МІНІСТЕРСТВО ОСВІТИ І НАУКИ УКРАЇНИ

**Український державний університет
науки і технологій**

Кафедра «Електронні обчислювальні машини»

В авторській редакції

МАТЕМАТИЧНІ ОСНОВИ ІНФОРМАЦІЙНОЇ БЕЗПЕКИ

Навчально-методичні рекомендації
щодо виконання курсового завдання

ДНІПРО
2024

УДК 004.056:519.87(072)
М 34

Упорядник:
В. М. Пахомова

Електронний аналог
друкованого видання

Схвалено Групою забезпечення якості освітньої програми
125 «Кібербезпека»
Протокол № 1 від 30.08.2024

М 34 **Математичні основи інформаційної безпеки** : навчально-методичні рекомендації щодо виконання курсового завдання / упоряд.: В. М. Пахомова ; Укр. держ. ун-т науки і технологій. – Дніпро : УДУНТ, 2024. – 16 с.

Навчально-методичні рекомендації призначені для використання здобувачами ступеню «бакалавр» безвідривної форми навчання спеціальності 125 «Кібербезпека та захист інформації» під час виконання курсового завдання з дисципліни «Математичні основи інформаційної безпеки».

Табл. 5. Бібліогр. назв. 3.

ЗМІСТ

ВСТУП

Методичні рекомендації щодо виконання курсового завдання з дисципліни «Математичні основи інформаційної безпеки» [1] призначені здобувачам ступеня «бакалавр» спеціальності «Кібербезпека».

Виконання здобувачами даного курсового завдання з дисципліни «Математичні основи інформаційної безпеки»сприяє досягненню наступних програмних результатів навчання: використовувати результати самостійного пошуку, аналізу та синтезу інформації з різних джерел для ефективного рішення спеціалізованих задач професійної діяльності; застосовувати теорії та методи захисту для забезпечення безпеки інформації в інформаційно-телекомунікаційних системах.

У [2] автором запропонована методика «MathFISLearn» щодо формування компетентностей здобувачів ступеня «бакалавр» при дистанційному навчанні з дисципліни «Математичні основи інформаційної безпеки». У [3] автором запропонована методика «ComparSystem_FIS» щодо формування фахових та предметних компетентностей у здобувачів при виконанні курсового завдання з цієї дисципліни.

На сучасному етапі математика скінченних полів широко застосовується у криптографії і стала основою багатьох криптосистем. У таких полях працює теорія чисел і «модулярна арифметика» (обчислення за модулем). Курсове завдання складається із двох частин: розв’язання лінійного порівняння за модулем з використанням різних засобів (випробуванням лишків повної системи, за розширеним евклідовим алгоритмом, з використанням теореми Ейлера, за допомогою властивостей скінченних ланцюгових дробів); розв’язання системи лінійних порівнянь за модулем на основі двох підходів (методом підстановки та з використанням китайської теореми про лишки). До кожної частини подані: стислі теоретичні відомості; розв’язання контрольного прикладу; постановка та варіанти курсового завдання. Крім того, на при кінці навчально-методичного видання представлені контрольні питання щодо захисту курсового завдання та бібліографічний список [1-5].

1. Структура курсового завдання

Задача 1. Розв'язати порівняння першого степеня за допомогою випробування лишків повної системи за модулем m, теореми Ейлера, властивостей скінченних ланцюгових дробів, розширеного евклідового алгоритму (табл.1).

Задача 2. Розв’язати систему порівнянь методом підстановки та методом на основі китайської теореми про лишки (табл. 2).

Таблиця 1

Варіанти порівняння першого степеня

№ вар.	Порівняння	№ вар.	Порівняння
1	$5x \equiv 8 (\mathrm{mod}\, 14)$	16	$13x \equiv 32 (\mathrm{mod}\, 28)$
2	$12x \equiv 15 (\mathrm{mod}\, 35)$	17	$5x \equiv 2 (\mathrm{mod}\, 8)$
3	$21x \equiv 10 (\mathrm{mod}\, 25)$	18	$7x \equiv 2 (\mathrm{mod}\, 13)$
4	$8x \equiv 17 (\mathrm{mod}\, 23)$	19	$15x \equiv 85 (\mathrm{mod}\, 355)$
5	$38x \equiv 4 (\mathrm{mod}\, 26)$	20	$15x \equiv 21 (\mathrm{mod}\, 18)$
6	$19x \equiv 4 (\mathrm{mod}\, 25)$	21	$18x \equiv 12 (\mathrm{mod}\, 30)$
7	$29x \equiv 35 (\mathrm{mod}\, 23)$	22	$75x \equiv 54 (\mathrm{mod}\, 21)$
8	$27x \equiv 1 (\mathrm{mod}\, 58)$	23	$39x \equiv 5 (\mathrm{mod}\, 11)$
9	$111x \equiv 49 (\mathrm{mod}\, 179)$	24	$183x \equiv 93 (\mathrm{mod}\, 111)$
10	$5x \equiv 7 (\mathrm{mod}\, 8)$	25	$11x \equiv 15 (\mathrm{mod}\, 24)$
11	$8x \equiv 5 (\mathrm{mod}\, 9)$	26	$45x \equiv 21 (\mathrm{mod}\, 132)$
12	$2x \equiv 13 (\mathrm{mod}\, 15)$	27	$21x \equiv 10 (\mathrm{mod}\, 25)$
13	$7x \equiv 10 (\mathrm{mod}\, 18)$	28	$8x \equiv 17 (\mathrm{mod}\, 23)$
14	$58x \equiv 87 (\mathrm{mod}\, 47)$	29	$15x \equiv 21 (\mathrm{mod}\, 6)$
15	$6x \equiv 4 (\mathrm{mod}\, 8)$	30	$2x \equiv 13 (\mathrm{mod}\, 15)$

Таблиця 2

Варіанти систем порівнянь першого степеня

№ вар.	a	b	m	№ вар	a	b	m	№ вар.	a	b	m
1	3	2	14	10	61	1	2	19	7	4	15
	5	8	17		82	12	17		3	23	28
	4	7	11		51	1	19		5	8	11

Продовження таблиці 2

2	8 80 38	1 40 3	15 53 7	11	10 37 59	4 6 18	13 81 19	20	24 69 66	16 7 17	74 31 65
3	9 79 83	1 5 14	65 7 16	12	74 19 21	42 12 57	65 21 67	21	67 57 3	68 4 4	73 5 67
4	93 31 33	17 1 18	29 5 48	13	66 74 97	2 22 38	47 27 46	22	59 38 13	9 11 17	95 37 92
5	51 14 44	62 6 62	67 8 97	14	57 26 75	75 1 4	88 7 29	23	53 29 19	1 43 13	2 67 49
6	3 5 7	5 1 2	14 9 25	15	66 16 66	4 51 24	8 67 97	24	53 77 3	23 83 13	71 97 56
7	33 67 11	37 2 10	61 3 68	16	41 1 88	17 46 12	24 73 17	25	95 55 88	36 3 5	77 29 13
8	49 28 9	13 54 5	47 73 38	17	10 35 26	28 2 10	57 16 11	26	39 31 95	25 4 4	67 88 7
9	22 98 74	4 20 80	7 39 86	18	58 8 93	15 14 40	31 89 53	27	5 23 97	1 28 43	6 67 65
28	48 27 63	8 2 18	82 7 19	29	57 62 91	57 6 11	87 7 16	30	73 35 69	96 1 1	101 9 10

2. Порівняння першого степеня

2.1. Основні поняття

Нехай $m>1$ – ціле додатне число, яке назвемо **модулем**. Два цілих числа a і b називаються **порівнянними 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

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

при цьому кажуть, що число a – це **лишок числа b за модулем m**.

Інколи порівняння скорочено записують як $a \equiv b(m)$, $a \overset{m}{\equiv} b$.

Властивості порівнянь:

1. $a \equiv a(\mathrm{mod}\, m)$ для будь-якого числа a.
2. Якщо $a \equiv b(\mathrm{mod}\, m)$, то $b \equiv a(\mathrm{mod}\, m)$.
3. Якщо $a \equiv b(\mathrm{mod}\, m)$ та $c \equiv b(\mathrm{mod}\, m)$, то $a \equiv c(\mathrm{mod}\, m)$.
4. Якщо $a \equiv b(\mathrm{mod}\, m)$ і k - довільне ціле число, то $ka \equiv kb(\mathrm{mod}\, m)$.
5. Якщо $ka \equiv kb(\mathrm{mod}\, m)$ і числа k, m – взаємно прості, то $a \equiv b(\mathrm{mod}\, m)$.
6. Якщо $a \equiv b(\mathrm{mod}\, m)$ і k - довільне натуральне число, то $ka \equiv kb(\mathrm{mod}\, km)$.
7. Якщо $ka \equiv kb(\mathrm{mod}\, km)$, де k, m - довільні натуральні числа, то $a \equiv b(\mathrm{mod}\, m)$.
8. Якщо $ka \equiv kb(\mathrm{mod}\, m)$, де d – найбільший спільний дільник чисел k та m, то $a \equiv b(\mathrm{mod}\, \frac{m}{d})$.
9. Якщо $a \equiv b(\mathrm{mod}\, m)$, $c \equiv d(\mathrm{mod}\, m)$ то $a \pm c \equiv b \pm d(\mathrm{mod}\, m)$, тобто порівняння за одним модулем можна додавати або віднімати.
10. Будь-який доданок лівої та правої частин порівняння можна переносити з протилежним знаком у іншу частину, тобто
    1) якщо $a \equiv b + c(\mathrm{mod}\, m)$, то $a - c \equiv b(\mathrm{mod}\, m)$ або $a - b \equiv c(\mathrm{mod}\, m)$;
    2) якщо $a + b \equiv c(\mathrm{mod}\, m)$, то $a \equiv c - b(\mathrm{mod}\, m)$.
11. У порівнянні можна відкидати або додавати доданки, що діляться на модуль, тобто якщо $a + c \equiv b(\mathrm{mod}\, m)$ і c діляться на m, то $a \equiv b(\mathrm{mod}\, m)$.
12. Якщо $a \equiv b(\mathrm{mod}\, m)$, $c \equiv d(\mathrm{mod}\, m)$, то $ac \equiv bd(\mathrm{mod}\, m)$, тобто порівняння за одним модулем можна перемножувати.

13. Якщо $a \equiv b(\mathrm{mod}\, m)$, то $a^n \equiv b^n(\mathrm{mod}\, m)$ для будь-якого цілого $n \geq 0$.
14. Якщо $a \equiv b(\mathrm{mod}\, m)$ і $f(x) = c_n x^n + c_{n-1} x^{n-1} + \ldots + c_1 x + c_0$ – довільний многочлен із цілими коефіцієнтами, то $f(a) \equiv f(b)(\mathrm{mod}\, m)$.
15. Якщо $a \equiv b(\mathrm{mod}\, m)$ і число d – дільник модуля m, то $a \equiv b(\mathrm{mod}\, d)$.
16. Якщо $a \equiv b(\mathrm{mod}\, m)$, то множина спільних дільників чисел a і m збігається з множиною спільних дільників чисел b і m, зокрема $НСД(a, m) = НСД(b, m)$.
17. Якщо $a \equiv b(\mathrm{mod}\, m_1)$, $a \equiv b(\mathrm{mod}\, m_2)$ і m – найменше спільне кратне модулів m_1 та m_2, то $a \equiv b(\mathrm{mod}\, m)$.
18. Якщо $a \equiv b(\mathrm{mod}\, m)$, то числа a і b у результаті ділення на m дають однакову остачу, тобто $a = mq_1 + r$ і $b = mq_2 + r$, де $0 \leq r < m$.
19. Якщо $a \equiv b(\mathrm{mod}\, m)$, то $a - b = mt$, де $t = 0, \pm 1, \pm 2, \ldots$. Отже, $a = b + mt$, $t = 0, \pm 1, \pm 2, \ldots$.

2.2. Умови існування рішення порівнянь першого степеня

Рівняння вигляду $ax \equiv b(\mathrm{mod}\, m)$, де a, b – цілі, називається **лінійним порівнянням**. Нехай $НСД(a, m) = d$ – найбільший спільний дільник чисел a і m. Тоді:

1) якщо число b не ділиться на число d, то порівняння $ax \equiv b(\mathrm{mod}\, m)$ не матиме розв'язку;

2) якщо число b кратне d, то порівняння $ax \equiv b(\mathrm{mod}\, m)$ має d-розв'язків, а саме: x_0; $x_0 + \frac{m}{d}$; $x_0 + 2\frac{m}{d}$; …; $x_0 + (d-1)\frac{m}{d}$, де x_0 - розв'язок порівняння $\frac{a}{d} x \equiv \frac{b}{d} (\mathrm{mod}\, \frac{m}{d})$;

3) якщо $НСД(a, m) = 1$, то порівняння $ax \equiv b(\mathrm{mod}\, m)$ має один розв'язок $x \equiv x_0(\mathrm{mod}\, m)$, причому порівняння задовольняє клас розв'язків $x = x_0 + mt, \quad t = 0, \pm 1, \pm 2, \ldots$

2.3. Способи рішення порівнянь першого степеня

Існує декілька способів рішення порівнянь першого степеня вигляду $ax \equiv b(\mathrm{mod}\, m)$ при $НСД(a, m) = 1$ за допомогою:

- випробування лишків повної системи за модулем *m;*

- теореми Ейлера;

- властивостей скінченних ланцюгових дробів;

- розширеного евклідового алгоритму.

Вирішення за допомогою випробування лишків повної системи за модулем m. Повна система вирахувань за модулем *m* - це будь-яка сукупність цілих чисел, яка містить по одному числу з кожного класу чисел по модулю *m* (два цілих числа *a* і *b* належать одному класу за модулем *m*, якщо $(a-b)$ ділиться на *m*. Наприклад, 5-й клас лишків за $\bmod m$ дорівнює

$$\{\ldots,-3m+5,-2m+5,-m+5,5,m+5,2m+5,3m+5,\ldots\}.$$

Якщо ми маємо *m* класів, то нам треба розглянути $0,1,2,\ldots,m-1$ класи. Будь-які *m* - чисел, які належать різним класам за модулем *m*, утворюють повну систему за цим модулем.

Приклад 1. Розв'язати порівняння $5x \equiv 7(\bmod 8)$.

Р і ш е н н я

$x=0;\ 5\cdot 0 \neq 7(\bmod 8)$ $\qquad$ $x=4;\ 5\cdot 4 \neq 7(\bmod 8)$

$x=1;\ 5\cdot 1 \neq 7(\bmod 8)$ $\qquad$ $x=5;\ 5\cdot 5 \neq 7(\bmod 8)$

$x=2;\ 5\cdot 2 \neq 7(\bmod 8)$ $\qquad$ $x=6;\ 5\cdot 6 \neq 7(\bmod 8)$

$x=3;\ 5\cdot 3 \equiv 7(\bmod 8)$ $\qquad$ $x=7;\ 5\cdot 7 \neq 7(\bmod 8)$

В і д п о в і д ь: $x \equiv 3(\bmod 8)$.

Вирішення за допомогою розширеного евклідового алгоритму. Якщо $НСД(a,m)=1$, тобто *a, m* – взаємно прості числа, тоді розширений алгоритм Евкліда до чисел *a, m* дасть такі цілі числа α,β, що $a\alpha+m\beta=1$. Отримане рівняння еквівалентне наступному $a\alpha \equiv 1(\bmod m)$, таким чином, для *a* знайдений зворотний елемент α. Помножимо обидві частки початкового лінійного порівняння на α, в результаті отримаємо рішення $x \equiv \alpha a x \equiv \alpha b(\bmod m)$.

Приклад 2. Розв'язати порівняння $7x \equiv 3(\bmod 15)$.

Р і ш е н н я. $НСД(15,7)=1;\ 1=15-2\cdot 7$. Зворотним елементом до числа $a=7$ за модулем $m=15$ буде $\alpha=-2\equiv 13(\bmod 15)$. Помножимо обидві частини порівняння на 13:

$$7\cdot 13\cdot x \equiv 3\cdot 13(\bmod 15),\ x \equiv 39(\bmod 15) \equiv 9(\bmod 15).$$

В і д п о в і д ь: $x \equiv 9(\bmod 15)$.

Вирішення за допомогою теореми Ейлера $a^{\varphi(m)} \equiv 1(\mathrm{mod}\, m)$, ***де*** $НСД(a,m)=1$. Для цього помножимо порівняння $ax \equiv b(\mathrm{mod}\, m)$ на $a^{\varphi(m)-1}$:

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

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

Приклад 3. Розв'язати порівняння $7x \equiv 5(\mathrm{mod}\, 9)$.

Р і ш е н н я. $НСД(7,9)=1$; $\varphi(9) = \varphi(3^2) = 9(1-\frac{1}{3}) = 6$, $\varphi(9)-1 = 6-1 = 5$;

$x \equiv 5 \cdot 7^5(\mathrm{mod}9) \equiv 5 \cdot 49^2 \cdot 7 \equiv 5 \cdot 4^2 \cdot 7 \equiv 560(\mathrm{mod}9) \equiv 2(\mathrm{mod}9)$.

В і д п о в і д ь: $x \equiv 2(\mathrm{mod}9)$.

Вирішення за допомогою властивостей скінченних ланцюгових дробів. Нехай $\frac{p_0}{q_0}, \frac{p_1}{q_1}, \frac{p_2}{q_2}, \ldots, \frac{p_{k-1}}{q_{k-1}}, \frac{p_k}{q_k} = \frac{m}{a}$ - послідовність підхідних дробів розкладання дробу $\frac{m}{a}$ на ланцюговий дріб і $НСД(a,m)=1$. За властивістю підхідних дробів $НСД(p_k, q_k)=1$ і тому $\frac{p_k}{q_k} = \frac{m}{a}$ являє собою рівність двох нескоротних дробів. У рекурентній формулі $p_k q_{k-1} - p_{k-1}q_k = (-1)^{k-1}$ для чисельників і знаменників підхідних дробів замінимо $p_k = m$ та $q_k = a$: $mq_{k-1} - ap_{k-1} = (-1)^{k-1}$. Звідси $ap_{k-1} = (-1)^k + mq_{k-1}$ або $ap_{k-1} = (-1)^k(\mathrm{mod}\, m)$. Помноживши останнє порівняння на $(-1)^k b$, дістанемо $a((-1)^k bp_{k-1}) \equiv b(\mathrm{mod}\, m)$. Таким чином, число $x \equiv (-1)^k bp_{k-1}(\mathrm{mod}\, m)$.

Приклад 4. Розв'язати порівняння $31x \equiv 19(\mathrm{mod}\, 83)$.

Р і ш е н н я. Розкладемо дріб $\frac{83}{31}$ на ланцюговий дріб $\frac{83}{31} = [2;1,2,10]$. Це розкладання дасть таку таблицю частинних знаменників a_k ланцюгового дробу та чисельників p_k підхідних дробів (табл. 3).

Таблиця 3

k	0	1	2	3
a_k	2	1	2	10
p_k	2	3	8	-

Тут $k=3;\ p_{k-1}=8$. Тоді

$$x \equiv (-1)^3 \cdot 19 \cdot 8 (\mathrm{mod} 83) \equiv -152 (\mathrm{mod} 83) \equiv 14 (\mathrm{mod} 83).$$

Відповідь: $x \equiv 14 (\mathrm{mod} 83)$.

3. Система порівнянь першого степеня

3.1. Основні поняття

Системою порівнянь називають систему вигляду

$$\begin{cases} f_1(x) \equiv 0 (\mathrm{mod}\, m_1), \\ f_2(x) \equiv 0 (\mathrm{mod}\, m_2), \\ \ldots \\ f_n(x) \equiv 0 (\mathrm{mod}\, m_n), \end{cases} \qquad (1)$$

де $f_1(x);\ f_2(x);\ \ldots;\ f_n(x)$ – задані многочлени з цілими коефіцієнтами. Нехай *M* – найменше спільне кратне всіх модулів $m_1,\ m_2\ \ldots,\ m_n$. Розв'язком системи (1) буде клас чисел за модулем *M*, що містить числа, які задовольняють кожне порівняння системи.

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

$$\begin{cases} a_1 x \equiv b_1 (\mathrm{mod}\, m_1), \\ a_2 x \equiv b_2 (\mathrm{mod}\, m_2), \\ \ldots \\ a_n x \equiv b_n (\mathrm{mod}\, m_n), \end{cases} \qquad (2)$$

де $НСД(a_1, m_1) = 1$; $НСД(a_2, m_2) = 1$;…; $НСД(a_n, m_m) = 1$.

Кожне порівняння у системі (2) можна розв'язати окремо, тобто спочатку записати порівняння у вигляді

$$\begin{cases} x \equiv c_1 (\mathrm{mod}\, m_1), \\ x \equiv c_2 (\mathrm{mod}\, m_2), \\ \ldots \\ x \equiv c_n (\mathrm{mod}\, m_n), \end{cases} \qquad (3)$$

Якщо хоч одне з порівнянь наведеної системи не має розв'язків, то система несумісна.

3.2. Фундаментальні теореми

Теорема 1. Нехай $НСД(m_1, m_2) = d$ – найбільший спільний дільник чисел $m_1 \text{і} m_2$, а $НСК(m_1, m_2) = M$ – їх найменше спільне кратне. Система двох порівнянь

$$\begin{cases} x \equiv c_1 (\text{mod}\, m_1), \\ x \equiv c_2 (\text{mod}\, m_2) \end{cases} \tag{4}$$

має розв'язок

$$x \equiv x_0 (\text{mod}\, M) \tag{5}$$

тільки за умови, що $c_2 \equiv c_1 (\text{mod}\, d)$.

Наслідок. Якщо $m_1 \text{і} m_2$ – взаємно прості числа, то $d = 1$ і система (4) завжди має єдиний розв'язок.

Метод підстановки. Якщо розв'язується система (3), що складається з n порівнянь, то спочатку необхідно розв'язати будь-які два з них і замінити їх у системі (3) виразом (5). Далі взяти здобуте порівняння і третє з системи та розв'язати їх і т.д. У кожним таким кроком кількість порівнянь у системі зменшується і наприкінці дістанемо одне порівняння вигляду (5), де M– найменше спільне кратне всіх модулів.

Теорема 2 (китайська теорема про остачі). Нехай в системі (3) модулі $m_1, m_2 \ ..., \ m_n$ – попарно взаємно прості; M – найменше спільне кратне чисел $m_1, \ m_2 \ ..., \ m_n$; числа $y_1, y_2, \ ..., y_n$ підібрані так, що виконуються порівняння $\frac{M}{m_1} y_1 \equiv 1 (\text{mod}\, m_1)$, $\frac{M}{m_2} y_2 \equiv 1 (\text{mod}\, m_2), \ldots, \frac{M}{m_n} y_n \equiv 1 (\text{mod}\, m_n)$.

Тоді система (3) матиме єдиний розв'язок $x \equiv x_0 (\text{mod}\, M)$, де $x_0 = \frac{M}{m_1} y_1 c_1 + \frac{M}{m_2} y_2 c_2 + \ldots + \frac{M}{m_n} y_n c_n$.

3.3. Приклад рішення задачі

Розв'язати систему порівнянь $\begin{cases} x \equiv 6 (\text{mod}\, 17), \\ x \equiv 4 (\text{mod}\, 11), \\ x \equiv -3 (\text{mod}\, 8). \end{cases}$

Рішення. 17, 11, 8 - попарно взаємно прості; $M = НСК(17,11,8) = 1496$ – найменше спільне кратне модулів.

I спосіб. Використовуючи метод підстановки, на початку вирішимо систему, що складається із останніх двох порівнянь: $\begin{cases} x \equiv 4 (\mathrm{mod} 11), \\ x \equiv -3 (\mathrm{mod} 8). \end{cases}$

Система має розв'язок, бо $НСД(11,18) = 1$. Друге порівняння системи свідчить, що $x = -3 + 8t, t = 0, \pm 1, \pm 2, \ldots$ Підставимо цей вираз замість x у перше порівняння: $-3 + 8t \equiv 4 (\mathrm{mod} 11)$ або $8t \equiv 7 (\mathrm{mod} 11)$, де $t = 0, \pm 1, \pm 2, \ldots$ Розв'яжемо порівняння за розширеним алгоритмом Евкліда (табл. 4).

Таблиця 4

Остача	Частка	x	y
11	-	1	0
8	-	0	1
3	1	$1 - 1 \cdot 0 = 1$	$0 - 1 \cdot 1 = -1$
2	2	$0 - 2 \cdot 1 = -2$	$1 - 2 \cdot (-1) = 3$
1	1	$1 - 1 \cdot (-2) = 3$	$-1 - 1 \cdot 3 = -4$
0	2	-	-

$НСД(11,18) = 1$; $1 = 11 \cdot 3 - 4 \cdot 8$. Оберненим елементом до числа 8 за модулем 11 є число –4, крім того, $-4 \equiv 7 (\mathrm{mod} 11)$. Помножимо порівняння на 7:

$$t \equiv 7 \cdot 7 (\mathrm{mod} 11) \equiv 49 (\mathrm{mod} 11) \equiv 5 (\mathrm{mod} 11) \Rightarrow t = 5 + 11k, k = 0, \pm 1, \pm 2, \ldots$$

Підставимо значення t у вираз для x:

$x = -3 + 8 \cdot (5 + 11k) = 37 + 88k \Rightarrow x \equiv 37 (\mathrm{mod} 88)$.

Далі вирішимо систему, яка складається із здобутого порівняння та першого порівняння (що залишився) початкової системи

$$\begin{cases} x \equiv 6 (\mathrm{mod} 17), \\ x \equiv 37 (\mathrm{mod} 88). \end{cases}$$

Система має розв'язок, бо $НСД(17,88) = 1$. Перше порівняння системи свідчить, що $x = 6 + 17t, t = 0, \pm 1, \pm 2, \ldots$ Підставимо цей вираз замість x у друге порівняння: $6 + 17t \equiv 37 (\mathrm{mod} 88)$ або $17t \equiv 31 (\mathrm{mod} 88)$, де $t = 0, \pm 1, \pm 2, \ldots$ Розв'яжемо порівняння за розширеним алгоритмом Евкліда (табл. 5).

$НСД(17,88) = 1$; $1 = 88 \cdot 6 - 31 \cdot 17$. Оберненим елементом до числа 17 за модулем 88 є число –31, крім того, $-31 \equiv 57 (\mathrm{mod} 88)$. Помножимо порівняння на 57:

$$t \equiv 57 \cdot 31 (\mathrm{mod} 88) \equiv 1767 (\mathrm{mod} 88) \equiv 7 (\mathrm{mod} 88) \Rightarrow t = 7 + 88k, k = 0, \pm 1, \pm 2, \ldots$$

Таблиця 5

Остача	Частка	x	y
88	-	1	0
17	-	0	1
3	5	$1-5\cdot 0=1$	$0-5\cdot 1=-5$
2	5	$0-5\cdot 1=-5$	$1-5\cdot(-5)=26$
1	1	$1-1\cdot(-5)=6$	$-5-1\cdot 26=-31$
0	2	-	-

Підставимо значення t у вираз для x:

$$x=6+17\cdot(7+88k)=125+1496k \Rightarrow x\equiv 125(\mathrm{mod}1496).$$

Відповідь: $x\equiv 125(\mathrm{mod}1496)$ - за методом підстановки.

ІІ спосіб. За китайською теоремою про остачі знайдемо:

1) $\frac{1496}{17}y_1\equiv 1(\mathrm{mod}17),\ 88y_1\equiv 1(\mathrm{mod}17),\ 3y_1\equiv 1(\mathrm{mod}17)\Rightarrow y_1=6;$

2) $\frac{1496}{11}y_2\equiv 1(\mathrm{mod}11),\ 136y_2\equiv 1(\mathrm{mod}11),\ 4y_2\equiv 1(\mathrm{mod}11)\Rightarrow y_2=3;$

3) $\frac{1496}{8}y_3\equiv 1(\mathrm{mod}8),\ 187y_3\equiv 1(\mathrm{mod}8),\ 3y_3\equiv 1(\mathrm{mod}8)\Rightarrow y_3=3;$

4) $x\equiv 88\cdot 6\cdot 6+136\cdot 3\cdot 4-187\cdot 3\cdot 3(\mathrm{mod}1496);$

$x\equiv 3168+1632-1683=3117(\mathrm{mod}1496)\Rightarrow x\equiv 125(\mathrm{mod}1496).$

Відповідь: $x\equiv 125(\mathrm{mod}1496)$ - за китайською теоремою про остачі.

Висновок: початкова система із трьох порівнянь має розв'язок $x\equiv 125(\mathrm{mod}1496)$, який одержаний як за методом підстановки, так і за китайською теоремою про остачі, тобто система вирішена вірно.

4. Контрольні питання

1. Лишок. Модуль. Приклади.
2. Порівняння (конгруенція) та їх запис. Приклади.
3. Властивості порівнянь.
4. Лінійне порівняння. Приклади.
5. Теореми Ейлера.
6. Скінченні ланцюгові дроби та їх властивості.
7. Евклідовий алгоритм.
8. Розширений евклідовий алгоритм.

9. Умови існування рішення порівнянь першого степеня.

10. Способи рішення порівнянь першого степеня.

11. Рішення порівнянь першого степеня за допомогою випробування лишків повної системи за модулем.

12. Рішення порівнянь першого степеня за допомогою теореми Ейлера.

13. Рішення порівнянь першого степеня за допомогою властивостей скінченних ланцюгових дробів.

14. Рішення порівнянь першого степеня за допомогою розширеного евклідового алгоритму.

15. Визначення системи порівнянь.

16. Визначення системи порівнянь першого степеня.

17. Способи рішення системи порівнянь першого степеня.

18. Фундаментальні теореми.

19. Рішення порівнянь першого степеня за методом підстановки.

20. Рішення порівнянь першого степеня за китайською теоремою.

БІБЛІОГРАФІЧНИЙ СПИСОК

1. Пахомова В. М Дистанційний курс в системі «Лідер» з дисципліни «Математичні основи інформаційної безпеки» для здобувачів ступеня «бакалавр» спеціальності «Кібербезпека». Сертифікат ДК0304 від 03.07.2019. *Український державний університет науки і технологій.*
2. Pakhomova V. Methodology for the formation of competences of first degree holders in the discipline «Mathematical foundation of information security». *Modern engineering and innovative technologies*. Germany, Karlsruhe : Sergeieva&Co, «ISE&E». 2023. Issue 25. Part 2. pp. 29-33.
3. Pakhomova V. Methods of forming competencies in applicants for the specialty «Cybersecurity» when performing a course assignment in the discipline «Mathematical foundation of information security». International scientific publication *«Technique and technology of the future'2024»*. Germany, Karlsruhe.
4. Математичні основи криптографії : навч. посіб. / Кузнецов Г. В., Фомичов В. В., Сушко С. О., Фомичова Л. Я. Дніпропетровськ : НГУ, 2004. 391 с.
5. Coutinho S. C. The mathematics of ciphers. Number theory and RSA cryptography. New York, 1999. 198 p.

Навчально-методичне видання

Пахомова Вікторія Миколаївна

МАТЕМАТИЧНІ ОСНОВИ ІНФОРМАЦІЙНОЇ БЕЗПЕКИ

Навчально-методичні рекомендації
щодо виконання курсового завдання

В авторській редакції
Комп’ютерна верстка В. М. Пахомової

Експертний висновок склав проф. І. В. Жуковицький

Зареєстровано НМВ УДУНТ (№ 774 від 04.11.2024)

Формат 60х84 1/16. Ум. друк. арк. 0,93. Обл.-вид. арк. 0,37.
Зам. № 98.

Видавець; Український державний університет науки і технологій
вул. Лазаряна, 2, ауд. 2216, м. Дніпро, 49010.
Свідоцтво суб’єкта видавничої справи ДК № 7709 від 14.12.2022

Адреса видавця та дільниці оперативної поліграфії:
вул. Лазаряна, 2, Дніпро, 49010