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 лабораторних робіт

ДНІПРО
2024

УДК 004.056:519.87(076.5)
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 лабораторних робіт / упоряд.: В. М. Пахомова ; Укр. держ. ун-т науки і технологій. – Дніпро : УДУНТ, 2024. – 35 с.

Навчально-методичні рекомендації призначені для використання студентами безвідривної форми навчання спеціальності 125 «Кібербезпека та захист інформації» під час виконання лабораторних робіт з дисципліни «Математичні основи інформаційної безпеки».

Іл. 1. Табл. 10. Бібліогр. назв. 3.

ЗМІСТ

ВСТУП

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

Виконання здобувачами лабораторних робіт сприяють досягненню наступних результатів навчання: застосовувати теорії та методи захисту для забезпечення безпеки інформації в інформаційно-телекомунікаційних системах; застосовувати теорії та методи захисту для забезпечення безпеки елементів інформаційно-телекомунікаційних систем.

У [2] автором запропонована методика «MathFISLearn» щодо формування компетентностей здобувачів ступеня «бакалавр» при дистанційному навчанні з дисципліни «Математичні основи інформаційної безпеки»: 1) вивчення основних математичних понять, теорем та методів за наступними розділами: теорія подільності; теорія розкладання; теорія чисел; теорія лишків та теорія алгебраїчних структур під час лекційних занятій, що проводяться за допомогою системи «Zoom», 2) алгоритмізація та програмування щодо реалізації: алгоритму Евкліда; розширеного евклідового алгоритму; алгоритму Ферма; розкладання числа діленням методом проб; решета Ератосфена; тесту Міллера та організації відповідних досліджень під час лабораторних робіт, 3) придбання практичних навиків розв’язання систем порівнянь за модулем на основі різних математичних підходів та засобів під час виконання самостійної роботи з використанням рекомендованих джерел, 4) опрацьовування теоретичного матеріалу з використанням презентацій лектора та проходження тестування в системі «Лідер». У [3] автором запропонована методика «SoftSkillsMathFIS» щодо формування відповідних навичок: розвиток уміння керувати власним часом; здатність працювати в команді; розвиток членів команди, коли результат групи визначається як сумарний і враховує досягнення кожного студента групи при виконанні бригадних завдань, що передбачені в роботах № 2_2 і № 4_2 з цієї дисципліни.

У методичних рекомендаціях представлені чотири роботи (кожна складається із двох частин). До кожної лабораторної роботи подані: теоретичні відомості, розв’язання контрольного прикладу, постановка та варіанти індивідуального завдання, а також послідовність виконання роботи та зміст звіту. Крім того, на при кінці кожної лабораторної роботи представлені контрольні питання та завдання щодо захисту відповідної теми, а на при кінці навчально-методичного видання поданий перелік використаних джерел [1-5].

ЛАБОРАТОРНА РОБОТА № 1_1

Тема: Фундаментальні алгоритми ділення: алгоритм Евкліда.

Мета: 1. Вивчити алгоритм Евкліда.

2. Набути практичні навики в алгоритмізації та програмуванні алгоритму Евкліда.

1. ТЕОРЕТИЧНІ ВІДОМОСТІ

1.1. Подільність чисел

Будь-яке ціле, на яке діляться одночасно цілі $a,b,\ldots,c$, називають їх спільним дільником. Найбільший із спільних дільників чисел називають **найбільшим спільним дільником (НСД)** та позначають $НСД(a,b,c)$.

Властивості НСД:

1. Якщо $a = bq$, $НСД(a,b) = b$.
2. Якщо $a = bq + r$, то спільні дільники чисел a і b збігаються із спільними дільниками чисел b і r. Зокрема, $НСД(a,b) = НСД(b,r)$.
3. Для будь-якого додатного цілого числа m виконується рівність $НСД(am,bm) = mНСД(a,b)$.
4. Якщо $НСД(a,b) = 1$, то $НСД(ac,b) = НСД(c,b)$.
5. Якщо $НСД(a,b) = 1$ і $ac : b$, то $c : b$.

Найбільший спільний дільник можна визначити за евклідовим алгоритмом.

Алгоритм Евкліда. Нехай в результаті ділення натуральних чисел a, b отримаємо залишок, який позначимо r_1. Якщо r_1 відмінно від нуля, то виконаємо ділення b на r_1. Отриманий залишок позначимо через r_2. Якщо r_2 відмінно від нуля, то виконаємо ділення r_1 на r_2 і т.д. На i-му кроці виконається одне ділення залишку отриманого на кроці $i-2$, на залишок, отриманий на $i-1$ кроці. Найбільшим спільним дільником натуральних чисел a,b є останній залишок, відмінний від нуля.

Покроковий алгоритм Евкліда.

Введення: натуральні числа a і b, $a \geq b$.

Виведення: $НСД(a,b)$.

Крок 1. Покласти $A = a$ *і* $R = B = b$.

Крок 2. Замінити значення R залишком від ділення A на B і перейти на крок 3.

Крок 3. Якщо $R = 0$, то повідомити: «найбільший спільний дільник чисел *a* і *b* дорівнює *B*», і зупинитися; в протилежному випадку перейти на крок 4.

Крок 4. Замінити значення *A* на значення *B*, значення *B* на значення *R* і повернутися на крок 2.

Зауваження: кількість *k* операцій послідовного ділення в евклідовому алгоритмі, потрібних для пошуку НСД натуральних чисел a і b ($a \geq b$), задовольняє умови: 1) $k < 5\lg b$; 2) $k < \frac{3}{2}\log_2 b$.

Будь-яке ціле, яке ділиться без остачі на всі дані числа *a,b,…,c*, називають їх спільним кратним. Найменше додатне спільне кратне називають **найменшим спільним кратним (НСК)** та визначають за формулою

$$\text{НСК}(a,b) = \frac{ab}{НСД(a,b)}. \qquad (1)$$

1.2. Ланцюгові дроби

Нехай α - дійсне число. Тоді його можна подати у вигляді:

$$\alpha = a_0 + \frac{1}{\alpha_1}, \text{ де } 0 < \frac{1}{\alpha_1} < 1;$$

$$\alpha_1 = a_1 + \frac{1}{\alpha_2}, \text{ де } 0 < \frac{1}{\alpha_2} < 1;$$

$$\alpha_2 = a_2 + \frac{1}{\alpha_3}, \text{ де } 0 < \frac{1}{\alpha_3} < 1;$$

$$\alpha_3 = a_3 + \frac{1}{\alpha_4}, \text{ де } 0 < \frac{1}{\alpha_4} < 1.$$

…

Тоді кінцеве число α прийме вигляд

$$\alpha = a_0 + \cfrac{1}{a_1 + \cfrac{1}{a_2 + \cfrac{1}{a_3 + \cfrac{1}{\ddots + \cfrac{1}{a_n}}}}} \qquad (2)$$

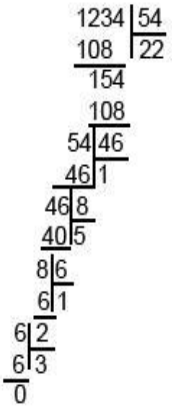
Подання дійсного числа у вигляді (2) називається **правильним скінченним ланцюговим дробом (неперервним дробом)**, де α_0 - число, ціле, a_1, a_2, …, a_n - натуральні числа, які називаються елементами

неперервного дробу. Коротка форма запису неперервного дробу $\alpha = [a_0; a_1, a_2, a_3, ..., a_n]$

1.3. Контрольний приклад

Знайти $НСД(1234,54)$ та $НСК(1234,54)$. Скласти повну та коротку форму неперервного дробу.

За алгоритмом Евкліда:



Отже, $НСД(1234,54) = 2$ та

$НСК(1234,54) = 33318$.

Повна форма запису неперервного дробу:

$$\frac{1234}{54} = 22 + \cfrac{1}{1 + \cfrac{1}{5 + \cfrac{1}{1 + \cfrac{1}{3}}}}$$

Коротка форма запису неперервного дробу: $\frac{1234}{54} = [22;1,5,1,3]$.

2. ІНДИВІДУАЛЬНЕ ЗАВДАННЯ

Використовуючи алгоритм Евкліда, знайти $НСД(a,b)$ та $НСК(a,b)$. Числа a,b подані в табл.1.1 згідно з варіантом. Скласти повну та коротку форми неперервного дробу $\frac{a}{b}$.

Таблиця 1.1

№ вар.	***1***	***2***	***3***	***4***	***5***	***6***	***7***	***8***	***9***	***10***
a	3508	2524	6643	3242	3242	3242	6188	81719	81719	8719
b	142	180	2873	272	828	282	4709	52003	33649	3107

Продовження табл. 1.1

№ вар.	***11***	***12***	***13***	***14***	***15***	***16***	***17***	***18***	***19***	***20***
a	5200	2003	3364	1634	5391	525	1360	3382	2204	7206
b	3364	307	1010	104	3976	231	98	108	282	429

Продовження табл. 1.1

№ вар.	***21***	***22***	***23***	***24***	***25***	***26***	***27***	***28***	***29***	***30***
a	1656	67298	1173	3150	18527	7650	2747	6499	12769	3503
b	1150	60214	323	1386	4171	2971	2173	2077	7571	2231

3. ПОСЛІДОВНІСТЬ ВИКОНАННЯ

3.1. Ознайомитися з теоретичними відомостями.

3.2. За алгоритмом Евкліда скласти блок-схему знаходження $НСД(a,b)$, $НСК(a,b)$ та перевірити її на контрольному прикладі.

3.3. За блок-схемою скласти програму та налагодити її за ЕОМ на контрольному прикладі.

3.4. Отримати у викладача варіант індивідуального завдання і виконати його математичне розв'язання (у письмовому вигляді).

3.5. Подати викладачу на ЕОМ рішення контрольного прикладу та індивідуального завдання.

3.6. Оформити звіт із лабораторної роботи:

- тема і мета лабораторної роботи;
- схема знаходження $НСД(a,b)$, $НСК(a,b)$ та її перевірка на контрольному прикладі;
- математичне розв'язання індивідуального завдання (у письмовому вигляді): ділення за Евклідом, повна та коротка форми неперервного дробу;
- роздрукований текст програми;
- роздруковані результати роботи програми (контрольний приклад та індивідуальне завдання);
- висновки складаються із 4-х пунктів (п.1- призначення алгоритму Евкліда; п.2- загальна характеристика складеної блок-схеми покрокового алгоритму Евкліда та її перевірка на контрольному прикладі; п.3- загальна характеристика створеної програмі на основі складеної блок-схеми алгоритму та її тестування на контрольному прикладі; п.4- співставлення отриманих результатів математичного та програмного розв'язання індивідуального завдання).

Зауваження:

1) схема алгоритму зобразити у звіті акуратно (з використанням лінійки та олівця), див. приклади в ДОДАТКУ;

2) на роздрукованому тексті програми і результатах її роботи слід вказати дату виконання, номер і тему лабораторної роботи, ПІБ та групу студента, номер варіанта індивідуального завдання.

ЛАБОРАТОРНА РОБОТА № 1_2

Тема: Фундаментальні алгоритми ділення: розширений алгоритм Евкліда.

Мета: 1. Вивчити розширений алгоритм Евкліда.

2. Набути практичні навики в алгоритмізації та програмуванні розширеного алгоритму Евкліда.

1. ТЕОРЕТИЧНІ ВІДОМОСТІ

1.1. Теорема Евкліда

Нехай d найбільший спільний дільник деяких натуральних чисел a і b. Тоді існують такі цілі числа α і β, що $\alpha a + \beta b = d$.

Обчислити значення α і β можна за допомогою **розширеного евклідового алгоритму,** який поданий у вигляді табл. 1.2.

Таблиця 1.2

Залишки	Часткові	x	y
a	*	x_{-1}	y_{-1}
b	*	x_0	y_0
r_1	q_1	x_1	y_1
r_2	q_2	x_2	y_2
r_3	q_3	x_3	y_3
...	...	...	...
r_{n-2}	q_{n-2}	x_{n-2}	y_{n-2}
r_{n-1}	q_{n-1}	x_{n-1}	y_{n-1}
r_n	q_n	*	*

Примітка: $x_{-1} = 1,\ x_0 = 0,\ y_{-1} = 0,\ y_0 = 1,\ \alpha = x_{n-1},\ \beta = y_{n-1}$.

$x_j = x_{j-2} - q_j x_{j-1};\ \ y_j = y_{j-2} - q_j y_{j-1}$, де $j = 1,...,n-1$.

1.2. Контрольний приклад

За розширеним евклідовим алгоритмом знайти $НСД(1234,54)$.

Розв'язання. Складемо таблицю за розширеним евклідовим алгоритмом (табл. 1.3).

Таблиця 1.3

Залишки	Часткові	x	y
1234	*	1	0
54	*	0	1
46	22	$1 - 22 \cdot 0 = 1$	$0 - 22 \cdot 1 = -22$
8	1	$0 - 1 \cdot 1 = -1$	$1 - 1 \cdot (-22) = 23$
6	5	$1 + 1 \cdot 5 = 6$	$-22 - 23 \cdot 5 = 137$
2	1	$-1 - 1 \cdot 6 = -7$	$23 - (-137) \cdot 1 = 160$
0	3	*	*

Отже, $НСД(1234,54) = -7 \cdot 1234 + 160 \cdot 54 = -8638 + 8640 = 2$ та $НСК(1234,54) = 33318$.

2. ІНДИВІДУАЛЬНЕ ЗАВДАННЯ

Використовуючи розширений алгоритм Евкліда, знайти $НСД(a,b)$ та $НСК(a,b)$. Числа a,b подані в табл.1.1 згідно з варіантом (див. лаб. роб. №1_1).

3. ПОСЛІДОВНІСТЬ ВИКОНАННЯ

3.1. Ознайомитися з теоретичними відомостями.

3.2. За розширеним алгоритмом Евкліда скласти блок-схему знаходження $НСД(a,b)$, $НСК(a,b)$ та перевірити її на контрольному прикладі.

3.3. За блок-схемою скласти програму та налагодити її на контрольному прикладі з використанням ЕОМ.

3.4. Виконати математичне розв'язання індивідуального завдання (у письмовому вигляді).

3.5. Подати викладачу на ЕОМ рішення контрольного прикладу та індивідуального завдання.

3.6. Зіставити результати визначення $НСД(a,b)$ за двома алгоритмами.

3.7. Оформити звіт із лабораторної роботи:

- тема і мета лабораторної роботи;
- схема визначення $НСД(a,b)$ за розширеним алгоритмом Евкліда та її перевірка на контрольному прикладі;
- математичне розв'язання індивідуального завдання (у письмовому вигляді);
- роздрукований текст програми;
- роздруковані результати роботи програми (контрольний приклад та індивідуальне завдання);
- висновки складаються із 5-ти пунктів (п.1- призначення розширеного евклідового алгоритму; п.2- загальна характеристика складеної блок-схеми за розширеним евклідовим алгоритмом та її перевірка на контрольному прикладі; п.3- загальна характеристика створеної програмі на основі складеної блок-схеми алгоритму та її тестування на контрольному прикладі; п.4- отримані результати математичного та програмного розв'язання індивідуального завдання; п.5- співставлення отриманих результатів

контрольного прикладу та індивідуального завдання на основі використання двох підходів).

3.8. Підготуватися до захисту теми «***Теорія подільності***».

КОНТРОЛЬНІ ПИТАННЯ до теми «*Теорія подільності*»

I. ТЕОРІЯ

1. Визначення кратного і дільника. Приклади.

2. Теореми 1-2 та їх доказ.

3. Теорема розподілу та її доказ.

4. Визначення НСД та його властивості. Взаємно прості і попарно прості числа. Обчислення НСК. Приклади.

5. Леми 1-2 та їх доказ.

6. Алгоритм Евкліда, доказ його коректності.

7. Розширений алгоритм Евкліда. Теорема.

8. Поняття неперервного дробу. Приклад. Зв'язок алгоритму Евкліда з неперервними дробами.

9. Визначення придатних дробів та їх обчислення. Приклади.

10. Розкладання раціонального числа в неперервний дріб і складання таблиці підхідних дробів. Приклад.

II. ПРАКТИКА

11. Знайти $НСД(a,b)$, використовуючи алгоритм Евкліда, та побудувати відповідну таблицю (числа *a,b* з табл. 1.1).

12. Знайти $НСД(a,b)$, використовуючи розширений алгоритм Евкліда, та побудувати відповідну таблицю (числа *a,b* з табл. 1.1).

13. Розкласти число $\alpha = \frac{a}{b}$ (числа *a,b* з табл. 1.1) у неперервний дріб і побудувати таблицю підхідних дробів.

14. Скласти схему алгоритму розподілу.

Введення: натуральні числа *a* і *b*.

Виведення: ненегативні цілі числа *q* і *r*, для яких виконана рівність: $a = bq + r$ і $0 \le r < b$.

Крок 1. Покласти $Q = 0$ і $R = a$.

Крок 2. Якщо $R < b$, то повідомити: «частка дорівнює *Q*, а залишок дорівнює *R*», і зупинитися; у противному випадку перейти до кроку 3.

Крок3. Якщо $R \ge b$, то відняти *b* з *R*, збільшити *Q* на 1 і повернутися до кроку 2.

Виконати на прикладі перевірку складеної схеми.

15. Скласти схему алгоритму: яка частина випадково згенерованих пар цілих чисел складається з взаємно простих чисел.

Введення: натуральне число m, загальна кількість генерованих пар.

Виконання: до кожної з цих пар застосовується алгоритм Евкліда, що визначає їх НСД, а потім підраховується число пар, для яких він дорівнює 1.

Виведення: $\frac{число\quad пар\quad взаємно\quad простих\quad чисел}{m}$.

ЛАБОРАТОРНА РОБОТА № 2_1

Тема: Розкладання числа на множники методом проб

Мета: 1. Вивчити алгоритм розкладання числа шляхом ділення методом проб.

2. Набути практичних навичок в алгоритмізації і програмуванні алгоритму.

1. ТЕОРЕТИЧНІ ВІДОМОСТІ

1.1. Основна теорема арифметики

Для будь-якого цілого числа $m \neq 1$ існує єдине канонічне розкладання на прості множники (із точністю до їх перестановки), тобто

$$m = p_1^{k_1} p_2^{k_2} \ldots p_n^{k_n}, \tag{3}$$

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

Наслідки

1. Число $m = p_1^{k_1} p_2^{k_2} \ldots p_n^{k_n}$ ділиться на число b тоді і тільки тоді, коли $b = p_1^{t_1} p_2^{t_2} \ldots p_n^{t_n}$, де $0 \le t_1 \le k_1$, $0 \le t_2 \le k_2$, … , $0 \le t_n \le k_n$.

2. Число $m = p_1^{k_1} p_2^{k_2} \ldots p_n^{k_n}$ тоді і тільки тоді буде точним l–м степенем деякого цілого числа, коли всі показники $p_1, p_2, \ldots, p_n$ будуть подільними на число l.

3. Кількість усіх дільників числа $m = p_1^{k_1} p_2^{k_2} \ldots p_n^{k_n}$ можна обчислити за формулою

$$\tau(m) = (k_1 + 1)(k_2 + 1)\ldots(k_n + 1). \tag{4}$$

Сума усіх дільників вказаного числа дорівнює

$$S(m)=\frac{p_1^{k_1+1}-1}{p_1-1}\cdot\frac{p_2^{k_2+1}-1}{p_2-1}\cdot\ldots\ \cdot\frac{p_n^{k_n+1}-1}{p_n-1} \qquad (5)$$

Функції $\tau(m)$ та $S(m)$ визначені тільки для цілих додатних значень (такі функції називають арифметичними).

Контрольний приклад. Знайти кількість та суму всіх дільників числа 60.

Розв'язання. Канонічне розкладання числа $60=2^2\cdot3\cdot5$. Отже,

$$\tau(60)=(2+1)(1+1)(1+1)=12;$$

$$S(60)=\frac{2^3-1}{2-1}\cdot\frac{3^2-1}{3-1}\cdot\frac{5^2-1}{5-1}=168.$$

Зауваження. Нехай $a=p_1^{k_1}p_2^{k_2}\ldots p_n^{k_n}$, $b=p_1^{m_1}p_2^{m_2}\ldots p_n^{m_n}$ - відповідно канонічні розкладання на множники чисел *a* і *b*, причому деякі показники k_i і m_i можуть дорівнювати нулю. Тоді найбільший спільний дільник чисел *a* і *b* визначиться за формулою

$$НСД(a,b)=p_1^{t_1}p_2^{t_2}\ldots\ p_n^{t_n}\text{, де } t_i=\min\{k_i;m_i\},\ i=1,2,\ldots n, \qquad (6)$$

а найменше спільне кратне цих чисел дорівнюватиме

$$НСК(a,b)=p_1^{s_1}p_2^{s_2}\ldots\ p_n^{s_n},\quad \text{де } s_i=\max\{k_i;m_i\},\ i=1,2,\ldots n. \qquad (7)$$

Приклад. Обчислити найбільший спільний дільник та найменше спільне кратне чисел $a=1400$ і $b=294$.

Розв'язання. Запишемо канонічні розкладання чисел:

$$a=1400=2^3\cdot3^0\cdot5^2\cdot7;\ \ b=294=2\cdot3\cdot5^0\cdot7^2.$$

Тоді $НСД(a,b)=2\cdot3^0\cdot5^0\cdot7=14;\ НСК(a,b)=2^3\cdot3\cdot5^2\cdot7^2=29400.$

1.2. Алгоритм розкладання шляхом ділення методом проб

Введення: натуральне число *n*.

Виведення: натуральне число $F>1$ – найменший простий дільник числа *n* або повідомлення про те, що *n* просте.

Крок 1. Покласти $F=2$.

Крок 2. Якщо $\frac{n}{F}$ ціле, то повідомити: «*F* є дільником числа *n*» і завершити роботу; інакше перейти до кроку 3.

Крок 3. Збільшити *F* на одиницю і перейти до кроку 4.

Крок 4. Якщо $F>\left[\sqrt{n}\right]$, то повідомити: «*n* просте» і завершити роботу; інакше перейти до кроку 2.

2. ІНДИВІДУАЛЬНЕ ЗАВДАННЯ

Знайти канонічне розкладання числа *n* на множники. Обчислити кількість та суму всіх дільників числа *n*. Число *n* взяти з табл. 2.1 за варіантом.

Таблиця 2.1

№ вар.	***1***	***2***	***3***	***4***	***5***	***6***	***7***	***8***	***9***	***10***
n	3542	6188	525	272	282	828	470	520	3364	3010

Продовження табл. 2.1

№ вар.	***11***	***12***	***13***	***14***	***15***	***16***	***17***	***18***	***19***	***20***
n	3634	920	3976	2310	480	920	285	366	840	760

Продовження табл. 2.1

№ вар.	***21***	***22***	***23***	***24***	***25***	***26***	***27***	***28***	***29***	***30***
n	1000	2800	1500	1680	970	860	4286	1110	999	478

3. ПОСЛІДОВНІСТЬ ВИКОНАННЯ

3.1. Ознайомитися з алгоритмом розкладання числа.

3.2. Отримати у викладача варіант індивідуального завдання. Використовуючи даний алгоритм, виконати математичне розв’язання індивідуального завдання (у письмовому вигляді).

3.3. Скласти блок-схему алгоритму та відповідну програму для розкладання числа шляхом ділення методом проб.

3.4. Виконати індивідуальне завдання на ЕОМ. Представити викладачеві роботу програми на ЕОМ.

3.5. Оформити звіт із лабораторної роботи:

- тема і мета лабораторної роботи;

- схема алгоритму розкладання числа на множники;

- розв’язання індивідуального завдання (у письмовому вигляді): канонічний розклад числа та обчислення функцій $\tau(m)$ та $S(m)$;

- роздрукований текст програми;

- роздруковані результати роботи програми;

- математичне обчислення НСД і НСК (у письмовому вигляді) з використанням канонічних розкладів чисел, що досліджуються в ЛАБ№1;

- висновки складаються із 5-ти пунктів (п.1- призначення алгоритму, що вивчається; загальна характеристика складеної блок-схеми за алгоритмом розкладання числа шляхом ділення методом проб та її перевірка на контрольному прикладі; п.3- загальна характеристика створеної програмі на основі складеної блок-схеми алгоритму та її тестування на контрольному

прикладі; п.4- результати математичного та програмного розв'язання індивідуального завдання; п.5- співставлення отриманих результатів контрольного прикладу та індивідуального завдання з використанням трьох підходів).

ЛАБОРАТОРНА РОБОТА № 2_2

Тема: Розкладання числа на множники за допомогою алгоритму Ферма

Мета: 1. Вивчити алгоритм Ферма.

2. Набути практичних навичок в алгоритмізації і програмуванні алгоритму Ферма.

1. ТЕОРЕТИЧНІ ВІДОМОСТІ

1.1. Складене число

Натуральне число $n > 1$ називають **складеним**, якщо n має принаймні один інший додатний цілий дільник, відмінний від 1 і самого себе. Таким чином, якщо n – складене число, то у n є такий цілий дільник a, що $n = ab$, $1 < b < n$, $b = \frac{n}{a}$. Очевидно, усі парні числа, крім 2, - складені.

1.2. Алгоритм Ферма

Введення: непарне натуральне число n.

Виведення: множник числа n або повідомлення про те, що n просте.

Крок 1. Покласти $x = \lceil \sqrt{n} \rceil$. Якщо $n = x^2$, то x є дільником числа n і робота алгоритму зупиняється; інакше збільшити x на 1 і перейти до кроку 2.

Крок 2. Якщо $x = \frac{n+1}{2}$, то число n просте і робота алгоритму зупиняється; інакше обчислити $y = \sqrt{x^2 - n}$.

Крок 3. Якщо число y ціле, тобто якщо $[y]^2 = x^2 - n$, то n розкладається в добуток $(x + y)(x - y)$ і робота алгоритму зупиняється; інакше збільшити x на 1 і перейти до кроку 2.

1.3. Контрольний приклад. За допомогою алгоритму Ферма розкласти число n = 45 на множники.

Розв'язання. Запишемо $x = \lceil \sqrt{n} \rceil = \lceil \sqrt{45} \rceil = 6$.

Якщо $n = x^2$? $45 = 6^2$? – ні, тоді $x = 6 + 1 = 7$.

Якщо $x = (n + 1)/2$? $7 = (45 + 1)/2$? – ні, тоді $y = \sqrt{x^2 - n} = \sqrt{7^2 - 45} = \sqrt{4} = 2$.

Якщо $[y]^2 = x^2 - n$? $2^2 = 7^2 - 45$? – так, тоді $n = (x + y)(x - y)$, тобто

$$45 = (7 + 2)(7 - 2) = 9 * 5.$$

2. БРИГАДНЕ ЗАВДАННЯ

За допомогою алгоритму Ферма розкласти число *n* на множники. Число *n* взяти з табл. 2.2 відповідно до варіанта.

Таблиця 2.2

№ вар.	***1***	***2***	***3***	***4***	***5***	***6***
n	1342127	175557	835107	1897637	2929997	2027651281

3. ПОСЛІДОВНІСТЬ ВИКОНАННЯ

3.1. Ознайомитися з алгоритмом Ферма.

3.2. Отримати у викладача варіант бригадного завдання. Використовуючи даний алгоритм, виконати математичне розв’язання бригадного завдання (у письмовому вигляді).

3.3. Скласти блок-схему за алгоритмом Ферма та відповідну програму. Представити викладачеві роботу програми на ЕОМ.

3.4. Бригадою організувати та провести дослідження різноманітних чисел (малих і великих, парних і непарних) з використанням засобів: алгоритму розкладання числа шляхом ділення методом проб та алгоритму Ферма. Отримані результати звести до таблиці.

3.5. Оформити звіт із лабораторної роботи:

- тема і мета лабораторної роботи;

- склад бригади та зміст проведеного дослідження (обсяг виконання кожного члена бригади);

- розв’язання контрольного прикладу та бригадного завдання (у письмовому вигляді);

- схема алгоритму розкладання числа на множники;

- роздрукований текст програми;

- роздруковані результати роботи програми (контрольний приклад і бригадне завдання);

- висновки складаються із 5-ти пунктів (п.1- призначення алгоритму Ферма; загальна характеристика складеної блок-схеми за алгоритмом Ферма та її перевірка на контрольному прикладі; п.3- загальна характеристика створеної програмі на алгоритмом Ферма та її тестування на контрольному прикладі; п.4- результати математичного та програмного розв’язання бригадного завдання; п.5- співставити можливості двох алгоритмів щодо розкладу числа на основі проведеного бригадою дослідження).

3.6. Підготуватися до захисту теми ***«Теорія розкладання».***

КОНТРОЛЬНІ ПИТАННЯ до теми *«Теорія розкладання»*

1. Визначення простого і складеного числа. Приклади.
2. Теореми 1-4 і їх докази.
3. Лема і її доказ.
4. Фундаментальна властивість простих чисел і її доказ.
5. Теорема про розкладання на множники та її доказ.
6. Визначення канонічного розкладання числа і кратностей множників. Наслідки.
7. Функції $\tau(m)$ та $S(m)$. Обчислення НСД та НСК. Приклади.
8. Закон Чебишева розподілу простих чисел.
9. Гіпотеза Бертрана і її перевірка на прикладах.
10. Теорема Софії Жермен і її доказ.
11. Визначення досконалого числа. Приклади.
12. Визначення евклідового числа. Приклади.
13. Визначення чисел «співдружності». Приклад.
14. Визначення сильно складених чисел. Приклади.
15. Визначення піфагорових чисел. Приклади. Зауваження.
16. Побудова трійок піфагорових чисел і їх особливості.
17. «Велике твердження» Ферма.
18. Алгоритм розкладності числа методом проб.
19. Алгоритм Ферма розкладності числа.
20. Проблема Гольдбаха-Ейлера: формулювання гіпотез і їх перевірка на прикладах.
21. Вирішення проблеми Гольдбаха-Ейлера: теорема Шнірельмана і теорема Виноградова.
22. Сучасний стан проблеми Гольдбаха (по Андронову).
23. Особливості чисел 1, 5, 6.
24. Особливості чисел 25, 76.
25. Безкінечні числа.

ЛАБОРАТОРНА РОБОТА № 3_1

Тема: Методи генерації простих чисел: «Решето Ератосфена»

Мета: 1. Вивчити метод «Решето Ератосфена».

2. Набути практичних навичок в алгоритмізації та програмуванні методу, що вивчається.

1. ТЕОРЕТИЧНІ ВІДОМОСТІ

1.1. Просте число

Натуральне число p називають **простим**, якщо $p>1$ і p має рівно два натуральних дільники, а саме тільки 1 і самого себе.

Властивості простих чисел:

1. Для будь-якого цілого числа $n>1$найменший, відмінний від одиниці додатний дільник, - це завжди просте число, бо у противному разі можна було б вибрати ще менший дільник.

2. Найбільший простий дільник, відмінний від 1, будь-якого складеного числа n не перевищує $\sqrt{n}$. Дійсно, за умови, що q – найбільший дільник числа n, маємо $n=qb$ і $b\geq q$, звідси $n\geq q^2$ або $q\leq\sqrt{n}$.

3. Простих чисел безліч. Це обумовлено тим, що для будь-яких різних простих чисел $p_1, p_2,..., p_k$ можна побудувати нове просте число, наприклад, таким буде простий дільник суми $p_1p_2...p_k+1$, який після розділення всієї суми не може збігатися з жодним із простих чисел $p_1, p_2,..., p_k$.

4. Якщо добуток натуральних чисел ab ділиться на просте число p, то принаймні одне з чисел a або b ділитиметься на p.

1.2. Взаємно прості числа

Якщо найбільший спільний дільник чисел a і b дорівнює одиниці, тобто $НСД(a,b)=1$, то числа називаються **взаємно простими**.

Властивості взаємно простих чисел:

1. Числа a і b, відмінні від 0 і ±1, взаємно прості тоді і тільки тоді, коли їх канонічне розкладання не містить однакових простих множників.

2. Добуток чисел, кожне з яких взаємно просте з одним і тим же числом, буде також взаємно простим з цим числом.

3. Якщо a і b – взаємно прості числа і $a\neq b$, то за будь-яких цілих додатних значень n і m числа a^n і b^m будуть взаємно простими.

4. Добуток двох взаємно простих чисел дорівнює квадрату цілого числа тоді і тільки тоді, коли кожен із співмножників є квадратом цілого числа.

1.3. Метод «РЕШЕТО ЕРАТОСФЕНА»

Введення: непарне натуральне число n.

Виведення: список всіх непарних позитивних простих чисел, менших або рівних n.

Крок 1. Почати зі створення вектора *v* з $\frac{n-1}{2}$ комірками, кожному з яких надано значення 1, і вважаємо $p = 3$.

Крок 2. Якщо $p^2 > n$, виписувати всі числа $2j+1$, для яких значення *j*–го вічка вектора дорівнює 1, і зупинитися; інакше перейти до кроку 3.

Крок 3. Якщо значення комірки вектора *v* з номером $\frac{p-1}{2}$ дорівнює 0, збільшити *p* на 2 і повернутися до кроку 2; інакше перейти до кроку 4.

Крок 4. Присвоїти новій змінній *T* значення p^2; замінити нулем значення комірки вектора *v* під номером $\frac{T-1}{2}$ і збільшити *T* на $2p$; повторяти ці дві дії до тих пір, поки $T \le n$, потім збільшити *p* на 2 і повернутися до кроку 2.

Контрольний приклад: виписати прості числа до 41 (див. розв'язання у відповідній лекції).

2. ІНДИВІДУАЛЬНЕ ЗАВДАННЯ

Побудувати таблицю простих чисел кожного десятка для заданого інтервалу, використовуючи «Решето Ератосфена». Інтервал узяти з табл. 3.1 відповідно до варіанта.

Таблиця 3.1

№ вар.	***1***	***2***	***3***	***4***	***5***	***6***	***7***	***8***	***9***	***10***
Інтервал	40	80	110	150	190	230	270	310	350	390
	80	110	150	190	230	270	310	350	390	430

Продовження табл. 3.1

№ вар.	***11***	***12***	***13***	***14***	***15***	***16***	***17***	***18***	***19***	***20***
Інтервал	430	470	510	550	590	630	670	710	750	790
	470	510	550	590	630	670	710	750	790	830

Продовження табл. 3.1

№ вар.	***21***	***22***	***23***	***24***	***25***	***26***	***27***	***28***	***29***	***30***
Інтервал	830	870	910	950	1130	1170	1210	1250	1290	1330
	870	910	950	990	1170	1210	1250	1290	1330	1370

3. ПОСЛІДОВНІСТЬ ВИКОНАННЯ

3.1. Вивчити метод «Решето Ератосфена» для побудови простих чисел.

3.2. Використовуючи даний метод, виконати математичне розв'язання контрольного прикладу (у письмовому вигляді); див. відповідну лекцію.

3.3. Скласти блок-схему за методом «Решето Ератосфена» та відповідну програму, яка передбачає виведення простих чисел кожного десятка.

3.4. Виконати завдання на ЕОМ. Подати викладачеві роботу програми за контрольним прикладом та індивідуальним завданням.

3.5. Оформити звіт із лабораторної роботи:

- тема і мета лабораторної роботи;
- математичне розв'язання контрольного прикладу;
- блок-схема алгоритму за «Решетом Ератосфена»;
- роздрукований текст програми;
- роздруковані результати роботи програми (контрольний приклад та індивідуальне завдання);
- висновки складаються із 5-ти пунктів (п.1- призначення методу «Решето Ератосфена»; загальна характеристика складеної блок-схеми за методом «Решето Ератосфена»та її перевірка на контрольному прикладі; п.3- загальна характеристика створеної програмі на основі складеної блок-схеми та її тестування на контрольному прикладі; п.4- результати програмного розв'язання індивідуального завдання - виведення простих чисел за десятками; п.5- результат дослідження розташування простих чисел за десятками).

ЛАБОРАТОРНА РОБОТА № 3_2

Тема: Теорія вирахувань: вирішення лінійного порівняння

Мета: 1. Ознайомитися з методикою вирішення лінійного порівняння.

2. Набути практичних навичок в алгоритмізації і програмуванні лінійного порівняння.

1. ТЕОРЕТИЧНІ ВІДОМОСТІ

1.1. 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

$$a \equiv b (\mathrm{mod}\, m), \tag{8}$$

при цьому кажуть, що число a – це **лишок числа *b* за модулем *m***. Інколи порівняння скорочено записують як $a \equiv b(m)$, $a \overset{m}{\equiv} b$.

Основні 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 $a \equiv b(\mathrm{mod}\, m)$, $c \equiv d(\mathrm{mod}\, m)$ то $a \pm c \equiv b \pm d(\mathrm{mod}\, m)$, тобто порівняння за одним модулем можна додавати або віднімати.
6. Будь-який доданок лівої та правої частин порівняння можна переносити з протилежним знаком в 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 $a \equiv c - b(\mathrm{mod}\, m)$.
7. 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.

1.2. Вирішення лінійного порівняння з використанням розширеного алгоритму Евкліда. Рівняння вигляду $ax \equiv b(\mathrm{mod}\, m)$, де *a, b* – цілі, називається **лінійним порівнянням**.

Якщо $НСД(a, m) = 1$, тобто *a, m* – взаємно прості, то розширений алгоритм Евкліда до чисел *a, m* дасть такі цілі числа α, β, що $a\alpha + m\beta = 1$. Отримане рівняння еквівалентне виразу $a\alpha \equiv 1(\mathrm{mod}\, m)$; таким чином для *a* знайдений зворотний елемент α. Помножимо обидві частки початкового лінійного порівняння на α, в результаті отримаємо рішення $x \equiv \alpha ax \equiv \alpha b(\mathrm{mod}\, m)$.

1.3. Контрольний приклад. Вирішити порівняння $7x \equiv 3(\mathrm{mod}15)$ на основі використання розширеного алгоритму Евкліда.

Розв'язання. $НСД(15,7) = 1$; $1 = 15 - 2 \cdot 7$. Зворотним елементом до числа $a = 7$ за модулем $m = 15$ буде $\alpha = -2 \equiv 13(\mathrm{mod}15)$. Помножимо обидві частини порівняння на 13: $7 \cdot 13 \cdot x \equiv 3 \cdot 13(\mathrm{mod}15)$, $x \equiv 39(\mathrm{mod}15) \equiv 9(\mathrm{mod}15)$.

Відповідь: $x \equiv 9(\mathrm{mod}15)$.

2. ІНДИВІДУАЛЬНЕ ЗАВДАННЯ

Вирішити лінійне порівняння $ax \equiv b(\mathrm{mod}\, m)$. Початкові дані узяти з табл. 3.2 відповідно до варіанта.

Таблиця 3.2

№ вар.	*1*	*2*	*3*	*4*	*5*	*6*	*7*	*8*	*9*	*10*
a	37	5	11	5	31	13	17	37	31	41
b	25	2	7	3	25	7	13	25	20	19
m	107	9	21	13	107	23	29	103	103	101

Продовження табл. 3.2

№ вар.	*11*	*12*	*13*	*14*	*15*	*16*	*17*	*18*	*19*	*20*
a	47	7	13	7	29	11	19	31	37	31
b	25	2	7	3	25	7	13	25	20	19
m	107	9	21	13	107	23	29	103	103	101

Продовження табл. 3.2

№ вар.	*21*	*22*	*23*	*24*	*25*	*26*	*27*	*28*	*29*	*30*
a	3	5	7	4	2	6	9	10	11	13
b	11	8	40	6	7	20	18	4	9	10
m	7	9	11	13	19	13	7	21	13	15

3. ПОСЛІДОВНІСТЬ ВИКОНАННЯ

3.1. Ознайомитися з методикою вирішення лінійного порівняння $ax \equiv b(\mathrm{mod}\, m)$, якщо a,m – взаємно прості, на основі використання розширеного евклідового алгоритму.

3.2. Використовуючи розглянуту методику, виконати математичне розв'язання контрольного прикладу та індивідуального завдання (у письмовому вигляді) з відображенням відповідних таблиць за розширеним евклідовим алгоритмом (див. ЛАБ № 1_2).

3.3. Скласти блок-схему та відповідну програму вирішення лінійного порівняння $ax \equiv b(\mathrm{mod}\, m)$, передбачивши видачу таблиці за розширеним евклідовим алгоритмом.

3.4. Виконати завдання на ЕОМ і надати викладачеві.

3.5. Оформити звіт із лабораторної роботи:

- тема і мета лабораторної роботи;

- математичне розв'язання контрольного прикладу та індивідуального завдання (у письмовому вигляді) з відображенням відповідних таблиць за розширеним евклідовим алгоритмом;

- блок-схема алгоритму вирішення лінійного порівняння $ax \equiv b(\mathrm{mod}\, m)$;

- роздрукований текст програми;

- роздруковані результати роботи програми (контрольний приклад та індивідуальне завдання);

- висновки складаються із 4-х пунктів (п.1- методика вирішення лінійного порівняння з використанням розширеного евклідового алгоритму; загальна характеристика складеної блок-схеми для вирішення лінійного порівняння та її перевірка на контрольному прикладі; п.3- загальна

характеристика створеної програмі на основі складеної блок-схеми та її тестування на контрольному прикладі; п.4- результати математичного та програмного розв'язання індивідуального завдання).

Зауваження: створення таблиці за розширеним евклідовим алгоритмом, що було здійснено в ЛАБ №1_2, представити у якості підпрограми (зв'язок підпрограми з основною програмою відобразити з використанням формальних і фактичних параметрів).

КОНТРОЛЬНІ ПИТАННЯ до теми «Теорія чисел»

I. ТЕОРІЯ

1. Просте число та його властивості. Приклади.
2. Взаємно прості числа та їх властивості. Приклади.
3. Спосіб виписування простих чисел за методом «Решето Ератосфена». Приклад.
4. Підвищення ефективності алгоритму «Решето Ератосфена». Комп'ютерна реалізація. Слабкі місця алгоритму «Решето Ератосфена».
5. Поліноміальні формули побудови простих чисел. Приклади.
6. Експоненціальна формула побудови простих чисел: числа Мерсенна. Приклади. Твердження. Зауваження.
7. Експоненціальна формула побудови простих чисел: числа Ферма. Приклади. Твердження. Зауваження. Теорема 2 (без доказу).
8. Прайморіальна формула побудови простих чисел. Приклади. Зауваження. Твердження. Прайморіально просте число.
9. Назвіть серед наведених значень

$$n = 2, 3, 4, 6, 9, 17, 19, 44, 51, 63, 100$$

ті, при яких числа Мерсенна $M_n = 2^n - 1$ обов'язково будуть складеними.

10. Який спеціальний тест використовують для перевірки простоти чисел Мерсенна?

11. Який спеціальний тест існує для перевірки простоти чисел Ферма $F_n = 2^{2^n} + 1,\ n \in N$?

II. ПРАКТИКА

12. Відомо, що непарне просте число може бути записано як $4n+1$(наприклад, 5 і 13) або як $4n+3$ (наприклад, 3, 7, 11 і 19). Хай x – позитивне дійсне число, тоді $\pi_1(x)$ - число позитивних простих чисел вигляду $4n+1$, які не перевершують x, а $\pi_3(x)$ - аналогічне число простих

вигляду $4n+3$. Виходячи з алгоритму «Решето Ератосфена», обчислити $\frac{\pi_1(x)}{\pi_3(x)}$ для $x=100k$, де $1 \le k \le 10^5$. Скласти схему алгоритму завдання.

13. Відомо, що непарне просте число може бути записано як $4n+1$ (наприклад, 5 і 13) або як $4n+3$ (наприклад, 3, 7, 11 і 19). Хай *x* – позитивне дійсне число, тоді $\pi_1(x)$ - число позитивних простих чисел вигляду $4n+1$, які не перевершують *x*, а $\pi_3(x)$ - аналогічне число простих вигляду $4n+3$. Виходячи з 639582*1алгоритма «Решето Ератосфена», визначити найменше число *x*, за якого $\pi_1(x) > \pi_3(x)$. Скласти схему алгоритму завдання.

14. Обчислити прайморіал заданого числа.

15. Написати програму, завдяки якій можна реалізувати тест Пепена для перевірки простоти чисел Ферма $F_n = 2^{2^n}+1,\ n \in N$. Початковими даними програми має бути показник $n \ge 0$, а на виході - повідомлення про простоту або складеність числа F_n.

16. За допомогою тесту Пепена перевірити простоту чисел Ферма: $F_2 = 2^{2^2}+1 = 17$; $F_3 = 2^{2^3}+1 = 257$; $F_5 = 2^{2^5}+1 = 4294967297$.

17. Перевірити простоту чисел Мерсенна із залученням тесту Люка-Лемера: $M_{11} = 2^{11}-1 = 2047$; $M_{15} = 2^{15}-1 = 32767$; $M_{17} = 2^{17}-1 = 131071$; $M_{19} = 2^{19}-1 = 524287$.

ЛАБОРАТОРНА РОБОТА № 4_1

Тема: Теорія вирахувань: тест Міллера

Мета: 1. Вивчити тест Міллера для перевірки числа на простоту.

2. Набути практичних навичок в алгоритмізації і програмуванні тесту Міллера.

1. ТЕОРЕТИЧНІ ВІДОМОСТІ

1.1. Тест Міллера. Хай $n > 0$ – непарне ціле. Основа *b* задовільняє нерівність $1 < b < n-1$. Оскільки *n* – непарне, то $n-1$ має бути парним числом. Парне число ділиться на 2, треба знайти найбільший ступінь двійки, що ділить $n-1$, тобто визначити такий показник $k \ge 1$, для якого $n-1 = 2^k \cdot q$, де *q* не ділиться на 2. Далі тест обчислює вирахування за модулем *n* у наступної послідовності ступенів: b^q, b^{2q}, ..., $b^{2^{k-1}q}$, $b^{2^k q}$.

За теоремою Ферма $b^{2^k q} \equiv b^{n-1} \equiv 1 (\mathrm{mod}\, n)$. Значить, якщо *n* – просте, то останнє вирахування в послідовності завжди дорівнює 1.

Хай j – найменший показник, для якого $b^{2^j q} \equiv 1 (\mathrm{mod}\, n)$. Якщо $j \geq 1$, то $b^{2^j q} - 1 = (b^{2^{j-1} q} - 1)(b^{2^{j-1} q} + 1)$. По припущенню, що n – просте і ділить або $b^{2^{j-1} q} - 1$, або $b^{2^{j-1} q} + 1$, оскільки воно ділить різницю квадратів $b^{2^j q} - 1$.

З іншого боку, через вибір показника j число n не може ділити $b^{2^{j-1} q} - 1$. Залишається тільки одна можливість: n – дільник числа $b^{2^{j-1} q} + 1$, тобто ці міркування показують, що в разі простого n серед послідовності ступенів: $b^q, b^{2q}, \ldots, b^{2^{k-1} q}$ знайдеться принаймні одна, порівнянна з –1 по модулю n.

Отже, якщо n – просте, то з послідовністю вирахувань за модулем n повинно статися одне з двох: або перше ж вирахування дорівнює 1, або серед них з'явиться $n - 1$. Інакше число n має бути складеним.

Зауваження. Послідовність вирахувань, використовувана в тесті Міллера, досить легко обчислюється, тому що кожне вирахування (за винятком першого) – квадрат попереднього. Насправді, $b^{2^j q} = (b^{2^{j-1} q})^2$ при $j \geq 1$. Звідси витікає, що як тільки в послідовності вирахувань за модулем n зустрінеться $n - 1$, решта всіх вирахувань дорівнюватиме 1.

Введення: непарне натуральне n і основа b, де $1 < b < n - 1$.

Виведення: одне з двох повідомлень: «n-складне» або «нічого визначеного сказати не можна».

Крок 1. Послідовно ділимо $n - 1$ на 2, поки не отримаємо непарної частки. У результаті знайдемо позитивне ціле k і непарне q, для яких $n - 1 = 2^k q$.

Крок 2. Присвоїмо i нульове значення, а r – значення вирахування bq за модулем n.

Крок 3. Якщо $i = 0$ і $r = 1$ або $i > 0$, а $r = n - 1$, то вивести повідомлення: «нічого певного сказати не можна»; інакше переходимо до кроку 4.

Крок 4. Збільшуємо i на 1 і заміняємо r на r^2 за модулем n; переходимо до кроку 5.

Крок 5. Якщо $i < k$, то повертаємося до кроку 3; інакше видаємо повідомлення: «n – складене».

1.2. Контрольний приклад. Перевірити за допомогою тесту Міллера простоту числа Кармайкла $n = 561$.

Розв'язання. Спочатку визначаємо: $n - 1 = 561 - 1 = 560 = 2^4 * 35$, тобто $q = 35$, $k = 4$. Далі обчислимо послідовність b^q, b^{2q}, …, $b^{2^{k-1}q}$, $b^{2^k q}$ (кожен лишок є квадратом попереднього лишку):

$$2^{35} \equiv 263 \pmod{561}; \quad 2^{2*35} \equiv 166 \pmod{561};$$

$$2^{2*2*35} \equiv 67 \pmod{561}; \quad 2^{2*4*35} \equiv 1 \pmod{561}.$$

Отримані значення у ході розрахунку зведемо до таблиці 4.1. Результати тесту Міллера дають зрозуміти, що число $n = 561$ - складене.

Таблиця 4.1

Степінь	35	2*35	2^2*35	2^3*35
Вирахування	263	166	67	1

2. ІНДИВІДУАЛЬНЕ ЗАВДАННЯ

За тестом Міллера виконати дослідження чисел n по підставі b (див. табл. 4.2), при цьому передбачити виведення таблиці ступенів і їх вирахувань.

Таблиця 4.2

n	341	561	25	25
b	2	2	2	7

3. ПОСЛІДОВНІСТЬ ВИКОНАННЯ

3.1. Ознайомитися з тестом Міллера.

3.2. За тестом Міллера виконати математичне розв'язання всіх чисел (у письмовому вигляді) з побудовою відповідних таблиць.

3.3. Скласти блок-схему та відповідну програму за тестом Міллера з побудовою відповідних таблиць.

3.4. Надати викладачеві роботу програми на ЕОМ.

3.5. Оформити звіт із лабораторної роботи:

- тема і мета лабораторної роботи;
- математичне розв'язання всіх чисел (у письмовому вигляді) з побудовою відповідних таблиць;
- блок-схема тесту Міллера;
- роздрукований текст створеної програми за тестом Міллера (передбачити виведення таблиці);
- роздруковані результати роботи програми за тестом Міллера (дослідження всіх чисел);

- висновки складаються із 5-ти пунктів (п.1- призначення тесту Міллера; загальна характеристика складеної блок-схеми тесту Міллера та її перевірка на контрольному прикладі; п.3- загальна характеристика створеної програми за тестом Міллера та її тестування на контрольному прикладі; п.4- результати математичного та програмного розв'язання всіх чисел, що досліджуються; п.5- результат тесту Міллера стосовно кожного числа, що досліджувалося, і яким воно являється).

3.6. Підготуватися до захисту теми «Теорія вирахувань».

ЛАБОРАТОРНА РОБОТА № 4_2

Тема: Теорія вирахувань: тест Соловея-Штрассена

Мета: 1. Вивчити тест Соловея-Штрассена перевірки числа на простоту.

2. Набути практичних навичок в алгоритмізації і програмуванні теста Соловея-Штрассена.

1. ТЕОРЕТИЧНІ ВІДОМОСТІ

1.1. Імовірнісні тести для визначення простоти числа

Для роботи імовірнісних тестів потрібна послідовність рівномірно розподілених випадкових чисел з відрізка [1; n]. Для кожного випадкового числа такої послідовності перевіряється виконання деяких умов. Якщо які-небудь з цих умов не виконуються, то число n - складене. Якщо ж усі умови виконуються, то з певною ймовірністю можна стверджувати, що n - просте число. Ця ймовірність тим ближча до 1, чим більша кількість випадкових чисел буде застосована. Таким чином, імовірнісні тести намагаються показати теоретико-імовірнісними методами, що будь-яке число, яке даний метод оголосив простим, з надзвичайно малою ймовірністю може насправді виявитися складеним.

Розглянемо підхід, що реалізований у імовірнісному тесті Соловея-Штрассена. Для непарного числа $n \geq 3$ через S_n позначимо підмножину мультиплікативної групи лишків Z_n^*, що складається з тих елементів a, які задовольняють порівняння

$$J(a; n) = a^{(n-1)/2} \pmod{n}, \qquad (9)$$

де $J(a; n)$ - символ Якобі. Через мультиплікативність символу Якобі підмножина S_n являє собою підгрупу групи Z_n^*. За теоремою Лагранжа порядок підгрупи S_n скінченної групи Z_n^* має бути дільником порядку групи.

Оскільки $\left|Z_n^* = \varphi(n)\right|$, де $\varphi(n)$- значення функції Ейлера, то порядок підгрупи S_n може бути щонайбільше $\varphi(n)/2$, тобто $|S_n| \le \frac{\varphi(n)}{2}$.

Рівність $|S_n| \le \frac{\varphi(n)}{2}$ дійсно має місце для деяких чисел Кармайкла, наприклад для числа 1729. Тому коли a є випадково вибране число з множини $\{1,2,3,\ldots,n-1\}$ і $a \in S_n$, ймовірність випадково прийняти n за просте число дорівнює $\frac{\varphi(n)}{2(n-1)} > \frac{1}{2}$.

1.2. Тест Соловея-Штрассена

Крок 1. Вибрати випадкове додатне число $1 < a < n-1$.

Крок 2. Якщо НСД(*a; n)* ≠ 1, то *n* - складене число і робота алгоритму припиняється.

Крок 3. Обчислити значення $j = a^{(n-1)/2} (\mathrm{mod}\, n)$.

Крок 4. Обчислити символ Якобі *J(a; n).*

Крок 5. Якщо $j \neq J(a;n)$, то число *n* – складене.

Крок 6. Якщо $j = J(a;n)$, то число *n* – просте і ймовірність того, що цей результат помилковий, не перевищує 0,5.

Просте число *n* витримує тест з імовірністю 1, бо для всіх цілих чисел $a \in (1; n-1)$ крок 2 алгоритму виконується за означенням простого числа, а крок 6 алгоритму - за критерієм Ейлера. Якщо число *n* - складене, то обидва ці кроки зможуть подолати лише елементи підгрупи S_n. Тому складене число *n* витримує тест з ймовірністю, не вище $\frac{\varphi(n)}{2(n-1)} < \frac{1}{2}$. Таким чином, логічний підсумок наступний: помилка у тесті Соловея-Штрассена однобічна. Повторення тестування *k* разів з різними значеннями *a* знижує ймовірність помилки до $1/2^k$. Це означає, що при 2^k різних реалізаціях цього алгоритму можна чекати щонайбільше одного неправильного висновку стосовно простоти числа *n.* При *k* = 30 ймовірність цієї помилки менша 10^{-9}. Часова складність тесту Соловея-Штрассена $O(\log^3 n)$.

1.3. Контрольний приклад № 1. Перевірити тестом Соловея-Штрассена простоту числа *n* = 2023, вибравши *a* = 792.

Розв’язання. НСД(*a; n)* = НСД (2023, 792) = 1. Далі обчислимо

$$j = a^{(n-1)/2} (\mathrm{mod}\, n) = 792^{(2023-1)/2} (\mathrm{mod}\, 2023) = 932.$$

Символ Якобі дорівнює $J(a; n) = J(792; 2023) = +1$.

Оскільки $j \neq J(a;n)$ за тестом Соловея-Штрассена число n = 2023 - складене. Дійсно, $2023 = 7 \cdot 17^2$.

1.4. Контрольний приклад № 2. Перевірити тестом Соловея-Штрассена простоту числа n = 5987, якщо ймовірність помилково прийняти за просте має бути меншою, ніж $\varepsilon = 0{,}001$.

Розв'язання. Складене число n витримує один тест з ймовірністю $< 1/2$. У разі помилкової відповіді на тест Соловея-Штрассена при k різних значеннях a ймовірність того, що число n все ж таки помилково прийнято за просте, менша або дорівнює $1/2^k$. Нехай k - таке натуральне число, для якого $1/2^k < \varepsilon$, тобто $1/2^k < 0{,}001$. Звідси $k \geq 10$. Отже, потрібно вибрати 10 різних значень a, щоб ймовірність помилково прийняти число n = 5987 за просте була меншою, ніж $\varepsilon = 0{,}001$. Виберемо як випадкове число

a = 3.

НСД(a; n) = НСД (3, 5987) = 1. Далі обчислимо

$$j = a^{(n-1)/2} (\mathrm{mod}\, n) = 3^{(5987-1)/2} (\mathrm{mod}\, 5987) \equiv 3^{2993} \equiv 1 (\mathrm{mod}\, 5987).$$

Символ Якобі дорівнює

$J(3; 5987) = - J(5987; 3) = J(5987(\mathrm{mod}\, 3); 5987) = - J(2; 3) = - (- 1) = +1 = j$.

Отже, при a = 3 число витримало тест на простоту. Результати тестування числа n = 5987 при інших значеннях a наведено у табл. 4.3.

Таблиця 4.3

a	$j = a^{(n-1)/2} (\mathrm{mod}\, n)$	$J(a; n)$
3	1	1
5	-1	-1
7	-1	-1
9	1	1
11	-1	-1
13	-1	-1
15	-1	-1
17	1	1
25	1	1
101	-1	-1

Отже, при всіх різних десяти значеннях числа a отримано $j = J(a;n)$, тобто десять разів число n = 5987 витримало тест на простоту і може вважатися простим з імовірністю помилки, меншою за 0,001.

2. БРИГАДНІ ЗАВДАННЯ

Завдання № 1. Перевірити тестом Соловея-Штрассена простоту числа n = 557, вибравши a = 18.

Завдання № 2. Перевірити тестом Соловея-Штрассена простоту числа n = 1381, якщо ймовірність помилково прийняти число за просте мусить бути нижчою за $\varepsilon = 0{,}01$.

3. ПОСЛІДОВНІСТЬ ВИКОНАННЯ

3.1. Ознайомитися з імовірнісним тестом Соловея-Штрассена для визначення простоти числа.

3.2. Використовуючи розглянуту методику, провести математичні розрахунки контрольних прикладів № 1-2 та бригадних завдань № 1-2.

3.3. Для визначення простоти числа з використанням тесту Соловея-Штрассена скласти блок-схему та відповідну програму, перевірив їх на контрольних прикладах № 1-2.

3.4. Виконати бригадні завдання № 1-2 на ЕОМ і надати викладачеві.

3.5. Оформити звіт із лабораторної роботи:

- тема і мета лабораторної роботи;
- склад бригади та обсяг виконання кожним членом бригади;
- математичні розрахунки контрольних прикладів № 1-2 та бригадних завдань № 1-2;
- блок-схема алгоритму визначення простоти числа за тестом Соловея-Штрассена;
- роздрукований текст програми за тестом Соловея-Штрассена;
- роздруковані результати роботи програми (контрольні приклади № 1-2 та бригадні завдання № 1-2);
- висновки складаються із 4-х пунктів (п.1- призначення тесту Соловея-Штрассена; загальна характеристика складеної блок-схеми тесту Соловея-Штрассена та її перевірка на контрольних прикладах № 1-2; п.3- загальна характеристика створеної програми за тестом Соловея-Штрассена та її тестування на контрольних прикладах № 1-2; п.4- результати математичного та програмного розв’язання бригадних завдань № 1-2).

3.6. Підготуватися до захисту теми «Теорія вирахувань».

КОНТРОЛЬНІ ПИТАННЯ до теми «Теорія вирахувань»

I. ТЕОРІЯ

1. Порівняння чисел за модулем. Приклади. Зауваження.

2. Основні властивості порівнянь. Приклади знаходження вирахування числа a за модулем n.

3. Клас еквівалентності порівняних чисел за модулем. Властивості класів.

4. Зворотний і оборотний клас. Теорема оборотності та її доказ.

5. Лема та її доказ.

6. Мала теорема Ферма та її доказ.

7. Теорема Ферма та її доказ.

8. Свідок розкладення числа. Теорема (тест на розкладення; без доказу).

9. Псевдопросте число по підставі b. Приклад.

10. Числа Кармайкла. Приклад. Теорема Корселта і її доказ.

11. Тест Міллера. Строго псевдопрості числа. Приклад. Теорема Рабіна (без доказу).

12. Китайська теорема про залишки. Заповнення таблиці. Приклад.

13. Символ Лежандра та його властивості.

14. Алгоритм обчислення символу Лежандра.

15. Символ Якобі та його властивості.

16. Алгоритм обчислення символу Якобі.

17. За яким з тестів (Рабіна чи Соловея-Штрассена) з теоретико-ймовірнісного погляду ймовірність помилково прийняти складене число за просте буде нижчою?

II. ПРАКТИКА

18. Завдання на вживання теореми Ферма.

19. Вирішення порівняння $ax \equiv b(\mathrm{mod}\, n)$, якщо a і n – взаємно прості.

20. Вирішення порівняння $ax \equiv b(\mathrm{mod}\, n)$, якщо b – кратне $НСД(a,n)$.

21. Вирішення порівняння будь-якого ступеня за складеним модулем.

22. Хай p і q - різні прості числа і $n = pq$. Передбачимо, що відомі вирішення рівнянь $x^2 \equiv a(\mathrm{mod}\, p)$ і $x^2 \equiv a(\mathrm{mod}\, q)$. Покажіть, як китайський алгоритм залишків можна використовувати для вирішення рівняння $x^2 \equiv a(\mathrm{mod}\, n)$.

23. Хай p і q - різні прості числа і $n = pq$. Передбачимо, що обидва прості числа мають залишок 3 при діленні на 4. Напишіть програму, яка за даними p, q і a вирішує рівняння $x^2 \equiv a(\mathrm{mod}\, n)$.

24. Написати програму, завдяки якій можна будувати всі числа Кармайкла, що будуть добутком d простих множників, кожен із яких не перевищує 10^3, $3 \le d \le 8$.

25. Написати програму для знаходження найменших псевдопростих чисел за даною основою та застосувати її для обчислення найменшого псевдопростого числа за основами 2, 3, 5 та 7.

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. Formation of competencies and soft skills when performing brigade discipline tasks «Mathematical foundation of information security». *Modern engineering and innovative technologies*. Germany, Karlsruhe : Sergeieva&Co, «ISE&E». 2024. Issue 35.
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.

ДОДАТОК

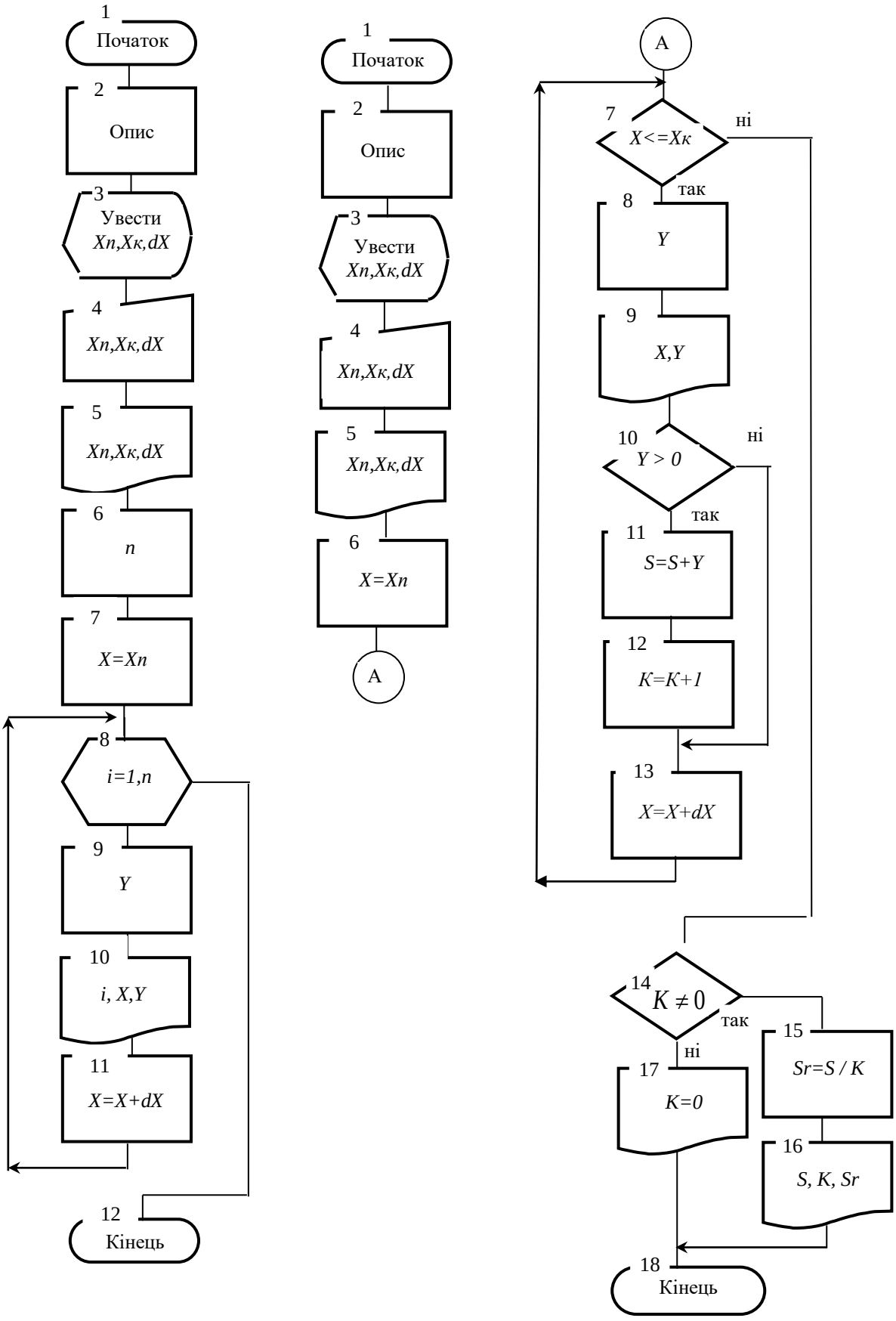


Рис. А.1. Приклади блок-схем циклічної та змішаної структур

Навчально-методичне видання

Пахомова Вікторія Миколаївна

МАТЕМАТИЧНІ ОСНОВИ ІНФОРМАЦІЙНОЇ БЕЗПЕКИ

Навчально-методичні рекомендації
щодо виконання лабораторних робіт

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

Експертний висновок склав проф. І. В. Жуковицький

Зареєстровано НМВ УДУНТ (№ 773 від 04.11.2024)

Формат 60x84 1/16. Ум. друк. арк. 2,03. Обл.-вид. арк. 1,15.

Зам. № 99.

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