_{i+1} = (a_2 x_i^2 + a_1 x_i + 41) (\mathrm{mod}\, m).$$

Які умови, накладені на коефіцієнти a_1 і a_2, забезпечать максимальність періоду псевдовипадкових послідовностей, що будуються цим генератором при різних значеннях m, наведених у першому стовпці таблиці? Для відповіді поставити прочку у відповідній клітинці.

m	$a_1 \vdots 2$ $a_2 \vdots 2$	$a_1 \vdots 3$ $a_2 \vdots 3$	$a_1 \vdots 5$ $a_2 \vdots 5$	$a_2 \equiv (a_1 - 1) (\mathrm{mod}\, 2)$	$a_2 = (a_1 - 1) (\mathrm{mod}\, 4)$	$a_2 \neq 3b (\mathrm{mod}\, 9)$
10						
12						
27						

4. Псевдовипадкова числова послідовність будується за допомогою адитивного генератора Фібоначчі $x_{i+1} = (x_i + x_{i-1}) (\mathrm{mod}\, 10)$ при $x_0 = 3$; $x_1 = 4$. Записати перші члени послідовності, що стоять до початку другого періоду.

а) 3,4,7,5,9,7,6,5,3,1,3,4,7; **б)** 3,4,7,1,8,9,7,6,3,9,2,1;
в) 3,4,17,21,38,59,97,156,253; **г)** 3,4,7,11,18,39,57,92,149.

У всіх подальших тестових завданнях вважати, що вихідний текст і текст, отриманий після шифрування, написані з використанням абетки з n букв.

5. Продовжити речення: «Послідовне шифрування тексту за допомогою шифру зсуву двічі, один раз з ключем k_1, а другий – з ключем k_2, еквівалентне одноразовому застосуванню шифру зсуву з ключем ....»

а) $k_1 - k_2$; **б)** $k_1 + k_2$; **в)** $k_1 k_2$; **г)** $k_1 + k_2 - n$; **д)** $k = \max\{k_1, k_2\}$.

6. За допомогою якого ключа k' розшифровується текст, зашифрований шифром зсуву $y=(x+k)\bmod n$ з ключем $k=23$, якщо кількість букв абетки $n=35$? Вважати рівняння дешифрування $x=(y+k')\bmod n$.

а) 12; **б)** 35; **в)** −12; **г)** −35; **д)** 47.

7. Яке з нижченаведених чисел можна вибрати за ключ k для лінійного шифру для шифрування тексту, записаного з використанням абетки з 33 букв ?

а) 3; **б)** 5; **в)** 11; **г)** −3; **д)** 81.

8. Якщо текст шифрується за допомогою лінійного шифру з рівнянням $y=k_1x\bmod n$, а розшифровується за допомогою рівняння $x=k_2y\bmod n$, то з яким числом порівняний добуток $k_1k_2\bmod n$?

а) k; **б)** 0; **в)** 1; **г)** n; **д)** k^2.

9. Продовжити речення: «Послідовне шифрування тексту за допомогою шифру Хілла двічі, спершу з матрицею A, а другий раз з матрицею B, еквівалентне одноразовому застосуванню шифру Хілла з матрицею ....»

а) BA; **б)** AB; **в)** $A+B$; **г)** $A+B-n$; **д)** $A-B$.

10. Яка з нижченаведених матриць може використовуватись як матриця шифрування для шифру Хілла, якщо текст, що шифрується, записаний з використанням абетки з 33 букв і поділений на блоки, довжиною 2?

а) $A=\begin{pmatrix}2 & 5\\ 4 & 10\end{pmatrix}\bmod 33$; **б)** $A=\begin{pmatrix}7 & 5\\ 2 & 3\end{pmatrix}\bmod 33$;

в) $A=\begin{pmatrix}1 & 0\\ 0 & 1\end{pmatrix}\bmod 33$; **г)** $A=\begin{pmatrix}2 & 3\\ 4 & 7\end{pmatrix}\bmod 33$.

11. Закритий ключ шифру RSA складають числа $p=17$, $q=11$, $d=3$, відкритий – пара $n=595$ і $e=121$. Який з цих ключів вибраний *неправильно*?

а) $p=17$; **б)** $q=11$; **в)** $e=121$; **г)** $n=595$; **д)** $d=3$.

12. Закритий ключ шифру RSA складають числа $p=5$, $q=11$, $d=17$, відкритий – пара чисел $n=55$ і $e=3$. Який з цих ключів вибраний *неправильно*?

а) $p=5$; **б)** $q=11$; **в)** $e=3$; **г)** $n=55$; **д)** $d=17$.

13. З якого порівняння визначається закритий ключ d шифру RSA , якщо $p=13$, $q=7$, $e=5$, $n=91$?

а) $ed\equiv pq(\bmod 91)$; **б)** $ed\equiv pq(\bmod 72)$; **в)** $ed\equiv 1(\bmod 91)$;

г) $ed\equiv 1(\bmod 72)$; **д)** $ed\equiv p+q(\bmod 72)$; **е)** $pd\equiv eq(\bmod 112)$.

14. Якщо відкритий ключ шифру RSA просте число $e>\max\{p;q\}$, де p, q – частина закритого ключа, $n=pq$, то чому дорівнює НСД$(e,\varphi(n))$?

а) $\varphi(n)$; **б)** e; **в)** 1; **г)** $p+q$; **д)** $\max\{p;q\}$.

15. Закритий ключ шифру RSA складають числа $p=7$, $q=23$, $d=7$, відкритий – пара $n=161$ і $e=19$, крім того, $\varphi(161)=132$. Записати рівняння шифрування символу x за допомогою цього шифру.

а) $y\equiv x^7(\bmod 161)$; **б)** $y\equiv x^7(\bmod 132)$; **в)** $y\equiv x^{19}(\bmod 161)$;

г) $y\equiv x^{19}(\bmod 132)$; **д)** $y\equiv x^{23}(\bmod 7)$; **е)** $y\equiv x^7(\bmod 19)$.

16. Закритий ключ шифру RSA складають числа $p=11$, $q=17$, $d=9$, а відкритий – пара $n=187$ і $e=89$, крім того, $\varphi(187)=160$. Записати рівняння дешифрування символу y за допомогою цього шифру.

а) $x\equiv y^9(\bmod 187)$; **б)** $x\equiv y^9(\bmod 160)$; **в)** $x\equiv y^{89}(\bmod 160)$;

г) $x\equiv y^{89}(\bmod 187)$; **д)** $x\equiv y^{11}(\bmod 17)$; **е)** $x\equiv y^{17}(\bmod 11)$.

Завдання для аудиторної роботи

Приклад 1. Чи буде псевдовипадкова числова послідовність, побудована лінійним конгруентним генератором $x_{i+1}=171x_i+11213(\bmod 53125)$, мати максимальний період?

Р о з в ' я з а н н я. НСД $(b,m)=$НСД $(11213, 53125)=1$. Розкладаємо модуль на прості множники: $53125=5^5\cdot 17$. Число $a-1=171-1=170$ ділиться націло на 5 і на 17, тобто на кожний простий дільник модуля. За цих умов побудована послідовність буде мати максимальний період 53125.

Приклад 2. Чи буде псевдовипадкова числова послідовність, побудована квадратичним конгруентним генератором $x_{i+1}=(30x_i^2+60x_i+11)(\bmod 90)$, мати максимальний період?

Р о з в ' я з а н н я. НСД $(b,m)=$НСД $(11, 90)=1$. Розкладаємо модуль на прості множники: $90=2\cdot 3^2\cdot 5$. Числа $a_2=30$ і $a_1=60$ діляться націло на кожний простий дільник модуля.

Перевіряємо умову $a_2\neq 3b(\bmod 9)$ або $a_2=30\neq 3\cdot 11(\bmod 9)$. Отже, період побудованої генератором послідовності – максимальний і дорівнює 90.

Приклад 3. Записати 5 перших членів псевдовипадкової послідовності, побудованої за допомогою інверсивного конгруентного генератора, рівняння роботи якого $x_{i+1}=3\cdot x_i^{-1}+6(\bmod 7)$ при $x_1=4$.

Розв'язання:

$x_1^{-1} = 4^{-1} \bmod 7 \equiv 2 \bmod 7 \Rightarrow x_2 = 3 \cdot 2 + 6 (\bmod 7) \equiv 5 \bmod 7;$

$x_2^{-1} = 5^{-1} \bmod 7 \equiv 3 \bmod 7 \Rightarrow x_3 = 3 \cdot 3 + 6 (\bmod 7) \equiv 1 \bmod 7;$

$x_3^{-1} = 1^{-1} \bmod 7 \equiv 1 \bmod 7 \Rightarrow x_4 = 3 \cdot 1 + 6 (\bmod 7) \equiv 2 \bmod 7;$

$x_4^{-1} = 2^{-1} \bmod 7 \equiv 4 \bmod 7 \Rightarrow x_5 = 3 \cdot 4 + 6 (\bmod 7) \equiv 4 \bmod 7.$

Отримали послідовність 4, 5, 1, 2, 4, ...

Приклад 4. За допомогою генератора BBS побудувати двійкову псевдовипадкову послідовність.

Розв'язання. Оскільки $19 \equiv 3 (\bmod 4)$, $23 \equiv 3 (\bmod 4)$ – прості числа, то виберемо $p = 19$, $q = 23$, $n = p \cdot q = 19 \cdot 23 = 437$. Число $x = 601$ – взаємно просте з модулем $n = 437$ (НСД$(601, 437) = 1$). Далі обчислюємо

$x_0 \equiv x^2 (\bmod n) \equiv 601^2 (\bmod 437) \equiv 239;$ $\quad b_1 = x_0 (\bmod 2) = 239 (\bmod 2) = 1;$

$x_1 = x_0^2 (\bmod n) = 239^2 (\bmod 437) = 311;$ $\quad b_2 = x_1 (\bmod 2) = 311 (\bmod 2) = 1;$

$x_2 = x_1^2 (\bmod n) = 311^2 (\bmod 437) = 144;$ $\quad b_3 = x_2 (\bmod 2) = 144 (\bmod 2) = 0;$

$x_3 = x_1^2 (\bmod n) = 144^2 (\bmod 437) = 197;$ $\quad b_4 = x_3 (\bmod 2) = 197 (\bmod 2) = 1;$

$x_4 = x_1^2 (\bmod n) = 197^2 (\bmod 437) = 363;$ $\quad b_5 = x_3 (\bmod 2) = 363 (\bmod 2) = 1.$

Шукана псевдовипадкова двійковою послідовність 1 1 0 1 1 ...

Приклад 5. Кожну букву деякого відкритого тексту замінили її номером в українській абетці згідно з таблицею, наведеною у додатку Б. Отримане в результаті цифрове повідомлення зашифрували за допомогою афінного шифру за рівнянням шифрування $y \equiv 7x + 25 \bmod 33$, де x і y – цифрові еквіваленти букви в повідомленні і шифрограмі відповідно. Від шифрограми у цифровій формі за тією ж таблицею перейшли до буквеного запису та дістали «Ц П Е Г Ю Г Ї П». Відновити відкритий текст.

Розв'язання. Повернемось до цифрової форми шифрограми. За таблицею у додатку встановлюємо, що букві «Ц» відповідає номер 26 в українській абетці, букві «П» – 19 і т.д. Уся шифрограма в цифровому записі – це послідовність «26 19 06 03 31 04 12 09».

Із рівняння шифрування визначаємо:

$y \equiv 7x + 25 \bmod 33 \Rightarrow 7x + 25 \equiv y \bmod 33 \Rightarrow 7x \equiv y - 25 \bmod 33 \Rightarrow$

$\Rightarrow x \equiv 7^{-1} (y - 25) \bmod 33.$

Шукаємо $7^{-1} (\bmod 33)$. За алгоритмом Евкліда: $33 = 7 \cdot 4 + 5$, $7 = 5 \cdot 1 + 2$, $5 = 2 \cdot 2 + 1$, $2 = 2 \cdot 1 \Rightarrow$ НСД$(7, 33) = 1$.

$1 = 5 - 2 \cdot 2 = 5 - 2(7 - 5) = 3 \cdot 5 - 2 \cdot 7 = 3(33 - 4 \cdot 7) - 2 \cdot 7 = 3 \cdot 33 - 14 \cdot 7 \Rightarrow$

$\Rightarrow 7^{-1} (\bmod 33) \equiv -14 \bmod 33 \equiv 19 \bmod 33$. Тоді

$x \equiv 19(y - 25) \bmod 33 = 19y - 475 \equiv 19y + 20 \bmod 33$ – рівняння дешифрування. Підставляємо у це рівняння числові еквіваленти букв шифрограми:

$x_1 \equiv 19 \cdot 26 + 20 \bmod 33 \equiv 514 \bmod 33 \equiv 19 \bmod 33;$

$x_2 \equiv 19 \cdot 19 + 20 \bmod 33 \equiv 381 \bmod 33 \equiv 18 \bmod 33;$

$x_3 \equiv 6 \cdot 19 + 20 \bmod 33 \equiv 134 \bmod 33 \equiv 2 \bmod 33;$

$x_4 \equiv 3 \cdot 19 + 20 \bmod 33 \equiv 77 \bmod 33 \equiv 11 \bmod 33;$

$x_5 \equiv 31 \cdot 19 + 20 \bmod 33 \equiv 609 \bmod 33 \equiv 15 \bmod 33;$

$x_6 \equiv 4 \cdot 19 + 20 \bmod 33 \equiv 96 \bmod 33 \equiv 30 \bmod 33;$

$x_7 \equiv 12 \cdot 19 + 20 \bmod 33 \equiv 248 \bmod 33 \equiv 17 \bmod 33;$

$x_8 \equiv 19 \cdot 19 + 20 \bmod 33 \equiv 381 \bmod 33 \equiv 18 \bmod 33.$

Цифровий запис відкритого тексту «19 18 02 11 15 30 17 18», звідки за таблицею відповідності букв та їх номерів в українській абетці читаємо слово «ПОВІЛЬНО».

Приклад 6. Нерухомою буквою відносно застосованого афінного шифру називається буква x з властивістю: $x = kx + t (\bmod n)$, тобто при шифруванні ця буква переходить сама в себе. Скільки букв залишається нерухомими при використанні абетки з n букв?

Розв'язання. Аналізуємо кількість розв'язків порівняння $x \equiv kx + t (\bmod n)$ або $x(k - 1) = t (\bmod n)$. Якщо НСД$(k - 1, n) = 1$, то порівняння має один розв'язок і тоді існує тільки одна нерухома буква. Якщо ж НСД$(k - 1, n)$ відрізняється від 1 і буде дільником числа t, то існуватиме НСД$(k - 1, n)$ нерухомих букв. І нарешті, за умови, що число t не ділиться НСД$(k - 1, n)$, таких букв не існуватиме.

Приклад 7. Вилучивши пробіл між словами, кожну букву тексту «НЕКАЖИ» замінили її номером згідно з таблицею, наведеною у додатку Б. Отримане в результаті цифрове повідомлення записали в стовпці матриці X розмірністю 2×3 та зашифрували за допомогою шифру Хілла з рівнянням шифрування $Y = AX$, де $A = \begin{pmatrix} 2 & 4 \\ 3 & 7 \end{pmatrix} \bmod 33$. Знайти шифрограму Y тексту, записати рівняння дешифрування та перевірити його.

Розв'язання. За таблицею переводу букв української абетки в цифровий еквівалент знаходимо, що «Н» відповідає номер 17, букві «Е» – 06 і т.д. Цифрова форма запису всього тексту «НЕКАЖИ» – це «17 06 14 00 08 10». Записуємо здобуту послідовність у стовпці матриці розмірністю 2×3: $\begin{pmatrix} 17 & 14 & 08 \\ 06 & 00 & 10 \end{pmatrix}$. За рівнянням шифрування визначаємо:

$$Y = AX = \begin{pmatrix} 2 & 4 \\ 3 & 7 \end{pmatrix} \begin{pmatrix} 17 & 14 & 08 \\ 06 & 00 & 10 \end{pmatrix} \bmod 33 \equiv \begin{pmatrix} 58 & 28 & 56 \\ 93 & 42 & 94 \end{pmatrix} \bmod 33 \equiv$$

$\equiv \begin{pmatrix} 25 & 28 & 23 \\ 27 & 9 & 28 \end{pmatrix} \bmod 33$. Результат записуємо як послідовність «25 27 28 09 23 28».

Буквений еквівалент отриманої шифрограми: «Х Ч Ш З У Ш».

Запишемо рівняння дешифрування: $X = A^{-1}Y$, де A^{-1} – обернена матриця до матриці A. Шукаємо A^{-1} у кільці лишків Z_{33}.

$$\Delta = \begin{vmatrix} 2 & 4 \\ 3 & 7 \end{vmatrix} \bmod 33 \equiv 14 - 12 \bmod 33 \equiv 2 \bmod 33.$$

$$\Delta^{-1} \equiv 2^{-1} \bmod 33 \equiv 17 \bmod 33.$$

$$A_{11} \equiv 7 \bmod 33;\ A_{12} \equiv -3 \bmod 33;\ A_{21} \equiv -4 \bmod 33;\ A_{22} \equiv 2 \bmod 33.$$

$$A^{-1} = 17 \begin{pmatrix} 7 & -4 \\ -3 & 2 \end{pmatrix} \bmod 33 = \begin{pmatrix} 119 & -68 \\ -51 & 34 \end{pmatrix} \bmod 33 \equiv \begin{pmatrix} 20 & 31 \\ 15 & 1 \end{pmatrix} \bmod 33.$$

Дешифрування: $X = A^{-1}Y \equiv \begin{pmatrix} 20 & 31 \\ 15 & 1 \end{pmatrix} \begin{pmatrix} 25 & 28 & 23 \\ 27 & 9 & 28 \end{pmatrix} \bmod 33 \equiv$

$$\equiv \begin{pmatrix} 1337 & 839 & 914 \\ 402 & 429 & 373 \end{pmatrix} \bmod 33 \equiv \begin{pmatrix} 17 & 14 & 08 \\ 06 & 00 & 10 \end{pmatrix} \bmod 33$$ або «НЕКАЖИ».

Приклад 8. Якщо у шифрі Хілла матриця для шифрування тексту збігається з матрицею, на якій ведеться розшифрування (тобто матриця A є оберненою сама до себе), то визначник матриці порівняний з ± 1 за простим модулем. Довести це.

Д о в е д е н н я. $Y \equiv AX \bmod p$, $X \equiv A^{-1}Y \bmod p$ – рівняння шифрування і дешифрування відповідно, p – просте число.

Звідси $X \equiv A^{-1}Y \bmod p \equiv A^{-1}AX \bmod p \Rightarrow X - A^{-1}AX \equiv 0 \bmod p$ або $X(E - A^{-1}A) \equiv 0 \bmod p$, де E – одинична матриця. За умовою $A = A^{-1}$, отже, $X(E - A^2) \equiv 0 \bmod p$. Оскільки $X \not\equiv 0 \bmod p$, то $A^2 \equiv E \bmod p$. Тоді $\det A^2 \equiv \det E \bmod p$ або $\det A^2 \equiv 1 \bmod p \Rightarrow \det A \equiv \pm 1 \bmod p$.

Приклад 9. Згенерувати ключі та зашифрувати за допомогою RSA повідомлення $x_1 = 4$, $x_2 = 20$, $x_3 = 15$.

Р о з в ' я з а н н я. Нехай $p = 2$, $q = 11$. Тоді $n = pq = 22$, $\varphi(n) = (p-1)(q-1) = 1 \cdot 10 = 10$. Виберемо $e = 7$, бо НСД(7,10) = 1. Число d визначаємо з порівняння $de \equiv 1 (\mathrm{mod}\,(\varphi(n))$. У нашому випадку $7d \equiv 1 (\mathrm{mod} 10)$. Оскільки $7 \cdot 3 = 21 \equiv 1 (\mathrm{mod} 10)$, то $d \equiv 3 (\mathrm{mod} 10)$. Отже, $n = 22$, $e = 7$ – відкритий ключ; $d = 3$ – закритий ключ.

За формулою $y \equiv x^e (\mathrm{mod}\, n)$ шифруємо відкритий текст:

$$y_1 \equiv 4^7 (\mathrm{mod}\, 22) \equiv 16384 (\mathrm{mod}\, 22) \equiv 16;$$

$$y_2 \equiv 20^7 (\mathrm{mod}\, 22) \equiv 1280000000 (\mathrm{mod}\, 22) = 4;$$

$$y_3 \equiv 15^7 (\mathrm{mod}\, 22) \equiv 50625 \cdot 3375 (\mathrm{mod}\, 22) \equiv 3 \cdot 9 (\mathrm{mod}\, 22) \equiv 5 (\mathrm{mod}\, 22).$$

Отже, шифроване повідомлення $y_1 = 16$, $y_2 = 4$, $y_3 = 5$.

Дешифрування: $x \equiv y^d (\mathrm{mod}\, n)$.

$$x_1 \equiv 16^3 (\mathrm{mod}\, 22) \equiv 4096 (\mathrm{mod}\, 22) \equiv 4;$$

$$x_2 \equiv 4^3 (\mathrm{mod}\, 22) \equiv 64 (\mathrm{mod}\, 22) \equiv 20 (\mathrm{mod}\, 22);$$

$$x_3 \equiv 5^3 (\mathrm{mod}\, 22) \equiv 125 (\mathrm{mod}\, 22) \equiv 15 (\mathrm{mod}\, 22).$$

Приклад 10. Відкритий ключ для шифрування повідомлень за системою RSA складається з чисел $n = 3149$, $e = 7$. Крім того, відомо значення функції Ейлера $\varphi(3149) = 3036$. Згенерувати закритий ключ та дешифрувати зашифроване повідомлення, що складається з трьох блоків: 2673, 335, 623. В отриманому цифровому записі розшифрованого повідомлення кожні дві цифри блоків визначають двоцифровий номер букви в українській абетці відповідно до таблиці додатку Б. Записати розшифрований текст.

Р о з в ' я з а н н я. Визначимо обернений елемент d до елемента $e = 7$ за модулем $\varphi(3149) = 3036$, тобто розв'язуємо порівняння $d \cdot 7 \equiv 1 (\mathrm{mod}\, 3036)$. За алгоритмом Евкліда: $3036 = 7 \cdot 433 + 5$; $7 = 5 \cdot 1 + 2$; $5 = 2 \cdot 2 + 1$; $2 = 2 \cdot 1$. Далі $1 = 5 - 2 \cdot 2 = 5 - 2(7 - 5) = 3 \cdot 5 - 2 \cdot 7 = 3(3036 - 7 \cdot 433) - 2 \cdot 7 = 3 \cdot 3036 - 1301 \cdot 7$.

$d = 7^{-1} \bmod 3036 \equiv -1301 \bmod 3036 \equiv 1735 \bmod 3036$.

Дешифрування виконуємо за формулою $x \equiv y^d (\mathrm{mod}\, n)$:

$$x_1 \equiv 2673^{1735} (\mathrm{mod}\, 3149) \equiv 2802 (\mathrm{mod}\, 3149);$$

$$x_2 \equiv 335^{1735} (\mathrm{mod}\, 3149) \equiv 1005 (\mathrm{mod}\, 3149);$$

$$x_3 \equiv 623^{1735} (\mathrm{mod}\, 3149) \equiv 1418 (\mathrm{mod}\, 3149).$$

Отримуємо цифрову форму запису розшифрованого повідомлення: 2802 1005 1418. Кожні дві цифри блоків визначають номер букви абетки: 28 02 10 09 14 18.

Користуючись таблицею додатку, за цими номерами встановлюємо букви тексту, що шифрувався: 28 – «Ш», 02 – «В», 10 – «И», 09 – «Д», 14 – «К», 18 – «О». Тепер очевидно, що шифрувалось слово «ШВИДКО».

Приклад 11. Супротивник може дізнатися значення закритого ключа d при шифруванні за системою RSA, якщо відомий розклад числа $n = pq$ на прості множники. Показати, як розкласти n на множники, якщо воно дорівнює добутку двох простих чисел-близнюків. Чи є сенс в такому виборі числа n?

Р о з в ' я з а н н я. Нехай p і q – прості числа-близнюки, тобто $q = p+2$. Тоді $n = pq = p(p+2) = p^2 + 2p$. Знайдемо $(p+1)^2 = p^2 + 2p + 1 = n+1$, тобто $n = (p+1)^2 - 1$. Послідовно перебираємо числа $t^2 > n$ і перевіряємо, чи буде різниця $t^2 - n$ точним квадратом якогось числа. Якщо таке число t знайдеться, то $t = p+1$, звідки $p = t-1$, $q = t+1$. Отже, вибирати числа-близнюки як числа p і q для шифру RSA не рекомендується.

Завдання для домашньої роботи

1. Чи буде псевдовипадкова числова послідовність, побудована лінійним конгруентним генератором $x_{i+1} = 211x_i + 1663 (\mathrm{mod}\, 7875)$, мати максимальний період?
(*Відповідь*: так).

2. Чи буде псевдовипадкова числова послідовність, побудована квадратичним конгруентним генератором $x_{i+1} = (99x_i^2 + 430x_i + 2531) \mathrm{mod}\, 11979$, мати максимальний період?
(*Відповідь*: так).

3. Записати 5 перших членів псевдовипадкової послідовності, побудованої за допомогою інверсивного конгруентного генератора, рівняння роботи якого $x_{i+1} = 8 \cdot x_i^{-1} + 9 (\mathrm{mod}\, 11)$ при $x_1 = 4$.
(*Відповідь*: 4, 0, 9, 5, 4,...).

4. За допомогою генератора BBS побудувати перші 12 членів двійкової псевдовипадкової послідовності з використанням чисел $p = 19$, $q = 23$, $x_0 = 233$.
(*Відповідь*: 101011100111).

5. Скільки букв абетки, що складається з 33 символів, залишаться нерухомими при шифруванні текстів за допомогою афінного шифру $y = 12x + 22 (\mathrm{mod}\, 33)$?
(*Відповідь*: 11 букв).

6. Кожну букву тексту «ЗУСТРІЧ» замінити її номером в українській абетці згідно з таблицею, наведеною у додатку Б. Отримане цифрове повідомлення зашифрувати за допомогою афінного шифру з рівнянням шифрування $y \equiv 13x + 16 \mathrm{mod}\, 33$, де x і y – цифрові еквіваленти букви в повідомленні і шифрограмі відповідно. Записати шифрограму тексту, знайти рівняння дешифрування та дешифрувати отриманий шифрований текст.

7. Вилучивши пробіл між словами, кожну букву тексту «НЕНАЗИВАЄМОІМЕН» замінити її номером в українській абетці згідно з таблицею, наведеною у додатку Б. Отримане в результаті цифрове повідомлення записати в стовпці

матриці X розмірністю 3×3 та зашифрувати повідомлення за допомогою шифру Хілла з рівнянням шифрування $Y = AX$, де $A = \begin{pmatrix} 3 & 2 & 6 \\ 4 & 1 & 1 \\ 1 & 2 & 3 \end{pmatrix} \mathrm{mod}\, 33$.
Знайти шифрограму тексту, записати рівняння дешифрування та перевірити його.

8. Згенерувати відкритий і закритий ключі для системи RSA на основі чисел $p = 7$, $q = 23$, $e = 7$ та зашифрувати повідомлення $x_1 = 3$, $x_2 = 15$, $x_3 = 21$.

(*Відповідь*: $y_1 = 94; y_2 = 57; y_3 = 56$).

9. Кожну букву тексту «ПОВІДОМТЕНОВИЙПАРОЛЬ» замінили її двоцифровим номером в українській абетці згідно з додатком Б. Отриману числову послідовність розбити на блоки по 4 цифри в кожному і далі зашифрувати за допомогою системи RSA з використанням відкритих ключів $n = 4189$, $e = 1229$. Для перевірки визначити закриті ключі і розшифрувати отримане шифроване повідомлення.

(*Відповідь*: 1350 1901 1479 1364 2441 2633 0604 0593 2304 2366).

10. Супротивник може дізнатися значення закритого ключа d при шифруванні за системою RSA, якщо відомий розклад числа $n = pq$ на прості множники. Показати, як розкласти n на множники, якщо різниця між числами p і q мала. Чи є сенс у такому виборі числа n?

11. $y_1 \equiv x^{e_1} (\mathrm{mod}\, n)$ і $y_2 \equiv x^{e_2} (\mathrm{mod}\, n)$ – два зашифрованих повідомлення, отримані в результаті шифрування одного й того ж вихідного тексту x за допомогою системи RSA з використанням однакового модуля і різних ключів e_1 і e_2. Показати, як можна відновити вихідне повідомлення x при відомих y_1, y_2, e_1, e_2, n, якщо виявилося, що e_1 і e_2 – взаємно прості.

(*Розв'язання*: 1) за допомогою алгоритму Евкліда визначити такі числа α і β, щоб виконувалась рівність $\alpha e_1 + \beta e_2 = 1$, тут невідмінно α і β різних знаків. Припустимо для визначеності, що $\alpha < 0$;

2) обчислити $y_1^{-1} (\mathrm{mod}\, n)$, $\left(y_1^{-1}\right)^{-\alpha} (\mathrm{mod}\, n)$, $y_2^{\beta} (\mathrm{mod}\, n)$;

3) врахувавши, що $\left(y_1^{-1}\right)^{-\alpha} (\mathrm{mod}\, n) \equiv \left(x^{-e_1}\right)^{-\alpha} (\mathrm{mod}\, n)$, $y_2^{\beta} (\mathrm{mod}\, n) \equiv x^{e_2 \beta} (\mathrm{mod}\, n)$, перемножимо ці два порівняння: $y_1^{\alpha} y_2^{\beta} (\mathrm{mod}\, n) \equiv x^{(-e_1)(-a)} x^{e_2 \beta} (\mathrm{mod}\, n) \Rightarrow$

4) $y_1^{\alpha} y_2^{\beta} (\mathrm{mod}\, n) \equiv x^{\alpha e_1 + \beta e_2} (\mathrm{mod}\, n) \equiv z (\mathrm{mod}\, n)$.

2.6. Квадратні порівняння. Критерій Ейлера. Символ Лежандра. Добування квадратних коренів за простим модулем та за модулем $n = pq$, де p, q – прості числа

Тестові завдання для перевірки теоретичних знань

1. Число a взаємно просте з числом $p > 2$ і задовольняє порівняння $a^{\frac{p-1}{2}} \equiv 1 (\mathrm{mod}\, p)$. Яке з наведених квадратних порівнянь обов'язково матиме корені?

а) $x^2 \equiv p (\mathrm{mod}\, a)$; **б)** $x^2 \equiv 1 (\mathrm{mod}\, p)$; **в)** $x^2 \equiv -a (\mathrm{mod}\, p)$;
г) $x^2 \equiv a (\mathrm{mod}\, p)$; **д)** $x^2 \equiv a (\mathrm{mod}\, p-1)$; **е)** жодне не матиме.

2. Число a взаємно просте з числом $p > 2$ і задовольняє порівняння $a^{\frac{p-1}{2}} \equiv -1 (\mathrm{mod}\, p)$. Яке з наведених квадратних порівнянь обов'язково матиме корені?

а) $x^2 \equiv p (\mathrm{mod}\, a)$; **б)** $x^2 \equiv a (\mathrm{mod}\, p+1)$; **в)** $x^2 \equiv -a (\mathrm{mod}\, p)$;
г) $x^2 \equiv a (\mathrm{mod}\, p)$; **д)** $x^2 + p^2 \equiv 1 (\mathrm{mod}\, a)$; **е)** жодне не матиме.

3. За умови, що $L(a;11) = 1$, указати серед наведених квадратних порівнянь те, що обов'язково матиме розв'язки.

а) $x^2 \equiv a - 1 (\mathrm{mod}\, 11)$; **б)** $x^2 + 11 \equiv 0 (\mathrm{mod}\, a)$; **в)** $x^2 \equiv a (\mathrm{mod}\, 11)$;
г) $x^2 \equiv 11 (\mathrm{mod}\, a)$; **д)** $x^2 \equiv a (\mathrm{mod}\, 10)$; **е)** $x^2 \equiv a (\mathrm{mod}\, 12)$.

4. За умови, що $L(17;p) = -1$, p – просте непарне, указати серед наведених квадратних порівнянь те, що обов'язково не матиме коренів.

а) $x^2 \equiv 17 (\mathrm{mod}\, p)$; **б)** $x^2 \equiv p (\mathrm{mod}\, 17)$; **в)** $x^2 \equiv -17 (\mathrm{mod}\, p)$;
г) $x^2 \equiv 16 (\mathrm{mod}\, p)$; **д)** $x^2 \equiv 17 (\mathrm{mod}\, 10)$; **е)** $x^2 \equiv 17 (\mathrm{mod}\, p-1)$.

5. Число 25 – квадратичний лишок за деяким модулем, а 3 – його квадратичний нелишок. Чи буде квадратичним лишком добуток 75 цих чисел?

а) так; **б)** ні; **в)** інша відповідь.

6. Числа 5 і 6 – квадратичні нелишки за деяким модулем. Чи буде квадратичним лишком добуток 30 за цим модулем?

а) так; **б)** ні; **в)** інша відповідь.

7. Числа $1, 3, 4, 5, 9$ – квадратичні лишки за модулем 11. Записати всі квадратичні нелишки числа 11.

а) 1, 9, 16, 25, 81; **б)** 2, 6, 7, 8, 10; **в)** 2, 3, 4, 8; **г)** 2, 4, 5, 6, 10.

8. Яке твердження правильне?

а) кількості квадратичних лишків і квадратичних нелишків за будь-яким простим непарним модулем однакові;

б) якщо $L(a;p) = 1$, то порівняння $x^2 \equiv p (\mathrm{mod}\, a)$ обов'язково має корені;

в) якщо $L(a;p) = 1$, то виконується порівняння $a^{\frac{p-1}{2}} \equiv -1 (\mathrm{mod}\, p)$;

г) якщо $L(a;p) = -1$, то виконується порівняння $a^{\frac{p-1}{2}} \equiv 1 (\mathrm{mod}\, p)$.

Завдання для аудиторної роботи

Приклад 1. Перевірити за критерієм Ейлера, чи будуть числа 7 і 13 квадратичними лишками за модулем 19.

Розв'язання. $\mathrm{НСД}(7, 19) = 1$, $\mathrm{НСД}(13, 19) = 1$. При $a = 7$ маємо

$$7^{\frac{19-1}{2}} \bmod 19 \equiv 7^9 \bmod 19 \equiv (7^3)^3 \bmod 19 \equiv 343^3 \bmod 19 \equiv (1)^3 \bmod 19 \equiv 1 \bmod 19.$$

Аналогічно при $a = 13$ дістаємо $13^{\frac{19-1}{2}} \bmod 19 \equiv 13^9 \bmod 19 \equiv 343^3 \bmod 19 \equiv (2197)^3 \bmod 19 \equiv 12^3 \bmod 19 \equiv 1728 \bmod 19 \equiv 18 \bmod 19 \equiv -1 \bmod 19$.

Отже, 7 – квадратичний лишок, а 13 – квадратичний нелишок за модулем 19.

Приклад 2. Довести, що для будь-якого простого непарного числа добуток двох квадратичних лишків або двох квадратичних нелишків є квадратичним лишком.

Доведення. Нехай $\mathrm{НСД}(a, p) = 1$ і $\mathrm{НСД}(b, p) = 1$. Тоді за критерієм Ейлера:

- якщо a і b – квадратичні лишки за простим непарним модулем p, то $a^{\frac{p-1}{2}} \equiv 1 (\mathrm{mod}\, p)$ і $b^{\frac{p-1}{2}} \equiv 1 (\mathrm{mod}\, p)$. Перемноживши почленно ці порівняння, дістаємо $(ab)^{\frac{p-1}{2}} \equiv 1 (\mathrm{mod}\, p)$;
- якщо a і b – квадратичні нелишки за простим непарним модулем p, то $a^{\frac{p-1}{2}} \equiv -1 (\mathrm{mod}\, p)$ і $b^{\frac{p-1}{2}} \equiv -1 (\mathrm{mod}\, p)$. Після множення цих порівнянь, так само дістанемо $(ab)^{\frac{p-1}{2}} \equiv 1 (\mathrm{mod}\, p)$.

Отже, в обох випадках добуток ab – квадратичний лишок за модулем p.

Приклад 3. Довести, що для будь-якого простого модуля p елемент, обернений до квадратичного лишка, є квадратичним лишком.

Д о в е д е н н я. Нехай НСД$(a, p)=1$, a – квадратичний лишок за модулем p, тобто за критерієм Ейлера $a^{\frac{p-1}{2}} \equiv 1(\mathrm{mod}\, p)$. Оскільки a^{-1} – обернений елемент до елемента a у кільці Z_p, то $1 \equiv a^{-1} \cdot a(\mathrm{mod}\, p)$ і ми можемо піднести обидві частини цього порівняння до степеня $(p-1)/2$:

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

Беручи до уваги очевидне порівняння $1^{\frac{p-1}{2}}(\mathrm{mod}\, p) \equiv 1(\mathrm{mod}\, p)$, дістанемо $\left(a^{-1}\right)^{\frac{p-1}{2}} \equiv 1(\mathrm{mod}\, p)$, отже, за критерієм Ейлера a^{-1} – квадратичний лишок за модулем p.

Приклад 4. Обчислити символи Лежандра: а) $L(79;211)$; б) $L(113;137)$; в) $L(438;593)$.

Р о з в ' я з а н н я: а) $L(79;211)=(-1)^{\frac{(79-1)(211-1)}{4}} L(211\,\mathrm{mod}\,79;79) =$

$=(-1)^{4095} L(53;79) = -L(53;79) = -(-1)^{\frac{52\cdot 78}{4}} L(79\,\mathrm{mod}\,53;53) = -(-1)^{1014} L(26;53) =$

$= -L(26;53) = -(-1)^{\frac{53^2-1}{8}} L(13;53) = -(-1)^{351} L(13;53) = L(13;53) =$

$=(-1)^{\frac{12\cdot 52}{4}} L(53\,\mathrm{mod}\,13;13) = (-1)^{156} L(1;13) = 1\cdot 1 = 1;$

б) $L(113;137)=(-1)^{\frac{(113-1)(137-1)}{4}} L(137\,\mathrm{mod}\,113;113) = (-1)^{3808} L(24;113) =$

$= L(24;113) = (-1)^{\frac{113^2-1}{8}} L(12;113) = (-1)^{1596} L(12;13) = L(12;13) = (-1)^{1596} L(6;113) =$

$= L(6;113) = (-1)^{1596} L(3;113) = L(3;113) = (-1)^{\frac{2\cdot 112}{4}} L(113\,\mathrm{mod}\,3;3) = (-1)^{56} L(2;3) =$

$= L(2;3) = (-1)^{\frac{9-1}{8}} L(1;3) = 1;$

в) $L(438;593)=(-1)^{\frac{593^2-1}{8}} L(219;593) = L(219;593) =$

$=(-1)^{\frac{218\cdot 592}{4}} L(593\,\mathrm{mod}\,219;219) = (-1)^{32412} L(155;219) = L(155;219) =$

$=(-1)^{\frac{154\cdot 218}{4}} L(219\,\mathrm{mod}\,155;155) = (-1)^{8393} L(64;155) = -L(64;155) =$

$= -(-1)^{\frac{155^2-1}{8}} L(32;155) = -(-1)^{3003} L(32;155) = L(32;155) = (-1)^{3003} L(16;155) =$

$= -L(16;155) = -(-1)^{3003} L(8;155) = L(8;155) = -L(4;155) = L(2;155) =$

$=(-1)^{\frac{155^2-1}{8}} L(1;155) = (-1)^{3003} L(1;155) = -1.$

Приклад 5. Чи мають розв'язки порівняння: а) $x^2 \equiv 67(\mathrm{mod}\, 79)$; б) $x^2 \equiv 34(\mathrm{mod}\, 199)$?

Р о з в ' я з а н н я: а) $L(67;79)=(-1)^{\frac{(67-1)(79-1)}{4}} L(12;67) = -L(12;67) =$

$(-1)^{\frac{67^2-1}{8}} L(6;67) = L(6;67) = -L(3;67) = -(-1)^{\frac{(67-1)(3-1)}{4}} L(1;3) = -(-1)^{33} = 1$. Якщо $L(a;p)=1$, то a – квадратичний лишок за модулем p, тобто існують квадратні корені з числа 67 за модулем 79 і порівняння має розв'язки;

б) $L(34;199)=(-1)^{\frac{199^2-1}{8}} L(17;199) = (-1)^{4950} L(17;199) = -L(17;199) =$

$(-1)^{\frac{(17-1)(199-1)}{4}} L(12;17) = (-1)^{\frac{17^2-1}{8}} L(6;17) = L(6;17) = L(3;17) = (-1)^{\frac{2\cdot 16}{4}} L(2;3) =$

$L(2;3) = (-1)^{\frac{9-1}{8}} L(1;3) = -1.$

Якщо $L(a;p)=-1$, то a – квадратичний нелишок за модулем p, тобто порівняння не має розв'язків і коренів з числа 34 за модулем 199 не існує.

Приклад 7. Довести, що квадратне порівняння $x^2 \equiv -1 \mathrm{mod}\, p$, де p – просте непарне, має корені тільки для модулів вигляду $p=4k+1$, $k=1,2,....$

Д о в е д е н н я. За критерієм Ейлера порівняння $x^2 \equiv -1 \mathrm{mod}\, p$, де p – просте, $p>2$, має корені, якщо $(-1)^{\frac{p-1}{2}} \equiv 1(\mathrm{mod}\, p)$. Це можливо, якщо $p-1 = 2k$, $k \in Z$, звідки $p=4k+1$, $k=1,2,....$

Приклад 8. Розв'язати порівняння $x^2 \equiv 55(\mathrm{mod}\, 79)$.

Р о з в ' я з а н н я. $a=55$, $p=79$, символ Лежандра $L(55;79)=1$, тому квадратне порівняння має розв'язки. Оскільки $79=4\cdot 19+3$, тобто простий модуль можна подати у вигляді $p=4\cdot k+3$, де $k=19$, то $x\equiv\pm a^{k+1} \bmod p\equiv\pm 55^{20} \bmod 79\equiv\pm 3025^{10} \bmod 79\equiv\pm 23^{10} \bmod 79\equiv\pm 529^{5} \bmod 79\equiv$ $\equiv\pm 55^{5} \bmod 79\equiv\pm 9150625\cdot 55 \bmod 79\equiv\pm 55^{2} \bmod 79\equiv\pm 23 \bmod 79$. Таким чином, $x_1\equiv 23 \bmod 79$, $x_2\equiv -23 \bmod 79\equiv 56 \bmod 79$.

Приклад 9. Здобути квадратні корені з числа 27 за модулем 71.

Р о з в ' я з а н н я. Це задача на пошук розв'язків порівняння $x^2\equiv 27(\bmod 71)$. $a=27$, $p=71=4\cdot 17+3$ – простий модуль. Символ Лежандра $L(27;71)=1$, отже, квадратні корені з числа 27 за модулем 71 існують.

Очевидно,

$$p=4k+3, \text{ де } k=17,$$

а тоді

$$x\equiv\pm a^{k+1} \bmod p\equiv\pm 27^{18} \bmod 71\equiv\pm 19683^{6} \bmod 71\equiv\pm 16^{6} \bmod 71\equiv\pm 4096^{2} \bmod 71\equiv$$
$$\equiv\pm 49^{2} \bmod 71\equiv\pm 2401 \bmod 71\equiv\pm 58 \bmod 71.$$

Отже, $x_1\equiv 58 \bmod 71$, $x_2\equiv -58 \bmod 71\equiv 13 \bmod 71$ – два шуканих кореня.

Приклад 10. Здобути квадратні корені з числа 135 за модулем 173.

Р о з в ' я з а н н я. Очевидно, $x^2\equiv 135(\bmod 173)$, $a=27$, $p=173=8\cdot 21+5$ – простий модуль. Обчислюємо символ Лежандра: $L(135;173)=1 \Rightarrow$ квадратні корені існують. Тут $p=8k+5$, де $k=21$, а тоді, аби вибрати формулу для здобуття коренів за таким модулем, потрібно обчислити $a^{2k+1} \bmod p$. У нашому випадку

$$a^{2k+1} \bmod p\equiv 135^{43} \bmod 173\equiv 1 \bmod 173.$$

За теорією при $a^{2k+1}\equiv 1 \bmod p$, тому корені будуть $x\equiv\pm a^{k+1} \bmod p$. Отже,

$$x\equiv\pm 135^{22} \bmod 173\equiv\pm 57 \bmod 173.$$

Звідси $x_1\equiv 57 \bmod 173$, $x_2\equiv -57 \bmod 173\equiv 116 \bmod 173$.

Приклад 11. Розв'язати порівняння:

а) $x^2\equiv 12(\bmod 109)$; б) $x^2\equiv 56(\bmod 61)$.

Р о з в ' я з а н н я: а) $a=12$, $p=109=8\cdot 13+5$.

Символ Лежандра $L(12;109)=1$, порівняння має розв'язки. $109=8\cdot 13+5$, тобто $109=8k+5$, де $k=13$. При такому модулі вигляд формули для здобуття коренів залежить від значення $a^{2k+1}(\bmod p)$. Отже, обчислюємо

$$a^{2k+1} \bmod p\equiv 12^{2\cdot 13+1} \bmod 109\equiv 12^{27} \bmod 109\equiv 1 \bmod 109.$$

У разі, коли $a^{2k+1}\equiv -1(\bmod p)$, корені визначаються за формулою $x\equiv\pm 2^{2k+1}\cdot a^{k+1}(\bmod p)$, тобто $x\equiv\pm 2^{27}\cdot 12^{14} \bmod 109\equiv\pm 11 \bmod 109$.

Таким чином, отримуємо два корені:

$$x_1\equiv 11 \bmod 109, \quad x_2\equiv -11 \bmod 109\equiv 98 \bmod 109;$$

б) $a=56$, $p=61=8\cdot 7+5$, $k=7$, $L(12;109)=1 \Rightarrow$ розв'язки існують. Обчислюємо $a^{2k+1} \bmod p\equiv 56^{15} \bmod 61\equiv 1 \bmod 61$. Тоді

$$x\equiv\pm 56^{8} \bmod 61\equiv\pm 19 \bmod 61. \qquad x_1\equiv 19 \bmod 61, \quad x_2\equiv 42 \bmod 61.$$

Приклад 12. Обчислити квадратні корені з числа: а) 67 за модулем 77; б) 511 за модулем 553.

Р о з в ' я з а н н я: а) за умовою прикладу потрібно розв'язати порівняння $x^2\equiv 67(\bmod 77)$. Оскільки $77=7\cdot 11$, то $n=pq$ – складений модуль, $p=7$, $q=11$, $\text{НСД}(a,n)=\text{НСД}(67,77)=1$. Дане порівняння еквівалентне системі порівнянь

$$\begin{cases} x^2\equiv 67(\bmod 7), \\ x^2\equiv 67(\bmod 11). \end{cases}$$

Після зведення за модулем маємо $\begin{cases} x^2=4(\bmod 7), \\ x^2=1(\bmod 11). \end{cases}$

Числа 4 та 1 є квадратичними лишками відповідно за модулями 7 і 11, а отже квадратичний лишок за модулем 77. Розв'язуємо кожне порівняння системи окремо.

$$x^2\equiv 4(\bmod 7) \Rightarrow x\equiv\pm 2(\bmod 7) \Rightarrow x_1=2 \bmod 7, \; x_1'=5 \bmod 7.$$

$$x^2=1(\bmod 11) \Rightarrow x\equiv\pm 1(\bmod 11) \Rightarrow x_2=1 \bmod 11, \; x_2'=10 \bmod 11.$$

Здобуті розв'язки скомбінуємо між собою у системи та за китайською теоремою про остачі визначимо шукані квадратні корені.

1) $\begin{cases} x=2(\bmod 7), \\ x=1(\bmod 11). \end{cases}$ $\text{НСД}(7,11)=1$, $\text{НСК}(7,11)=77$;

$$\frac{77}{7}y_1\equiv 1(\bmod 7) \Rightarrow 11y_1\equiv 1(\bmod 7) \Rightarrow y_1=2(\bmod 7);$$

$$\frac{77}{11}y_2\equiv 1(\bmod 11) \Rightarrow 7y_2\equiv 1(\bmod 11) \Rightarrow y_2=8(\bmod 11);$$

$$x=11\cdot 2\cdot 2+7\cdot 8\cdot 1(\bmod 77)\equiv 100(\bmod 77)=23(\bmod 77);$$

2) $\begin{cases} x\equiv 5(\bmod 7), \\ x\equiv 1(\bmod 11). \end{cases}$

$$x = 11\cdot 2\cdot 5 + 7\cdot 8\cdot 1 (\mathrm{mod}\, 77) \equiv 166 (\mathrm{mod}\, 77) = 12 (\mathrm{mod}\, 77).$$

Ще два корені $x = 54 (\mathrm{mod}\, 77)$ і $x = 65 (\mathrm{mod}\, 77)$ – протилежні до вже знайдених;

б) $x^2 \equiv 541 (\mathrm{mod}\, 553)$; $553 = 7\cdot 79$ – складений модуль, $p = 7$, $q = 79$, $\mathrm{НСД}(a, n) = \mathrm{НСД}(541, 553) = 1$. Складаємо еквівалентну систему порівнянь

$$\begin{cases} x^2 \equiv 541 (\mathrm{mod}\, 7), \\ x^2 \equiv 541 (\mathrm{mod}\, 79). \end{cases} \Rightarrow \begin{cases} x^2 = 4 (\mathrm{mod}\, 7), \\ x^2 = 1 (\mathrm{mod}\, 11). \end{cases}$$

Перше порівняння: $x^2 \equiv 2 (\mathrm{mod}\, 7)$; $L(2;7) = 1$. Випробуванням лишків $1,2,3,4,5,6$ повної системи лишків визначаємо $x_1 = 3 \bmod 7$, $x_1' = 4 \bmod 7$.

Друге порівняння: $x^2 \equiv 67 (\mathrm{mod}\, 79)$, $p = 79 = 4\cdot 19 + 3 \Rightarrow k = 19$.

$$x \equiv \pm 67^{20} \bmod 79 \equiv \pm 64 \bmod 79 \Rightarrow x_2 = 64 \bmod 79,\ x_2' = 15 \bmod 79.$$

1) $\begin{cases} x = 3 (\mathrm{mod}\, 7), \\ x = 15 (\mathrm{mod}\, 79). \end{cases}$ $\mathrm{НСД}(7, 79) = 1$, $\mathrm{НСК}(7, 79) = 553$;

$$79 y_1 \equiv 1 (\mathrm{mod}\, 7) \Rightarrow 2 y_1 \equiv 1 (\mathrm{mod}\, 7) \Rightarrow y_1 = 4 (\mathrm{mod}\, 7);$$
$$7 y_2 \equiv 1 (\mathrm{mod}\, 79) \Rightarrow y_2 = 34 (\mathrm{mod}\, 79);$$

$$x = 79\cdot 4\cdot 3 + 7\cdot 34\cdot 15 (\mathrm{mod}\, 553) \equiv 4518 (\mathrm{mod}\, 553) = 94 (\mathrm{mod}\, 553);$$

2) $\begin{cases} x = 3 (\mathrm{mod}\, 7), \\ x = 64 (\mathrm{mod}\, 11). \end{cases}$

$$x = 79\cdot 4\cdot 3 + 7\cdot 34\cdot 64 (\mathrm{mod}\, 553) \equiv 16180 (\mathrm{mod}\, 553) = 143 (\mathrm{mod}\, 553).$$

Решта коренів $x = 459 (\mathrm{mod}\, 553)$ і $x = 143 (\mathrm{mod}\, 553)$.

Приклад 13. Обчислити квадратні корені з числа 34 за модулем 133, використавши лінійну комбінацію для НСД множників модуля.

Р о з в ' я з а н н я: $n = 133 = 7\cdot 19$, $p = 7$, $q = 19$.

$\mathrm{НСД}(a, n) = \mathrm{НСД}(34, 133) = 1$. Дане порівняння еквівалентне системі порівнянь за модулями $p = 7$ і $q = 19$.

$$\begin{cases} x^2 \equiv 92 (\mathrm{mod}\, 7), \\ x^2 \equiv 92 (\mathrm{mod}\, 19). \end{cases} \Rightarrow \begin{cases} x^2 \equiv 1 (\mathrm{mod}\, 7), \\ x^2 \equiv 16 (\mathrm{mod}\, 19). \end{cases} \Rightarrow \begin{cases} x_1 \equiv 1 (\mathrm{mod}\, 7), \\ x_2 \equiv 4 (\mathrm{mod}\, 19). \end{cases}$$

$$\mathrm{НСД}(7, 19) = 1 = -8\cdot 7 + 3\cdot 19 = up + vq \Rightarrow u = -8,\ v = 3.$$

$$x = upx_2 + vqx_1 = -8\cdot 7\cdot 4 + 3\cdot 19\cdot 1 \equiv -167 (\mathrm{mod}\, 133) \equiv 34 \bmod 133;$$
$$x = upx_2 - vqx_1 = -8\cdot 7\cdot 4 - 3\cdot 19\cdot 1 \equiv -281 (\mathrm{mod}\, 133) \equiv 118 \bmod 133;$$
$$x \equiv -34 \bmod 133 \equiv 99 \bmod 133; \qquad x \equiv -118 \bmod 133 \equiv 15 \bmod 133.$$

Завдання для домашньої роботи

1. За критерієм Ейлера перевірити, чи будуть квадратичними лишками числа 3, 5, 7 і 9 за модулем 13.

(*Відповідь*: 3, 9 – лишки, 5, 7 – нелишки).

2. Обчислити символи Лежандра:

а) $L(94;109)$; б) $L(2115;6269)$; в) $L(1864;2029)$.

(*Відповідь*: а) 1; б) 1; в) -1).

3. Довести, що для будь-якого простого непарного числа добуток квадратичного лишка і квадратичного нелишка є квадратичним нелишком.

4. Довести, що для будь-якого числа елемент, обернений до квадратичного нелишка, є квадратичним нелишком.

5. Добуток чисел $ab...d$ дає квадратичний лишок або нелишок за простим модулем p залежно від парності або непарності кількості лишків серед множників. Довести це.

6. Довести, що $L(-1;p) = 1$, якщо просте число p можна подати у вигляді $p = 4k + 1$, $k = 1,2,....$

7. Довести, що $L(-1;p) = -1$, якщо просте число p можна подати у вигляді $p = 4k - 1$, $k = 1,2,....$

8. Довести, що квадратне порівняння $x^2 \equiv -1 \bmod p$, де p – просте непарне, не має коренів при модулях $p = 4k + 3$, $k = 0,1,2,....$

9. Розв'язати порівняння:

а) $x^2 \equiv 38 \bmod 127$; б) $x^2 \equiv 13 \bmod 61$; в) $x^2 \equiv 13 \bmod 29$; г) $x^2 \equiv 161 \bmod 197$.

(*Відповідь*: а) $x \equiv 61 \bmod 127$, $x \equiv 89 \bmod 127$; б) $x \equiv 47 \bmod 61$, $x \equiv 14 \bmod 61$; в) $x \equiv 19 \bmod 29$, $x \equiv 10 \bmod 1 = 29$; г) $x \equiv 113 \bmod 197$, $x \equiv 84 \bmod 197$).

10. Здобути квадратні корені з числа 10 за модулем 37.

(*Відповідь*: $x \equiv 11 \bmod 37$, $x \equiv 26 \bmod 37$).

11. Обчислити квадратні корені з числа:

а) 67 за модулем 77; б) 541 за модулем 553.

12. Визначити квадратні корені з числа 34 за модулем 133, використавши лінійну комбінацію для НСД множників модуля.

2.7. Первісні корені. Дискретні логарифми. Властивості дискретних логарифмів. Дискретні логарифми за простим модулем

Тестові завдання для перевірки теоретичних знань

1. Яким умовам має задовольняти ціле число g, щоб воно було первісним коренем за модулем m?

а) $g^{\varphi(m)} \equiv 1 (\mathrm{mod}\, m)$; **б)** $g^{\gamma} \equiv 1 (\mathrm{mod}\, m)$, γ – цілі числа від 1 до $\varphi(m)-1$;

в) НСД$(g,m)=1$; **г)** $g^{\gamma} \not\equiv 1 (\mathrm{mod}\, m)$, γ – цілі числа від 1 до $\varphi(m)-1$;

д) $g^{\varphi(m)} \not\equiv 1 (\mathrm{mod}\, m)$.

2. З яким твердженням Ви *не* згодні?

а) 2 – первісний корінь за модулем 17;
б) 5 – первісний корінь за модулем 17;
в) 3 – найменший первісний корінь за модулем 17;
г) усі попередні твердження правильні.

3. Для якого з цих складених модулів *не* існує первісних коренів?

а) 4; **б)** 8; **в)** 18; **г)** 25; **д)** 49.

4. Які з нижченаведених порівнянь повинні виконуватися, щоб ціле число g було первісним коренем за простим модулем 11?

а) $g^5 \equiv 1 (\mathrm{mod}\, 11)$; **б)** $g^5 \not\equiv 1 (\mathrm{mod}\, 11)$; **в)** $g^2 \equiv 1 (\mathrm{mod}\, 11)$;

г) $g^{10} \equiv 1 (\mathrm{mod}\, 11)$; **д)** $g^2 \not\equiv 1 (\mathrm{mod}\, 11)$.

5. В якому випадку значення дискретного логарифма визначено *неправильно*, якщо 2 – первісний корінь за модулем 5?

а) $2 \equiv 2 (\mathrm{mod}\, 5) \Rightarrow ind_2 2 = 1$; **б)** $2^3 \equiv 3 (\mathrm{mod}\, 5) \Rightarrow ind_3 2 = 3$;

в) $2^2 \equiv 4 (\mathrm{mod}\, 5) \Rightarrow ind_2 4 = 2$; **г)** $2^3 \equiv 3 (\mathrm{mod}\, 5) \Rightarrow ind_2 3 = 3$.

6. Яке з наведених порівнянь дає змогу визначити дискретний логарифм числа 6 за модулем 13 і основою 2?

а) $2^3 \equiv 8 (\mathrm{mod}\, 13)$; **б)** $2^6 \equiv 12 (\mathrm{mod}\, 13)$; **в)** $2^4 \equiv 3 (\mathrm{mod}\, 13)$;

г) $2^5 \equiv 6 (\mathrm{mod}\, 13)$; **д)** $2^2 \equiv 4 (\mathrm{mod}\, 13)$.

Завдання для аудиторної роботи

Приклад 1. Довести, що: а) 2 – первісний корінь за простим модулем 53; б) 3 – не первісний корінь за простим модулем 11.

Доведення: а) $p-1=52=2^2\cdot 13$. За критерієм для пошуку первісних коренів визначаємо

$$a^{\frac{p-1}{p_1}} = 2^{\frac{52}{13}} = 2^4 = 16 \not\equiv 1 (\mathrm{mod}\, 53);$$

$$a^{\frac{p-1}{p_2}} = 2^{\frac{52}{2}} = 2^{26} = (8192)^2 \equiv 30^2 \equiv -1 \not\equiv 1 (\mathrm{mod}\, 53).$$

Отже, 2 – первісний корінь за модулем 53;

б) $p-1=10=2\cdot 5$.

$$a^{\frac{p-1}{p_1}} = 3^{\frac{10}{5}} = 9 \not\equiv 1 (\mathrm{mod}\, 11);$$

$$a^{\frac{p-1}{p_2}} = 3^{\frac{10}{2}} = 3^5 = 729 \equiv 1 (\mathrm{mod}\, 11).$$

Умови критерію порушуються, число 2 не є первісним коренем за модулем 11.

Приклад 2. Знайти найменший первісний корінь за модулем p 7.

Розв'язання: $p-1=7-1=6=2\cdot 3$. Отже, число g буде первісним коренем за модулем 7, якщо не виконується жодне з порівнянь $g^1 \equiv 1 (\mathrm{mod}\, 7)$ і $g^2 \equiv 1 (\mathrm{mod}\, 7)$. Первісні корені g слід шукати серед чисел 1,2,3,4,5,6. Тому обчислюємо:

$1^2 \equiv 1 (\mathrm{mod}\, 7)$ – число 1 не є первісний корінь;

$2^2 \equiv 4 (\mathrm{mod}\, 7)$, $2^3 \equiv 8 (\mathrm{mod}\, 7) \equiv 1 (\mathrm{mod}\, 7)$ – число 2 не є первісний корінь;

$3^2 \equiv 2 (\mathrm{mod}\, 7)$, $3^3 \equiv 27 (\mathrm{mod}\, 7) \equiv 6 (\mathrm{mod}\, 7)$ – число 3 є найменший первісний корінь за модулем 7.

Приклад 3. Знайти найменший з первісних коренів за модулем p 37 і скласти таблицю дискретних логарифмів, прийнявши цей корінь за основу логарифма. Скласти таблицю для визначення числа за заданим логарифмом.

Розв'язання. $p-1=36=2^2\cdot 3^2$. Отже, число g буде первісним коренем за модулем 37, якщо не виконується жодне з порівнянь $g^{18} \equiv 1 (\mathrm{mod}\, 37)$ і $g^{12} \equiv 1 (\mathrm{mod}\, 37)$.

$1^{18} \equiv 1 (\mathrm{mod}\, 7)$ – число 1 не є первісний корінь;

$$2^{18} \equiv 1024 \cdot 256 (\mathrm{mod}\, 37) \equiv 25 \cdot 34 (\mathrm{mod}\, 37) \equiv 36 \,\mathrm{mod}\, 37,$$

$2^{12} \equiv 1024 \cdot 4 (\mathrm{mod}\, 37) \equiv 25 \cdot 4 (\mathrm{mod}\, 37) \equiv 26 \,\mathrm{mod}\, 37$ – число 2 є найменший первісний корінь. Це число приймаємо за основу логарифмів. Обчислюємо найменші додатні лишки $2^x \,\mathrm{mod}\, 37$, коли x послідовно дорівнює $0,1,2,\ldots, 35$.

$2^0 \equiv 1$	$2^8 \equiv 34$	$2^{16} \equiv 9$	$2^{24} \equiv 10$	$2^{32} \equiv 7$
$2^1 \equiv 2$	$2^9 \equiv 31$	$2^{17} \equiv 18$	$2^{25} \equiv 20$	$2^{33} \equiv 14$
$2^2 \equiv 4$	$2^{10} \equiv 25$	$2^{18} \equiv 36$	$2^{26} \equiv 3$	$2^{34} \equiv 28$
$2^3 \equiv 8$	$2^{11} \equiv 13$	$2^{19} \equiv 35$	$2^{27} \equiv 6$	$2^{35} \equiv 19$.
$2^4 \equiv 16$	$2^{12} \equiv 26$	$2^{20} \equiv 33$	$2^{28} \equiv 12$	
$2^5 \equiv 32$	$2^{13} \equiv 15$	$2^{21} \equiv 29$	$2^{29} \equiv 24$	
$2^6 \equiv 27$	$2^{14} \equiv 30$	$2^{22} \equiv 21$	$2^{30} \equiv 11$	
$2^7 \equiv 17$	$2^{15} \equiv 23$	$2^{23} \equiv 5$	$2^{31} \equiv 22$	

Будь-яке з цих порівнянь дає змогу визначити дискретний логарифм числа. Наприклад, $2^{21} \equiv 29 \Rightarrow ind_2 29 = 21$, тобто дискретні логарифми чисел є показниками степеня 2. Значення логарифмів числа N заносимо до таблиці, а саме дискретний логарифм числа N записуємо на перетині рядка з номером, що дорівнює кількості десятків числа N, і стовпця з номером, що дорівнює кількості десятків числа N. Наприклад, оскільки $ind_2 29 = 21$, то $N = 29$, отже, і пишемо 21 на перетині другого рядка та дев'ятого стовпця.

Таблиця дискретних логарифмів

N	0	1	2	3	4	5	6	7	8	9
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			

Таблиця для визначення числа за його дискретним логарифмом

ind	0	1	2	3	4	5	6	7	8	9
0	1	2	4	8	16	32	27	17	34	31
1	25	13	26	15	30	23	9	18	36	35
2	33	29	21	5	10	10	3	6	12	24
3	11	22	7	14	28	28				

Приклад 4. Користуючись таблицями дискретних логарифмів, розв'язати порівняння $13x^3 \equiv 24 (\mathrm{mod}\, 37)$.

Р о з в ' я з а н н я. Злогарифмуємо обидві частини порівняння за основою 2: $ind 13 + ind x^3 \equiv ind 24 (\mathrm{mod}\, 36)$ або $ind 13 + 3ind\, x \equiv ind 24 (\mathrm{mod}\, 36)$.

З побудованої вище таблиці індексів визначаємо $ind 13 \equiv 11 (\mathrm{mod}\, 36)$, $ind 24 \equiv 29 (\mathrm{mod}\, 36)$. Тоді $11 + 3ind\, x \equiv 29 (\mathrm{mod}\, 36) \Rightarrow 3ind\, x \equiv 18 (\mathrm{mod}\, 36)$.

НСД$(3,36) = 3$, $18 \vdots 3$, отже, порівняння має три розв'язки. Після спрощення отримуємо $ind\, x \equiv 6 (\mathrm{mod}\, 12)$, звідки $ind\, x_1 \equiv 6 (\mathrm{mod}\, 36)$, $ind\, x_2 \equiv 18 (\mathrm{mod}\, 36)$ та $ind\, x_3 \equiv 30 (\mathrm{mod}\, 36)$. За таблицею дискретних логарифмів знаходимо три корені вихідного порівняння:

$$x_1 \equiv 27 (\mathrm{mod}\, 37),\ x_2 \equiv 36 (\mathrm{mod}\, 37),\ x_3 \equiv 11 (\mathrm{mod}\, 37).$$

Приклад 5. Розв'язати порівняння $21^{3x} \equiv 21^5 (\mathrm{mod}\, 29)$

Р о з в ' я з а н н я. Злогарифмуємо обидві частини порівняння та застосуємо властивості дискретних логарифмів: $3x \cdot ind 21 \equiv 5ind 21 (\mathrm{mod}\, 28)$. За таблицею логарифмів знаходимо: $ind 21 \equiv 17 (\mathrm{mod}\, 28)$. Тоді

$51x \equiv 85 (\mathrm{mod}\, 28) \Rightarrow 17(3x - 5) \equiv 0 (\mathrm{mod}\, 28)$.

Оскільки $17 \not\equiv 0 (\mathrm{mod}\, 28)$, то $3x - 5 \equiv 0 (\mathrm{mod}\, 28)$ або $3x \equiv 5 (\mathrm{mod}\, 28)$.

Таким чином, $x \equiv 11 (\mathrm{mod}\, 28)$.

Завдання для домашньої роботи

1. Знайти найменший первісний корінь за модулем: а) 13; б) 23; в) 11; г) 47.

(*Відповідь*: а) 2; б) 5; в) 2; г) 5;).

2. Знайти всі первісні корені з такими модулями: а) 13; б) 17; в) 19.

3. Скласти таблицю дискретних логарифмів:
а) за модулем 29 з основою 2; б) за модулем 23 з основою 5.

4. Розв'язати порівняння:
а) $5x^4 \equiv 3 (\mathrm{mod}\, 11)$; б) $2x^8 \equiv 5 (\mathrm{mod}\, 13)$; в) $27x^5 \equiv 25 (\mathrm{mod}\, 31)$.

5. Визначити кількість розв'язків кожного з порівнянь:
а) $3x^{12} \equiv 2 (\mathrm{mod}\, 41)$; б) $x^{15} \equiv 6 (\mathrm{mod}\, 37)$; в) $x^5 \equiv 6 (\mathrm{mod}\, 101)$; г) $x^{15} \equiv 1 (\mathrm{mod}\, 61)$.

3. ЗРАЗОК МОДУЛЬНОЇ КОНТРОЛЬНОЇ РОБОТИ

Критерії оцінки знань

Модульна контрольна робота оцінюється за 5-бальною шкалою.

Кожний варіант складається з 5 завдань. При наявності грубої помилки у вирішенні завдання віднімається 0,3 бала, а негрубої – від 0,1 до 0,3 бала в залежності від недоліків у розв'язанні.

Набрана кількість балів сумується і переводиться в оцінку:

4,6 – 5 балів – «відмінно»

3,7–4,5 бала – «добре»

2,7–3,6 бала – «задовільно»

менше за 2,7 бала – «незадовільно».

Нижченаведений зразок модульної контрольної роботи розрахований на 2 академічні години.

1. Яке з нижченаведених чисел є найбільшим спільним дільником чисел 8 та 24?

а) 2; **б)** 3; **в)** 12; **г)** 24; **д)** 8.

(*Відповідь:* д).

2. Розв'язати порівняння $17x \equiv 25 (\mathrm{mod}\, 52)$.

Розв'язання. Визначаємо $d = \mathrm{НСД}(17, 52) = 1$, тому дане порівняння має один розв'язок. Використаємо алгоритм Евкліду:

$$\begin{array}{r|l} -52 & 17 \\ \underline{51} & 3 \\ 1 & \end{array} \qquad \begin{array}{r|l} -3 & 1 \\ \underline{3} & 3 \\ 0 & \end{array} \quad \Rightarrow \quad 1 = 52 - 17 \cdot 3 = -3 \cdot 17 + 1 \cdot 52 .$$

Звідси $17^{-1} (\mathrm{mod}\, 52) \equiv -3 (\mathrm{mod}\, 52) \equiv 49 (\mathrm{mod}\, 52)$.

$$x \equiv 25 \cdot 17^{-1} (\mathrm{mod}\, 52) \equiv 25 \cdot 49 (\mathrm{mod}\, 52) \equiv 29 (\mathrm{mod}\, 52) .$$

(*Відповідь:* $x \equiv 29 (\mathrm{mod}\, 52)$).

3. Знайти обернену матрицю A^{-1} для матриці $A = \begin{pmatrix} 6 & 7 \\ 3 & 14 \end{pmatrix}$ у кільці Z_{19}.

Розв'язання. $A^{-1} = (\det A)^{-1} \begin{pmatrix} A_{11} & A_{21} \\ A_{12} & A_{22} \end{pmatrix} (\mathrm{mod}\, n)$.

$$\det A = \begin{vmatrix} 6 & 7 \\ 3 & 14 \end{vmatrix} (\mathrm{mod}\, 19) \equiv 84 - 21 \equiv 63 (\mathrm{mod}\, 19) \equiv 6 (\mathrm{mod}\, 19) .$$

$$\mathrm{НСД}(\det A, n) = \mathrm{НСД}(6, 19) = 1 ,$$

тому обернена матриця в кільці Z_{19} існує.

Для знаходження $(\det A)^{-1} (\mathrm{mod}\, 19) \equiv 6^{-1} (\mathrm{mod}\, 19)$ застосуємо теорему Ейлера

$a^{-1} \equiv a^{\varphi(m)-1} (\mathrm{mod}\, m)$. Тобто $6^{-1} \equiv 6^{\varphi(19)-1} (\mathrm{mod}\, 19) \equiv 6^{18-1} (\mathrm{mod}\, 19) \equiv$

$\equiv 6^{17} (\mathrm{mod}\, 19) \equiv 6^2 \cdot \left(6^3\right)^5 (\mathrm{mod}\, 19) \equiv 36 \cdot 216^5 (\mathrm{mod}\, 19) \equiv 17 \cdot 7^5 (\mathrm{mod}\, 19) \equiv$

$\equiv 17 \cdot 7 \cdot 49^2 (\mathrm{mod}\, 19) \equiv 119 \cdot 11^2 (\mathrm{mod}\, 19) \equiv 5 \cdot 121 (\mathrm{mod}\, 19) \equiv 16 (\mathrm{mod}\, 19)$.

Обчислюємо алгебраїчні доповнення елементів матриці:

$A_{11} \equiv 14 (\mathrm{mod}\, 19)$; $A_{12} \equiv -3 (\mathrm{mod}\, 19) \equiv 16 (\mathrm{mod}\, 19)$;

$A_{21} \equiv -7 (\mathrm{mod}\, 19) \equiv 12 (\mathrm{mod}\, 19)$; $A_{22} \equiv 6 (\mathrm{mod}\, 19)$.

$$A^{-1} = 16 \begin{pmatrix} 14 & 12 \\ 16 & 6 \end{pmatrix} (\mathrm{mod}\, 19) = \begin{pmatrix} 224 & 192 \\ 256 & 96 \end{pmatrix} (\mathrm{mod}\, 19) \equiv \begin{pmatrix} 15 & 2 \\ 9 & 1 \end{pmatrix} (\mathrm{mod}\, 19) .$$

(*Відповідь:* $A^{-1} \equiv \begin{pmatrix} 15 & 2 \\ 9 & 1 \end{pmatrix} (\mathrm{mod}\, 19)$).

4. Розв'язати систему порівнянь $\begin{cases} x \equiv 1 (\mathrm{mod}\, 12), \\ x \equiv 7 (\mathrm{mod}\, 14). \end{cases}$

Розв'язання. Визначаємо $d = \mathrm{НСД}(12, 14) = 2$, $C_1 = 1$, $C_2 = 7$. Система має розв'язок, бо $C_2 - C_1 \vdots d$, тобто $6 \vdots 2$.

З першого порівняння знаходимо невідоме $x = 1 + 12t$, $t \in Z$, і підставляємо цей вираз у друге порівняння: $1 + 12t \equiv 7 (\mathrm{mod}\, 14)$.

Тоді $12t \equiv 6 (\mathrm{mod}\, 14) \Rightarrow 6t \equiv 3 (\mathrm{mod}\, 7)$. Випробуванням лишків повної системи отримаємо $t \equiv 4 (\mathrm{mod}\, 7) \Rightarrow t = 4 + 7k$, $k \in Z$. Підставимо це значення t у вираз для x:

$x = 1 + 12t = 1 + 12(4 + 7k) = 1 + 48 + 84k = 49 + 84k \Rightarrow x \equiv 49 (\mathrm{mod}\, 84)$.

(*Відповідь:* $x \equiv 49 (\mathrm{mod}\, 84)$).

5. Обчислити символ Лежандра $L(241; 593)$.

Розв'язання. За допомогою символу Лежандра $L(a; p)$ можна встановити існування коренів квадратного порівняння $x^2 \equiv a (\mathrm{mod}\, p)$ за простим модулем p.

$$L(241; 593) = (-1)^{\frac{(241-1)(593-1)}{4}} L(593 (\mathrm{mod}\, 241); 241) = (-1)^{60 \cdot 592} L(111; 241)$$

$$L(111; 241) = (-1)^{\frac{(111-1)(241-1)}{4}} L(241 (\mathrm{mod}\, 111); 111) = (-1)^{110 \cdot 60} L(19; 111) \quad L(19; 111) =$$

$$(-1)^{\frac{(19-1)(111-1)}{4}} L(111 (\mathrm{mod}\, 19); 19) = (-1)^{495} L(16; 19) = -L(16; 19) = -(-1)^{\frac{19^2-1}{8}} L\left(\frac{16}{2}; 19\right)$$

$$(-1)^{45} L(8; 19) = L(8; 19) = (-1)^{\frac{19^2-1}{8}} L(4; 19) = -L(4; 19) = -(-1)^{\frac{19^2-1}{8}} L(2; 19) \quad L(2; 19) =$$

$$(-1)^{\frac{19^2-1}{8}} L(1; 19) = -L(1; 19) = -1 .$$

(*Відповідь:* $L(241; 593) = -1$).

Оцінювання відповіді	*Номер завдання*	1	2	3	4	5
	Кількість балів	0,4	0,8	1,5	1,5	0,8

СПИСОК ЛІТЕРАТУРИ

1. Математичні основи криптографії [Текст] / Г.В. Кузнецов, В.В. Фомичов, С.О. Сушко, Л.Я. Фомичова. – Д.: Національний гірничий університет, 2004. – 391 с.

2. Айерлэнд К. Классическое введение в современную теорию чисел [Текст] / К. Айерлэнд, М. Роузен. – М.: Мир, 1987. – 144 с.

3. Коутинхо С. Введение в теорию чисел. Алгоритм RSA [Текст] / С. Коутинхо. – М.: Постмаркет, 2001. – 328 с.

4. Боревич З.И. Теория чисел [Текст] / З.И. Боревич, И.Р. Шафаревич. – М.: Наука, 1985. – 504 с.

5. Вербицький О.В. Вступ до криптології [Текст] / О.В. Вербицький. – Л.: Вид-во наук.-техн. літ., 1998. – 247 с.

6. Основы криптографии [Текст] / А.П. Алфёров, А.Ю. Зубов, А.С. Кузьмин, А.В. Черемушкин. – М.: Гелиос АРВ, 2002. – 480 с.

7. Нестеренко Ю.В. Теория чисел [Текст]: учеб. для студ. высш. учеб. завед. / Ю.В. Нестеренко. – М.: Изд-ский центр «Академия», 2008. – 272 с.

8. Серпинский В. 250 задач по элементарной теории чисел [Текст] / В. Серпинский. – М.: Просвещение, 1968. – 160 с.

ДОДАТОК А

Таблиця простих чисел

2	3	5	7	11	13	17	19	23	29	31	37
41	43	47	53	59	61	67	71	73	79	83	89
97	101	103	107	109	113	127	131	137	139	149	151
157	163	167	173	179	181	191	193	197	199	211	223
227	229	233	239	241	251	257	263	269	271	277	281
283	293	307	311	313	317	331	337	347	349	353	359
367	373	379	383	389	397	401	409	419	421	431	433
439	443	449	457	461	463	467	479	487	491	499	503
509	521	523	541	547	557	563	569	571	577	587	593
599	601	607	613	617	619	631	641	643	647	653	659
661	673	677	683	691	701	709	719	727	733	739	743
751	757	761	769	773	787	797	809	811	821	823	827
829	839	853	857	859	863	877	881	883	887	907	911
919	929	937	941	947	953	967	971	977	983	991	997

ДОДАТОК Б

Номери букв української абетки

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

Предметний покажчик

Навчальне видання

Кузнецов Георгій Віталійович
Сушко Світлана Олександрівна
Фомичова Людмила Яківна
Корабльов Анатолій Володимирович

СПЕЦІАЛЬНІ РОЗДІЛИ МАТЕМАТИКИ

Розділ «Теорія чисел»
(теоретичні відомості, тестові завдання, приклади)

Навчальний посібник

Редактор Ю.В. Рачковська

Підписано до друку 10.02.10. Формат 30×42/4.
Папір офсетний. Ризографія. Ум. друк. арк. 4,8.
Обл.-вид. арк. 4,8. Тираж 150 прим. Зам № 83.

Підготовлено до друку та видрукувано
у Національному гірничому університеті.
Свідоцтво про внесення до Державного реєстру № 1842

49005, м. Дніпропетровськ, просп. К. Маркса, 19.