

МІНІСТЕРСТВО ОСВІТИ І НАУКИ УКРАЇНИ
НАЦІОНАЛЬНИЙ ТЕХНІЧНИЙ УНІВЕРСИТЕТ
«ДНІПРОВСЬКА ПОЛІТЕХНІКА»

Факультет інформаційних технологій
Кафедра прикладної математики

Т.С. Кагадій, А.Г. Шпорта

Основи теорії чисел

КОНСПЕКТ ЛЕКЦІЙ

для здобувачів ступеня бакалавра
спеціальності 113 Прикладна математика

Дніпро
НТУ «ДП»
2025



Кагадій Т.С.

Основи теорії чисел [Електронний ресурс] : конспект лекцій для здобувачів ступеня бакалавра спеціальності 113 Прикладна математика / Т.С. Кагадій, А.Г. Шпорта ; М-во освіти і науки України, Нац. техн. ун-т «Дніпровська політехніка». – Дніпро : НТУ «ДП», 2025. – 140 с.

Автори:

Т.С. Кагадій, д-р фіз.-мат. наук, проф.

А.Г. Шпорта. канд. фіз.-мат. наук, доц.

Затверджено науково-методичною комісією зі спеціальності 113 Прикладна математика (протокол № 11-1/24 від 20.11.2024) за поданням кафедри прикладної математики (протокол № 11/24 від 04.11.2024)

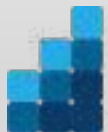
Розглянуто основні поняття та розділи дисципліни «Теорія чисел», що викладається здобувачам ступеня бакалавра спеціальності 113 Прикладна математика. Надані означення, алгоритми та правила, спрямовані на підготовку здобувачів до вивчення таких дисциплін, як «Основи криптографії та захисту даних», «Математичне моделювання», «Дискретна математика».

Конспект лекцій спрямований на те, щоб допомогти здобувачеві сформувати нову математичну лексику, ознайомитись з поняттями, що не зустрічались раніше при вивченні математичного аналізу, алгебри та геометрії. Нові поняття і підходи, що існують в теорії чисел, допоможуть здобувачеві розширити математичний світогляд, можуть зацікавити його, дозволять подивитися на математичні дисципліни з точки зору їх практичного застосування.

Відповідальний за випуск завідувачка кафедри прикладної математики О.О. Сдвижкова, д-р техн. наук, проф.

ЗМІСТ

- ❖ Тема 1. Подільність чисел.
- ❖ Тема 2. Прості числа.
- ❖ Тема 3. Неперервні (ланцюгові) дроби.
- ❖ Тема 4. Порівняння чисел.
- ❖ Тема 5. Класи лишків за модулем.
- ❖ Тема 6. Алгебраїчні структури.
- ❖ Тема 7. Функція Ейлера. Теореми Ейлера та Ферма.
- ❖ Тема 8. Порівняння першого степеня.
- ❖ Тема 9. Система порівнянь першого степеня. Китайська теорема про остачі.



ВСТУП

Мета дисципліни – формування компетентностей щодо здатності до абстрактного мислення, аналізу та синтезу, здатності використовувати й адаптувати математичні теорії, методи та прийоми для доведення математичних тверджень при захисті інформації і теорем при професійній підготовці бакалаврів за спеціальністю 113 Прикладна математика.

ОЧІКУВАНІ РЕЗУЛЬТАТИ НАВЧАННЯ

В освітньо-професійній програмі НТУ «Дніпровська політехніка» спеціальності 113 Прикладна математика здійснено розподіл програмних результатів навчання за організаційними формами освітнього процесу. Зокрема, до дисципліни Ф7 «Теорія чисел» віднесені такі результати навчання:

PH02	Володіти основними положеннями та методами математичного, комплексного та функціонального аналізу, лінійної алгебри та теорії чисел, аналітичної геометрії, теорії диференціальних рівнянь, зокрема рівнянь у частинних похідних, теорії ймовірностей, математичної статистики та випадкових процесів, чисельними методами.
PH06	Володіти основними методами розробки дискретних і неперервних математичних моделей об'єктів та процесів, аналітичного дослідження цих моделей на предмет існування та єдиності їх розв'язку.

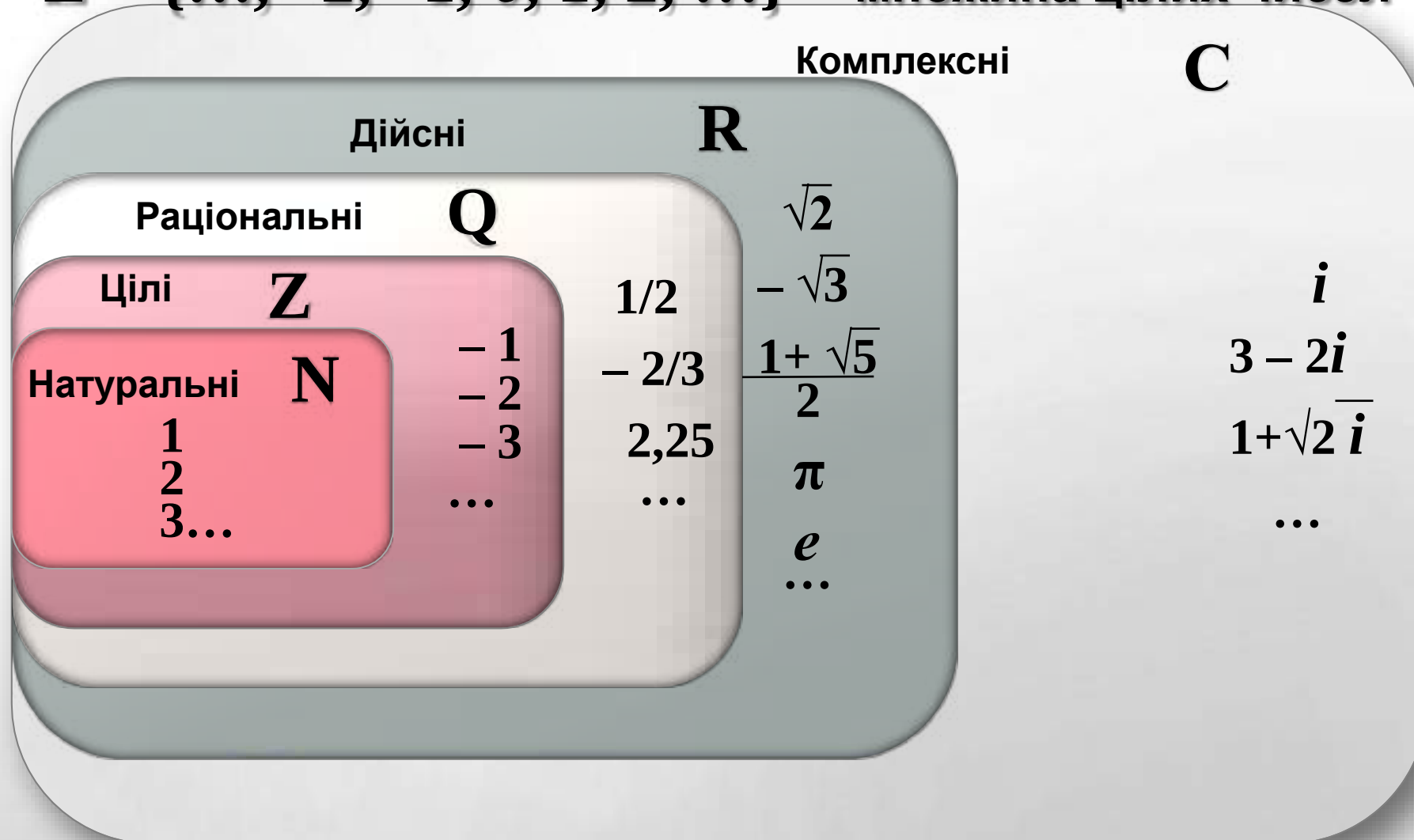
Основи теорії чисел

Тема 1. Подільність чисел.



Тема 1. Подільність чисел

$\mathbb{Z} = \{..., -2, -1, 0, 1, 2, ...\}$ – множина цілих чисел



Ділення цілих чисел

Теорема про подільність чисел з остачею

Для цілого числа a та додатного цілого числа b існує єдина пара чисел q та r , таких, що

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



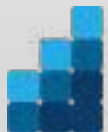
q – неповна частка; r – остача від ділення;



Якщо $r = 0$, тоді $a = bq$; кажуть, що b – дільник числа a
або a кратне b ;



Якщо число a ділиться на число b без остачі ($r = 0$), тоді
пишуть $b|a$ або $a:b$



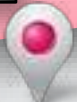
Тема 1. Подільність чисел (продовження -1.3)

Ділення цілих чисел

ПРИКЛАДИ:

 $a = 34, b = 8 \Rightarrow 34 = 8 \cdot 4 + 2 \Rightarrow q = 4, r = 2$

 $a = -34, b = 8 \Rightarrow -34 = 8 \cdot (-5) + 6 \Rightarrow q = -5, r = 6$

 Якщо $m|a$ і $b|m$,
тоді $b|a$;

 $a|0, 1|a, a|a$ для
будь-якого $a \in \mathbb{Z}$;

 Якщо $a|b$ і $b|a$,
тоді $b = \pm a$;

 Якщо $a+b=c, m|a$ і
 $m|b$, тоді $m|c$



Тема 1. Подільність чисел (продовження -1.4)

Найбільший спільний дільник (НСД) чисел

Найбільший спільний дільник чисел a і b – це найбільше натуральне число, на яке діляться без остачі числа a та b



Означення:

НСД (a, b), (a, b),
 $\gcd(a, b)$
(англ. Greatest Common Divisor)



Якщо $\text{НСД}(a, b) = 1$,
то числа a і b
називаються **взаємно простими**

ПРИКЛАДИ: 1) $\text{НСД}(18, 45) = 9$;
2) 20 і 11 – взаємно прості,
 $\text{НСД}(20, 11) = 1$

Властивості НСД



Якщо $b|a$, то $\text{НСД}(a, b) = b$



Якщо $a = bq + r$, то
 $\text{НСД}(a, b) = \text{НСД}(b, r)$



$\text{НСД}(0, a) = 0$ для
цілого $a \neq 0$



$\text{НСД}(am, bm) =$
 $= m \cdot \text{НСД}(a, b)$



$\text{НСД}(a, b, c) =$
 $= \text{НСД}(\text{НСД}(a, b), c)$



Найменше спільне кратне чисел

Найменше спільне кратне чисел a і b – це найменше натуральне число, що ділиться без остачі на числа a та b



Означення:

$\text{НСК}(a, b),$

$[a, b],$

$\text{lcm}(a, b)$

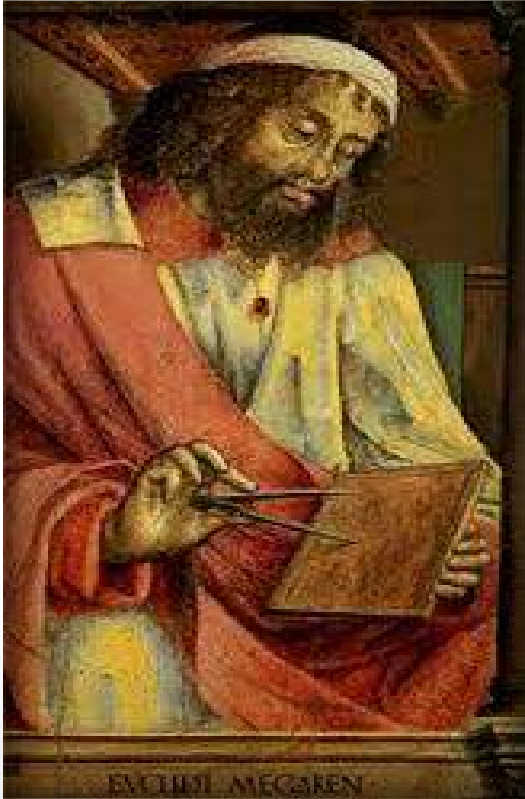
(англ. Least Common Multiple)

ПРИКЛАД: $\text{НСК}(16, 6) = 48$



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

Алгоритм Евкліда



Алгоритм Евкліда – ефективний алгоритм для
знаходження НСД (a, b)
без розкладання чисел a та b на множники

Евклід
(др. грецьк. Εὐκλείδης – добра слава)
бл. 300 р. до н. е.

Алгоритм Евкліда

Виконуємо послідовно ділення, знаходимо частку та остачу:

$$a = bq_1 + r_1, \quad 0 < r_1 < b; \quad a \text{ ділиться на } b$$

$$b = r_1q_2 + r_2, \quad 0 < r_2 < r_1; \quad b \text{ ділиться на остачу } r_1$$

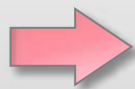
$$r_1 = r_2q_3 + r_3, \quad 0 < r_3 < r_2; \quad r_1 \text{ ділиться на остачу } r_2$$

.....

$$r_{n-3} = r_{n-2}q_{n-1} + r_{n-1}, \quad 0 < r_{n-1} < r_{n-2};$$

$$r_{n-2} = r_{n-1}q_n, \quad r_n = 0.$$

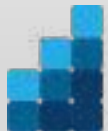
$$\begin{aligned} \text{НСД}(a, b) &= \text{НСД}(b, r_1) = \text{НСД}(r_1, r_2) = \dots = \text{НСД}(r_{n-2}, r_{n-1}) = \\ &= \text{НСД}(r_{n-1}, 0) = r_{n-1} \end{aligned}$$



$$\text{НСД}(a, b) = r_{n-1}$$



Остання відмінна від нуля остача



Алгоритм Евкліда

Найти НСД (1239, 735).

РОЗВ'ЯЗАННЯ:

$$1239 : 735 \rightarrow 1239 = 1 \cdot 735 + 504$$

$$735 : 504 \rightarrow 735 = 1 \cdot 504 + 231$$

$$504 : 231 \rightarrow 504 = 2 \cdot 231 + 42$$

$$231 : 42 \rightarrow 231 = 5 \cdot 42 + 21$$

$$42 : 21 \rightarrow 42 = 2 \cdot 21$$

Остання відмінна від нуля остача

$$\rightarrow \text{НСД}(1239, 735) = 21$$

Кількість ділень в алгоритмі Евкліда не більше $5 \lg \max\{|a|, |b|\}$



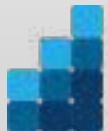
Лінійна форма НСД чисел

Теорема

Для будь-яких цілих чисел a та b , не рівних одночасно нулю, існує така пара цілих чисел α та β , що

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

Розширений алгоритм Евкліда знаходить не тільки $\text{НСД}(a, b)$, але й визначає коефіцієнти α та β в лінійній формі $\text{НСД}(a, b) = \alpha a + \beta b$



Тема 1. Подільність чисел (продовження -1.11)

Розширений алгоритм Евкліда

За алгоритмом Евкліда виконується ділення

$$r_{i-2} = r_{i-1}q_i + r_i \quad \Rightarrow \quad r_i = r_{i-2} - r_{i-1}q_i$$

Запишемо кожну остачу у вигляді

$$r_i = ax_i + by_i$$

$$r_{i-1} = ax_{i-1} + by_{i-1}$$

$$r_{i-2} = ax_{i-2} + by_{i-2}$$

$$ax_i + by_i = ax_{i-2} + by_{i-2} - (ax_{i-1} + by_{i-1})q_i$$

$$ax_i + by_i = a(x_{i-2} - x_{i-1}q_i) + b(y_{i-2} - y_{i-1}q_i)$$

$$x_i = x_{i-2} - x_{i-1}q_i;$$

$$y_i = y_{i-2} - y_{i-1}q_i$$

– рекурентні формули для обчислення коефіцієнтів

Тема 1. Подільність чисел (продовження -1.12)

Розширений алгоритм Евкліда

За аналогією ($x=\alpha, y=\beta$)

$$a = ax_{-1} + by_{-1}, \quad b = ax_0 + by_0 \quad \rightarrow$$

$$\begin{aligned}x_{-1} &= 1, \\y_{-1} &= 0, \\x_0 &= 0, \\y_0 &= 1\end{aligned}$$



ПРИКЛАД: знайти коефіцієнти x та y в розкладанні

$$\text{НСД}(a,b) = ax + by,$$

$$\text{якщо } a=1769, b=551$$



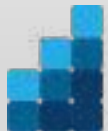
Тема 1. Подільність чисел (продовження -1.13))

Розширений алгоритм Евкліда

Ділення	Частка	Остача	$x_i = x_{i-2} - x_{i-1}q_i$	$y_i = y_{i-2} - y_{i-1}q_i$
			$x_{-1} = 1$	$y_{-1} = 0$
			$x_0 = 0$	$y_0 = 1$
1769:551	$q_1=3$	$r_1=116$	$x_1 = x_{-1} - x_0 \cdot q_1 = 1$	$y_1 = y_{-1} - y_0 \cdot q_1 = -3$
551:116	$q_2=4$	$r_2=87$	$x_2 = x_0 - x_1 \cdot q_2 = -4$	$y_2 = y_0 - y_1 \cdot q_2 = 13$
116:87	$q_3=1$	$r_3=29$	$x_3 = x_1 - x_2 \cdot q_3 = 5$	$y_3 = y_1 - y_2 \cdot q_3 = -16$
87:29	$q_4=3$	$r_4=0$		

$r_4 = 0 \rightarrow x = 5, y = -16$

$\text{НСД}(1769, 551) = 29 = 5 \cdot 1769 - 16 \cdot 551$



Тема 1. Подільність чисел (продовження -1.14)

Коефіцієнти лінійної форми НСД чисел

ПРИКЛАД: $\text{НСД}(a,b) = ax + by$, $a = 2322$, $b = 654$.

Знайти x та y .

Алгоритм Евкліда:



$$2322 = 3 \cdot 654 + 360$$

$$654 = 1 \cdot 360 + 294$$

$$360 = 1 \cdot 294 + 66$$

$$294 = 4 \cdot 66 + 30$$

$$66 = 2 \cdot 30 + 6$$

$$30 = 6 \cdot 5$$

$$\begin{aligned} \text{НСД}(2322, 654) &= 6 = 66 - 2 \cdot 30 = 66 - 2(294 - 4 \cdot 66) = 9 \cdot 66 - 2 \cdot 294 = \\ &= 9 \cdot (360 - 294) - 2 \cdot 294 = 9 \cdot 360 - 11 \cdot 294 = 9 \cdot 360 - 11 \cdot (654 - 360) = \\ &= 20 \cdot 360 - 11 \cdot 654 = 20 \cdot (2322 - 3 \cdot 654) - 11 \cdot 654 = 20 \cdot 2322 - 71 \cdot 654 \end{aligned}$$

$$\Rightarrow x = 20; \quad y = -71$$



Контрольні питання:

1. Як поділити цілі числа з остачею?
2. Які значення приймає остача від ділення?
3. Що таке найбільший спільний дільник та найменше спільне кратне?
4. Які числа називають взаємно простими?
5. Для чого використовується алгоритм Евкліда?



Основи теорії чисел

Тема 2. Прості числа.



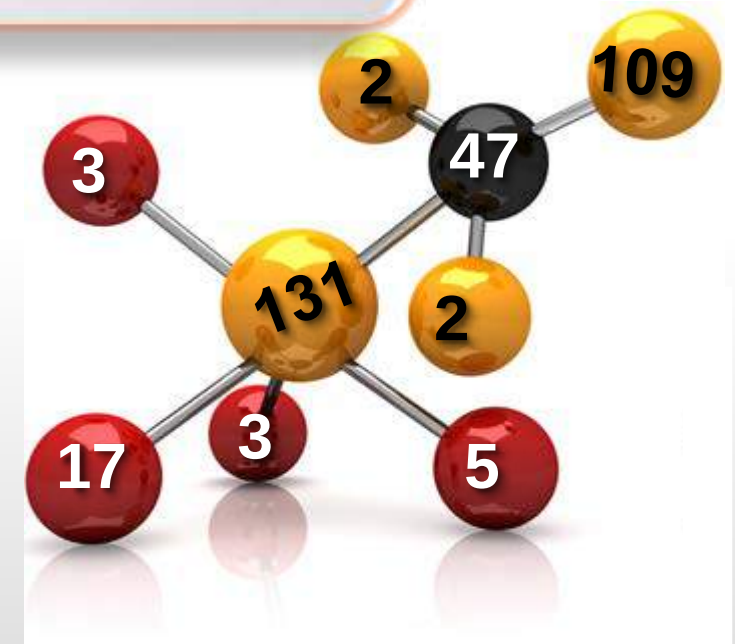
Тема 2. Прості числа

Натуральне число p , більше одиниці, називається **простим**, якщо воно ділиться націло тільки на 1 та на себе. Всі інші числа, крім 1, є **складеними**.

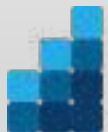
Число 1 не відноситься ні до простих, ані до складених.

Начало послідовності простих чисел:
2, 3, 5, 7, 11, 13, 17, 19, 23, 29, 31,...

Всі складені числа можна отримати як добуток простих чисел, тому прості числа іноді називають «атомами чисел»



$$131 \cdot 2^2 \cdot 3^2 \cdot 17 \cdot 5 \cdot 47 \cdot 109 = 2053605780$$



1

Найменший, відмінний від 1, дільник будь-якого числа є просте число

2

Найбільший простий дільник будь-якого складеного числа n , не перебільшує $\sqrt{n}$

Доведення: нехай $n = pb$ і p – найменший простий дільник числа n .

$$b \geq p \rightarrow n \geq p^2 \rightarrow p \leq \sqrt{n}$$

3

Простих чисел нескінченно багато (Евклід)

Доведення: нехай кількість простих чисел скінченна. Перемножимо їх та додамо до результату 1. Отримане число ділиться без остачі тільки на 1 та на себе, тобто, просте. Гіпотеза хибна.



4

Якщо p – просте $p|ab$, тоді $p|a$ або $p|b$

5

Будь-яка арифметична прогресія вигляду $a, a+q, a+2q, a+3q, \dots$, де $\text{НСД}(a, q) = 1$, містить нескінченно багато простих чисел

6

Будь-яке просте число, більше 3, можна представити у вигляді $6k+1$ або $6k-1$, де k — натуральне число.



Основна теорема арифметики

Теорема

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

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

де $p_1, p_2, \dots, p_n$ – різні прості числа;

$k_1, k_2, \dots, k_n$ – кратності простих множників (натуральні числа)

$$\begin{array}{r|l} 150 & 2 \\ 75 & 3 \\ 25 & 5 \\ 5 & 5 \\ 1 & 1 \end{array}$$



$$150 = 2 \cdot 3 \cdot 5^2$$



Наслідки основної теореми арифметики

Нехай $a = p_1^{k_1} p_2^{k_2} \dots p_n^{k_n}$; $b = p_1^{k'_1} p_2^{k'_2} \dots p_n^{k'_n}$

1

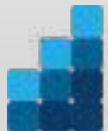
$$\text{НСД}(a, b) = p_1^{\min(k_1, k'_1)} p_2^{\min(k_2, k'_2)} \dots p_n^{\min(k_n, k'_n)}$$

$$\text{НСК}(a, b) = p_1^{\max(k_1, k'_1)} p_2^{\max(k_2, k'_2)} \dots p_n^{\max(k_n, k'_n)}$$

2

Число a ділиться на число b , якщо

$$k_1 \geq k'_1, k_2 \geq k'_2, \dots, k_n \geq k'_n$$



Наслідки основної теореми арифметики

3

Число a є l -ий степень деякого цілого числа, коли всі показники $k_1, k_2, \dots, k_n$ діляться на l

4

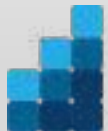
Кількість всіх дільників числа $a = p_1^{k_1} p_2^{k_2} \dots p_n^{k_n}$ дорівнює

$$\tau(a) = (k_1 + 1)(k_2 + 1) \dots (k_n + 1)$$

5

Сумма всіх дільників числа $a = p_1^{k_1} p_2^{k_2} \dots p_n^{k_n}$ дорівнює

$$S(a) = \frac{p_1^{k_1 + 1} - 1}{p_1 - 1} \frac{p_2^{k_2 + 1} - 1}{p_2 - 1} \dots \frac{p_n^{k_n + 1} - 1}{p_n - 1}$$



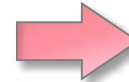
Факторизація чисел

Процес розкладання числа на прості множники називається **факторизацією**.

ПРИКЛАД: Знайти НСД і НСК чисел 945 та 252.



945	3	252	2
315	3	126	2
105	3	63	3
35	5	21	3
7	7	7	7
1	1	1	1

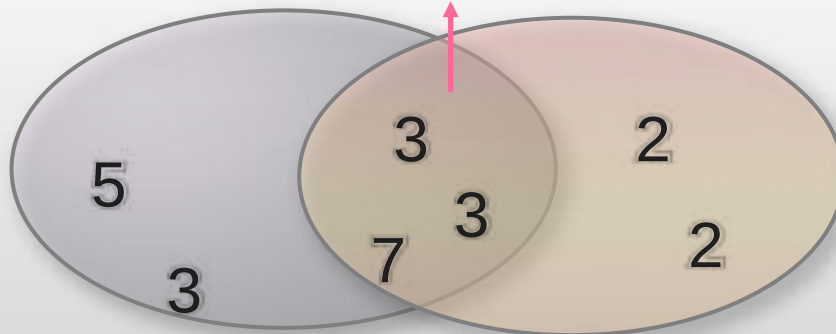


$$945 = 3^3 \cdot 5 \cdot 7;$$
$$252 = 2^2 \cdot 3^2 \cdot 7.$$

Дільники 945

Спільні дільники

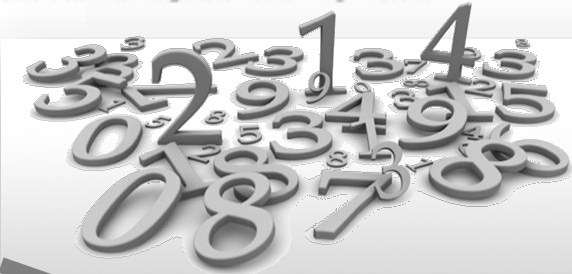
Дільники 252



$$\text{НСД}(945, 252) = 3^2 \cdot 7 = \mathbf{63}$$

$$\text{НСК}(945, 252) = 3^3 \cdot 2^2 \cdot 5 \cdot 7 = \mathbf{3780}$$

Решето Ератосфена



Чи існує
загальний закон, за
яким генеруються
прості числа



Сучасна теорія чисел
не знає точні відповіді на
це питання

Решето Ератосфена – історично
перший алгоритм знаходження
всіх простих чисел, менших
даного цілого числа n



Eratosthenes

Ερατοσθένης ὁ Κυρηναῖος
276 р. до н.е. – 194 р. до н.е.
грецький математик, астроном,
географ і поет

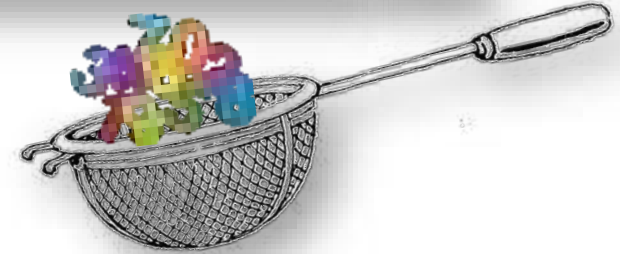
Решето Ератосфена



Тема 2. Прості числа (продовження -2.10)

Решето Ератосфена

	2	3	4	5	6	7	8	9	10
11	12	13	14	15	16	17	18	19	20
21	22	23	24	25	26	27	28	29	30
31	32	33	34	35	36	37	38	39	40
41	42	43	44	45	46	47	48	49	50
51	52	53	54	55	56	57	58	59	60
61	62	63	64	65	66	67	68	69	70
71	72	73	74	75	76	77	78	79	80
81	82	83	84	85	86	87	88	89	90
91	92	93	94	95	96	97	98	99	100



-  – кратні 2
-  – кратні 3
-  – кратні 5
-  – кратні 7

$$\sqrt{n} = \sqrt{100} = 10 < 11$$

(11 – перше просте число після 7)



Процес завершено

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

Тема 2. Прості числа (продовження -2.11)

Поліноміальні формули побудови простих чисел



$m = n^2 + n + 41$ –
просте при $0 \leq n \leq 39$



$m = n^2 - 79n + 1601$ –
просте при $0 \leq n \leq 79$



Леонард Ейлер
(1707 -1783)



$m = 2n^2 + 29$ – просте при $0 \leq n \leq 28$

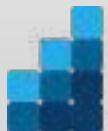


Адрієн-Марі
Лежандр
(1752 – 1833)



ДОВЕДЕНО:

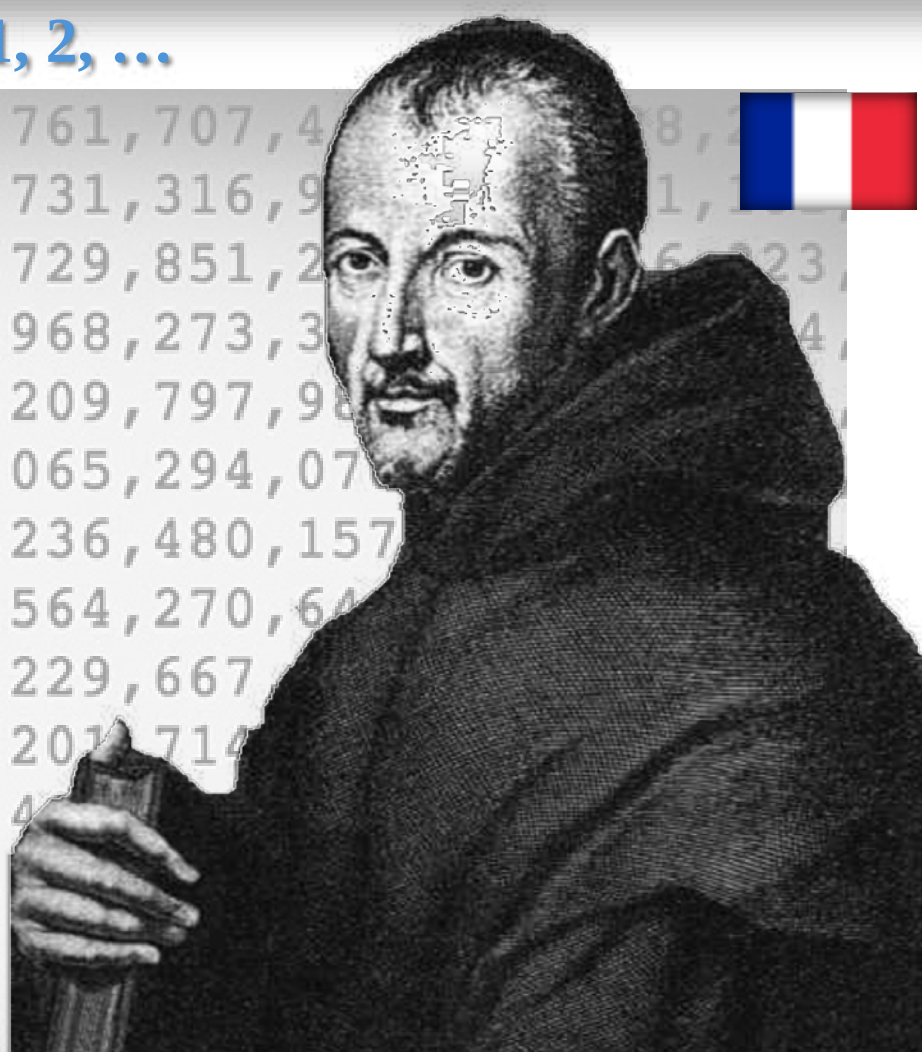
не існує многочлена $f(n)$, всі
значення якого є прості числа
при всіх цілих n



Тема 2. Прості числа (продовження -2.12)

Числа Марсена $M_n = 2^n - 1$, де $n = 1, 2, \dots$

n	M_n	Просте ?
1	1	
2	3	Так
3	7	Так
4	15	Ні
5	31	Так
6	63	Ні
8	255	Ні
7	127	Так
9	511	Ні
10	1023	Ні
11	2047	Ні
12	4095	Ні
13	8191	Так



Марен Марсен
(1588 – 1648)

Властивості чисел Марсена

1

Якщо парне $n \geq 4$, тоді число Марсена — складене:

$$2^n - 1 = (2^{n/2} - 1)(2^{n/2} + 1)$$

2

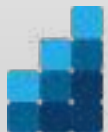
Якщо непарне $n = ab$ складене, то число Марсена — складене:

$$2^{ab} - 1 = (2^a - 1)(1 + 2^a + \dots + 2^{a(b-1)})$$

3

При простому індексі p використовують запис M_p .

Якщо M_p — просте число, то p — просте число. Навпаки невірно. Наприклад, при простих $p = 2, 3, 4, 7, 13, 17, 19, \dots$ числа Марсена прості, при простих $p = 11, 23, 29, \dots$ числа Марсена складені.



Властивості чисел Марсена

4

Відомо 51 просте число Марсена. (2018 р)
Останнє містить 24 862 048 знаків.

5

Для перевірки простоти чисел Марсена існує ефективний тест Люка –Лемера.

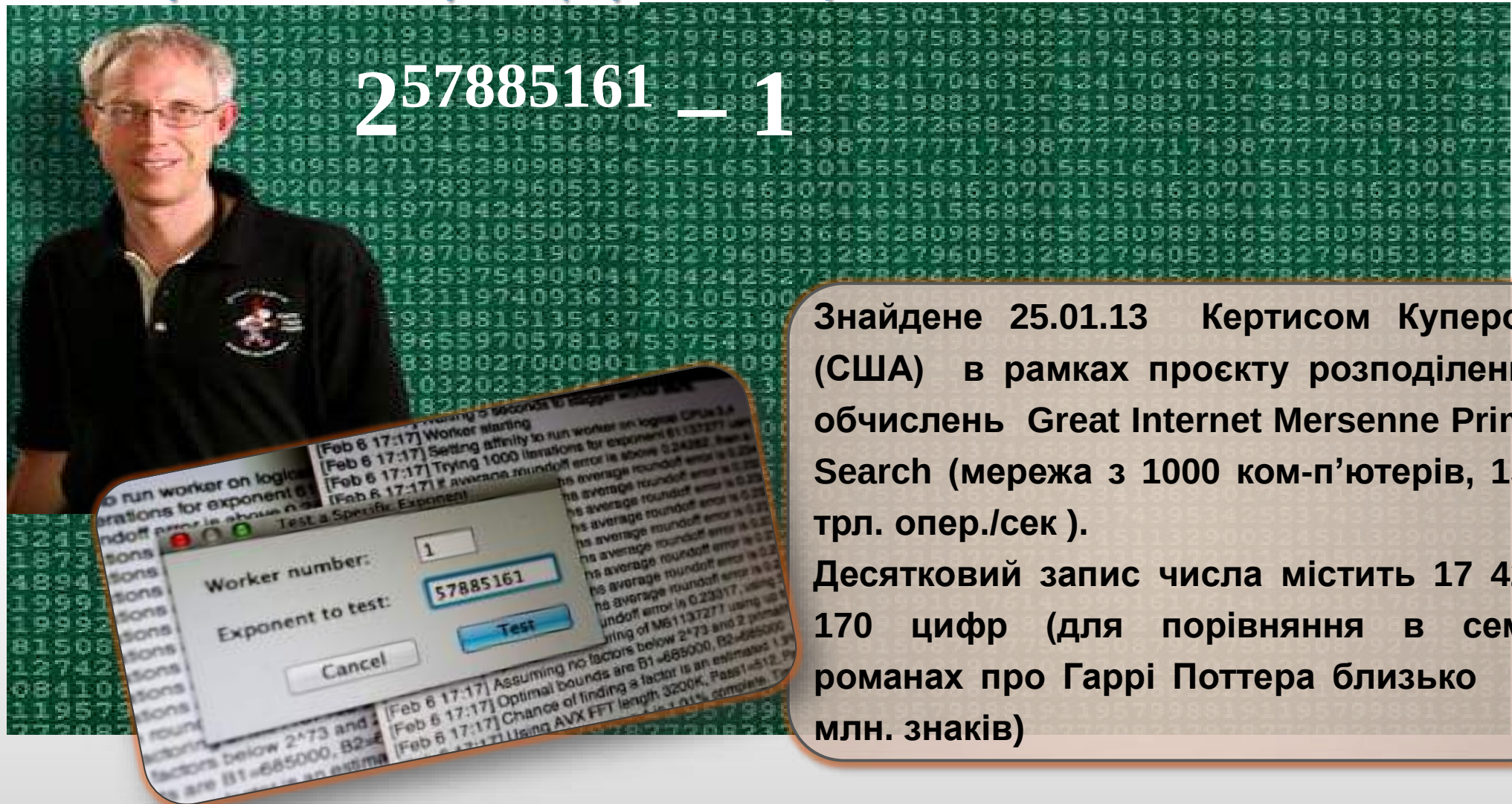
6

Невідомо, чи є скінченною множина простих чисел Марсена.



Тема 2. Прості числа (продовження -2.15)

Найбільше просте число Марсена (вересень 2013)



The image is a composite. On the left, a man with glasses and a dark polo shirt is smiling. In the center, the number **257885161** is displayed in large white font, followed by a minus sign and a subscript 1 (-1). On the right, a computer screen shows a software interface for testing Mersenne primes. The interface includes a 'Worker number' field set to 1, an 'Exponent to test' field set to 57885161, and a 'Test' button. The background of the entire image is a green field of binary code (0s and 1s).

Знайдене 25.01.13 Кертисом Купером (США) в рамках проєкту розподілених обчислень Great Internet Mersenne Prime Search (мережа з 1000 ком-п'ютерів, 150 трл. опер./сек).

Десятковий запис числа містить 17 425 170 цифр (для порівняння в семи романах про Гаррі Поттера близько 10 млн. знаків)

Тема 2. Прості числа (продовження -2.16)

Числа Ферма $F_n = 2^{2^n} + 1$, $n = 0, 1, 2, \dots$

n	F_n	Просте ?
0	3	Так
1	5	Так
2	17	Так
3	257	Так
4	65537	Так
5	4294967297	Ні
6	18446744073709551617	Ні



П'єр де Ферма
(1601 – 1665)

Властивості чисел Ферма

1

Серед чисел $F_n = 2^{2^n} + 1$ простими є F_0, F_1, F_2, F_3, F_4

2

Ферма припустив, що всі числа виду $F_n = 2^{2^n} + 1$ – прості. Гипотезу спростував Ейлер, він показав в 1732 р., що $F_5 = 4294967297 = 641 \cdot 6700417$

3

Кожний дільник числа Ферма $F_n = 2^{2^n} + 1$ має вигляд $k \cdot 2^{m+2} + 1$ при деяких k та m

4

На тепер простих чисел Ферма при $n > 4$ не знайдено. Останні досягнення:

$$303472680883 \cdot 2^{420} + 1$$

$$406860969 \cdot 2^{3322} + 1$$



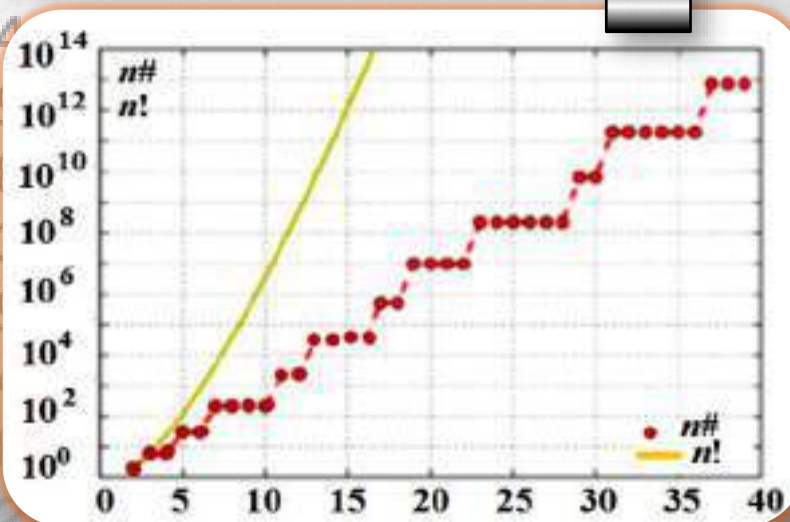
Тема 2. Подільність чисел (продовження -2.18)

Прайморіальні прості числа вигляду $p\# + 1$

Прайморіал $p\#$ – це добуток простих чисел, не більших за число p

Наприклад,

$$11\# = 2 \cdot 3 \cdot 5 \cdot 7 \cdot 11 = 2310$$



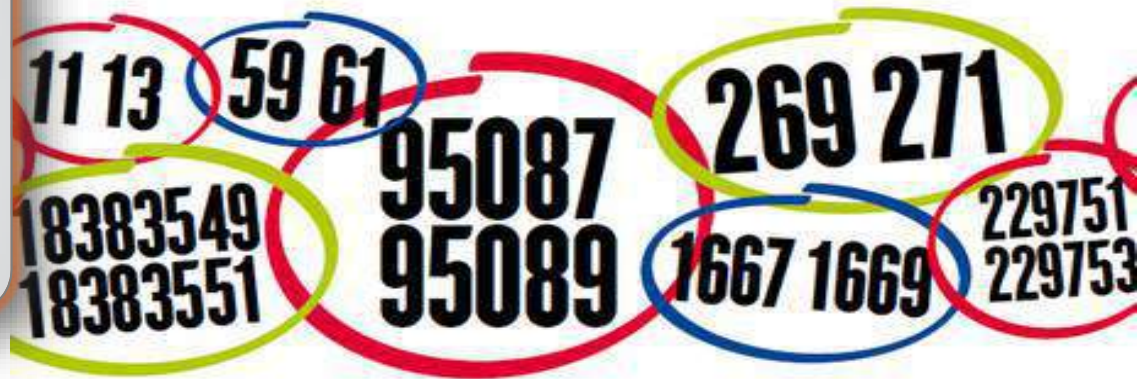
p	$p\# + 1$	Просте ?
2	3	Так
3	7	Так
5	31	Так
7	211	Так
11	2311	Так
13	30031	Ні
17	510511	Ні
31	200560490130	Так

Останні дані за 2019 р.:

$392113\# + 1$ – просте число
(169966 десяткових знаків)

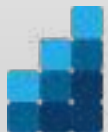
Нерегулярності в розподілі простих чисел

Поява
чисел-близнюків
(це два простих
числа, різниця між
якими дорівнює 2)



На 2015 р. Найбільша и
пара близнюків

$3756801695685 \cdot 2^{666669} - 1$,
 $3756801695685 \cdot 2^{666669} + 1$
(200700 знаків)



Нерегулярності в розподілі простих чисел

Для будь-якого цілого n в натуральному ряду існує відрізок довжини n , що не містить простих чисел (це $n!+2, n!+3, \dots, n!+n$). При великих n цей відрізок може бути досить довгим



На 2015 р. найбільший інтервал між двома послідовними простими числами складав 3 311 852 (самі прості числа містять 97 953 знака)



Розподіл простих чисел в натуральному ряді

Функція розподілу простих чисел – це функція $\pi(x)$, значення якої дорівнюють кількості простих чисел, менших або рівних x



$\pi(1) = 0$ (немає простих ≤ 1)

$\pi(2) = 1$ (просте $2 \leq 2$)

$\pi(3) = 2$ (прості $2, 3 \leq 3$)

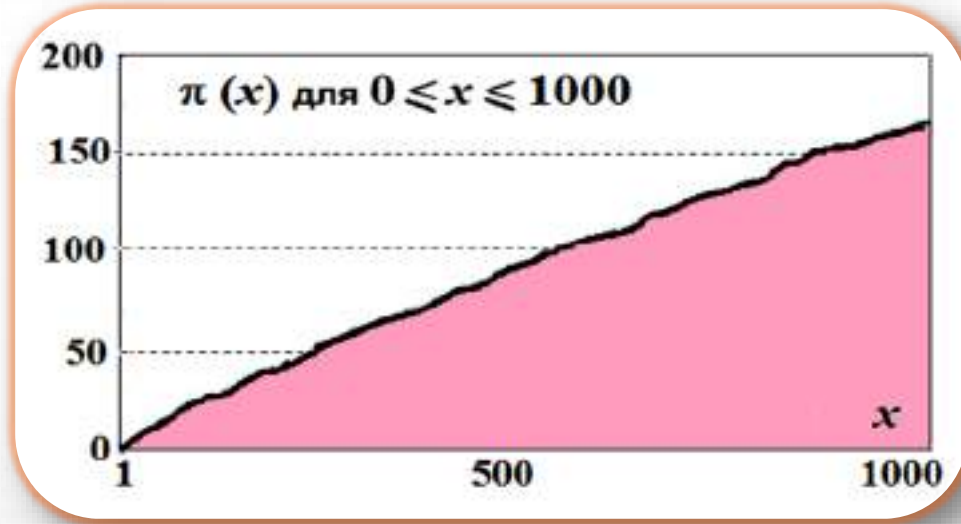
$\pi(10) = 4$ (прості $2, 3, 5, 7 \leq 10$)

$\pi(100) = 25; \quad \pi(1000) = 168$



Тема 2. Прості числа (продовження -2.22)

Розподіл простих чисел в натуральному ряді



n	$\pi(10^n)$
1	4
2	25
3	168
4	1 229
5	9 562
6	78 498
7	664 579
8	5 761 455
9	50 847 534
10	255 052 511



Асимптотичний закон розподілу простих чисел

К. Ф. Гаусс



$$\pi(x) \sim \frac{x}{\ln x}$$



$$\pi(x) \sim \int_2^x \frac{dn}{\ln n} \text{ при } x \rightarrow \infty$$

1792 г.

1796 г.

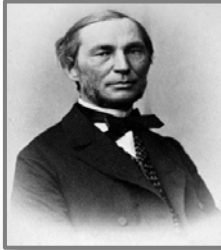
1849 г.



А.- М. Лежандр

$$\pi(x) \sim \frac{x}{\ln x - 1,08}$$

Асимптотичний закон розподілу простих чисел



П.Л. Чебишев

$$0,9213 \leq \frac{\pi(x)}{x/\ln x} \leq 1,1056$$

- Якщо існує, то він дорівнює 1

$$\lim_{x \rightarrow \infty} \frac{\pi(x)}{x/\ln x}$$

1848 –
1850 гг.

1896 г.

1949 г.

П. Ердьош,
А. Сельберг
Елементарне
доведення
асимптотичного
закону



Ж. Адамар

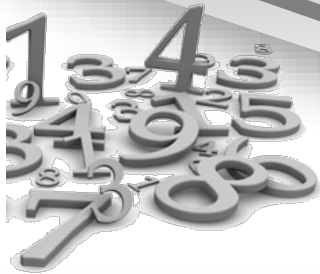


Ш.Ж. Валле Пуссен

Доведення
асимптотичного закону (з
використанням
комплексного аналізу на
базі гіпотези Рімана)

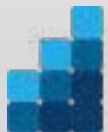
Асимптотичний закон розподілу простих чисел

Важлива для криптографії
евристична трактовка
асимптотичного закона
розподілу простих чисел:



Ймовірність того, що випадкове
число x – просте число,
приблизно дорівнює

$$\frac{1}{\ln x}$$



Асимптотичний закон розподілу простих чисел



Яка ймовірність, що випадкове 512-бітове число просте



РОЗВ'ЯЗАННЯ:

$x_1 = 2^{511}$ – найменше 512-бітове число;

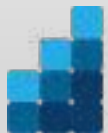
$x_2 = 2^{512} - 1$ – найбільше 512-бітове число;

$$\pi(x_2) - \pi(x_1) = \frac{x_2}{\ln x_2} - \frac{x_1}{\ln x_1} = \frac{2^{512}}{\ln 2^{512}} - \frac{2^{511}}{\ln 2^{511}} = \frac{2^{511} \cdot 255}{256 \cdot 511 \cdot \ln 2}$$



Ймовірність, що випадкове 512-бітове число просте:

$$P = \frac{\pi(x_2) - \pi(x_1)}{x_2 - x_1} = \frac{2^{511} \cdot 255}{256 \cdot 511 \cdot \ln 2 \cdot 2^{511}} \approx \frac{1}{356}$$



Тема 2. Прості числа (продовження -2.27)

Оцінка відстані між сусідніми простими числами

Ж. Л. Бертран



Постулат: для будь-якого
натурального числа $n \geq 2$ в інтервалі
 $(n; 2n)$ знайдеться просте число

В інтервалі $(n; n + n^{107/200})$
знайдеться просте число

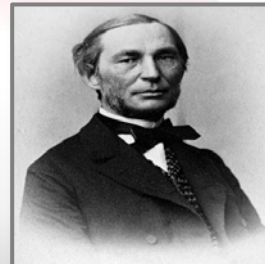
1845
г.

1852 г.

...

Наш
час

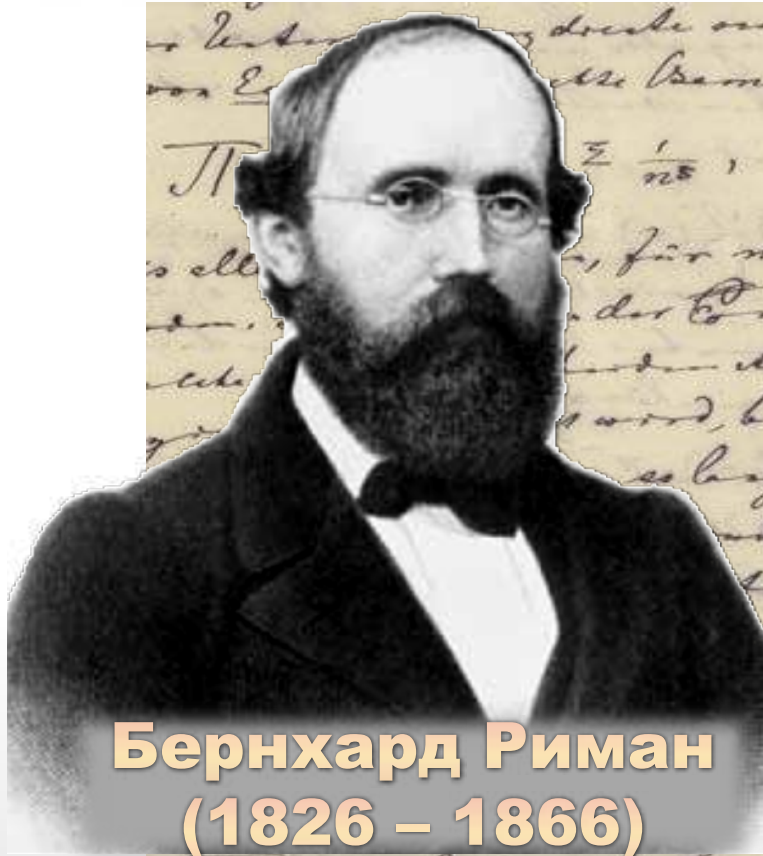
Доведення
постулата
Бертрана



П.Л. Чебишев

Тема 2. Прості числа (продовження -2.28)

Прості числа «дражнять» математиків



Багато теорем про розподіл простих чисел доведені при умові, що гіпотеза Рімана є вірною. Він показав, що функція розподілу простих чисел

$$\pi(x) = \int_2^x \frac{dx}{\ln x} - \frac{1}{2} \int_2^{\sqrt{x}} \frac{dx}{\ln x} + \sum_{\zeta(s)=0} \int_2^{x^s} \frac{dx}{\ln x} + \text{малі доданки}$$

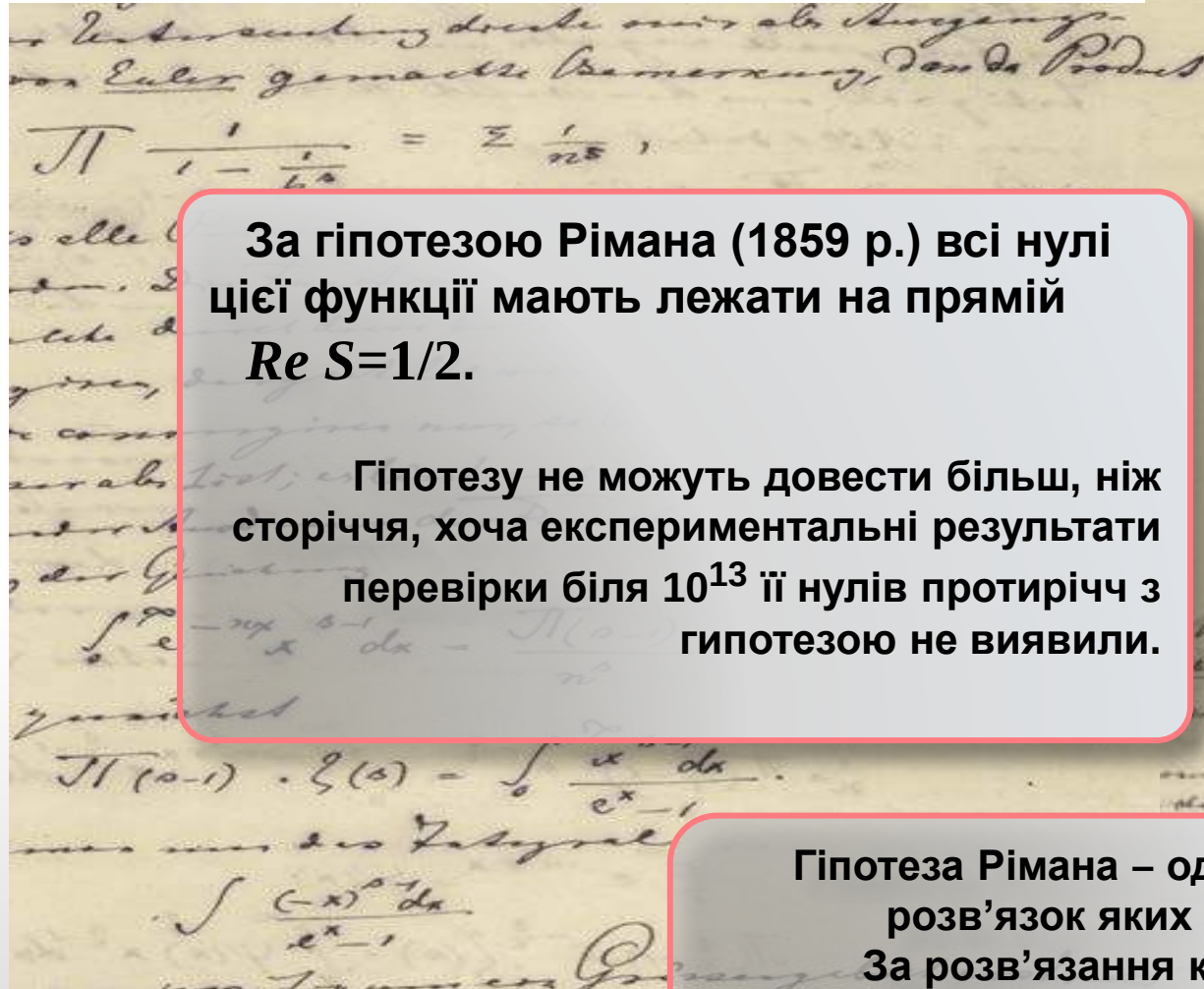
де сумування ведеться за комплексними нетривіальними нулями дзета-функції Рімана

$$\zeta(S) = \sum_{n=1}^{\infty} \frac{1}{n^S} = \prod_p (1 - p^{-S})^{-1}$$

добуток береться за всіма простими числами, $S = \sigma + it$

Тема 2. Прості числа (продовження -2.29)

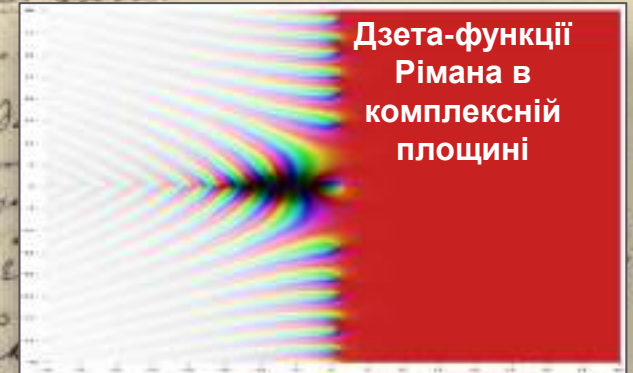
Прості числа «дражнять» математиків



За гіпотезою Рімана (1859 р.) всі нулі цієї функції мають лежати на прямій $Re S=1/2$.

Гіпотезу не можуть довести більш, ніж сторіччя, хоча експериментальні результати перевірки біля 10^{13} її нулів протирічч з гіпотезою не виявили.

Гіпотеза Рімана – одна з 7 проблем тисячоліття, розв'язок яких не знайдено за багато років. За розв'язання кожної з них інститутом Клея запропоновано приз в \$ 1млн. США



Дзета-функції Рімана в комплексній площині



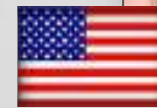
Прості числа «дражнять» математиків



Невідомо, чи існує нескінченна
множина пар простих близнюків.



Чжан Ітан (Yitang Zhang) в травні 2013 г.
довів більш слабкий варіант гіпотези про
нескінченність простих близнюків: існує
нескінченно багато простих чисел, які
можуть розділяти не більше 70 млн.
інших



Yitang Zhang

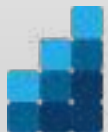
Прості числа «дражнять» математиків

В серпні 2013г. видатний математик з США Теренс Тао покращив результат Чжан Итана, показав, що існує нескінченно багато простих чисел, що розділені вже тільки не більше, ніж 4680 інших.



Теренс Тао

Значну роль в присудженні Тао Премії Філда (аналог Нобелівської премії для математиків) відіграла теорема Грина – Тао, за якою існують арифметичні прогресії довільної довжини, що повністю складаються з простих чисел



Контрольні питання:

1. Які числа називають простими?
2. Які властивості мають прості числа?
3. Що таке числа-близнюки?
4. Що стверджує основна теорема арифметики?



Основи теорії чисел

Тема 3. Неперервні (ланцюгові) дроби



Тема 3. Неперервні (ланцюгові) дроби (продовження -3.2)



При $a = 214$, $b = 35$
за алгоритмом Евкліда:

$$214 = 35 \cdot 6 + 4;$$

$$35 = 4 \cdot 8 + 3;$$

$$4 = 3 \cdot 1 + 1;$$

$$3 = 1 \cdot 3 + 0$$

$$\frac{214}{35} = 6 + \frac{4}{35} \Rightarrow \frac{214}{35} = 6 + \frac{1}{\frac{35}{4}}$$

$$\frac{35}{4} = 8 + \frac{3}{4} \Rightarrow \frac{214}{35} = 6 + \frac{1}{8 + \frac{3}{4}} = \frac{214}{35} = 6 + \frac{1}{8 + \frac{1}{\frac{4}{3}}}$$

$$\frac{4}{3} = 1 + \frac{1}{3} \Rightarrow \frac{214}{35} = 6 + \frac{1}{8 + \frac{1}{1 + \frac{1}{3}}}$$

Розкладання числа в
ланцюговий
дріб



Тема 3. Неперервні (ланцюгові) дроби (продовження -3.3)

Розкладання раціонального числа в неперервний дріб



Нехай $\frac{p}{q}$ – раціональне число. За алгоритмом Евкліда:

$$\frac{p}{q} = a_0 + \frac{r_1}{q}, \quad 0 < r_1 < q; \quad \frac{q}{r_1} = a_1 + \frac{r_2}{r_1}, \quad 0 < r_2 < r_1;$$

$$\frac{r_1}{r_2} = a_2 + \frac{r_3}{r_2}, \quad 0 < r_3 < r_2; \quad \dots; \quad \frac{r_{n-2}}{r_{n-1}} = a_{n-1} + \frac{r_n}{r_{n-1}}, \quad 0 < r_n < r_{n-1};$$

$$\frac{r_{n-1}}{r_n} = a_n$$

$$\frac{p}{q} = a_0 + \frac{r_1}{q} = a_0 + \frac{1}{\frac{q}{r_1}} = a_0 + \frac{1}{a_1 + \frac{r_2}{r_1}} = a_0 + \frac{1}{a_1 + \frac{1}{\frac{r_1}{r_2}}} = \dots$$



Тема 3. Неперервні (ланцюгові) дроби (продовження -3.4)

Розкладання раціонального числа в неперервний дріб

В результаті отримаємо:

$$\frac{p}{q} = a_0 + \frac{1}{a_1 + \frac{1}{a_2 + \frac{1}{a_3 + \dots + \frac{1}{a_n}}}}$$

де a_0 – ціле, $a_i \in \mathbb{N}$

Скінченний
правильний
неперервний
(ланцюговий)
дріб

Скорочене означення цього дробу:

$$\frac{p}{q} = [a_0; a_1, a_2, \dots, a_n] \text{ або } \frac{p}{q} = a_0 + \frac{1}{a_1} + \frac{1}{a_2} + \dots + \frac{1}{a_n}$$

Тема 3. Неперервні (ланцюгові) дроби (продовження -3.5)

Розкладання раціонального числа в неперервний дріб



$$\frac{p}{q} = a_0 + \frac{1}{a_1 + \frac{1}{a_2 + \frac{1}{a_3 + \dots + \frac{1}{a_n}}}}$$



$a_0, a_1, a_2, \dots, a_n$
називаються елементами
неперервного дроби або
неповними частками

Будь-яке раціональне
число розкладається в
скінченний неперервний
дріб єдиним чином



Тема 3. Неперервні (ланцюгові) дроби (продовження -3.6)

Розкладання раціонального числа в неперервний дріб

1

Представити число $\frac{95}{42}$ у вигляді неперервного дробу

$$\begin{aligned}\frac{95}{42} &= 2 + \frac{11}{42} = 2 + \frac{1}{\frac{42}{11}} = 2 + \frac{1}{3 + \frac{9}{11}} = \\ &= 2 + \frac{1}{3 + \frac{1}{\frac{11}{9}}} = 2 + \frac{1}{3 + \frac{1}{1 + \frac{2}{9}}} = 2 + \frac{1}{3 + \frac{1}{1 + \frac{1}{\frac{9}{2}}}} = \\ &= 2 + \frac{1}{3 + \frac{1}{1 + \frac{1}{4 + \frac{1}{2}}}} = [2 ; 3, 1, 4, 2]\end{aligned}$$

Приклад

Тема 3. Неперервні (ланцюгові) дроби (продовження -3.7)

Підхідні дроби

Для даного неперервного дробу $\frac{p}{q} = [a_0 ; a_1, a_2, \dots, a_n]$ підхідними дробами називаються неперервні дроби вигляду

$$\frac{p_0}{q_0} = a_0 ; \quad \frac{p_1}{q_1} = [a_0 ; a_1] ; \quad \frac{p_2}{q_2} = [a_0 ; a_1, a_2] ; \quad \dots ;$$

$$\frac{p_k}{q_k} = [a_0 ; a_1, a_2, \dots, a_k].$$

Дріб $\frac{p_{k-1}}{q_{k-1}}$ може бути отримана з дробу $\frac{p_k}{q_k}$ заміною a_{k-1} на $a_k + 1/a_{k+1}$;

При $k = n$ підхідний дріб дає вихідний неперервний дріб



Тема 3. Неперервні (ланцюгові) дроби (продовження -3.8)

Рекурентні формули для підхідних дробів

Для k – ого підхідного дробу чисельник p_k та знаменник q_k можна записати через чисельник та знаменник двох попередніх підхідних дробів:

$$p_k = a_k p_{k-1} + p_{k-2}; \quad q_k = a_k q_{k-1} + q_{k-2};$$



При цьому

$$p_{-2} = 0; \quad p_{-1} = 1;$$

$$q_{-2} = 1; \quad q_{-1} = 0;$$

Тема 3. Неперервні (ланцюгові) дробу (продовження -3.9)

Обчислення підхідних дробів для неперервного дробу

2

Знайти підхідні дробу для числа

$$\frac{95}{42} = [2; 3, 1, 4, 2]$$

a_k		2	3	1	4	2
p_k	1	2	$3 \cdot 2 + 1 = 7$	$1 \cdot 7 + 2 = 9$	$4 \cdot 9 + 7 = 43$	$2 \cdot 43 + 9 = 95$
q_k	0	1	$3 \cdot 1 + 0 = 3$	$1 \cdot 3 + 1 = 4$	$4 \cdot 4 + 3 = 19$	$2 \cdot 19 + 4 = 42$

$$q_k = a_k q_{k-1} + q_{k-2} \quad p_k = a_k p_{k-1} + p_{k-2}$$

$$\frac{p_0}{q_0} = \frac{2}{1}; \quad \frac{p_1}{q_1} = \frac{7}{3}; \quad \frac{p_2}{q_2} = \frac{9}{4}; \quad \frac{p_3}{q_3} = \frac{43}{19}; \quad \frac{p_4}{q_4} = \frac{95}{42}.$$

Приклад

Властивості підхідних дробів

$$p_k q_{k-1} - p_{k-1} q_k = (-1)^{k-1}$$

$$\frac{p_k}{q_k} - \frac{p_{k-1}}{q_{k-1}} = \frac{(-1)^{k-1}}{q_k q_{k-1}}$$

Для будь-якого числа x

$$\left| x - \frac{p_k}{q_k} \right| < \frac{1}{q_k^2}$$

p_k/q_k – найкраще наближення числа x серед всіх дробів, знаменник яких не перевищує q_k



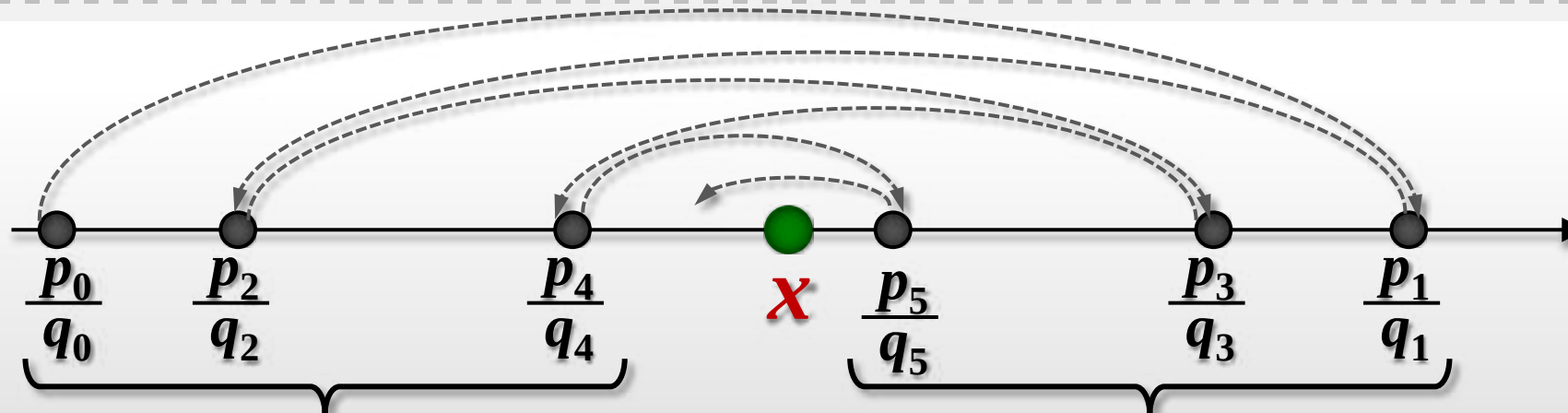
Тема 3. Неперервні (ланцюгові) дроби (продовження -3.11)

Властивості підхідних дробів



Для підхідних дробів неперервного дроби, що відповідає числу x , виконуються нерівності

$$\frac{p_0}{q_0} < \frac{p_2}{q_2} < \frac{p_4}{q_4} < \dots \leq x \leq \dots < \frac{p_5}{q_5} < \frac{p_3}{q_3} < \frac{p_1}{q_1}$$



Послідовності підхідних дробів з парними індексами зростають

Послідовності підхідних дробів з непарними індексами спадають



Тема 3. Неперервні (ланцюгові) дроби (продовження -3.12)

Як перейти від неперервного дробу до звичайного ?

І МЕТОД: «згорнути» неперервний дріб, послідовно виконуючи додавання та «перевертання» дробів



3

Якому раціональному числу відповідає дріб $[1 ; 2, 1, 7]$?

$$\begin{aligned} [1 ; 2, 1, 7] &= 1 + \frac{1}{2 + \frac{1}{1 + \frac{1}{7}}} = 1 + \frac{1}{2 + \frac{1}{8/7}} = 1 + \frac{1}{2 + \frac{7}{8}} = \\ &= 1 + \frac{1}{23/8} = 1 + \frac{8}{23} = \frac{31}{23} \end{aligned}$$



Тема 3. Неперервні (ланцюгові) дробу (продовження -3.13)

Як перейти від неперервного дробу до звичайного ?

II МЕТОД: для неперервного дробу $[a_0; a_1, a_2, \dots, a_n]$
з рекурентної формули для розрахунку
підхідних дробів знаходимо



$$\begin{pmatrix} a_0 & 1 \\ 1 & 0 \end{pmatrix} \cdot \begin{pmatrix} a_1 & 1 \\ 1 & 0 \end{pmatrix} \cdot \begin{pmatrix} a_2 & 1 \\ 1 & 0 \end{pmatrix} \cdot \dots \cdot \begin{pmatrix} a_k & 1 \\ 1 & 0 \end{pmatrix} = \begin{pmatrix} p_k & p_{k-1} \\ q_k & q_{k-1} \end{pmatrix}$$

4

Знайти всі підхідні дробу для
неперервного дробу $[2 ; 3, 1, 4, 2]$

$$\begin{pmatrix} 2 & 1 \\ 1 & 0 \end{pmatrix} \cdot \begin{pmatrix} 3 & 1 \\ 1 & 0 \end{pmatrix} \cdot \begin{pmatrix} 1 & 1 \\ 1 & 0 \end{pmatrix} \cdot \begin{pmatrix} 4 & 1 \\ 1 & 0 \end{pmatrix} \cdot \begin{pmatrix} 2 & 1 \\ 1 & 0 \end{pmatrix} = \begin{pmatrix} p_k & p_{k-1} \\ q_k & q_{k-1} \end{pmatrix}$$

Приклад



Тема 3. Неперервні (ланцюгові) дроби (продовження -3.14)

Як перейти від неперервного дробу до звичайного ?



$$\begin{pmatrix} 2 & 1 \\ 1 & 0 \end{pmatrix} \cdot \begin{pmatrix} 3 & 1 \\ 1 & 0 \end{pmatrix} = \begin{pmatrix} 7 & 2 \\ 3 & 1 \end{pmatrix} \Rightarrow \begin{pmatrix} 7 & 2 \\ 3 & 1 \end{pmatrix} \cdot \begin{pmatrix} 1 & 1 \\ 1 & 0 \end{pmatrix} = \begin{pmatrix} 9 & 7 \\ 4 & 3 \end{pmatrix}$$

$p_1; q_1$ $p_0; q_0$ $p_2; q_2$ $p_1; q_1$

$$\begin{pmatrix} 9 & 7 \\ 4 & 3 \end{pmatrix} \cdot \begin{pmatrix} 4 & 1 \\ 1 & 0 \end{pmatrix} = \begin{pmatrix} 43 & 9 \\ 19 & 4 \end{pmatrix} \Rightarrow \begin{pmatrix} 43 & 9 \\ 19 & 4 \end{pmatrix} \cdot \begin{pmatrix} 2 & 1 \\ 1 & 0 \end{pmatrix} = \begin{pmatrix} 95 & 19 \\ 42 & 4 \end{pmatrix}$$

$p_3; q_3$ $p_2; q_2$ $p_4; q_4$ $p_3; q_3$

$$\Rightarrow \frac{p_0}{q_0} = \frac{2}{1}; \quad \frac{p_1}{q_1} = \frac{7}{3}; \quad \frac{p_2}{q_2} = \frac{9}{4}; \quad \frac{p_3}{q_3} = \frac{43}{19}; \quad \frac{p_4}{q_4} = \frac{95}{42}.$$



Тема 3. Неперервні (ланцюгові) дроби (продовження -3.15)

Неперервні дроби та сонячний календар

При розробці сонячного календаря необхідно знайти раціональне наближення для числа днів у році, що дорівнює 365,2421988... Підхідні дроби для дробової частини цього числа:

$$\frac{1}{4}; \frac{7}{29}; \frac{8}{33}; \frac{31}{128}; \frac{132}{545} \dots$$

Раз в 4 роки
треба додавати
зайвий день,
похибка в 1 день
накопичується за
128 лет. Принцип
юліанського
календаря

Не
викорис-
тали

Дає 8 високісних роки
за 33 роки,
запропоноване Омаром
Хайямом в XI в. та
започаткувало
персидський календар.
Похибка в день
накопичується за 4500
років.



Тема 3. Неперервні (ланцюгові) дроби (продовження -3.7)

Деякі застосування неперервних дробів



1

Розв'язання лінійних порівнянь

2

Доведення ірраціональності чисел. Наприклад, значення дзета-функції Рімана $\zeta(3)$

3

В роботі алгоритмів факторизації чисел:

- SQUFOF (SQUare FORM Factorization), безумовного лідера серед алгоритмів факторизації для чисел від 10^{10} до 10^{18} (Шенкс, 1975 р.);
- CFRAC (Моррисон та Бріллхарт, 1975 р.);
- метод квадратичного решета (Померанц, 1982 р.)

4

Одна з відомих атак на криптосистему RSA – атака Вінера спирається на розкладання раціональних чисел в неперервний дріб





Контрольні питання:

1. Який вигляд має ланцюговий дріб?
2. Що називається підхідними дробами?
3. Як перейти від неперервного дроби до звичайного?
4. Для чого використовують неперервні дроби?



Основи теорії чисел

Тема 4. Теорія порівнянь



Тема 4: Порівняння чисел



Визначення

Два цілих числа a та b **порівняні за модулем m** , якщо їх різниця $a - b$ ділиться без остачі на m .

Символічно порівнянність записується у вигляді **порівняння** (конгруенції):

$$a \equiv b \pmod{m}$$

НАПРИКЛАД:

$$21 \equiv 5 \pmod{8}, \text{ оскільки } 21 - 5 = 16, 8|16 ;$$

$$32 \equiv -10 \pmod{7}, \quad 32 - (-10) = 42, 7|42 ;$$

$$18 \equiv 0 \pmod{3}, \quad 18 - 0 = 18, 3|18$$



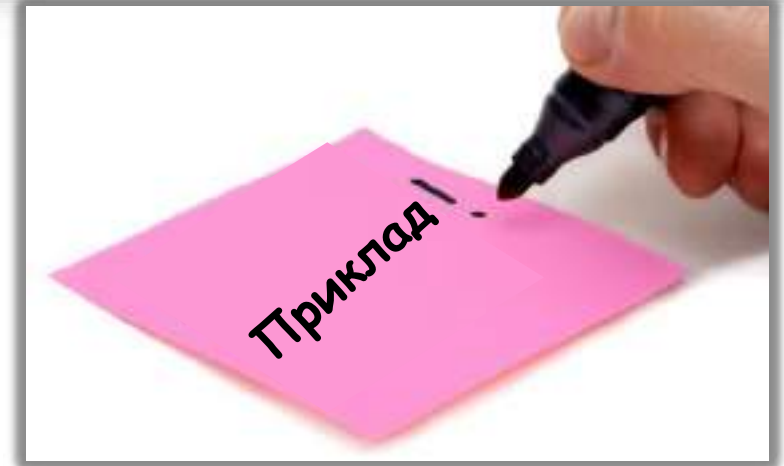
№ 1 Знайти: $113 \pmod{24}$, $-29 \pmod{7}$

$$\begin{array}{r|l} 113 & 24 \\ -96 & 4 \\ \hline 17 & \end{array}$$

$$113 \pmod{24} \equiv 17$$

$$\begin{array}{r|l} -29 & 7 \\ -35 & 5 \\ \hline 6 & \end{array}$$

$$-29 \pmod{7} \equiv 6$$



№ 2 Які порівняння записані правильно

?

А) $3 \equiv 3 \pmod{17}$;

Б) ~~$3 \equiv -3 \pmod{17}$;~~

В) $172 \equiv 177 \pmod{5}$;

Г) $-13 \equiv 13 \pmod{26}$

ТЕРМІНОЛОГІЯ ТА ІНШІ ОЗНАЧЕННЯ:

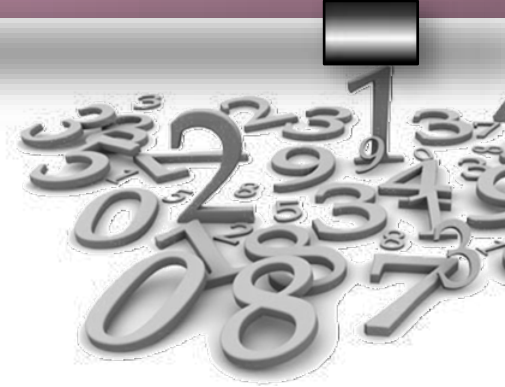


$$a \equiv b \pmod{m}$$

Число a конгруентне числу b за модулем m

Лишок числа a за модулем m

Модуль порівняння



Інші способи запису порівнянь: $a \equiv b(m)$, $a \overset{m}{\equiv} b$, $a \equiv b_m$



Операція $a \bmod m$ (без дужок) означає остачу від ділення числа a на m і називається зведенням числа a за модулем. Наприклад, $7 \bmod 3 \equiv 1$.



Тема 4. Порівняння чисел (продовження 4-4)

Еквівалентні визначення

Два цілих числа a і b порівнянні за модулем m , якщо їх різниця $a - b$ ділиться без остачі на m .

Два цілих числа a і b порівнянні за модулем m , якщо існує таке ціле число t , що $a = b + mt$, де $t \in \mathbb{Z}$

Два цілих числа a і b порівнянні за модулем m , якщо вони при діленні на m мають однакову остачу



Тема 4. Порівняння чисел (продовження 4-5)

Порівняння - відношення еквівалентності

1

Рефлексивність
порівняння:

$$a \equiv a \pmod{m}$$

2

Симетричність
порівняння:

якщо

$$a \equiv b \pmod{m},$$

то

$$b \equiv a \pmod{m}$$

3

Транзитивність
порівняння:

якщо

$$a \equiv b \pmod{m} \text{ и}$$

$$b \equiv c \pmod{m},$$

то

$$a \equiv c \pmod{m}$$



Відношення порівнянності є відношенням еквівалентності на
множині цілих чисел



Тема 4. Порівняння чисел (продовження 4-6)

Властивості порівнянь

1

Порівняння за однаковими модулями можна почленно додавати і множити: $a \equiv b \pmod{m}$, $c \equiv d \pmod{m}$, тоді $a \pm c \equiv b \pm d \pmod{m}$ і $ac \equiv bd \pmod{m}$.

Наприклад:

$$\begin{array}{r} + \quad 7 \equiv 3 \pmod{4} \\ \quad 10 \equiv 2 \pmod{4} \\ \hline \quad 17 \equiv 5 \pmod{4} \end{array}$$

$$\begin{array}{r} - \quad 7 \equiv 3 \pmod{4} \\ \quad 10 \equiv 2 \pmod{4} \\ \hline \quad 1 \equiv 1 \pmod{4} \end{array}$$

$$\begin{array}{r} \times \quad 7 \equiv 3 \pmod{4} \\ \quad 10 \equiv 2 \pmod{4} \\ \hline \quad 70 \equiv 2 \pmod{4} \end{array}$$

2

Доданок з однієї частини порівняння можна переносити до іншої, змінивши його знак:

$$a + b \equiv c \pmod{m} \Rightarrow a \equiv (c - b) \pmod{m}$$

Приклад: $15 + 16 \equiv 22 \pmod{9}$; $15 \equiv 22 - 16 \pmod{9}$; $15 \equiv 6 \pmod{9}$

Тема 4. Порівняння чисел (продовження 4-7)

Властивості порівнянь

3

До будь-якої частини порівняння можна додати число, кратне модулю:

$$a \equiv b \pmod{m} \Rightarrow a + mk \equiv b \pmod{m}$$

4

Обидві частини можна піднести в один і той же степінь:

$$a \equiv b \pmod{m} \Rightarrow a^n \equiv b^n \pmod{m}$$

Наприклад: $8 \equiv 3 \pmod{5}$; $8^2 \equiv 3^2 \pmod{5}$; $64 \equiv 9 \pmod{5}$

5

Якщо $a_0 \equiv b_0 \pmod{m}$, $a_1 \equiv b_1 \pmod{m}$, ..., $a_n \equiv b_n \pmod{m}$,
 $x \equiv y \pmod{m}$, то

$$a_0 x^n + a_1 x^{n-1} + \dots + a_n \equiv (b_0 y^n + b_1 y^{n-1} + \dots + b_n) \pmod{m}$$

Тема 4. Порівняння чисел (продовження 4-8)

Властивості порівнянь

6

Обидві частини порівняння можна скоротити на їх спільний множник, якщо він взаємно простий з модулем, тобто якщо $ac \equiv bc \pmod{m}$ та $\text{НСД}(m, c) = 1$, тоді

$$a \equiv b \pmod{m}$$

7

Обидві частини порівняння і модуль можна скоротити на їх спільний дільник, тобто якщо $ac \equiv bc \pmod{mc}$, то

$$a \equiv b \pmod{m}$$

НЕМАЄ АНАЛОГІЇ с числовими рівностями !!!

Наприклад:

$$45 \equiv 15 \pmod{6}$$

$9 \equiv 3 \pmod{6}$ – скорочення на 3, $\text{НСД}(3, 6) = 3$

$15 \not\equiv 5 \pmod{6}$ – скорочення на 3, $\text{НСД}(3, 6) = 3$

Тема 4. Порівняння чисел (продовження 4-9)

Властивості порівнянь

8

Якщо $a \equiv b \pmod{m_1}$ і $a \equiv b \pmod{m_2}$, то

$$a \equiv b \pmod{M}, \quad \text{де } M = \text{НСК}(m_1, m_2)$$

Наприклад: $120 \equiv 20 \pmod{4}$; $120 \equiv 20 \pmod{10}$;

$$M = \text{НСК}(4, 10) = 20 \quad \rightarrow$$

$$120 \equiv 20 \pmod{20}$$

9

Якщо $a \equiv b \pmod{m}$, то $\text{НСД}(a, m) = \text{НСД}(b, m)$



Тема 4. Порівняння чисел (продовження 4-10)

Властивості операції зведення за модулем

$$a \square b \bmod m \equiv (a \bmod m \square b \bmod m) \bmod m,$$

де $\square$ – це $+$, $-$, $\times$

$$\begin{aligned} &1595 \cdot 2372862 + 731^2 \bmod 7 \equiv \\ &\equiv 1595 \bmod 7 \cdot 2372862 \bmod 7 + (731 \bmod 7)^2 \bmod 7 \equiv \\ &\equiv 6 \cdot 2 \bmod 7 + 3^2 \bmod 7 \equiv 5 + 2 \bmod 7 \equiv 0. \end{aligned}$$



Тема 4. Порівняння чисел (продовження 4-11) Піднесення в степінь за модулем

$$a^{15}$$

Скільки множень необхідно, щоб
обчислити це значення ?

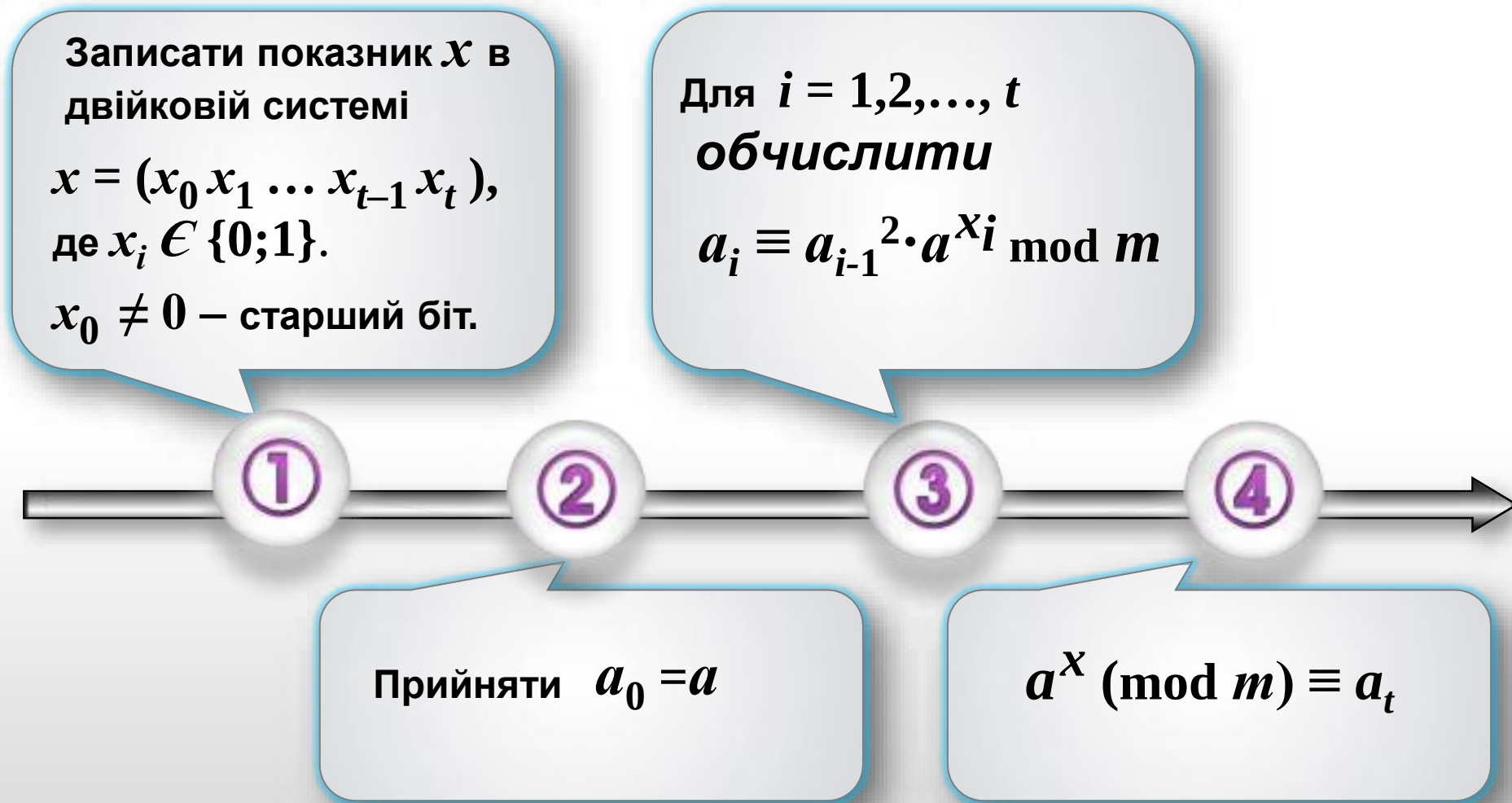
Традиційна думка: $a \rightarrow a^2 \rightarrow a^3 \rightarrow a^4 \rightarrow \dots \rightarrow a^{15}$
14 множень !!!

Бінарний метод: $a \rightarrow a^2 \rightarrow a^3 \rightarrow a^6 \rightarrow a^7 \rightarrow a^{14} \rightarrow a^{15}$
6 множень !!!



Тема 4. Порівняння чисел (продовження 4-12)

Бінарний алгоритм обчислення $a^x \pmod m$



Тема 4. Порівняння чисел (продовження 4-13)

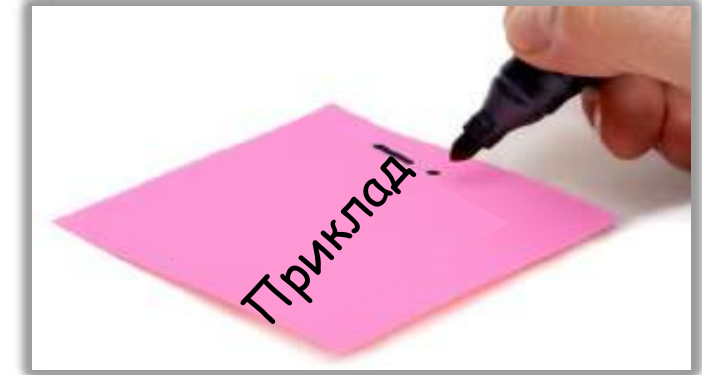
Бінарний алгоритм обчислення $a^x \pmod m$

Обчислити $3^{100} \pmod 7$

1 $x = 100 = 1100100_2$
 $x_0 x_1 x_2 x_3 x_4 x_5 x_6 \equiv 1100100$

2 $a_0 = a = 3$

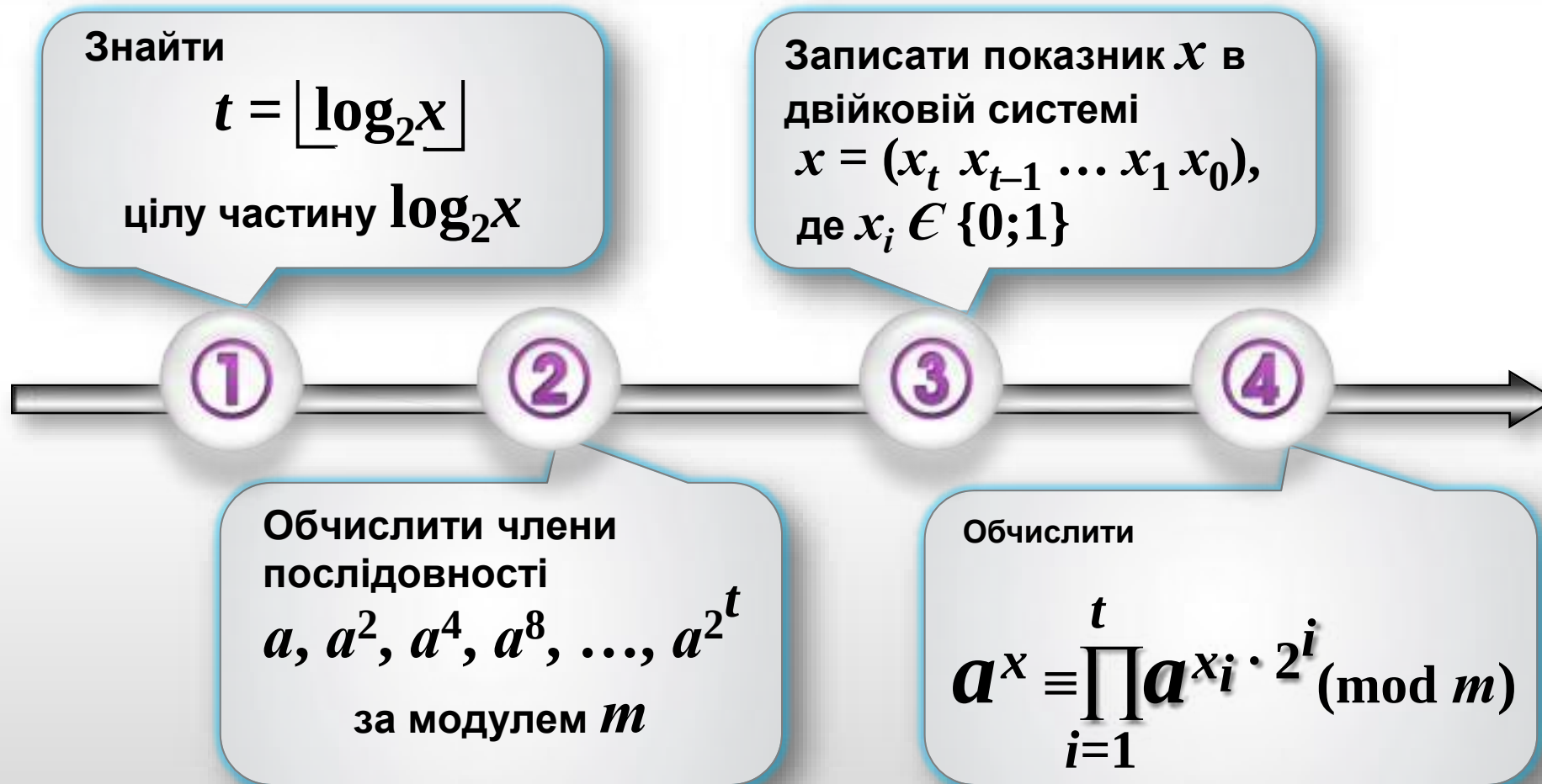
3 $a_1 = a_0^2 \cdot a^{x_1} \pmod 7 \equiv 3^2 \cdot 3^1 \equiv 6;$
 $a_2 = a_1^2 \cdot a^{x_2} \pmod 7 \equiv 6^2 \cdot 3^0 \equiv 1;$
 $a_3 = a_2^2 \cdot a^{x_3} \pmod 7 \equiv 1^2 \cdot 3^0 \equiv 1;$
 $a_4 = a_3^2 \cdot a^{x_4} \pmod 7 \equiv 1^2 \cdot 3^1 \equiv 3;$
 $a_5 = a_4^2 \cdot a^{x_5} \pmod 7 \equiv 3^2 \cdot 3^0 \equiv 2;$
 $a_6 = a_5^2 \cdot a^{x_6} \pmod 7 \equiv 2^2 \cdot 3^0 \equiv 4$



4 $3^{100} \pmod 7 \equiv 4$

Тема 4. Порівняння чисел (продовження 4-14)

Алгоритм обчислення $a^x \pmod m$ (розпаралелювання за допомогою каскадної схеми множення)



Алгоритм обчислення $a^x \pmod m$

Обчислити $3^{100} \pmod 7$

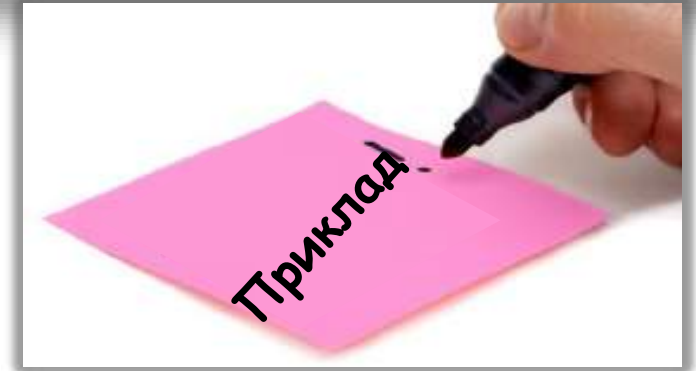
① $t = \lfloor \log_2 100 \rfloor = \lfloor 6,65 \rfloor = 6$ – ціла частина показника

② $x = 100 = 1100100_2 \rightarrow x_6 x_5 x_4 x_3 x_2 x_1 x_0 = 1100100$

③

a	$a^2 \pmod 7$	$a^4 \pmod 7$	$a^8 \pmod 7$	$a^{16} \pmod 7$	$a^{32} \pmod 7$	$a^{64} \pmod 7$
3	2	4	2	4	2	4

④ $3^{100} \pmod 7 \equiv 3^{1 \cdot 2^6} \cdot 3^{1 \cdot 2^5} \cdot 3^{0 \cdot 2^4} \cdot 3^{0 \cdot 2^3} \cdot 3^{1 \cdot 2^2} \cdot 3^{0 \cdot 2^1} \cdot 3^{0 \cdot 2^0} \pmod 7 \equiv$
 $\equiv 3^{64} \cdot 3^{32} \cdot 3^0 \cdot 3^0 \cdot 3^4 \cdot 3^0 \cdot 3^0 \pmod 7 \equiv 4 \cdot 2 \cdot 1 \cdot 1 \cdot 4 \cdot 1 \cdot 1 \pmod 7 \equiv 4$





Контрольні питання:

1. Що називається порівнянням або конгруенцією?
2. Які властивості мають порівняння?
3. В яких методах обчислення великих чисел застосовують порівняння?



Основи теорії чисел

Тема 5. Класи лишків за модулем m



ТЕМА 5: Класи лишків за модулем m

Множина всіх чисел, порівнянних з числом a за модулем m , називається класом лишків a за модулем m

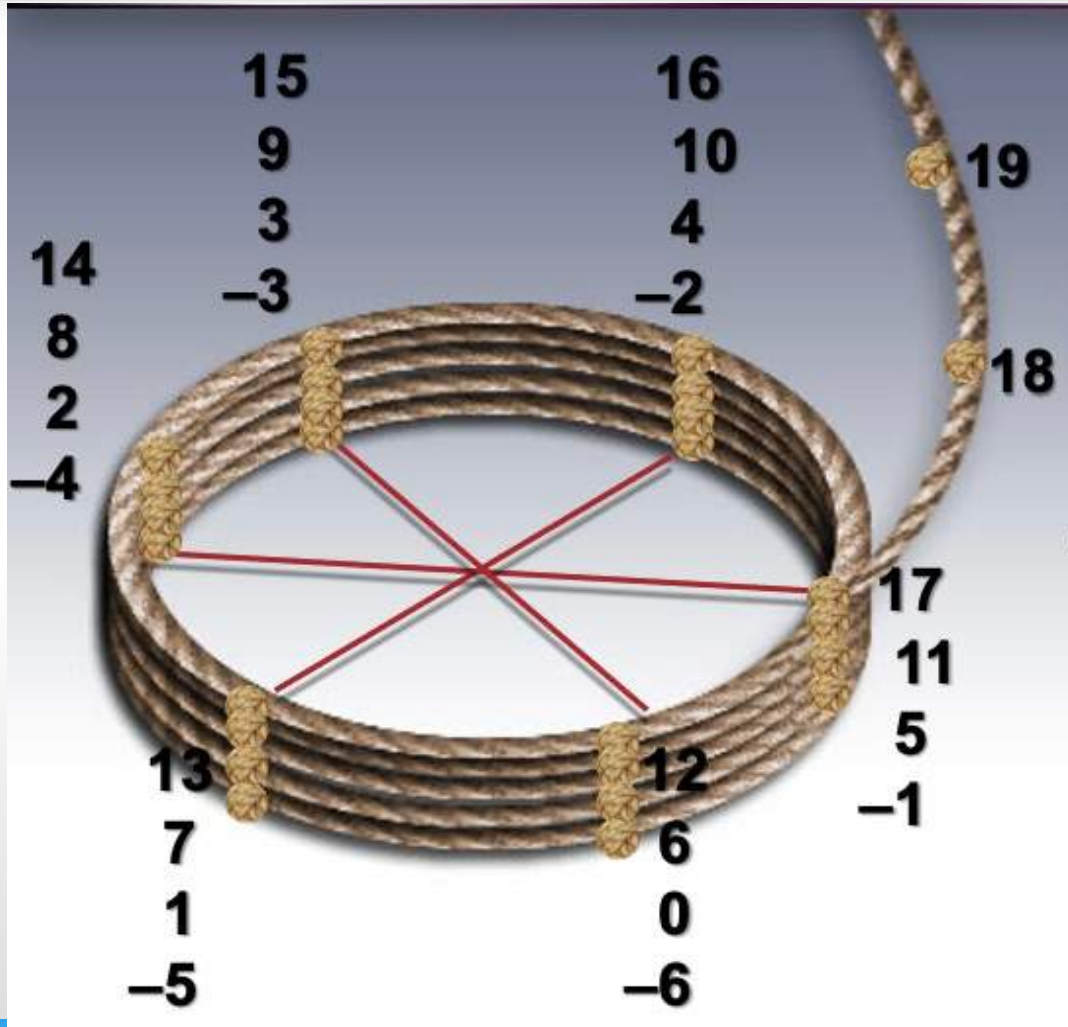
Позначення класу $\bar{a}_m$, $\bar{a}$, $[a]_m$

Клас лишків $\bar{a}$ за модулем m - це

$$\bar{a}_m = \{ x \equiv a \pmod{m}, x \in \mathbb{Z} \}$$

Тема 5. Класи лишків за модулем m (продовження 5-2)

Розподіл чисел за класами лишків за $\text{mod } 6$



«Намотування» ланцюга з цілих чисел на кільце з 6 поділками. На один поділ автоматично потрапляють числа, що порівняні між собою за $\text{mod } 6$.

Так множина $\mathbb{Z}$ цілих чисел розпадається на 6 класів лишків, кожен з яких породжується будь-яким числом з класу.

Класи лишків за модулем m

Існує 5 класів лишків за модулем 5:

$$\overline{0} = \{ \dots, -15, -10, -5, 0, 5, 10, 15 \dots \}$$

(числа, що діляться на 5 націло)

$$\overline{1} = \{ \dots, -14, -9, -4, 1, 6, 11, 16 \dots \}$$

(числа, що діляться на 5 з остачею 1)

$$\overline{2} = \{ \dots, -13, -8, -3, 2, 7, 12, 17 \dots \}$$

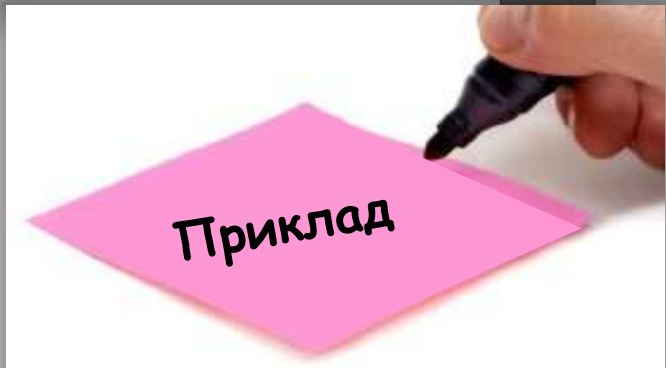
(числа, що діляться на 5 з остачею 2)

$$\overline{3} = \{ \dots, -12, -7, -2, 3, 8, 13, 18 \dots \}$$

(числа, що діляться на 5 з остачею 3)

$$\overline{4} = \{ \dots, -11, -6, -1, 4, 9, 14, 19 \dots \}$$

(числа, що діляться на 5 з остачею 4)



Приклад

1

Для будь-якого m число класів лишків за модулем m скінченне і дорівнює m .
Це класи: $\overline{0}, \overline{1}, \overline{2}, \dots, \overline{m-1}$

Множина класів лишків за модулем m позначають Z_m (або Z/mZ , або Z/m), тобто

$$Z_m = \{ \overline{0}, \overline{1}, \overline{2}, \dots, \overline{m-1} \}$$

2

Кожний клас за модулем m містить одне з чисел $0, 1, \dots, m-1$ разом з усіма числами, що порівняні з цим числом за модулем m



Властивості класів лишків за модулем

3

Клас лишків $\bar{a}$ співпадає з множиною чисел $a+km$, де $k \in \mathbb{Z}$

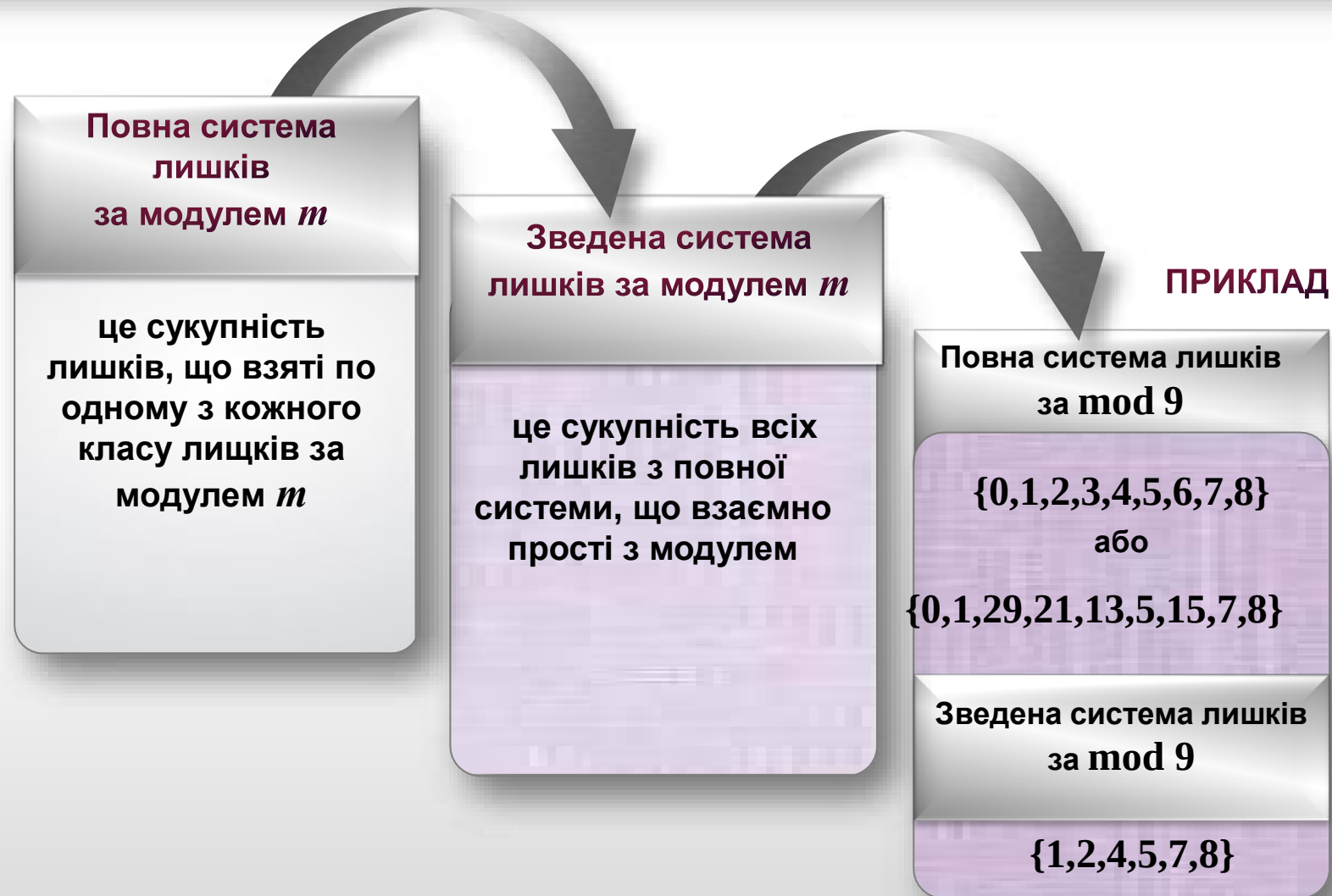
4

Якщо $a \equiv b \pmod{m}$, тоді $\bar{a} = \bar{b}$;
якщо $a \not\equiv b \pmod{m}$, тоді $\bar{a} \cap \bar{b} = \emptyset$
(класи не перетинаються)



Тема 5. Класи лишків за модулем m (продовження 5-6)

Системи лишків за модулем m



Теорема

Якщо $\text{НСД}(a, m) = 1$, x проходить повну систему лишків за модулем m , тоді числа $ax + b$ також утворюють повну систему лишків за цим модулем.

ДОВЕДЕННЯ: нехай $x_1 \not\equiv x_2 \pmod{m}$,

x_1 та x_2 — представники різних класів за модулем m .

Будемо вважати, що $ax_1 + b \equiv ax_2 + b \pmod{m}$. Тоді

$$ax_1 \equiv ax_2 \pmod{m}.$$

$$\text{НСД}(a, m) = 1 \quad \Rightarrow \quad x_1 \equiv x_2 \pmod{m}$$

$$\Rightarrow ax_1 + b \equiv ax_2 + b \pmod{m}$$

Протиріччя

Тема 5. Класи лишків за модулем m (продовження 5-8)

Операції над класами лишків за модулем m

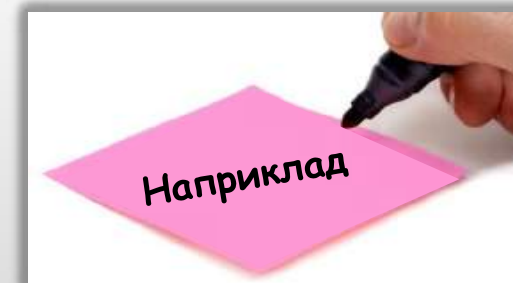
Сумою класів $\overline{a}$ та $\overline{b}$ лишків за модулем m називається клас $\overline{a+b}$, що утворюється елементом $a+b$ за модулем m

Добутком класів $\overline{a}$ та $\overline{b}$ лишків за модулем m називається клас $\overline{ab}$, що утворений елементом ab за модулем m

Клас $-\overline{a} = \overline{m-a}$ називається протилежним класу $\overline{a}$ за модулем m

Операції над класами лишків за модулем 6:

$$\begin{aligned}\overline{5} + \overline{4} &= \overline{2}, \text{ оскільки } 5+4 \equiv 2 \pmod{6} \\ \overline{7}; \overline{5} \cdot \overline{4} &= \overline{6}, \text{ оскільки } 5 \cdot 4 \equiv 6 \pmod{7} \\ \overline{7}; -\overline{2} &= \overline{5}, \text{ оскільки } -2 \equiv 5 \pmod{7}\end{aligned}$$



Тема 5. Класи лишків за модулем m (продовження 5-9)

Операції над класами лишків по модулю m

Наприклад, додавання та множення класів за модулем 5:

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

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

Додавання та множення класів за модулем 6:

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

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



Контрольні питання:

1. Що називають класом лишків за модулем?
2. Які основні властивості класів лишків за модулем?
3. Що називається повною системою лишків?
4. Які операції над класами лишків за модулем існують?

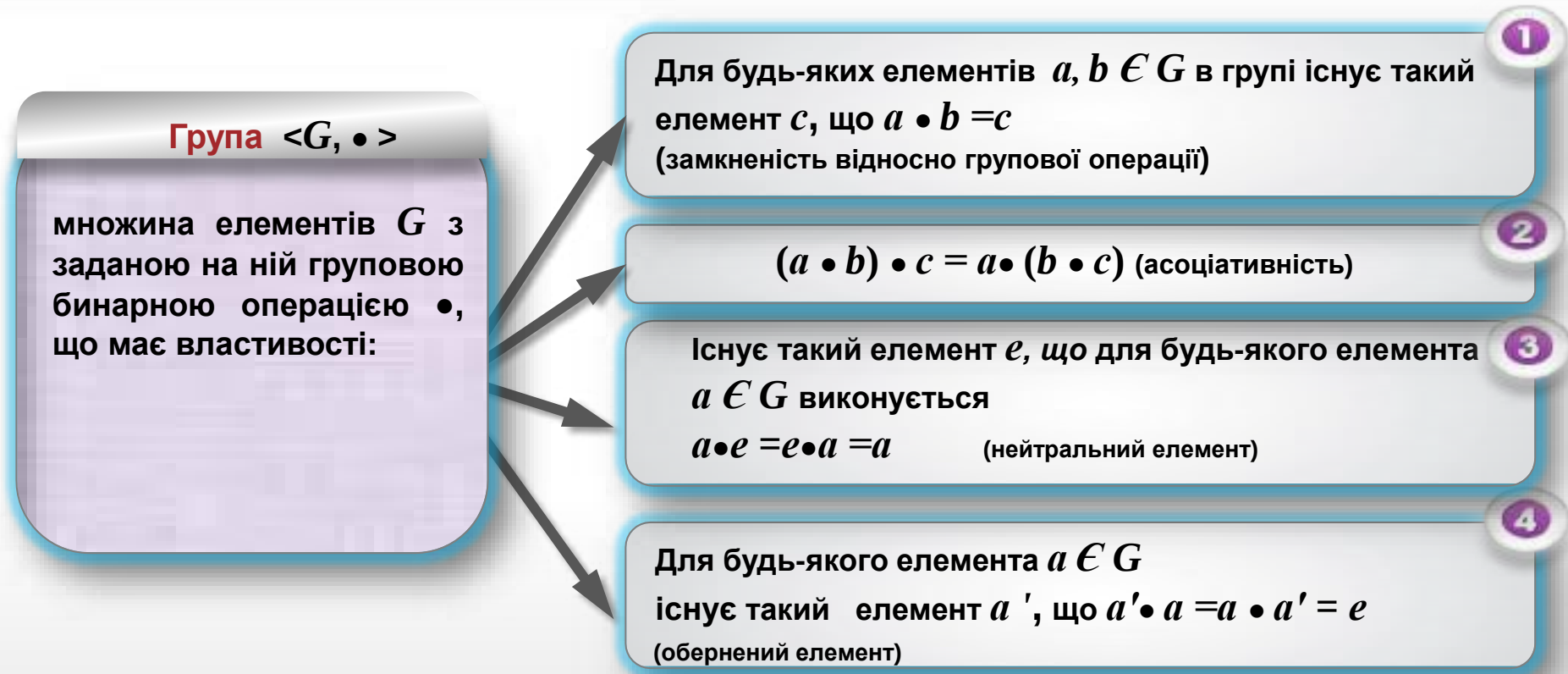


Основи теорії чисел

Тема 6. Алгебраїчні структури. Групи.



ТЕМА 6: Алгебраїчні структури. Групи.



Якщо для всіх елементів $a \bullet b = b \bullet a$, тоді група називається **комутативною**



Порядком групи називають кількість елементів множини G

МУЛЬТИПЛИКАТИВНА ГРУПА

Групова
операція: множення
Нейтральний
елемент: $e = 1$
Обернений
елемент: $a' = a^{-1}$

АДИТИВНА ГРУПА

Групова
операція: додавання
Нейтральний
елемент: $e = 0$
Обернений
елемент: $a' = -a$

Множина Z_m класів лишків
за модулем m є адитивною
комутативною групою
 $\langle Z_m, + \bmod m \rangle$
з груповою операцією
додавання класів:

$$\begin{aligned}\overline{a} + \overline{b} &= \overline{a+b} \\ -\overline{a} &= \overline{m-a}\end{aligned}$$

$$\overline{0} = \{x \equiv 0 \bmod m \mid x \in \mathbb{Z}\}$$

Група називається **скінченною**,
якщо її порядок – скінченне число

Визначення

Елемент a^{-1} кільця Z_m називається оберненим до елементу a по модулю m , якщо

$$a \cdot a^{-1} \equiv 1 \pmod{m}$$

НАПРИКЛАД: $9^{-1} \equiv 2 \pmod{17}$, оскільки $9 \cdot 2 \equiv 1 \pmod{17}$;
 $7^{-1} \equiv 3 \pmod{10}$, оскільки $7 \cdot 3 \equiv 1 \pmod{10}$



Тема 6. Алгебраїчні структури (продовження 6-4)

Алгебраїчні структури: кільця

Кільце $\langle R, +, \cdot \rangle$

множина R елементів заданими на ній бінарними операціями «+» (додавання) та « $\cdot$ » (множення) що мають властивості:

$(a+b)+c=a+(b+c)$ (адитивна асоціативність) 1

$a+b=b+a$ (комутативність за додаванням) 2

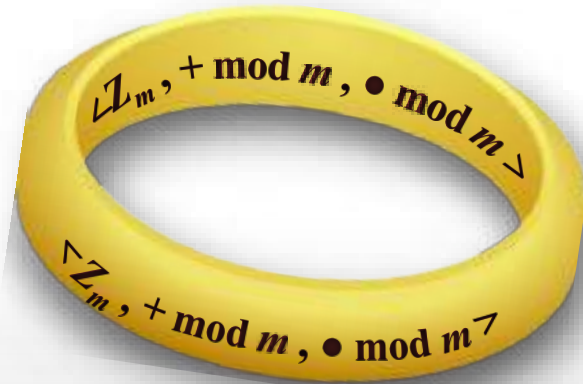
$a+0=0+a=a$ (адитивний нейтральний елемент) 3

$a+(-a)=(-a)+a=0$ (аддитивна інверсія) 4

$a \cdot (b+c) = a \cdot b + a \cdot c, (b+c) \cdot a = b \cdot a + c \cdot a$
(дистрибутивність) 5

$(a \cdot b) \cdot c = a \cdot (b \cdot c)$ (мультиплікативна асоціативність) 6

Кільце називається скінченним, якщо множина R містить скінченну кількість елементів



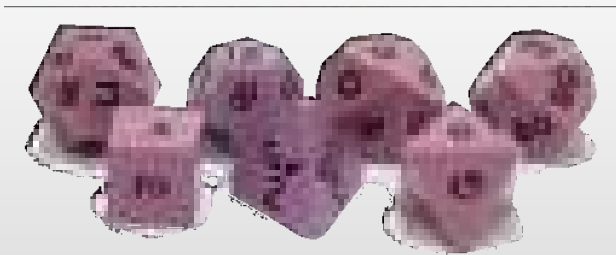
Множина $\mathbb{Z}_m$ класів лишків за модулем m є скінченним кільцем

$$\langle \mathbb{Z}_m, + \bmod m, \cdot \bmod m \rangle$$

відносно операцій додавання та множення класів за модулем



В кільці лишків Z_m обернений елемент по модулю m існує тільки для тих елементів кільця, що взаємно прості з модулем m



Тема 6. Алгебраїчні структури (продовження 6-7)

Алгебраїчні структури: поля

Поле F

множина F елементів з заданими на ній 2 бінарними операціями «+» (додавання) та « $\cdot$ » (множення), що мають властивості:

F – є кільцем

1

$a \cdot b = b \cdot a$ (мультипликативна коммутативність)

2

$a \cdot 1 = 1 \cdot a = a$ (мультипликативний нейтральний елемент)

3

$a + (-a) = (-a) + a = 0$ (адитивна інверсія)

4

Для будь-якого елемента $a \neq 0$
існує обернений елемент a^{-1} , для якого
$$a \cdot a^{-1} = a^{-1} \cdot a = 1$$

5

(мультипликативна інверсія)

Алгебраїчні структури: поля

Множення по модулю 5

x	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



a	1	2	3	4
$a^{-1} \bmod 5$	1	3	2	4

Множина Z_5 класів лишків по модулю 5 – поле (для всіх ненулевих елементів існують обернені)

Множення по модулю 6

x	0	1	2	3	4	5
0	0	0	0	0	0	0
1	0	1	2	3	4	5
2	0	2	4	0	2	4
3	0	3	0	3	0	3
4	0	4	2	0	4	2
5	0	5	4	3	2	1



a	1	2	3	4	5
$a^{-1} \bmod 6$	1	–	–	–	5

Множина Z_6 класів лишків по модулю 6 – не поле (не для всіх ненулевих елементів існують обернені)



Визначення

Множина класів лишків за модулем m , взаємно простих з модулем, утворюють комутативну групу відносно множення, що називається **мультипликативною групою лишків за модулем m** та позначається Z_m^* або $U(Z_m)$

Порядок $|Z_m^*|$ групи Z_m^* дорівнює кількості чисел, менших ніж m та взаємно простих з m .

ПРИКЛАД:

$$Z_9 = \{0,1,2,3,4,5,6,7,8\}, \quad Z_9^* = \{1,2,4,5,7,8\}, \quad |Z_9^*| = 6;$$

$$Z_5 = \{0,1,2,3,4\}, \quad Z_5^* = \{1,2,3,4\}; \quad |Z_5^*| = 4.$$



Теорема

В кільці лишків Z_m обернений елемент за модулем m існує тільки для тих елементів кільця, що взаємно прості з модулем m

ДОВЕДЕННЯ: якщо елемент $a \in Z_m$ та модуль m – взаємно прості числа, тоді $\text{НСД}(a, m) = 1 \implies$ існують такі числа x та y , що $ax + my = 1 \implies ax \equiv 1 \pmod{m} \implies x \equiv a^{-1} \pmod{m}$.

З іншого боку, з умови $a \cdot a^{-1} \equiv 1 \pmod{m}$ витікає, що $a \cdot a^{-1} = qm + 1$ (q – ціле).

Тоді число 1 має ділитися на кожний спільний дільник чисел a та m . Це можливо, тільки якщо $\text{НСД}(a, m) = 1$, тобто числа a і m – взаємно прості.





Контрольні питання:

1. Які основні алгебраїчні структури використовуються в теорії чисел?
2. Яка алгебраїчна структура називається кільцем?
3. Що називається оберненим елементом по модулю?
4. Яка алгебраїчна структура називається полем?



Основи теорії чисел

Тема 7. Функція Ейлера. Теореми Ейлера та Ферма



ТЕМА 7. Функція Ейлера. Теореми Ейлера та Ферма

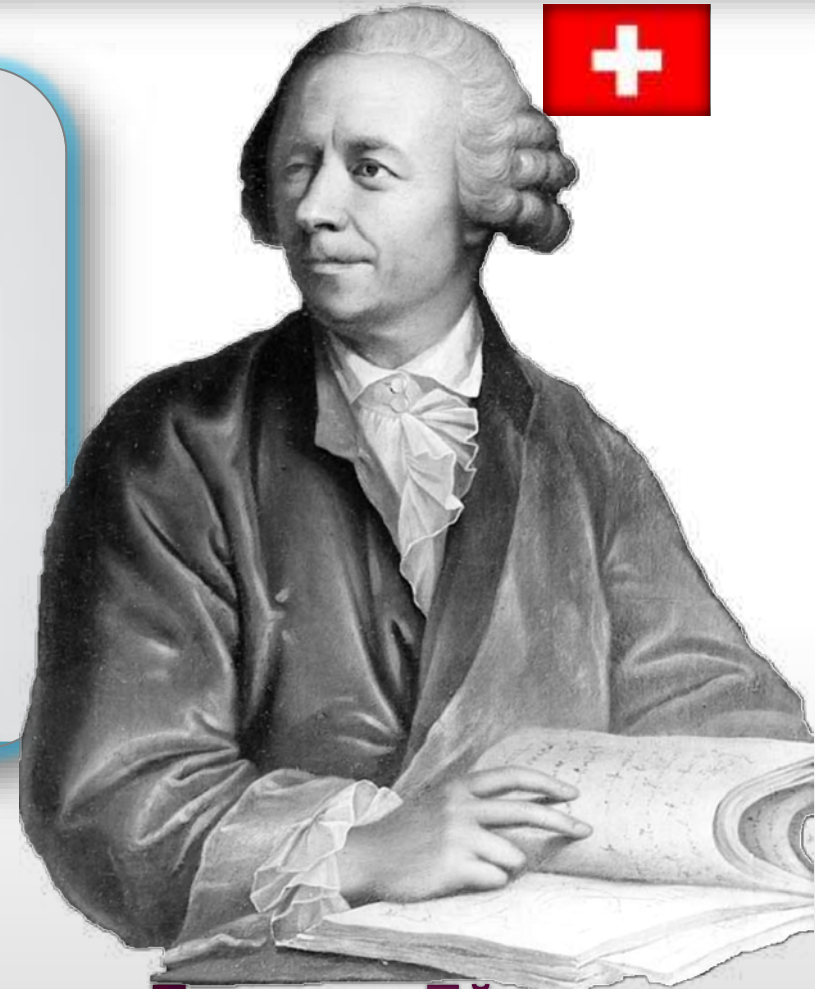
Функція Ейлера $\varphi(n)$, де n – натуральне число, дорівнює кількості натуральних чисел, менших за n та взаємно простих з n .

При цьому вважають, що:

 $\varphi(1) = 1;$

 число 1 – взаємно просте з усіма натуральними числами.

Наприклад: $\varphi(18) = 6$,
оскільки менших та взаємно простих з 18
існує 6 чисел: 1, 5, 7, 11, 13, 17



**Леонард Ейлер
(1707 – 1783)**



Якщо m і n – взаємно прості числа, тоді

$$\varphi(mn) = \varphi(m) \cdot \varphi(n),$$

функція Ейлера мультиплікативна.

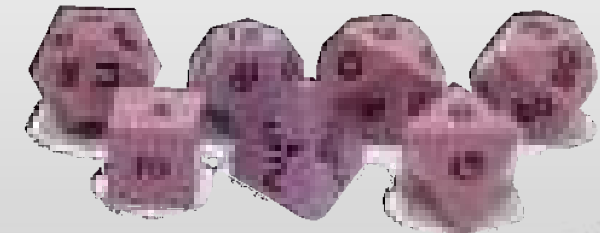


Якщо число p – просте, $n > 0$, то

$$\varphi(p^n) = p^n - p^{(n-1)}$$

Або, якщо число p – просте, тоді

$$\varphi(p) = p - 1$$



3

Якщо $m = p_1^{k_1} p_2^{k_2} \dots p_n^{k_n}$ – канонічне розкладання числа m на прості множники, тоді

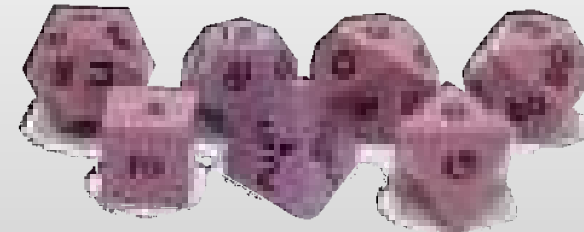
$$\varphi(m) = m \cdot \left(1 - \frac{1}{p_1}\right) \left(1 - \frac{1}{p_2}\right) \dots \left(1 - \frac{1}{p_n}\right)$$

4

Функція Ейлера багатозначна і може приймати тільки парні значення.

5

Порядок $|Z_m^*|$ мультипликативної групи Z_m^* (кількість чисел в приведеній системі лишків) дорівнює $\varphi(m)$.



Тема 7. Функція Ейлера. Теорема Ейлера та Ферма. (продовження 7-4)

Функція Ейлера

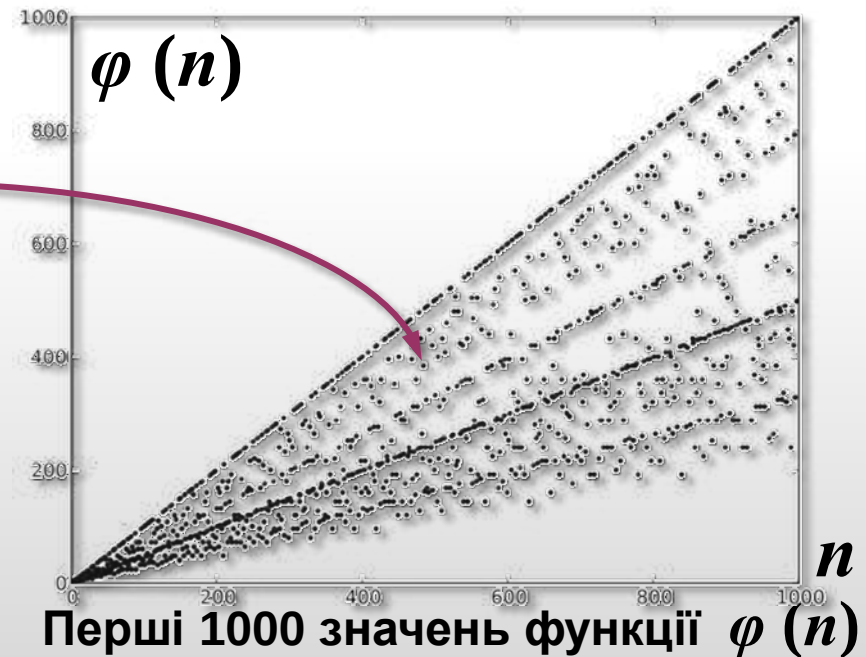
$$\varphi(29) = 29 - 1 = 28;$$

$$\varphi(625) = \varphi(5^4) = 5^4 - 125 = 500;$$

$$\begin{aligned}\varphi(540) &= \varphi(2^2 \cdot 3^3 \cdot 5) = \\ &= 540 \left(1 - \frac{1}{2}\right) \left(1 - \frac{1}{3}\right) \left(1 - \frac{1}{5}\right) = 144.\end{aligned}$$



На прямій $y = n - 1$ лежать значення
 $\varphi(n) = n - 1$, де n – просте



Теорема

Якщо a та m – взаємно прості числа, тоді

$$a^{\varphi(m)} \equiv 1 \pmod{m}$$

ДОВЕДЕННЯ:

нехай $r_1, r_2, \dots, r_{\varphi(m)}$ – приведена система
лишків за модулем m .

Утворимо добутки:

$$ar_1, ar_2, \dots, ar_{\varphi(m)}$$

НСД $(ar_i, m) = 1$ для всіх i

$ar_i \not\equiv ar_j \pmod{m}$ при $i \neq j$



Теорема Ейлера

Кожне з чисел $ar_1, ar_2, \dots, ar_{\varphi(m)}$ може бути порівнянним тільки з одним з чисел $r_1, r_2, \dots, r_{\varphi(m)}$:

$$ar_1 \equiv r_\alpha \pmod{m},$$

$$ar_2 \equiv r_\beta \pmod{m},$$

.....

$$ar_{\varphi(m)} \equiv r_\gamma \pmod{m}$$

де $r_1 r_2 \dots r_{\varphi(m)} = r_\alpha r_\beta \dots r_\gamma$,
оскільки це однакові набори чисел.

перемножимо
почленно



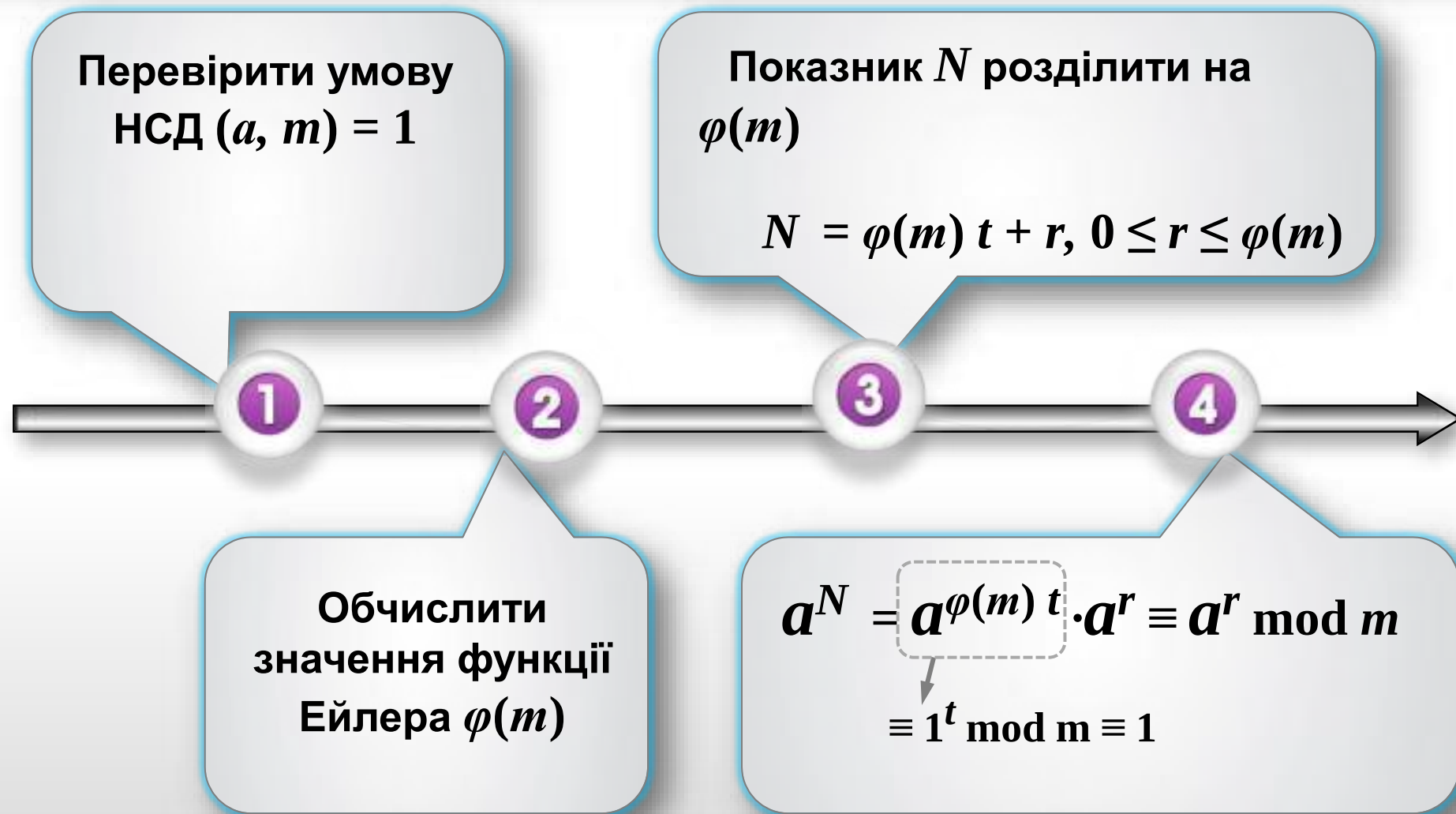
$$ar_1 \cdot ar_2 \cdot \dots \cdot ar_{\varphi(m)} \equiv r_\alpha \cdot r_\beta \cdot \dots \cdot r_\gamma \pmod{m}$$



Після скорочення $a^{\varphi(m)} \equiv 1 \pmod{m}.$



Тема 7. Функція Ейлера. Теорема Ейлера та Ферма. (продовження 7-7) Використання теореми Ейлера для обчислення $a^N \bmod m$



1

Знайти остачу від ділення 243^{132} на 34.

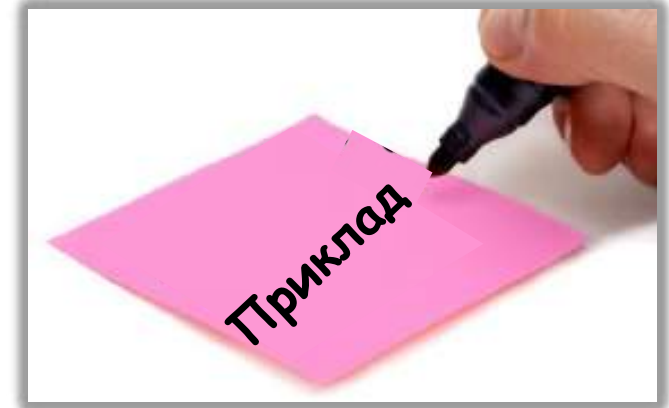
$$243^{132} \pmod{34} \equiv 5^{132} \pmod{34}$$

$$\text{НСД}(5, 34) = 1 \quad \Rightarrow$$

$$\text{По теоремі Ейлера} \quad 5^{\varphi(34)} \equiv 1 \pmod{34}$$

$$\varphi(34) = \varphi(2 \cdot 17) = \varphi(2) \varphi(17) = (2-1)(17-1) = 16 \quad \Rightarrow$$

$$\begin{aligned} 243^{132} \pmod{34} &\equiv 5^{132} \pmod{34} \equiv 5^{16 \cdot 8 + 4} \pmod{34} \equiv \\ &\equiv (5^{16})^8 5^4 \pmod{34} \equiv 1^8 \cdot 625 \pmod{34} \equiv 13 \pmod{34} \end{aligned}$$



Тема 7. Функція Ейлера. Теорема Ейлера та Ферма. (продовження 7-9)

Теорема Ейлера

2

Знайти дві останні цифри числа 1988^{1988} .

Знайти дві останні цифри числа

$$1988^{1988} \equiv x \pmod{100}.$$

$$1988 \pmod{100} \equiv 88 \pmod{100} \equiv -12 \pmod{100}$$

$$x \equiv (-12)^{1988} \equiv 12^{1988} \pmod{100}.$$

$\text{НСД}(12, 100) = 4 \Rightarrow$ теорема Ейлера поки «не працює» !!!

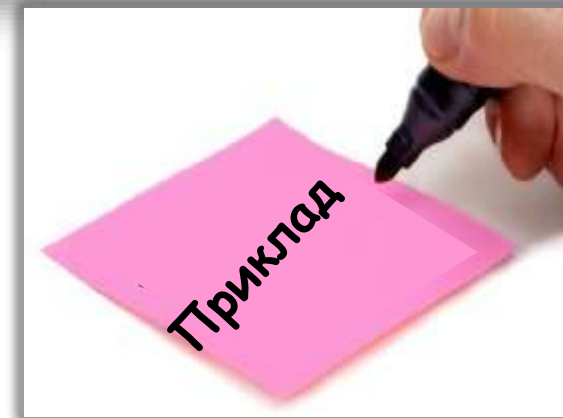
Нехай $x = 4y$. Тоді $4y \equiv 12 \cdot 12^{1987} \pmod{4 \cdot 25}$; $y \equiv 3 \cdot 12^{1987} \pmod{25}$

$\text{НСД}(12, 25) = 1 \Rightarrow$ За теоремою $12^{\varphi(25)} \equiv 1 \pmod{25}$

$$\varphi(25) = \varphi(5^2) = 25 - 5 = 20; \quad 12^{20} \equiv 1 \pmod{25}$$

$$y \equiv 3 \cdot (12^{20})^{99} \cdot 12^7 \equiv 3 \cdot 12^7 \pmod{25} \equiv 24 \pmod{25} \Rightarrow x \equiv 96 \pmod{100}$$

Дві останні цифри числа – 9 та 6.



Мала теорема Ферма

Теорема

Для будь-якого цілого числа a і простого числа p при умові, що a не ділиться на p , справедливо

$$a^{p-1} \equiv 1 \pmod{p}$$

Еквівалентне формулювання

Для простого числа p і цілого a справедливо

$$a^p \equiv a \pmod{p}$$



П'єр Ферма
(1601 – 1665)



Тема 7. Функція Ейлера. Теорема Ейлера та Ферма. (продовження 7-11) «Біномінальна теорема ідіота»

Теорема Ферма – окремий випадок теореми Ейлера для простого модуля (тогда $\varphi(p) = p - 1$)

Наслідок з
теореми
Ферма:

Якщо p – просте число, тоді для цілих чисел a та b виконується порівняння
$$(a + b)^p \equiv a^p + b^p \pmod{p}$$

ДОВЕДЕННЯ:

$$(a + b)^p \equiv a + b \equiv a^p + b^p \pmod{p}.$$

(Idiot's Binominal Theorem)



Тема 7. Функція Ейлера. Теорема Ейлера та Ферма. (продовження 7-12)

Теорема Ферма

1

Довести, що

$$1^{18} + 2^{18} + 3^{18} + 4^{18} + 5^{18} + 6^{18} \equiv -1 \pmod{7}$$

Числа 1, 2, 3, 4, 5, 6 – взаємно прості з числом 7.

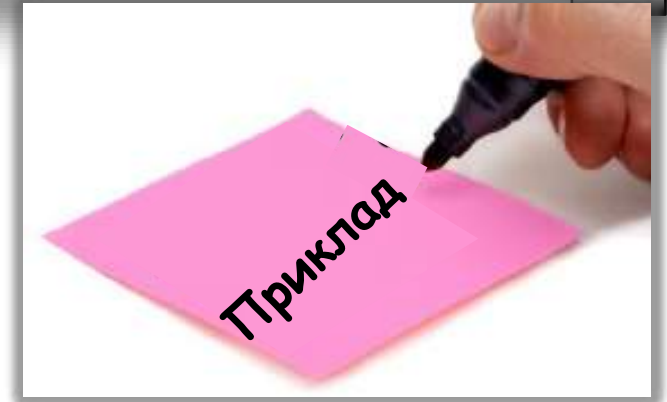
Тоді за теоремою Ферма

$$a^6 \equiv 1 \pmod{7}, \text{ де } a = 1, 2, 3, 4, 5, 6$$



$$a^{18} \equiv 1 \pmod{7}, \text{ де } a = 1, 2, 3, 4, 5, 6$$

$$1^{18} + 2^{18} + 3^{18} + 4^{18} + 5^{18} + 6^{18} \equiv 1+1+1+1+1+1 \equiv 6 \equiv -1 \pmod{7}$$



Теорема Ферма

2

Довести, що $a^{13} \equiv a \pmod{2730}$

$$2730 = 2 \cdot 3 \cdot 5 \cdot 7 \cdot 13 = \text{НСК}(2, 3, 5, 7, 13)$$

Необхідно показати, що $a^{13} \equiv a$ за модулем 2, 3, 5, 7, 13.



За малою теоремою Ферма:

$$a^2 \equiv a \pmod{2} \Rightarrow a^{13} \pmod{2} \equiv (a^2)^6 \cdot a \equiv a^6 \cdot a \equiv a^3 \cdot a \equiv a^2 \equiv a \pmod{2};$$

$$a^3 \equiv a \pmod{3} \Rightarrow a^{13} \pmod{3} \equiv (a^3)^4 \cdot a \equiv a^4 \cdot a \equiv a^3 \cdot a \cdot a \equiv a \pmod{3};$$

$$a^5 \equiv a \pmod{5} \Rightarrow a^{13} \pmod{5} \equiv (a^5)^2 \cdot a^3 \equiv a^2 \cdot a^3 \equiv a \pmod{5};$$

$$a^7 \equiv a \pmod{7} \Rightarrow a^{13} \pmod{7} \equiv a^7 \cdot a^6 \equiv a \cdot a^6 \equiv a \pmod{7};$$

$$a^{13} \equiv a \pmod{13} \Rightarrow a^{13} \equiv a \pmod{2730}$$



Контрольні питання:

1. Яка функція називається функцією Ейлера?
2. Які основні властивості функції Ейлера?
3. Що доводить теорема Ейлера?
4. Як формулюється теорема Ферма?



Основи теорії чисел

Тема 8. Порівняння першого степеня



Порівняння першого ступеня (лінійне порівняння) має вигляд:

$$ax \equiv b \pmod{m}$$

де a, b – цілі задані числа, ступень порівняння співпадає зі ступенем невідомого x .

Якщо число x_0 задовольняє порівнянню (розв'язок або корінь порівняння), тоді увесь клас лишків, представником якого є x_0 також вважається розв'язком порівняння.



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
 $x = x_0 \pmod{m}$

Немає
розв'язків

Існує рівно d розв'язків:
 $x_0, x_0 + \frac{m}{d}, x_0 + 2\frac{m}{d}, \dots, x_0 + (d-1)\frac{m}{d}$,
де x_0 – розв'язок порівняння
 $\frac{a}{d} x = \frac{b}{d} x_0 \pmod{\frac{m}{d}}$

Способи розв'язування порівнянь першого степеня

1

Випробування лишків повної системи за модулем m .

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

2

За допомогою теореми Ейлера $a^{\varphi(m)} \equiv 1 \pmod{m}$, де $\text{НСД}(a;m)=1$

Почленно помножимо обидві частини порівняння на $a^{\varphi(m)-1}$:

$$aa^{\varphi(m)-1}x \equiv ba^{\varphi(m)-1} \pmod{m} \Rightarrow a^{\varphi(m)}x \equiv ba^{\varphi(m)-1} \pmod{m}$$

$$\Rightarrow x \equiv ba^{\varphi(m)-1} \pmod{m}$$

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

Способи розв'язування порівнянь першого степеня

3

Заміна данного порівняння еквівалентними на основі теореми.

Якщо $\text{НСД}(a;m)=1$ і $(b+km):a$, то розв'язком порівняння $x \equiv \frac{b+km}{a} \pmod{m}$.

За цією теоремою порівняння $ax \equiv b \pmod{m}$ послідовно замінюємо еквівалентними порівняннями:

$$ax \equiv b \pm m \pmod{m},$$

$$ax \equiv b \pm 2m \pmod{m},$$

$$ax \equiv b \pm 3m \pmod{m},$$

.....

Поки не дістанемо порівняння, в якому ліву та праву частини можна скоротити на a .
При цьому кількість випробувань буде не більшою за a .

Способи розв'язування порівнянь першого степеня

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} , дістанемо x :



$$a^{-1}ax \equiv a^{-1}b \pmod{m}$$



$$x \equiv a^{-1}b \pmod{m}$$

Порівняння $ax \equiv b \pmod{m}$ являє собою інакше записане алгебраїчне рівняння першого степеня з двома невідомими $ax - b = my$ або $ax - my = b$.

Тому розв'язувати такі рівняння можна як звичайні алгебраїчні порівняння.

Контрольні питання:

1. Яке означення порівняння першого степеня?
2. Що називається розв'язком порівняння?
3. Які умови існування розв'язків порівняння першого степеня?
4. Які існують способи розв'язання порівнянь першого степеня?



Основи теорії чисел

Тема 9. Система порівнянь першого степеня. Китайська теорема про остачі



Тема 9. Система порівнянь першого степеня. Китайська теорема про остачі

Система порівнянь першого степеня

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

$$\left\{ \begin{array}{l} a_1x \equiv b_1(mod m_1), \\ a_2x \equiv b_2(mod m_2), \\ \\ a_nx \equiv b_n(mod m_n), \end{array} \right.$$

Де $HCD(a_1; m_1)=1, HCD(a_2; m_2)=1, \dots, HCD(a_n; m_n)=1, M=HCK(m_1, m_2, \dots, m_n)$.

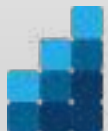
Тема 9. Система порівнянь першого степеня. Китайська теорема про остачі(продовження -9.2)

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

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

$$\left\{ \begin{array}{l} x_1 \equiv c_1(mod\ m_1), \\ x_2 \equiv c_2(mod\ m_2), \\ \\ x_n \equiv c_n(mod\ m_n), \end{array} \right.$$

Якщо хоч одне з порівнянь системи не має розв'язків, то вся система вважається несумісною.



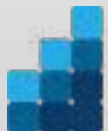
Тема 9. Система порівнянь першого степеня. Китайська теорема про остачі(продовження -9.3)

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

$$\begin{cases} x_1 \equiv c_1 \pmod{m_1}, \\ x_2 \equiv c_2 \pmod{m_2}, \end{cases}$$

вважається сумісною.



Тема 9. Система порівнянь першого степеня. Китайська теорема про остачі(продовження -9.4)

Китайська теорема про остачі

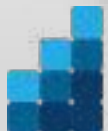
Нехай у системі порівнянь модулі $m_1, m_2, \dots, m_n$ попарні взаємно прості числа, $M = HSK(m_1, m_2, \dots, m_n)$ – найменше спільне кратне модулів, а числа $y_1, y_2, \dots, y_n$ є розв'язками порівнянь

$$\frac{M}{m_1} y_1 \equiv 1(\text{mod } m_1), \quad \frac{M}{m_2} y_2 \equiv 1(\text{mod } m_2), \quad \dots, \quad \frac{M}{m_n} y_n \equiv 1(\text{mod } m_n).$$

Тоді така система порівнянь першого ступеня має єдиний розв'язок

$x \equiv x_0 (\text{mod } M)$, де

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



Тема 9. Система порівнянь першого степеня. Китайська теорема про остачі(продовження -9.4)

Контрольні питання:

1. Як виглядає система порівнянь першого степеня?
2. Що називається розв'язком системи порівнянь першого степеня?
3. При яких умовах система порівнянь сумісна?
4. Як розв'язати систему за допомогою китайської теореми про остачі?





РЕКОМЕНДОВАНА ЛІТЕРАТУРА

1. Клесов, О. І. Елементарна теорія чисел та елементи криптографії [Електронний ресурс] : підручник / О. І. Клесов. – Електронні текстові дані (1 файл: 5,35 Мбайт). – Київ : ТВіМС, 2016. – 412 с. – Режим доступу : <https://ela.kpi.ua/handle/123456789/30046>
2. Требенко Д.Я., Требенко О.О. Алгебра і теорія чисел: У 2 ч. – К.: НПУ імені М.П. Драгоманова, 2006. – Ч.1. – 400 с.; 2-ге вид. переробл. та доповн. 2009. - 420 с. (з Грифом МОНУ) – ISBN 978-966-660-655-9
3. Требенко Д.Я., Требенко О.О. Збірник індивідуальних розрахункових завдань з курсу «Алгебра і теорія чисел»: У 2 ч. – К.: НПУ імені М.П. Драгоманова, 2009. – Ч.1. – 172 с.; 2-ге вид. уточнене, 172 с. (з Грифом МОНУ) – Режим доступу : <http://enpuir.npu.edu.ua/handle/123456789/39448>
4. Требенко Д.Я., Требенко О.О. Алгебра і теорія чисел: У 2 ч. – К.: НПУ імені М.П. Драгоманова, 2018. – Ч.2. – 500 с.– Режим доступу : <http://enpuir.npu.edu.ua/handle/123456789/39449>
5. Number Theory / ed. by D. Chudnovsky, G. Chudnovsky, M. Nathanson. New York, NY : Springer New York, 2004. URL: <https://doi.org/10.1007/978-1-4419-9060-0>
6. Number Theory / ed. by K. Kurşungöz, A. Zeytin. De Gruyter, 2021. URL: <https://doi.org/10.1515/9783110761115>



Навчальне видання

Кагадій Тетяна Станіславівна
Шпорта Анна Григорівна

ОСНОВИ ТЕОРІЇ ЧИСЕЛ
Конспект лекцій
для здобувачів ступеня бакалавра
спеціальності 113 Прикладна математика

Видано в авторській редакції

Електронний ресурс.
Підписано до видання 14.01.2025

Національний технічний університет «Дніпровська політехніка»
49005, м. Дніпро, просп. Д. Яворницького, 19.

