Міністерство освіти і науки України
ДВНЗ "Ужгородський національний університет"
Фізичний факультет
Кафедра твердотільної електроніки та інформаційної безпеки

Ю.М. Мисло, М.М. Пагіря, В.М. Різак

Математичні основи криптографії

Методичний посібник до практичних занять

Ужгород – 2022

УДК 003.26:51
ББК 32.973.26–18.2
М–65

Мисло Ю.М., Пагіря М.М., Різак В.М. Математичні основи криптографії. Методичний посібник до практичних занять. Ужгород, УжНУ, 2022. 77 с.

Методичний посібник розрахований в першу чергу на студентів фізичного факультету Ужгородського національного університету (напрями підготовки "Безпека інформаційних і комунікаційних систем" та "Системи технічного захисту інформації"), а також буде корисним для студентів факультету інформаційних технологій, факультету математики та цифрових технологій, інженерно-технічного факультету.

Рецензенти:

Рубіш Василь Михайлович— доктор фізико–математичних наук, професор, академік Академії технологічних наук України, завідувач Ужгородської лабораторії матеріалів оптоелектроніки та фотоніки Інституту проблем реєстрації інформації НАН України;

Мич Ігор Андрійович — кандидат фізико–математичних наук, доцент, доцент кафедри кібернетики і прикладної математики Ужгородського національного університету.

Перелік умовних позначень

$\circ$	—	бінарна операція
$[\ ]$	—	ціла частина числа
$\blacklozenge$	—	позначка завершення розв'язання
$\sim$	—	еквівалентність
$\emptyset$	—	порожня множина
a^{-1}	—	обернений елемент до a
$a \equiv b \pmod m$	—	порівняння (конгруенція) за модулем m
A_n^m	—	розміщення (без повторення)
$\overline{A_n^m}$	—	розміщення (з повторенням)
$A \cup B$	—	сума (об'єднання) множин
$A \cap B$	—	добуток (переріз) множин
$A \backslash B$	—	різниця множин
C_n^m	—	сполучення (без повторення),
$\overline{C_n^m}$	—	сполучення (з повторення),
$C_n(n_1, \ldots, n_k)$	—	перестановки (з повторенням)
$\mathbb{C}$	—	множина комплексних чисел
$f_n(x)$	—	многочлен степеня n
$\ker f$	—	ядро гомоморфізму
$\bar{k}$	—	клас лишків за модулем
$\mathbb{N}$	—	множина натуральних чисел
P_n	—	перестановки (без повторення)
$p^{\#}$	—	прайморіал числа
$\mathbb{Q}$	—	множина раціональних чисел
$\mathbb{R}$	—	множина дійсних чисел
$\mathbb{R}^+$	—	множина додатних дійсних чисел
$(x; y)$	—	впорядкована пара
$X \times Y$	—	декартів добуток множин
$\mathbb{Z}$	—	множина цілих чисел
$\mathbb{Z} \backslash m\mathbb{Z}$	—	множина класів лишків за модулем m
НСД	—	найбільший спільний дільник
НСК	—	найменше спільне кратне

Вступ

Захист інформації актуальний з давніх часів. Людство завжди мало і має потребу оберігати свої потаємні знання, навички, технології, дані від сторонніх очей. Інформація перетворилася у високо-цінний товар, стратегічний ресурс. Спотворення інформації чи її викривлення може призвести до серйозних наслідків.

Сучасні способи захисту особливо цінної інформації ґрунтуються як на технічних засобах, так і методах одного із підрозділів прикладної математики — криптології. Термін криптологія походить від двох давньогрецьких слів $\kappa\rho\upsilon\pi\tau\acute{o}\varsigma$ — прихований, скритний і $\lambda\acute{o}\gamma o\varsigma$ — слово. Наука криптологія, яка традиційно ділиться на криптографію та криптоаналіз, бере свої початки в багатьох фундаментальних математичних теоріях і ввібрала в себе велику кількість термінів, теорем, тверджень, на яких спираються криптографічні схеми та алгоритми. Криптологічні методи розвиваються разом із досягненнями в сучасних математичних теоріях. Інші шляхи удосконалення та розвитку методів шифрування, дешифрування та криптоаналізу пов'язанні із розширенням можливостей комп'ютерів.

В рамках підготовки фахівців із напрямів підготовки "Безпека інформаційних і комунікаційних систем" та "Системи технічного захисту інформації" на фізичному факультеті Ужгородського національного університету читається ряд курсів із криптології. Цей методичний посібник має на меті доповнити відомі джерела [1, 2, 3, 4, 5, 6, 7, 8], на яких ґрунтуються курси "Прикладна криптографія" та "Криптографічні перетворення". Основна увага зосереджена на розв'язанні типових прикладів.

Посібник містить наступні основні розділи "Теорія множин", "Комбінаторика", "Алгебра","Теорія чисел","Многочлени".

Перед "Вступом" наведено "Перелік умовних позначень", які використовуються в методичному посібнику. Перший розділ розглянуто основні поняття з теорії множин, операції над множинами та відображення множин. Другий розділ містить основні поняття з комбінаторики. Елементи

вищої алгебри викладено в третьому розділі. Тут зокрема розглянуто перестановки, підстановки, бінарні алгебричні операції, групи, гомоморфізм та ізоморфізм груп. Теорії чисел присвячений четвертий розділ. Подільність цілих чисел, алгоритм Евкліда, елементи правильних ланцюгових дробів, прості числа, основна теорема арифметики та її наслідки, елементи теорії лишків за модулем розглянуто в цьому розділі. Відомості про многочлени однієї змінної над деяким полем наведено в п'ятому розділі. Розглянуто арифметичні дії над многочленами та деякі методи відшукання найбільшого спільного дільника двох многочленів. В кінці методичного посібника вміщено предметний покажчик основних термінів.

Всі підрозділи мають схожу структуру. Спочатку наведені необхідні теоретичні відомості, далі розглянуто розв'язки типових задач. Закінчення розв'язків прикладів позначено значком "♦". Після розгляду прикладу запропоновано аналогічні задачі для самостійного розв'язання.

Розділ 1

Теорія множин

1.1 Поняття множини

Поняття **множини** належить до первинних понять сучасної математики, тобто найпростіших, які не можна визначити через поняття ще більш прості. Поряд із такими первинними поняттями, як **точка, пряма, площина, поверхня, тіло тощо**, які добре відомі із курсу шкільної геометрії, поняття **множини** не означають.

Засновник теорії множин німецький математик Георг Кантор стверджував, що **множина — це багато дечого, мислимого нами як єдине**. Можна уявляти собі множину як сукупність (сім'ю, набір, зібрання) деяких об'єктів, що мають спільну властивість.

Приклад 1.1. *Множина студентів 3–го курсу фізичного факультету УжНУ напрямку підготовки "Безпека інформаційних та комунікаційних систем".*

Ця множина складається із усіх студентів УжНУ, а лише з тих, які навчаються на 3–му курсі вказаного напрямку.

Приклад 1.2. *Множина літер української абетки, що використовуються при записі речення —* ***Криптографія древня наука****.*

Приклад 1.3. *Множина коренів квадратного рівняння*

$$ax^2 + bx + c = 0.$$

Числа, які складають дану множину, мають бути коренями квадратного рівняння.

Множини складаються із окремих об'єктів, які називаються **елементами множини**. Множини, як правило, позначають великими латинськими буквами A, B, C, а елементи множин — малими латинськими буквами

a, b, c, або малими буквами із індексами $a_1, a_2, \ldots$. Щоб вказати належність елемента a до множини A будемо писати $a \in A$. А щоб вказати, що елемент b не належить множині C будемо записувати $b \notin C$.

Означення 1.1. *Множина, елементи якої є множини, називається* ***класом (сімейством)****.*

Означення 1.2. *Якщо елементи всіх множин вибирають з якоїсь однієї, досить широкої множини U, то таку множину називається* ***універсальною****.*

Множину можна задати трьома способами:

1. **Переліченням елементів**, які входять до множини. Так можна задавати ті множини, які містять скінчену кількість елементів. Наприклад: $A = \{a_1; a_2; \ldots; a_n\}$.

2. **Характеристичним предикатом**, тобто за допомогою деякого логічного твердження. Наприклад: $B = \{b \in \mathbb{R} \,|\, 2 < b < 5\}$ — множина всіх дійсних чисел, що знаходять між числами 2 і 5.

3. **Рекурсивною процедурою**, тобто формулою, за допомогою якої послідовно отримують даний елемент множини через попередні елементи. Наприклад: послідовність чисел Фібоначчі:

$$C = \{c \in \mathbb{N} \,|\, c_1 = 1, c_2 = 1, c_k = c_{k-1} + c_{k-2}, k = 3, 4, 5, \ldots\} =$$

$$= \{1, 1, 2, 3, 5, 8, 13, 21, 34, 55, 89, 144, 233, \ldots\}.$$

Множина, яка не містить жодного елемента, називається**порожньою** і позначається символом $\varnothing$.

Приклад 1.4. *Множина коренів квадратного рівняння $x^2 + 1 = 0$ буде порожньою множиною $A = \{x \,|\, x^2 + 1 = 0\} = \varnothing$.*

Приклади множин, які будуть зустрічатися в курсі криптографії.

Приклад 1.5. *Множина натуральних чисел*

$$\mathbb{N} = \{1, 2, 3, \ldots, n, \ldots\} \ .$$

Приклад 1.6. *Множина невід'ємних цілих чисел*

$$\mathbb{Z}_0 = \{0, 1, 2, 3, \ldots, n, \ldots\}.$$

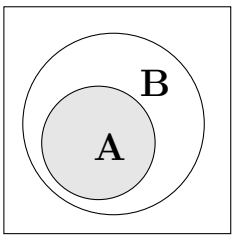
Приклад 1.7. *Множина цілих чисел*

$$\mathbb{Z} = \{0, \pm 1, \pm 2, \pm 3, \dots, \} \ .$$

Приклад 1.8. *Множина літер української абетки*
$\boldsymbol{A}$=*{а,б,в,г,ґ,д,е,є,ж,з,и,і,ї,й,к,л,м,н,о,п,р,с,т,у,ф,х,ц,ч,ш,щ,ь,ю,я}.*

Приклад 1.9. *Множина літер латинської абетки*
$\boldsymbol{A}$=*{a,b,c,d,e,f,g,h,i,j,k,l,m,n,o,p,q,r,s,t,u,v,w,x,y,z}.*

Означення 1.3. *Множина A називається* ***підмножиною*** *множини B, що записується так $A \subset B$ або так $B \supset A$, якщо кожний елемент множини A також є елементом множини B.*



Числові множини, які розглянуті вище, задовольняють наступну послідовність включень $\mathbb{N} \subset \mathbb{Z}_0 \subset \mathbb{Z}$.

Означення 1.4. *Множини A і B називаються* ***рівними****, якщо $A \subset B$ і $B \subset A$.*

Означення 1.5. *Кажуть, що між множинами A і B встановлено взаємно–однозначна відповідність , якщо*

1. *кожному елементу $a \in A$ поставлено у відповідність* ***один і тільки один*** *елемент $b \in B$, тобто $a \in A \to b \in B$;*
2. *різним елементам $a \in A$ відповідають різні елементи $b \in B$;*
3. *кожен елемент $b \in B$ відповідає лише одному елементу $a \in A$.*

Означення 1.6. *Множини A і B, між якими встановлена взаємно–однозначна відповідність називаються* ***еквівалентними*** *і позначають так: $A \sim B$.*

Нехай множина $A \sim \{1, 2, \dots, n\}$. Тоді кажуть, що множина A має **потужність** n (записують $|A|$.) Потужність $|\varnothing| = 0$. Якщо $|A| = |B|$, то множини **рівнопотужні**.

Потужність множини це її **кардинальне (головне)** число. Потужність це така властивість множини, яка притаманна всім еквівалентним, а отже рівнопотужним множинам.

Множина всіх підмножин множини A називається **булеаном** і позначається 2^A. Для скінчених множин потужність булеана рівна $|2^A| = 2^{|A|}$.

Приклад 1.10. *З'ясувати, чи належить літера* ***"ю"*** *до множини літер повідомлення* ***"гарний текст"****.*

Розв'язання. Множина **A={а,г,е,и,й,к,н,р,с,т}** є множиною літер повідомлення **"гарний текст"**. Множина не містить літери **"ю"**.

♦

Приклад 1.11. *Чи буде множина літер повідомлення* ***секрет*** *підмножиною множини літер шифровки* ***еаиаокгрестшi****.*

Розв'язання. Повідомлення **секрет** записано за допомогою множини літер **A={е,к,р,с,т}**. Шифровка **еаиаокгрестшi** записана за допомогою літер **B={а,г,е,и,і,к,о,р,с,т,ш}**. Легко бачити, що літери множини **A** також належать до множини **B**. Тоді $\mathbf{A} \subset \mathbf{B}$.

♦

Приклад 1.12. *Записати булеан множини літер шифровки* ***уосоус****.*

Розв'язання. Множина літер шифровки **A={о,с,у}**. Потужність множини $|A| = 3$. Тоді булеан 2^A буде мати потужність $2^{|A|} = 8$ і складається із таких множин 2^A={ {$\varnothing$}, {о}, {с}, {у}, {о,с}, {о,у}, {с,у}, {о,с,у} }.

♦

Вправа 1.1. З'ясувати, чи належить літера **"ь"** множині літер виразу **"знову снігова заметіль"**.

Вправа 1.2. Маємо шифрограму **"сіцноправувашлоерта"**. Чи множина літер слова **"орел"** буде підмножиною літер шифрограми.

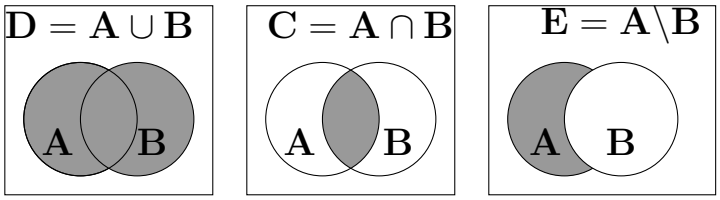
Вправа 1.3. Отримали шифровку "павуувапу". Записати булеан множини літер шифровки.

1.2 Операції над множинами

Над множинами можна виконувати операції.

Означення 1.7. *Будемо називати* ***сумою (об'єднанням)*** *множин A та B множину $D = A \cup B$, якщо вона містить всі елементи обох множин.*

Означення 1.8. *Будемо називати* ***добутком (перерізом)*** *множин A та B множину $C = A \cap B$, елементами якої є тільки ті елементи, які одночасно належать і множині A, і множині B.*



Означення 1.9. *Будемо називати* ***різницею*** *множин A та B множину $E = A\backslash B$, якщо вона містить ті елементи множини A, які не належать множині B.*

Зауваження 1.1. Операції перетину та об'єднання множин можна узагальнити на більшу кількість множин, тобто $\bigcup\limits_{i=1}^{n} A_i = A_1 \cup A_2 \cup \cdots \cup A_n$ — об'єднання n множин, $\bigcap\limits_{i=1}^{n} A_i = A_1 \cap A_2 \cap \cdots \cap A_n$ — переріз n множин.

Приклад 1.13. *Нехай множини A, B визначені наступним чином*

$$A = \{-2, -1, 0, 1, 2, 3, 4\}, \qquad B = \{-3, -1, 1, 3, 5\}.$$

Знайти множини $C = A \cup B, D = A \cap B, E = A\backslash B, F = B\backslash A$.

Розв'язання. Знаходимо:

$$C = A \cup B = \{-3, -2, -1, 0, 1, 2, 3, 4, 5\}, \quad D = A \cap B = \{-1, 1, 3\},$$

$$E = A\backslash B = \{-2, 0, 2, 4\}, \quad F = B\backslash A = \{-3, 5\}.$$

♦

Вправа 1.4. Нехай **A** — множина літер повідомлення **"дрібна дислокація"**, а **B** — множина літер повідомлення **"велика частина"**. Знайти суму, різниці та добуток цих множин.

Вправа 1.5. Отримали три радіограми:

1. ґрунтову дорогу заміновано;

2. річка броду не має;

3. болотом проходить стежка.

Утворити множину літер кожного повідомлення. Знайти суму та добуток трьох знайдених множин.

1.3 Впорядковані пари

Означення 1.10. *Нехай $x \in X$ і $y \in Y$. Пару елементів x та y, яка записана у вигляді $(x; y)$ називають* ***упорядкованої парою*** *(елемент x — перша компонента пари, y — друга компонента пари).*

Означення 1.11. *Впорядковані пари $(x_1; y_1)$ і $(x_2; y_2)$ рівні тоді і тільки тоді, коли $x_1 = x_2$ і $y_1 = y_2$.*

Означення 1.12. *Множина, усі елементи якої є впорядковані пари, називається* ***прямим (декартовим) добутком множин****:*

$$X \times Y = \{(x; y) \mid x \in X, y \in Y\} \ .$$

Потужність прямого добутку $|X \times Y| = |X| \cdot |Y|$.

Зауваження 1.2. Очевидно, що $X \times Y = Y \times X$ тільки тоді, коли $X = Y$.

Зауваження 1.3. Аналогічно, набір із n елементів $(x_1, x_2, \ldots, x_n)$ називаються **кортежем**. Прямий (декартів) добуток n множин $X_1 \times X_2 \times \cdots \times X_n$.

Означення 1.13. *Прямий (декартів) добуток множини X саму на себе n разів називається* ***n–м степенем множини X****:*

$$X^n = \underbrace{X \times X \times \cdots \times X}_{n \textbf{ разів}} \ .$$

Означення 1.14. ***Відображенням множини X у множину Y*** *називається правило, за яким кожному елементу $x \in X$ ставиться у відповідність один елемент $y \in Y$.*

Відображення позначають $f : X \to Y$. Відображення можна також трактувати, як операцію, яка переводить елемент x, належить множині X в деякий елемент $y \in Y$, який називають **образом елемента** x при відображені та позначають $f(x)$, X — **область визначення відображення**.

Означення 1.15. *Образом підмножини* $X_1 \subset X$ *при відображені* f *називається об'єднання образів всіх елементів* $x \in X_1$. *Образ підмножини позначаємо* $f(X_1)$.

Якщо $y \in Y$ фіксоване, то його **повним прообразом** при відображенні f називається множина всіх елементів із X, для яких y є образом при цьому відображенні. Повний прообраз позначають $f^{-1}(y)$. Довільний елемент із $f^{-1}(y)$ називають **прообразом елемента** y.

Нехай $X = (x_1, x_2, \ldots, x_n)$ деяка скінчена множина, тоді відображення $f : X \to Y$ можна записати у вигляді дворяду

$$f = \begin{pmatrix} x_1 & x_2 & x_3 & \cdots & x_n \\ f(x_1) & f(x_2) & f(x_3) & \cdots & f(x_n) \end{pmatrix}.$$

Означення 1.16. *Якщо* $f : X \to Y$ *— однозначне відображення, то відображення* $f^{-1} : Y \to X$, *яке ставить у відповідність кожному елементу* $y \in Y$ *його прообраз* $f^{-1}(y) \in X$, *називається* ***оберненим*** *для відображення* f.

Нехай визначені два відображення $f : X \to Y$ і $g : Y \to Z$. Якщо поставити у відповідність кожному елементу $x \in X$ елемент $g(f(x)) \in Z$, то відображення множини X у множину Z називається **добутком (композицією)** відображень f і g та позначається gf.

Приклад 1.14. *Задані множини* $X = \{a, b\}, Y = \{e, h, g\}$. *Знайти декартові добутки множин* $X \times Y$, $Y \times X$ *та степені множин* X^3, Y^2.

Розв'язання. Згідно із означенням

$$X \times Y = \{(a, e), (a, h), (a, g), (b, e), (b, h), (b, g)\},$$

$$Y \times X = \{(e, a), (e, b), (h, a), (h, b), (g, a), (g, b)\},$$

$$X^3 = X \times X \times X = \{(a, a, a), (a, a, b), (a, b, a), (a, b, b), (b, a, a), (b, a, b), (b, b, a), (b, b, b)\}$$

$$Y^2 = Y \times Y = \{(e, e), (e, h), (e, g), (h, e), (h, h), (h, g), (g, a), (g, h), (g, g)\}.$$

♦

Приклад 1.15. *Відображення* $f : X \to Y$ *кожному елементу множини* $X = \{2, 3, 5, 6\}$ *ставить у відповідність найменше спільне кратне цього числа і числа* 4. *Записати вказане відображення у вигляді дворяду.*

Розв'язання. Оскільки $f(2) = 4, f(3) = 12, f(5) = 20, f(6) = 12$, то отримаємо

$$f = \begin{pmatrix} 2 & 3 & 5 & 6 \\ 4 & 12 & 20 & 12 \end{pmatrix}.$$

♦

Приклад 1.16. *Нехай відображення f, g, які діють із $\mathbb{R}$ в $\mathbb{R}$, визначені співвідношеннями $f(x) = x^3, g(x) = \ln(x^2 + 1)$. Знайти відображення fg, gf, f^3, g^2, f^{-1}.*

Розв'язання. Знаходимо

$$fg = f(g(x)) = (\ln(x^2 + 1))^3 = \ln^3(x^2 + 1),$$

$$gf = g(f(x)) = \ln((x^3)^2 + 1) = \ln(x^6 + 1),$$

$$f^3 = f(f(f(x))) = ((x^3)^3)^3 = x^{27},$$

$$g^2 = g(g(x)) = \ln((\ln(x^2 + 1))^2 + 1) = \ln(\ln^2(x^2 + 1) + 1).$$

$$f^{-1}(x) = \sqrt[3]{x}.$$

♦

Вправа 1.6. Для множин $X = \{S, T\}, Y = \{b, c, d\}$, $Z = \{1, 2, 3, 4\}$, знайти декартові добутки множин $X \times Y$, $X \times Z, Z \times Y$ та степені множин X^4, Y^3, Z^2.

Вправа 1.7. Відображення $f : X \to Y$ елементу множини **X**={а,в,ґ,і,к} ставить у відповідність порядковий номер літери в українській абетці. Записати вказане відображення у вигляді дворяду.

Вправа 1.8. Знайти відображення fg, gf, f^2, g^3, g^{-1}, якщо $f(x) = \sin x^2$, $g(x) = e^x$.

Розділ 2

Комбінаторика

2.1 Комбінаторні схеми

Означення 2.1 (**Правило суми.**). *Якщо A і B — скінчені множини, які не перетинаються, тобто $A \cap B = \varnothing$ і крім того $|A| = n, |B| = m$, тоді $|A \cup B| = n + m$.*

Означення 2.2 (**Правило прямого добутку.**). *Нехай A і B — скінчені множини, $|A| = n, |B| = m$. Тоді $|A \times B| = n \cdot m$.*

Зауваження 2.1. Нехай множини $X_1, X_2, X_3, \ldots, X_k$, мають потужності $|X_i| = n_i$, $i = 1, 2, 3, \ldots, k$, тоді виконуються рівності

$$\Big|X_1 \times X_2 \times X_3 \times \cdots \times X_k\Big| = n_1 \cdot n_2 \cdot n_3 \cdot \ldots \cdot n_k = \prod_{i=1}^{k} n_i,$$

$$\Big|\bigcup_{i=1}^{k} X_i\Big| = n_1 + n_2 + n_3 + \cdots + n_k = \sum_{i=1}^{k} n_i, \quad X_i \cap X_j = \varnothing.$$

Приклад 2.1. *Скільки тризначних парних чисел можна утворити із наступних цифр $\{0; 1; 2; 3; 4; 5; 6\}$, якщо цифри повторюються?*

Розв'язання. Утворенні числа мають містити три цифри

$$A_1 A_2 A_3.$$

У першому, найстаршому, розряді A_1 можуть бути всі цифри крім 0. Отже, потужність $|A_1| = 6$.

В якості другої цифри можна взяти довільну цифру, $|A_2| = 7$.

Оскільки число має бути парним, то в молодшому розряді має бути одна із цифр $A_3 = \{0; 2; 4; 6\}$, $|A_3| = 4$.

Згідно із **правилом прямого добутку, основного правила комбінаторики**, кількість тризначних непарних чисел N

$$N = |A_1 \times A_2 \times A_3| = |A_1| \cdot |A_2| \cdot |A_3| = 6 \cdot 7 \cdot 4 = 168$$

Вправа 2.1. Шифр сейфу містить 4 значки і складається із малих літер {a;b;c;d;e;f;h} та цифр {2;3;4;5;6}, що повторюються. Перший значок не може бути цифра, а останній — літера. Скільки різних шифрів можна утворити?

Нехай X — скінчена, $|X| = n$. Вибираємо m елементів. Утворюються деякі підмножини із X, які називають **комбінаціями із n по m.**

Залежно від того, чи враховується **черговість** елементів, чи **входять всі елементи** чи тільки **частина**, розрізняють:

- розміщення із n елементів по m без повторення;
- перестановки із n елементів;
- сполучення із n елементів по m без повторення;
- розміщення із n по m з повторенням;
- перестановки із n елементів з повторенням;
- сполучення із n елементів по m з повторенням.

2.2 Розміщення із n елементів по m без повторення

Означення 2.3. *Комбінації, кожна з яких містить m елементів, які вибрані із n різних елементів, $m \leqslant n$, і які відрізняються одна від одної або складом елементів або їх порядком, називаються* ***розміщення із n елементів по m (без повторення)***.

Кількість розміщень без повторень обчислюється за формулою

$$A_n^m = \underbrace{n(n-1) \cdot (n-2) \cdots (n-m+1)}_{m\text{–співмножників}} = \frac{n!}{(n-m)!}, \qquad (2.1)$$ MPR1

де $n! = 1 \cdot 2 \cdot \ldots \cdot n$.

Приклад 2.2. *Скільки семизначних чисел можна утворити (скласти) із цифр {1;2;3;4;5;6;7;8;9}, щоб жодна із цифр не повторювалася?*

Розв'язання. Цифри не мають повторюватися. Водночас, порядок входження цифр в число важливе. Маємо задачу на розміщення із 9 елементів (цифр) по 7. Скористаємося формулою (2.1). Тоді, кількість семизначних чисел N буде рівна

$$N = A_9^7 = 9 \cdot 8 \cdot 7 \cdot 6 \cdot 5 \cdot 4 \cdot 3 = 181440.$$

♦

Вправа 2.2. Задано множину літер {б,в,г,ґ,к,л,м,н,с,т,х,ц}. Шифр сховища містить різних 6 літер із вказаної множини. Скільки існує різних шифрів?

2.3 Перестановки із n елементів

Означення 2.4. *Комбінації, кожна з яких містить усі n елементів із n можливих елементів, які взяті у певному порядку, називаються* ***перестановкою із n елементів****.*

Так як перестановка є розміщенням без повторення із n елементів по n, то кількість перестановок

$$P_n = A_n^n = n \cdot (n-1) \cdot \ldots \cdot 2 \cdot 1 = n!. \qquad (2.2)$$ MPR2

Надалі будемо вважати, що $0! = 1$.

Приклад 2.3. *Скільки шестизначних парних чисел можна утворити із цифр $\{1; 2; 3; 5; 7; 9\}$, якщо цифри в числі не повторюються?*

Розв'язання. Утворені числа мають бути парними. Отже, всі вони в молодшому розряді мусять містити цифру 2. Решта 5 цифр можуть в довільній послідовності без повторень займати 5 старших розрядів числа. Тоді згідно із формулою (2.2) маємо

$$N = A_5^5 = 5! = 120.$$

♦

Приклад 2.4. *У підгрупі 7 студентів. Староста складає графік чергування по одному студенту на день. Скільки існує різних варіантів графіку чергування?*

Розв'язання. Кожен студент потрапляє у графік чергування один раз. Порядок чергування суттєвий. Маємо розміщення із 7 елементів по 7, тобто кількість перестановок із 7 елементів. За формулою (2.2) знаходимо

$$N = A_7^7 = 7! = 5040.$$

♦

Вправа 2.3. Диск сейфу містить цифри $\{0, 1, 2, 3, 4, 5, 6, 7, 8, 9\}$. Скільки існує 10–ти значних шифрів, якщо кожна цифра набирається лише один раз?

2.4 Сполучення із n елементів по m без повторення

Означення 2.5. *Комбінації, кожна з яких містить m елементів із можливих n різних елементів, $m \leqslant n$, які відрізняються одна від одної принаймні одним елементом називаються* ***сполученнями із n елементів по m без повторення***.

Зауваження 2.2. На відміну від розміщень, елементи у сполученнях не впорядковані.

Кількість сполучень визначається формулою

$$C_n^m = \frac{n \cdot (n-1) \cdot \cdots \cdot (n-m+1)}{m!} = \frac{n!}{(n-m)!\, m!}. \qquad (2.3)$$ MPR3

Взаємозв'язок між розміщеннями та сполученнями без повторення задається співвідношенням

$$A_n^m = m! \cdot C_n^m$$

Числа C_n^m також називаються **біноміальними коефіцієнтами**, оскільки для довільного n має місце формула для бінома Ньютона

$$(a+b)^n = C_n^0 a^n b^0 + C_n^1 a^{n-1} b^1 + \cdots + C_n^n a^0 b^n.$$

Комбінації або біноміальні коефіцієнти володіють такими властивостями:

$$1.\ C_n^m = C_n^{n-m}; \quad 2.\ C_n^0 = C_n^n = 1;\ C_n^1 = n, \quad 3.\ C_n^0 + C_n^1 + \cdots + C_n^{n-1} + C_n^n = 2^n.$$

$$4.\ C_n^m = C_{n-1}^m + C_{n-1}^{m-1}, \qquad n > 1,\ 0 < m < n.$$

Властивості біноміальних коефіцієнтів можна проілюструвати за допомогою **трикутника Паскаля**

$n=0$						1					
$n=1$					1		1				
$n=2$				1		2		1			
$n=3$			1		3		3		1		
$n=4$		1		4		6		4		1	
$n=5$	1		5		10		10		5		1
$n=6$	1	6		15		20		15		6	1
	⋮		⋮		⋮		⋮		⋮		⋮

Приклад 2.5. *Скільки добутків можна утворити із чисел* $a, b, c, d, e \in \mathbb{R}$*, якщо кожний добуток містить три різні множники?*

Розв'язання. Із середньої школи відомо, що у множині дійсних чисел $\mathbb{R}$ операція множення комутативна, тобто $ab = ba$. Тоді, порядок входження чисел у добуток не є важливим. Маємо сполуки із 5 елементів по 3. Згідно із формулою (2.3) маємо

$$K = C_5^3 = \frac{5 \cdot 4 \cdot 3}{6} = 10.$$

♦

Приклад 2.6. *Скільки існує дільників числа* 210*?*

Розв'язання.

Розкладемо число 210 на прості множники: $210 = 2 \cdot 3 \cdot 5 \cdot 7$. Дільниками будуть числа $1, 2, 3, 5, 7, 210$, тобто 6 чисел. Дільниками будуть добутки двох довільних простих дільників — $2, 3, 5, 7$

$$C_4^2 = 6, \qquad \text{числа} \qquad 6, 10, 14, 15, 21, 35.$$

Дільниками також будуть добутки трьох простих дільників

$$C_4^3 = 4, \qquad \text{числа} \qquad 30, 42, 70, 105.$$

Число 210 має $6 + 6 + 4 = 16$ дільників.

♦

Вправа 2.4. У підгрупі 7 студентів. Староста складає графік чергування по два студенти. Скільки різних варіантів графіку чергування по два студенти можна сформувати?

Вправа 2.5. У волейбольній команді "Буревісник–УжНУ" нараховується 18 спортсменів. Скільки існує можливостей сформувати стартову шістку?

2.5 Розміщення з повтореннями

Означення 2.6. *Розміщеннями із n елементів по m з повтореннями називаються такі розміщення із n елементів, у кожне з яких входять всі m елементів, причому кожен елемент може повторюватися.*

Число таких розміщень

$$\overline{A_n^m} = n^m. \tag{2.4}$$ MPR4

Приклад 2.7. *Визначити кількість семизначних чисел, які утворені із чисел {3, 4, 5, 6}, якщо цифри можуть повторюватися.*

Розв'язання. Маємо розміщення з повтореннями. Скористаємося формулою (2.4) коли $n = 4, m = 7$.

$$\overline{A_4^7} = 4^7 = 16384.$$

♦

Приклад 2.8. *Сейф замикається на замок, що має* 5 *дисків, на кожному з яких зображені цифри* $\{0, 1, 2, 3, 4, 5, 6, 7, 8, 9\}$. *Замок відімкнуто, коли на дисках набрана певна комбінація цифр. Чи можна "зламати" сейф за* 10 *днів, якщо працювати щодня по* 13 *годин, а набір однієї комбінації цифр потребує* 5 *секунд.*

Розв'язання. Всіх можливих комбінацій на 5 дисках буде $\overline{A_{10}^5} = 100000$. Щоб набрати всі можливі комбінацій потрібно затратити 500000 секунд, або $500000/3600 = 138,888888889$ годин, або $138,888888889/13 = 10,6838$ "робочих днів". Отже, за 10 днів всі можливі комбінації не набрати.

♦

Приклад 2.9. *Для шифрування тексту виготовлено трафарет, ґратка Кардано, з квадратного паперового аркушу у клітинку розміром $\ell \times \ell$, де ℓ—парне число. Одну із сторін трафарету помічено. Деякі із клітинок вирізано так, щоб при накладанні чистий квадрат такого ж розміру чотирма способами (помічена сторона* ***угорі, праворуч, унизу, ліворуч****) вирізані клітинки покрили всю площу квадрата, причому кожна клітинка мала опинитися під вирізом тільки один раз. Скільки різних трафаретів можна виготовити?*

Розв'язання. Усі клітинки квадрата розіб'ємо на групи, які не перетинаються, по чотири клітинки у кожній групі. Віднесемо клітинки до однієї

1	2	3	4	5	1
5	**6**	7	8	**6**	2
4	8	9	9	7	3
3	7	9	9	8	4
2	**6**	8	7	**6**	5
1	5	4	3	2	1

Рис. 2.1: Групи кліток при 6×6

групи, якщо при кожному повороті квадрата до його суміщення вони пересуваються на місця кліток із цієї групи. На рисунку показано розбиття на групи кліток квадрата при 6×6, де клітинки однієї групи помічено однаковою цифрою. Усього таких груп $m = \ell^2/4$ (m–ціле, бо ℓ–парне число.) При накладанні трафарету на квадрат рівно одна клітинка із заданою групи опиниться під вирізом. Кожному трафарету поставимо у відповідність упорядкований набір усіх кліток з таких груп, що будуть під вирізами при накладанні трафарету на квадрат поміченим боком угору. Усього таких трафаретів буде стільки, скільки існує відображень із m елементів у множину із чотирьох елементів ($n = 4$). Тобто маємо задачу про розміщення із повтореннями і за формулою $n^m = 4^{\ell^2/4}$ — кількість різних можливих трафаретів.

♦

Вправа 2.6. Паролем доступу до комп'ютера є 10–літерне слово у складі якого лише: а) дві літери — {a,b}; б) лише три літери — {K,L,M}. Скільки паролів доступу існує?

Вправа 2.7. Задана множина літер {а, в, д, і, к, л, о }. Скільки слів, не обов'язково змістовних, що складаються із 4 літер можна утворити із літер множини, якщо літери можуть повторюватися?

2.6 Перестановки з повтореннями

Означення 2.7. *Перестановками із n елементів з повтореннями називаються перестановки з n елементів, в кожну з яких входить n_1 однакових елемент першого типу, n_2 однакових елементів другого типу і т.д. — до n_k однакових елементів k–го типу, де $n_1 + n_2 + \cdots + n_k = n$.*

Загальну кількість таких перестановок позначають

$$C_n(n_1, n_2, \ldots, n_k) = \frac{n!}{n_1! n_2! \cdots n_k!}. \qquad (2.5)$$ MPR5

Приклад 2.10. *Скільки існує семизначних чисел, у яких цифра* 6 *зустрічається* 3 *рази, а цифра* 5 *зустрічається* 4 *раз?*

Розв'язання. Маємо перестановки з повтореннями. Використаємо формулу (2.5). Тоді

$$C_7(3,4) = \frac{7!}{3! \cdot 4!} = 35.$$

♦

Приклад 2.11. *Скільки різних слів (не обов'язково зі змістом) можна утворити, якщо переставляти літери у словах:*
a) ***абракадабра****; b)* ***баран****; c)* ***зебра****?*

Розв'язання. a) Слово **абракадабра** містить 5 літер **а**, по 2 літери **б** та **р** і по 1 літері **д** і **к**. Загалом у слові 11 літер. Тоді загальна кількість слів

$$N_a = C_{11}(5,2,2,1,1) = \frac{11!}{5! \cdot 2! \cdot 2! \cdot 1! \cdot 1!} = 83160.$$

b) У слові **баран** дві літери **а** і по одній літері **б, р, н**. Слово має 5 літер. Загальна кількість слів

$$N_b = C_5(2,1,1,1) = \frac{5!}{2! \cdot 1! \cdot 1! \cdot 1!} = 60.$$

c) Слово **зебра** містить по одній літері **а, б, з, е, р**. Тоді

$$N_c = C_5(1,1,1,1,1) = \frac{5!}{1! \cdot 1! \cdot 1! \cdot 1! \cdot 1!} = 120.$$

♦

Вправа 2.8. Ключ до шифру утворюється в результаті перестановки літер в слові **диверсифікація**. Скільки існує різних шифрів?

Вправа 2.9. Скільки різних слів, не обов'язково змістовних, можна утворити якщо переставляючи літери у слові **кардинально**?

2.7 Сполучення з повтореннями

Означення 2.8. *Сполученнями із* n *елементів по* m *з повтореннями називаються комбінації, що містять* m *елементів без врахування порядку, при цьому кожен елемент може входити у комбінацію декілька разів, але не більше* m *раз .*

Приклад 2.12. *При утворенні сполучень для $m = 4$ комбінації $\{a,a,b,a\}$, $\{b,a,a,a\}$ не розрізняються, а $\{a,c,a,a\}$ відрізняється від попередніх.*

Кількість сполучень із n елементів по m з повтореннями рівна

$$\overline{C_n^m} = C_{n+m-1}^m = C_{n+m-1}^{n-1}. \qquad (2.6)$$ MPR6

Приклад 2.13. *В кондитерському магазині продавали тістечка 4 видів: еклер, наполеон, пісочне та струдель. Скільки існує способів вибрати 7 тістечок?*

Розв'язання. Кожен спосіб вибору 7 тістечок — це комбінація з повторенням елементів вибору у якій порядок входження не відіграє ролі. Отже, маємо сполучення із 4 елементів по 7. За формулою (2.6) знаходимо

$$\overline{C_4^7} = C_{10}^7 = \frac{10!}{7! \cdot 3!} = 120.$$

♦

Приклад 2.14. *В деякому ящику знаходиться достатня кількість літер $\{a,b,c,d,e\}$. Скільки існує способів вибрати 11 літер із ящика, щоб далі утворити з них шифр?*

Розв'язання. Коли вибирають 11 літер з ящика, в якому є літери 5 видів, то деякі з них, якщо не всі, мусять повторюватися. Маємо сполуки із 5 елементів по 11. За (2.6) маємо

$$\overline{C_5^{11}} = C_{15}^{11} = \frac{15!}{11! \cdot 4!} = 1365.$$

♦

Вправа 2.10. В пакетику знаходяться карамельки зі смаком вишні, черешні, яблука, абрикоса та полуниці. Скільки є варіантів взяти із пакетика 10 карамельок?

Вправа 2.11. Розсипані на підлозі лото з літерами {а, б, в, г}. Кожної літери по 15 штук. Скільки маємо варіантів підняти з підлоги 9 лото з літерами?

Розділ 3

Алгебра

3.1 Перестановки. Підстановки

Означення 3.1. *Будь–яке впорядковане розміщення елементів множини* $X = \{x_1, x_2, x_3, \ldots, x_n\}$*, тобто розміщення, в якому вказано, який елемент перший, який другий і т.д. називається* ***перестановкою*** *множини* X*.*

Перестановки будемо позначати $(x_1, x_2, \ldots, x_n)$.

Означення 3.2. *Дві перестановки* ***однакові****, якщо порядок елементів в них однаковий.*

Наприклад

$$(a, b, c, d, e), \quad (a, c, d, e, b), \quad (d, e, a, b, c), \quad (a, b, c, e, d)$$

різні перестановки множини $\{a, b, c, d, e\}$.

Візьмемо одну перестановку і перенумеруємо її елементи від 1 до n. Нас цікавить тільки порядок елементів у перестановці.

Теорема 1. *Різних перестановок, які можна утворити із* n *чисел дорівнює* $n!$*.*

Означення 3.3. *Якщо в перестановці* $(x_1, x_2, \ldots, x_n)$ *для елементів* x_i *і* x_j *має місце нерівність* $x_i > x_j$ *при* $i < j$*, то пара* (x_i, x_j) *називається* ***інверсією****.*

Кількість інверсій у перестановці позначимо $J(x_1, x_2, \ldots, x_n)$.

Означення 3.4. *Перестановка множини* X *називається* ***парною****, якщо кількість інверсій* J *число парне і* ***непарною*** *у протилежному випадку.*

Приклад 3.1. *Визначити парність перестановки* $Y = (5, 2, 1, 6, 4, 3)$.

Розв'язання. В перестановці Y:

- перед елементом 1 містяться 2 два елементи $5, 2$;
- перед елементом 2 міститься 1 елемент 5;
- перед елементом 3 містяться 3 елементи $5, 6, 4$;
- перед елементом 4 містяться 2 елементи $5, 6$;
- перед елементом 5 містяться 0 елементів;
- перед елементом 6 містяться 0 елементів.

Тоді, $J(5, 2, 1, 6, 4, 3) = 2 + 1 + 3 + 2 + 0 + 0 = 8$ — перестановка парна.

♦

Вправа 3.1. Визначити парності перестановок:

$$a)\ X_1 = (3, 5, 7, 1, 4, 8, 2, 6); \quad b)\ X_2 = (6, 8, 1, 5, 2, 9, 3, 10, 7, 4).$$

Означення 3.5. *Будь–яке взаємно–однозначне перетворення множини* X *називається* ***підстановкою*** *цієї множини.*

Якщо множина скінчена, то вважаємо, що вона складається із n елементів $(1, 2, \ldots, n)$, то відображення $\pi : X \to X$ буде **підстановкою** n**–го степеня** і запишеться

$$\pi = \begin{pmatrix} 1 & 2 & 3 & \cdots & n \\ \pi_1 & \pi_2 & \pi_3 & \cdots & \pi_n \end{pmatrix}, \quad \text{де } \pi_i = \pi(x_i) \text{ образ } x_i, i = 1, \ldots, n.$$

Означення 3.6. ***Тотожньою (одиничною) підстановкою*** *е називається підстановка, яка елементи множини переводить самі в себе, тобто* $e(x_i) = x_i, i = 1, 2, \ldots, n$ *або*

$$e = \begin{pmatrix} 1 & 2 & \cdots & n \\ 1 & 2 & \cdots & n \end{pmatrix}.$$

Добуток підстановок $\pi : X \to X$ і $\sigma : X \to X$ визначається як послідовне виконання підстановок π та σ і задається формулою $\pi\sigma(x) = \pi(\sigma(x)), \forall x \in X$.

Означення 3.7. *Підстановка* π^{-1} *називається* ***оберненою*** *для підстановки* π, *якщо* $\pi^{-1}\pi = \pi\pi^{-1} = e$.

Означення 3.8. *Добуток* $\pi^k = \underbrace{\pi \cdot \ldots \cdot \pi}_{k \text{ разів}}$ *називається* k*–м степенем підстановки* π*.*

Означення 3.9. *Найменше натуральне число* m*, для якого* $\pi^m = e$*, називається* ***порядком підстановки*** π*.*

Приклад 3.2. *Знайти добутки підстановок* $\pi\sigma$ *і* $\sigma\pi$ *та обернену підстановку* π^{-1}*, якщо*

$$\pi = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 \\ 4 & 3 & 5 & 1 & 2 \end{pmatrix}, \qquad \sigma = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 \\ 3 & 4 & 5 & 1 & 2 \end{pmatrix}.$$

Розв'язання.

$$\pi\sigma = \pi(\sigma) = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 \\ 4 & 3 & 5 & 1 & 2 \end{pmatrix} \cdot \begin{pmatrix} 1 & 2 & 3 & 4 & 5 \\ 3 & 4 & 5 & 1 & 2 \end{pmatrix} = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 \\ 5 & 1 & 2 & 4 & 3 \end{pmatrix}.$$

$$\sigma\pi = \sigma(\pi) = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 \\ 3 & 4 & 5 & 1 & 2 \end{pmatrix} \cdot \begin{pmatrix} 1 & 2 & 3 & 4 & 5 \\ 4 & 3 & 5 & 1 & 2 \end{pmatrix} = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 \\ 1 & 5 & 2 & 3 & 4 \end{pmatrix}.$$

$$\pi^{-1} = \begin{pmatrix} 4 & 3 & 5 & 1 & 2 \\ 1 & 2 & 3 & 4 & 5 \end{pmatrix} = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 \\ 4 & 5 & 2 & 1 & 3 \end{pmatrix}.$$

♦

Вправа 3.2. Знайти добутки підстановок $\pi\sigma$ і $\sigma\pi$ та обернені підстановки π^{-1} та σ^{-1}, якщо

$$\pi = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 & 7 \\ 2 & 7 & 4 & 6 & 3 & 1 & 5 \end{pmatrix}, \quad \sigma = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 & 7 \\ 7 & 6 & 1 & 3 & 2 & 5 & 4 \end{pmatrix}.$$

Вправа 3.3. Знайти добутки підстановок $\pi\sigma$ і $\sigma\pi$ та обернені підстановки π^{-1} та σ^{-1}, якщо

$$\pi = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 & 7 & 8 \\ 8 & 6 & 5 & 3 & 1 & 2 & 4 & 7 \end{pmatrix}, \quad \sigma = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 & 7 & 8 \\ 7 & 3 & 1 & 8 & 2 & 5 & 4 & 6 \end{pmatrix}.$$

Приклад 3.3. *Знайти підстановку* χ *з рівності* $\pi\chi\sigma = \varphi$*, якщо*

$$\pi = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 & 7 \\ 7 & 3 & 2 & 1 & 6 & 5 & 4 \end{pmatrix}, \quad \sigma = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 & 7 \\ 3 & 1 & 2 & 7 & 4 & 5 & 6 \end{pmatrix},$$

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

Розв'язання. Шукану підстановку

$$\chi = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 & 7 \\ \chi_1 & \chi_2 & \chi_3 & \chi_4 & \chi_5 & \chi_6 & \chi_7 \end{pmatrix}$$

знайдемо із співвідношення $\chi = \pi^{-1}\varphi\sigma^{-1}$. Маємо, що

$$\pi^{-1} = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 & 7 \\ 4 & 3 & 2 & 7 & 6 & 5 & 1 \end{pmatrix}, \quad \sigma^{-1} = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 & 7 \\ 2 & 3 & 1 & 5 & 6 & 7 & 4 \end{pmatrix}.$$

Тоді

$$\chi = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 & 7 \\ 4 & 3 & 2 & 7 & 6 & 5 & 1 \end{pmatrix} \cdot \begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 & 7 \\ 5 & 1 & 3 & 6 & 4 & 7 & 2 \end{pmatrix} \cdot \begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 & 7 \\ 2 & 3 & 1 & 5 & 6 & 7 & 4 \end{pmatrix} =$$

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

Отже, шукана підстановка

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

♦

Вправа 3.4. Знайти підстановку χ з рівності $\pi\chi\sigma = \varphi$, якщо

$$\pi = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 & 7 & 8 & 9 \\ 2 & 3 & 8 & 9 & 1 & 4 & 7 & 5 & 6 \end{pmatrix}, \quad \sigma = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 & 7 & 8 & 9 \\ 6 & 4 & 5 & 9 & 3 & 8 & 7 & 1 & 2 \end{pmatrix},$$

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

Вправа 3.5. Знайти підстановку χ з рівності $\pi\chi\sigma = \varphi$, якщо

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

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

Означення 3.10. *Підстановка π, в результаті якої елементи $i_1, i_2, \ldots, i_k$ переходять за правилом $\pi(i_1) = i_2, \pi(i_2) = i_3, \ldots, \pi(i_{k-1}) = i_k, \pi(i_k) = i_1$, а решта елементів залишаються на своїх місцях називається* ***циклом довжини*** *k і позначається $(i_1, i_2, \ldots, i_k)$.*

Кожна нетотожна підстановка π єдиним способом розкладається на добуток незалежних циклів $\sigma_1, \sigma_2, \ldots, \sigma_r$ (з точністю до перестановки множників).

Порядок m підстановки π дорівнює найменшому спільному кратному довжин циклів, на добуток яких вона розкладається.

Приклад 3.4. *Знайти* π^{100}*, якщо*

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

Розв'язання. Розкладемо підстановку π в добуток циклів

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

Довжини незалежних циклів $3, 3, 3, 1$. Найменше спільне кратне циклів рівне 3. Тоді $\pi^3 = e, \pi^{100} = \pi^{99}\pi = (\pi^3)^{33}\pi = \pi$.

♦

Вправа 3.6. Знайти π^{182}, якщо

$$\pi = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 & 7 & 8 & 9 & 10 & 11 & 12 \\ 5 & 6 & 4 & 7 & 11 & 8 & 9 & 10 & 3 & 12 & 1 & 2 \end{pmatrix}.$$

Вправа 3.7. Знайти π^{241}, якщо

$$\pi = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 & 7 & 8 & 9 & 10 & 11 & 12 & 13 & 14 & 15 \\ 9 & 12 & 14 & 15 & 1 & 2 & 3 & 6 & 11 & 8 & 5 & 10 & 4 & 7 & 13 \end{pmatrix}.$$

3.2 Бінарна операція

Означення 3.11. *Нехай* $X \neq \varnothing$ *— деяка множина. Кажуть* ***бінарна алгебрична операція*** $\circ$ *визначена на множині* X*, якщо кожній упорядкованій парі* (x, y) *елементів множини* X *поставлено у відповідність однозначно визначений елемент* $z \in X$*. Цей елемент* $z = x \circ y$ *називають* ***композицією*** *елементів* x, y *відносно даної алгебричної операції.*

Якщо $X = \{x_1, x_2, \ldots, x_n\}$ — скінчена множина, то алгебричну операцію можна записати за допомогою таблиці Келі.

Означення 3.12. ***Нейтральним елементом*** *відносно визначеної алгебричної операції* $\circ$ *називається елемент* $n \in X$*, що для будь–якого елемента* $x \in X$ *виконується рівність* $n \circ x = x \circ n = x$.

Таблиця Келі

$\circ$	x_1	x_2	x_3	x_4	$\dots$	x_n
x_1	z_{11}	z_{12}	z_{13}	z_{14}	$\cdots$	z_{1n}
x_2	z_{21}	z_{22}	z_{23}	z_{24}	$\cdots$	z_{2n}
x_3	z_{31}	z_{32}	z_{33}	z_{34}	$\cdots$	z_{3n}
$\vdots$	$\vdots$	$\vdots$	$\vdots$	$\vdots$	$\ddots$	$\vdots$
x_n	z_{n1}	z_{n2}	z_{n3}	z_{n4}	$\cdots$	z_{nn}

Означення 3.13. *Алгебрична операція називається:*

- ***комутативною**, якщо $x \circ y = y \circ x$,*
- ***асоціативною**, якщо $(x \circ y) \circ z = x \circ (y \circ z)$, де $x, y, z \in X$ — довільні елементи множини.*

Означення 3.14. *Елемент $x \in X$ називається **симетричним** до елемента $y \in X$ відносно алгебричної операції $\circ$, якщо $x \circ y = y \circ x = n$, де n — нейтральний елемент.*

Часто зручно і природно називати алгебричну операцію **множенням** або **додаванням**.

Операція	Композиція	Нейтральний елемент	Симетричний елемент
Множення $\otimes$	добуток елементів xy	одиниця 1 або e	обернений x^{-1}
Додавання $\oplus$	сума елементів $x+y$	нуль 0	протилежним $-x$

Приклад 3.5. *На множині натуральних чисел $\mathbb{N}$ задана алгебрична операція наступним чином $a \circ b = \max\{a, b\}$. З'ясувати, чи ця операція: комутативна? асоціативна? Чи існує нейтральний елемент?*

Розв'язання. 1) Оскільки для довільних натуральних чисел $a, b \in \mathbb{N}$ максимальний елемент також буде натуральним числом, то визначена бінарна операція на $\mathbb{N}$.

2) Виконується співвідношення $\max\{a, b\} = \max\{b, a\}$. Отже, операція комутативна.

3) Вірною є рівність $\max\{\max\{a, b\}, c\} = \max\{a, \max\{b, c\}\}$. Звідси робимо висновок, що операція асоціативна.

4) Для довільного $a \in \mathbb{N}$ вірною є рівність $\max\{1, a\} = \max\{a, 1\} = a$. Отже, існує нейтральний елемент відносно введеної операції.

♦

Вправа 3.8. На множині цілих чисел $\mathbb{Z}$ визначена алгебрична операція наступним чином $a \circ b = a - b$. З'ясувати, чи ця операція: комутативна? асоціативна? Чи існує нейтральний елемент?

Вправа 3.9. На множині цілих чисел $\mathbb{Z}$ визначена алгебрична операція наступним чином $a \circ b = a \times b$. З'ясувати, чи ця операція: комутативна? асоціативна? Чи існує нейтральний елемент?

Приклад 3.6. *Задана множина A, яка містить перші 7–м простих чисел $A = \{2, 3, 5, 7, 11, 13, 17\}$. Скласти таблицю Келі операції $\odot$, яка визначена на множині A наступним чином $x \odot y = \min\{x, y\}$. За допомогою побудованої таблиці з'ясувати: чи операція бінарна? чи операція комутативна? чи операція асоціативна? чи існує відносно операції нейтральний елемент?*

Розв'язання.

Утворимо табличку Келі вказаної операції.

Таблиця Келі операції $\odot$

$\odot$	2	3	5	7	11	13	17
2	2	2	2	2	2	2	2
3	2	3	3	3	3	3	3
5	2	3	5	5	5	5	5
7	2	3	5	7	7	7	7
11	2	3	5	7	11	11	11
13	2	3	5	7	11	13	13
17	2	3	5	7	11	13	17

Із побудованої таблиці безпосередньо випливає:

1) Що задана операція є бінарною операцією на множині A. Результат операції, композиція двох довільних елементів із множини є елемент, який належить множині.

2) Розглянута операція комутативна та асоціативна.

3) Нейтрального елемента не існує.

♦

Вправа 3.10. Множина $A = \{0, 1, 2, 3, 4, 5, 6, 7\}$. Алгебрична операція визначена наступним чином $a \circ b = 7 - \max\{a, b\}$. Скласти таблицю Келі операції і за допомогою побудованої таблиці з'ясувати: чи операція бінарна? чи операція комутативна? чи операція асоціативна? чи існує відносно операції нейтральний елемент?

Вправа 3.11. Множина $A = \{0, 2, 4, 6, 8, 10, 12, 14, 16, 18, 20\}$. Алгебрична операція визначена наступним чином $a \circ b = |a - b|$. Скласти таблицю Келі операції і за допомогою побудованої таблиці з'ясувати: чи операція бінарна? чи операція комутативна? чи операція асоціативна? чи існує відносно операції нейтральний елемент?

3.3 Група

Означення 3.15. ***Групою*** *називається непорожня множина G, на якій визначена бінарна алгебрична операція $\circ$, що називається* ***груповою*** *і задовольняє умови (аксіоми групи):*

1. *кожній упорядкованій парі $(a; b)$ елементів множини G однозначно поставлено у відповідність за допомогою введеної алгебричної операції визначений елемент $c \in G$, що записується як $a \circ b = c$ (**аксіома замкненості**);*

2. *операція $\circ$ асоціативна, тобто для будь–яких елементів a, b, c виконується $(a \circ b) \circ c = a \circ (b \circ c)$ (**аксіома асоціативності**);*

3. *у множині G існує нейтральний елемент e відносно введеної операції, тобто $a \circ e = e \circ a = a$, де $a \in G$ (**аксіома нейтрального елемента**);*

4. *для кожного елемента a множини G у цій множині існує симетричний елемент (**аксіома симетричного елемента**).*

Якщо в додаток до умов (аксіом групи) групова операція буде ще і комутативної, тобто $a \circ b = b \circ a$, то група називається **комутативною** або **абелевою**. Групу називають **мультиплікативною**, якщо в ній групова операція є множення і **адитивною**, якщо групова операція є додавання.

Означення 3.16. *Якщо у групі скінчена кількість елементів, то її називають скінченною, а кількість елементів — порядком і позначають $|G|$.*

В протилежному випадку, коли група має нескінчену кількість елементів її називають нескінченною .

Наведемо приклади.

- Множина цілих чисел $\mathbb{Z}$ буде адитивна група.
- Множина $\mathbb{Z}$ не є мультиплікативна група, бо для цілих чисел відмінних від ± 1 не існує обернених елементів, що належать $\mathbb{Z}$.
- Множина раціональних чисел $\mathbb{Q}$ буде адитивна група.
- Множина $\mathbb{Q}$ не буде мультиплікативна група, бо ділення на нуль неможливе.
- Якщо вилучити нуль з $\mathbb{Q}$, то множина всіх раціональних чисел відмінних від нуля, тобто $\mathbb{Q}\backslash\{0\}$, стане і мультиплікативною групою.
- Множини $\mathbb{R}$ та $\mathbb{C}$ — нескінчені адитивні абелеві групи дійсних та комплексних чисел відповідно.
- Множини всіх відмінних від нуля дійсних та комплексних чисел — мультиплікативні абелеві групи дійсних та комплексних чисел ($\mathbb{R}\backslash\{0\}$, $\mathbb{C}\backslash\{0\}$).
- Множина всіх невироджених квадратних матриць порядку n — нескінчена не комутативна мультиплікативна група.
- Множина всіх підстановок множини $X = \{1; 2; 3; \ldots; n\}$ — скінченна мультиплікативна група, яку називають симетричною групою степеня n і позначають S_n. Роль одиничного елемента в цій групі відіграє тотожна підстановка, підстановка π^{-1} обернений елемент до підстановки $\pi \in S_n$. Симетрична група S_2 степеня 2 — абелева, а при $n \geqslant 3$, група S_n не буде абелева. Порядок симетричної групи — $|S_n| = n!$.

Приклад 3.7. *На множині парних цілих чисел визначена операція додавання. З'ясувати, чи буде множина групою? абелевою групою?*

Розв'язання.

Досліджувана множина $A = \{a : a = 2k, k \in \mathbb{Z}\}$. Нехай маємо три елемента $a = 2k, b = 2m, c = 2n$, що належать A. Групова операція — додавання чисел $+$. Перевіримо виконання всіх аксіом групи.

1) При довільних значеннях $k, m \in \mathbb{Z}$ як результат додавання двох чисел $a+b = 2k+2m = 2(k+m)$ отримуємо парне ціле число. Аксіома замкненості виконується.

2) Оскільки $(a + b) + c = 2(k + m) + 2n = 2(k + m + n)$ і $a + (b + c) = 2k + 2(m + n) = 2(k + m + n)$, то аксіома асоціативності має місце.

3) Якщо $k = 0$, то $a = 0 \in A$. Число 0 буде виконувати роль *нейтрального елемента*, оскільки $0 + a = a + 0 = a$ для довільного $a \in A$. Аксіома нейтрального елемента справедлива.

4) Враховуючи те, що якщо $a \in A$, то $-a = 2(-k) \in A$ і $a + (-a) = 0$, приходимо до висновку, що аксіома симетричного елемента також вірна.

Отже, множина A є групою. Крім того $a + b = 2(k + m) = b + a$, тобто групова операція комутативна, то A — *адитивна абелева група.*

♦

Вправа 3.12. З'ясувати чи множина додатних дійсних чисел $\mathbb{R}^+$ утворює групу відносно операції множення. Визначити чи буде група абелева.

Вправа 3.13. Дослідити чи множина раціональних чисел, знаменниками яких є степені числа 2 з цілими невід'ємними показниками, відносно операції множення утворює групи. У випадку позитивної відповіді з'ясувати, чи буде група абелева.

Означення 3.17. *Якщо підмножина H групи G відносно введеної групової операції сама утворює групу, то H називається* ***підгрупою*** *групи G.*

Підгрупи групи G, які відмінні від її тривіальних підгруп $\{e\}$ та G називаються **власними підгрупами групи** G.

Теорема 2. *Якщо група G має підгрупи H_1 та H_2, то їх перетин $H_1 \cap H_2$ також буде підгрупою групи G. Наведемо приклади.*

- *Адитивна група всіх парних чисел буде власною підгрупою групи всіх цілих чисел.*
- *Адитивна група всіх цілих чисел буде власною підгрупою в адитивній групі всіх дійсних чисел.*
- *Множина всіх парних підстановок з n чисел утворює власну підгрупу симетричної групи підстановок S_n.*

Приклад 3.8. *Задана множина* $A = \{a : a = 3n, n \in \mathbb{Z}\}$. *Показати, що* A *власна підгрупа адитивної групи цілих чисел.*

Розв'язання. Очевидно, що $A \subset \mathbb{Z}$. Перевіримо, що множина A є адитивна група.

1) Аксіома замкненості виконується, оскільки, якщо $a = 3n, b = 3m$, де $n, m \in \mathbb{Z}$, то $a + b = 3(n + m) \in A$.

2) Аксіома асоціативності також має місце. Якщо $c = 3k$, то $(a+b)+c = = a + (b + c) = 3(n + m + k)$.

3) Нейтральним елементом буде $e = 3 \cdot 0$.

4) Аксіома симетричного елемента виконується. Симетричним для довільного елемента $a = 3n$ буде елемент $(-a) = 3(-n)$.

Аксіоми групи для множини A вірні, отже A власна підгрупа адитивної групи цілих чисел.

Вправа 3.14. Показати, що множина

$$nZ = \{a : a = n \cdot k, n, k \in \mathbb{Z}, n\text{— фіксоване}\}$$

буде власною підгрупою адитивної групи цілих чисел.

3.4 Гомоморфізм та ізоморфізм груп

Означення 3.18. *Нехай* G_1 *та* G_2 *— дві групи із груповими операціями* $\circ$ *та* $\bullet$ *відповідно. Кажуть, що відображення* $f : G_1 \to G_2$ *зберігає групову операцію, якщо для всіх елементів* $a, b \in G_1$ *виконується рівність* $f(a \circ b) = f(a) \bullet f(b)$, *а саме відображення при цьому називається* ***гомоморфізмом*** *з групи* G_1 *у групу* G_2.

Означення 3.19. *Множина елементів* $a \in G_1$, *для яких* $f(a) = e'$, *де* e' *— нейтральний елемент групи* G_2, *називається* ***ядром*** $\ker f$ ***гомоморфізму*** $f : G_1 \to G_2$.

Наведемо деяка властивості гомоморфізму.

- Нейтральному елементу групи G_1 ставиться у відповідність нейтральний елемент групи G_2.
- Якщо елементу $a \in G_1$ відповідає елемент $a_1 = f(a) \in G_2$, то елементу $a^{-1} \in G_1$ буде відповідати $a_1^{-1} \in G_2$.

Теорема 3. *Ядро* $\ker f$ *відображення* $f : G_1 \to G_2$ *є підгрупа групи* G_1.

Означення 3.20. *Якщо гомоморфізм є ще і взаємно однозначне відображення, то він називається* ***ізоморфізмом*** .

Означення 3.21. *Якщо існує ізоморфізм групи* G_1 *на групу* G_2, *то кажуть, що група* G_1 *ізоморфна групі* G_2 *та записують* $G_1 \cong G_2$.

Наведемо приклади ізоморфізмів груп.

- Ізоморфні між собою *адитивна група цілих чисел* та *адитивна група парних чисел*, хоча друга є підгрупою першої. Відображення, яке ставить довільному цілому числу nT парне число $2n$ є взаємно однозначне.

- Мультиплікативна група всіх додатних дійсних чисел

$$\mathbb{R}^+ = \{x : x \in \mathbb{R}, x > 0\}$$

  ізоморфна адитивній групі всіх дійсних чисел $\mathbb{R}$, бо кожному додатному числу $a \in \mathbb{R}^+$ можна поставити у відповідність число $\ln a \in \mathbb{R}$. Таке відображення зберігає групову операцію, бо $\ln(ab) = \ln a + \ln b$.

З погляду алгебри ізоморфні групи не відрізняються, бо відображення, яке породжує ізоморфізм, як дзеркало, переводить елементи і групову операцію однієї групи в елементи і групову операцію іншої групи.

Розділ 4

Теорія чисел

4.1 Подільність чисел

У множині цілих чисел $\mathbb{Z} = \{\ldots, -3, -2, -1, 0, 1, 2, 3, \ldots\}$ сума $a + b$, різниця $a - b$ і добуток $a \cdot b$ також будуть цілими числами, проте частка a/b від ділення a на $b, b \neq 0$, може і не бути цілим числом. Те, що частка a/b — ціле число, позначають як $a = qb$, де $q \in \mathbb{Z}$ — ціле число. Число b називають **дільником** числа a і стисло записують: $b|a$ або $a{:}b$. Загалом, для довільних чисел a та b можна єдиним чином підібрати такі числа q та r, що буде виконуватися умова

$$a = bq + r, \qquad 0 \leqslant r < b.$$

Число r називається **остачею від ділення**, а q — **неповною часткою**. Далі будемо розглядати лише **додатні дільники**.

Означення 4.1. *Будь–яке ціле число d, на яке діляться одночасно цілі числа $a_1, a_2, \ldots, a_k$, називається їх* ***спільним дільником.***

Числа можуть мати декілька спільних дільників.

Означення 4.2. *Ціле число $d \neq 0$ називається* ***найбільшим спільним дільником (НСД)*** *чисел $a_1, a_2, \ldots, a_k$ називається і позначається* ***НСД***$(a_1, a_2, \ldots, a_k)$*, якщо виконуються умови:*

1. *кожне із чисел $a_1, a_2, \ldots, a_k$ ділиться на d;*
2. *якщо $d_1 \neq 0$ — інший спільний дільник чисел $a_1, a_2, \ldots, a_k$, то d ділиться на d_1.*

Означення 4.3. *Якщо* ***НСД***$(a, b) = 1$*, то числа a і b називаються* ***взаємно простими.***

Приклад 4.1. *Так як* $\boldsymbol{НСД}(30, 20) = 10$*, то числа* 20 *та* 30 *не є взаємно–простими, а оскільки* $\boldsymbol{НСД}(16, 27) = 1$*, то числа* 16 *і* 27 *взаємно прості числа.*

Властивості НСД.

1. Якщо $a = bq$, то $\mathbf{НСД}(a, b) = b$.
2. Якщо $a = bq+r$, то спільні дільники чисел a і b збігаються із спільними дільниками чисел b і r. Зокрема $\mathbf{НСД}(a, b) = \mathbf{НСД}(b, r)$.
3. Для будь–якого додатного цілого числа m справджується рівність $\mathbf{НСД}(am, bm) = m \cdot \mathbf{НСД}(a, b)$.
4. Якщо $\mathbf{НСД}(a, b) = 1$, то $\mathbf{НСД}(ac, b) = \mathbf{НСД}(c, b)$.
5. Якщо $\mathbf{НСД}(a, b) = 1$ і $ac \vdots b$, то $c \vdots b$.

4.2 Алгоритм Евкліда знаходження НСД двох чисел

Найбільший спільний дільник можна визначити за **евклідовим алгоритмом**.

1. Нехай a і b — цілі додатні числа і для визначеності $a > b$. Складемо низку рівностей:

$$\begin{array}{cc}
a = bq_1 + r_1, & 0 < r_1 < b; \\
b = r_1q_2 + r_2, & 0 < r_2 < r_1; \\
r_1 = r_2q_3 + r_3, & 0 < r_3 < r_2; \\
\cdots\cdots\cdots\cdots\cdots\cdots\cdots\cdots\cdots\cdots & \\
r_{n-3} = r_{n-2}q_{n-1} + r_{n-1}, & 0 < r_{n-1} < r_{n-2}; \\
r_{n-2} = r_{n-1}q_n & r_n = 0.
\end{array}$$

Остання рівність обов'язкова, бо $b > r_1 > r_2 > \cdots > r_{n-1} > r_n = 0$ послідовність спадних цілих чисел і не може містити більше, ніж b додатних чисел.

2. Із вказаних формул та властивостей **НСД** випливає, що

$$\mathbf{НСД}(a, b) = \mathbf{НСД}(b, r_1) = \mathbf{НСД}(r_1, r_2) = \cdots$$

$$\cdots = \mathbf{НСД}(r_{n-2}, r_{n-1}) = \mathbf{НСД}(r_{n-1}, 0) = r_{n-1}.$$

Отже, найбільший спільний дільник дорівнює останній нерівній нулю остачі r_{n-1} вказаного алгоритму.

Приклад 4.2. *Знайти найбільший спільний дільник чисел* 4171 *і* 18527*.*

Розв'язання. Скористаємося евклідовим алгоритмом:

$$\begin{aligned} 18527 &= 4171 \cdot 4 + 1843, \\ 4171 &= 1843 \cdot 2 + 485, \\ 1843 &= 485 \cdot 3 + 388, \\ 485 &= 388 \cdot 1 + 97, \\ 388 &= 97 \cdot 4 + 0. \end{aligned}$$

Отже, $\mathbf{НСД}(18527, 4171) = 97$.

Вправа 4.1. Знайти найбільший спільний дільник чисел 1989792 і 608580.

Вправа 4.2. Знайти найбільший спільний дільник чисел 2465680 і 623672.

Приклад 4.3. *Перевірити чи числа* 16675 *та* 6496 *будуть взаємно простими.*

Розв'язання. Знайдемо $\mathbf{НСД}(16675, 6496)$. Для цього скористаємося евклідовим алгоритмом:

$$\begin{aligned} 16675 &= 6496 \cdot 2 + 3683, \\ 6496 &= 3683 \cdot 1 + 2813, \\ 3683 &= 2813 \cdot 1 + 870, \\ 2813 &= 870 \cdot 3 + 203, \\ 870 &= 203 \cdot 4 + 58, \\ 203 &= 58 \cdot 3 + 29, \\ 58 &= 29 \cdot 2 + 0. \end{aligned}$$

Оскільки $\mathbf{НСД}(16675, 6496) = 19$, то числа не є взаємно простими.

Приклад 4.4. *Перевірити чи числа* 22275 *та* 5681 *будуть взаємно простими.*

Розв'язання. Знайдемо $\mathbf{НСД}(22275, 5681)$ за допомогою евклідового

алгоритму.

$$\begin{aligned}
22275 &= 5681\cdot 3 \;+5232,\\
5681 &= 5232\cdot 1 \;+449,\\
5232 &= 449\cdot 11+293,\\
449 &= 293\cdot 1 \;+156,\\
293 &= 156\cdot 1 \;+137,\\
156 &= 137\cdot 1 \;+19,\\
137 &= 19\cdot 7 \;+4,\\
19 &= 4\cdot 4 \;+3,\\
4 &= 3\cdot 1 \;+1,\\
3 &= 1\cdot 3 \;+0.
\end{aligned}$$

Отримали, що $\mathbf{НСД}(22275, 5681) = 1$. Числа є взаємно простими.

♦

Вправа 4.3. Перевірити чи числа 45747 та 20387 будуть взаємно простими.

Вправа 4.4. Перевірити чи числа 71148 та 8325 будуть взаємно простими.

Будь–яке ціле, яке ділиться без остачі на всі числа $a_1, a_2, \ldots, a_k$ називається їх спільним кратним. Найменше серед спільних кратних чисел називається **найменшим спільним кратним** (**НСК**). Для чисел a і b найменше спільне кратне позначають $\mathbf{НСК}(a, b)$. Має місце співвідношення:

$$\mathbf{НСК}(a, b) = \frac{a \cdot b}{\mathbf{НСД}(a, b)}. \qquad (4.1)$$ MPR7

Так

$$\mathbf{НСК}(4171, 18527) = \frac{4171 \cdot 18527}{97} = 796661$$

.

Приклад 4.5. *Знати найбільший спільний дільник (**НСД**) та найменше спільне кратне (**НСК**) чисел* 16303 *та* 34661.

Розв'язання. За допомогою евклідового алгоритму знайдемо $\mathbf{НСД}(34661, 16303)$.

$$\begin{aligned}
34661 &= 16303\cdot 2 \;+2055,\\
16303 &= 2055\cdot 7 \;+1918,\\
2055 &= 1918\cdot 1 \;+137,\\
1918 &= 137\cdot 14+0.
\end{aligned}$$

Отже, **НСД**$(34661, 16303) = 137$. Згідно із формулою (4.1) отримуємо

$$\mathbf{НСК}(34661, 16303) = \frac{34661 \cdot 116303}{137} = 4124659.$$

Вправа 4.5. Знати найбільший спільний дільник (**НСД**) та найменше спільне кратне (**НСК**) чисел 701688 та 1117758.

Вправа 4.6. Знати найбільший спільний дільник (**НСД**) та найменше спільне кратне (**НСК**) чисел 456987 та 96877719.

4.3 Правильні ланцюгові дроби

Означення 4.4. ***Ланцюговим (неперервним) дробом*** *називають вираз вигляду*

$$f = b_0 + \cfrac{a_1}{b_1 + \cfrac{a_2}{b_2 + \ddots + \cfrac{a_n}{b_n + \ddots}}}.$$

Ланцюговий дріб коротко записують:

$$f = b_0 + \frac{a_1}{b_1} + \frac{a_2}{b_2} + \cdots + \frac{a_n}{b_n} + \cdots = b_0 + \mathop{\mathrm{K}}_{i=1}^{\infty} \frac{a_i}{b_i}.$$

Скінчений ланцюговий дріб f_n, n–й підхідний дріб, n–е наближення ланцюгового дробу f, коротко записують

$$f_n = b_0 + \frac{a_1}{b_1} + \frac{a_2}{b_2} + \cdots + \frac{a_n}{b_n} = b_0 + \mathop{\mathrm{K}}_{i=1}^{n} \frac{a_i}{b_i}.$$

Розглядаємо **правильний ланцюговий дріб** вигляду

$$f = a_0 + \frac{1}{a_1} + \frac{1}{a_2} + \cdots + \frac{1}{a_n} + \cdots = [a_0; a_1, a_2, \ldots, a_n, \ldots], \quad a_i \in \mathbb{N}.$$

Числа $a_i, i = 1, 2, \ldots,$ називають **частинними знаменниками,** a_0 — **вільним членом**.

Для ланцюгового дробу f розглянемо підхідні дроби

$$\frac{p_0}{q_0} = a_0, \quad \frac{p_1}{q_1} = a_0 + \frac{1}{a_1} = [a_0; a_1], \quad \frac{p_2}{q_2} = a_0 + \frac{1}{a_1} + \frac{1}{a_2} = [a_0; a_1, a_2], \quad \cdots,$$

$$\frac{p_k}{q_k} = a_0 + \frac{1}{a_1} + \frac{1}{a_2} + \cdots + \frac{1}{a_k} = [a_0; a_1, a_2, \ldots, a_k], \qquad k = 1, 2, 3, \ldots.$$

Числа p_k та q_k називаються k–м канонічним чисельником та знаменником підхідного дробу.

Значення підхідних дробів p_k/q_k можна обчислювати або за допомогою рекурентних співвідношень (формул Волліса)

$$p_k = a_k p_{k-1} + p_{k-2}, \qquad q_k = a_k q_{k-1} + q_{k-2}, \qquad k = 1, 2, 3, \ldots, \qquad (4.2)$$ MPR8

$$p_{-1} = 1, \quad q_{-1} = 0, \quad p_0 = a_0, \quad q_0 = 1.$$

Властивості підхідних дробів правильного ланцюгового дробу

1. Має місце "детермінантна формула"

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

2. Підхідні дроби правильного ланцюгового дробу нескоротні.

3. Підхідні дроби парного порядку утворюють монотонно зростаючу послідовність, а підхідні дроби непарного порядку — монотонно спадну послідовність і при цьому

$$\frac{p_{2k}}{q_{2k}} < \frac{p_{2i-1}}{q_{2i-1}}, \qquad \forall i, k \in \mathbb{N}.$$

при довільних значеннях i, k.

4. Підхідні дроби правильного ланцюгового дробу задовольняють так званий **"принцип вилки"**

$$\frac{p_0}{q_0} < \frac{p_2}{q_2} < \cdots < \frac{p_{2k}}{q_{2k}} < \cdots < f < \cdots < \frac{p_{2i-1}}{q_{2i-1}} < \cdots < \frac{p_3}{q_3} < \frac{p_1}{q_1},$$

де

$$f = [a_0; a_1, a_2, \ldots].$$

Приклад 4.6. *Знайти розвинення* $\sqrt{2}$ *в правильний ланцюговий дріб і обчислити наближене значення з недостачею та надлишком з точністю* $\varepsilon = 0{,}00001$.

Розв'язання. За умовою задачі потрібно знайти такі a_-, a_+, щоб

$$a_- < \sqrt{2} < a_+, \qquad \text{та} \quad |a - a_-| < \varepsilon,\ |a - a_+| < \varepsilon.$$

Виконаємо еквівалентні перетворення

$$\sqrt{2} = 1 + \sqrt{2} - 1 = 1 + \frac{(\sqrt{2}-1)(\sqrt{2}+1)}{\sqrt{2}+1} = 1 + \frac{1}{1+\sqrt{2}}.$$

Послідовно вкладаючи отримане співвідношення само в себе, отримаємо

$$\sqrt{2} = 1 + \frac{1}{1+\sqrt{2}} = 1 + \frac{1}{2} + \frac{1}{1+\sqrt{2}} = 1 + \frac{1}{2} + \frac{1}{2} + \frac{1}{1+\sqrt{2}} = \cdots =$$

$$= 1 + \frac{1}{2} + \cdots + \frac{1}{2} + \frac{1}{1+\sqrt{2}} = \cdots = 1 + \frac{1}{2} + \cdots + \frac{1}{2} + \cdots = [1; 2, 2, \dots].$$

Використовуючи формули (4.2) обчислимо послідовність підхідних дробів $p_i/q_i, i = 0, 1, 2, \dots$

$$\begin{aligned}
&p_0 = 1, && q_0 = 1, && \frac{p_0}{q_0} = \frac{1}{1} = 1,\\
&p_1 = 2\cdot 1 + 1 = 3, && q_1 = 2\cdot 1 + 0 = 2, && \frac{p_1}{q_1} = \frac{3}{2} = 1{,}5,\\
&p_2 = 2\cdot 3 + 1 = 7, && q_2 = 2\cdot 2 + 1 = 5, && \frac{p_2}{q_3} = \frac{7}{5} = 1{,}4,\\
&p_3 = 2\cdot 7 + 3 = 17, && q_3 = 2\cdot 5 + 2 = 12, && \frac{p_3}{q_3} = \frac{17}{12} \approx 1{,}41667,\\
&p_4 = 2\cdot 17 + 7 = 41, && q_4 = 2\cdot 12 + 5 = 29, && \frac{p_4}{q_4} = \frac{41}{29} \approx 1{,}41379,\\
&p_5 = 2\cdot 41 + 17 = 99, && q_5 = 2\cdot 29 + 12 = 70, && \frac{p_5}{q_5} = \frac{99}{70} \approx 1{,}41429,\\
&p_6 = 2\cdot 99 + 41 = 239, && q_6 = 2\cdot 70 + 29 = 169, && \frac{p_6}{q_6} = \frac{239}{169} \approx 1{,}41420,\\
&p_7 = 2\cdot 239 + 99 = 577, && q_7 = 2\cdot 169 + 70 = 408, && \frac{p_7}{q_7} = \frac{577}{408} \approx 1{,}41422,\\
&p_8 = 2\cdot 577 + 239 = 1393, && q_8 = 2\cdot 408 + 169 = 985, && \frac{p_8}{q_8} = \frac{1393}{985} \approx 1{,}41423.
\end{aligned}$$

Згідно із "принципом вилки" маємо, що

$$1 < \frac{7}{5} < \frac{41}{29} < \frac{239}{169} < \frac{1393}{985} < \cdots < \sqrt{2} < \cdots < \frac{577}{408} < \frac{99}{70} < \frac{17}{12} < \frac{3}{2}.$$

Крім того,

$$\frac{p_7}{q_7} - \frac{p_8}{q_8} < 0{,}000002.$$

Отже,

$$a_- = \frac{1393}{985}, \quad a_+ = \frac{577}{408}.$$

Або виконавши обчислення до 6 знаку після десяткової коми, маємо

$$1,414213 < 1,414214 < 1,414216.$$

♦

Вправа 4.7. Число

$$\varphi = \frac{\sqrt{5}-1}{2}$$

називається **золотим перерізом**. Отримати розвинення (зображення) числа φ у правильний ланцюговий дріб та знайти наближене значення з точністю до шостого знаку після десяткової коми.

Вказівка до розв'язання. Скористатися тотожністю

$$\frac{\sqrt{5}-1}{2} = 1 + \frac{1}{1 + \dfrac{\sqrt{5}-1}{2}}.$$

Вправа 4.8. Отримати розвинення (зображення) числа $\sqrt{3}$ у правильний ланцюговий дріб та обчислити наближене значення числа з точністю до шостого знака після десяткової коми.

Вказівка до розв'язання. Обґрунтувати та скористатися тотожністю

$$\sqrt{3} = 1 + \frac{1}{1 + \dfrac{1}{1+\sqrt{3}}}.$$

4.4 Алгоритм Евкліда та розвинення раціонального дробу у правильний ланцюговий дріб

Нехай $p, q \in \mathbb{N}$ і дріб p/q — нескоротний. Операцію ділення з остачею в алгоритмі Евкліда запишемо у вигляді

$$\begin{aligned}
\frac{p}{q} &= a_0 + \frac{r_1}{q}, && 0 < r_1 < q;\\
\frac{q}{r_1} &= a_1 + \frac{r_2}{r_1}, && 0 < r_2 < r_1;\\
\frac{r_1}{r_2} &= a_2 + \frac{r_3}{r_2}, && 0 < r_3 < r_2;\\
&\vdots && \vdots\\
\frac{r_{n-2}}{r_{n-1}} &= a_{n-1} + \frac{r_n}{r_{n-1}}, && 0 < r_n < r_{n-1};\\
\frac{r_{n-1}}{r_n} &= a_n, && a_n > 1.
\end{aligned}$$

Перепишемо дріб p/q наступним чином

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

$$= a_0 + \frac{1}{a_1 + \frac{1}{a_2 + \frac{r_3}{r_2}}} = \cdots = a_0 + \frac{1}{a_1 + \frac{1}{a_2 + \frac{1}{a_3 + \cdots + \frac{1}{a_n}}}} =$$

$$= [a_0; a_1, a_2, a_3, \ldots, a_n],$$

де $a_0 \in \mathbb{Z}, a_i \in \mathbb{N}$.

Приклад 4.7. *Розвинути раціональний дріб* $\frac{1638}{1495}$ *у правильний ланцюговий дріб.*

Розв'язання. Послідовно виконуємо дії

$$\frac{1639}{1495} = 1 + \frac{144}{1495} = 1 + \frac{1}{\frac{1495}{144}} = 1 + \frac{1}{10 + \frac{55}{144}} = 1 + \frac{1}{10 + \frac{1}{\frac{144}{55}}} = 1 + \frac{1}{10 +}$$

$$+ \frac{1}{2 + \frac{34}{55}} = 1 + \frac{1}{10 + \frac{1}{2 + \frac{1}{\frac{55}{34}}}} = 1 + \frac{1}{10 + \frac{1}{2 + \frac{1}{1 + \frac{21}{34}}}} = 1 + \frac{1}{10 + \frac{1}{2 +}}$$

$$+\cfrac{1}{1}+\cfrac{1}{\cfrac{34}{21}}=1+\cfrac{1}{10}+\cfrac{1}{2}+\cfrac{1}{1}+\cfrac{1}{1}+\cfrac{13}{21}=1+\cfrac{1}{10}+\cfrac{1}{2}+\cfrac{1}{1}+\cfrac{1}{1}+\cfrac{1}{\cfrac{21}{13}}=$$

$$=1+\cfrac{1}{10}+\cfrac{1}{2}+\cfrac{1}{1}+\cfrac{1}{1}+\cfrac{1}{1}+\cfrac{8}{13}=1+\cfrac{1}{10}+\cfrac{1}{2}+\cfrac{1}{1}+\cfrac{1}{1}+\cfrac{1}{1}+\cfrac{1}{\cfrac{13}{8}}=$$

$$=1+\cfrac{1}{10}+\cfrac{1}{2}+\cfrac{1}{1}+\cfrac{1}{1}+\cfrac{1}{1}+\cfrac{1}{1}+\cfrac{5}{8}=1+\cfrac{1}{10}+\cfrac{1}{2}+\cfrac{1}{1}+\cfrac{1}{1}+\cfrac{1}{1}+\cfrac{1}{1}+$$

$$+\cfrac{1}{\cfrac{8}{5}}=1+\cfrac{1}{10}+\cfrac{1}{2}+\cfrac{1}{1}+\cfrac{1}{1}+\cfrac{1}{1}+\cfrac{1}{1}+\cfrac{1}{1}+\cfrac{3}{5}=1+\cfrac{1}{10}+\cfrac{1}{2}+\cfrac{1}{1}+$$

$$+\cfrac{1}{1}+\cfrac{1}{1}+\cfrac{1}{1}+\cfrac{1}{1}+\cfrac{1}{\cfrac{5}{3}}=1+\cfrac{1}{10}+\cfrac{1}{2}+\cfrac{1}{1}+\cfrac{1}{1}+\cfrac{1}{1}+\cfrac{1}{1}+$$

$$+\cfrac{1}{1}+\cfrac{1}{1}+\cfrac{2}{3}=1+\cfrac{1}{10}+\cfrac{1}{2}+\cfrac{1}{1}+\cfrac{1}{1}+\cfrac{1}{1}+\cfrac{1}{1}+\cfrac{1}{1}+\cfrac{1}{1}+\cfrac{1}{\cfrac{3}{2}}=$$

$$=1+\cfrac{1}{10}+\cfrac{1}{2}+\cfrac{1}{1}+\cfrac{1}{1}+\cfrac{1}{1}+\cfrac{1}{1}+\cfrac{1}{1}+\cfrac{1}{1}+\cfrac{1}{1}+\cfrac{1}{2}.$$

♦

Вправа 4.9. Розвинути раціональний дріб $\frac{8220}{2533}$ у правильний ланцюговий дріб.

Вправа 4.10. Розвинути раціональний дріб $\frac{3632}{3033}$ у правильний ланцюговий дріб.

4.5 Прості числа

Означення 4.5. *Натуральне число $p \in \mathbb{N}$ називається* ***простим****, якщо $p > 1$ і p ділиться тільки само на себе і на 1. В протилежному випадку натуральне число називається* ***складеним****, тобто якщо воно ділиться не лише на один, само на себе, а ще хоча б одне натуральне число.*

Першими простими натуральними числами є:

$$2, 3, 5, 7, 11, 13, 17, 19, 23, 29, 31, 37, 41, 43, 47, 53, 59, 61, 67, 71, 73, 79, 83, \ldots$$

Якщо n — число складене, то знайдеться таке ціле $a \in \mathbb{N}$, що

$$n = a \cdot b, 1 < b < n, b = \frac{n}{a}.$$

Очевидно, що всі парні числа, крім 2, — складені.

Множина натуральних чисел $\mathbb{N}$ може бути розбита на три підмножини: множину простих чисел; множину складених чисел; число 1, яке не відноситься ні до складених ні до простих.

Властивості простих чисел

1. Для будь–якого цілого числа $n > 1$ найменший відмінний від одиниці додатний дільник — це завжди просте число.
2. Найбільший простий дільник, який відмінний від 1, будь–якого складеного числа n не перевищує $\sqrt{n}$.
3. Простих чисел безліч.
4. Якщо добуток натуральних чисел $a \cdot b$ ділиться на просте число p, то хоча б одне з них ділиться на p.

4.6 Решето Ератосфена

Найпростішою процедурою отримання послідовності простих чисел є **решето Ератосфена**. Мета методу — визначити (просіяти) всі додатні прості числа, які менші за деяку верхню цілу межу $n > 0$.

Випишемо всі натуральні числа від 2 до n. Перше просте число у цьому ряді — 2. Викреслимо із ряду всі числа, які кратні 2 крім нього самого:

$$2, 3, \not{4}, 5, \not{6}, 7, \not{8}, 9, \not{10}, 11, \not{12}, 13, \not{14}, 15, \not{16}, 17, \not{18}, 19, \not{20}, 21, \not{22}, 23, \not{24}, 25, \ldots, n$$

Тепер перше не викреслене число після 2 буде 3 і воно просте. Викреслимо в ряді після 3 всі числа, які кратні 3:

$$2, 3, \not{4}, 5, \not{6}, 7, \not{8}, \not{9}, \not{10}, 11, \not{12}, 13, \not{14}, \not{15}, \not{16}, 17, \not{18}, 19, \not{20}, \not{21}, \not{22}, 23, \not{24}, 25, \ldots, n$$

Першим не викресленим числом після 3 буде число 5. Викреслимо в ряді чисел, що залишилися всі числа, які кратні 5:

$$2, 3, \not{4}, 5, \not{6}, 7, \not{8}, \not{9}, \not{10}, 11, \not{12}, 13, \not{14}, \not{15}, \not{16}, 17, \not{18}, 19, \not{20}, \not{21}, \not{22}, 23, \not{24}, \not{25}, \ldots, n$$

Якщо викреслювати таким чином в ряді всі числа, які кратні простим числам, що менші за $\sqrt{n}$, то всі числа, які залишаться будуть простими.

Приклад 4.8. *За допомогою "решета Ератосфена" отримати всі прості числа, які менші за* 100*.*

Розв'язання. Оскільки всі парні числа крім 2 є складеними, то запишемо 2 і всі непарні числа від 3 до 99

$$2,\ 3,\ 5,\ 7,\ 9,\ 11,\ 13,\ 15,\ 17,\ 19,\ 21,\ 23,\ 25,\ 27,\ 29,\ 31,\ 33,\ 35,$$

$$37,\ 39,\ 41,\ 43,\ 45,\ 47,\ 49,\ 51,\ 53,\ 55,\ 57,\ 59,\ 61,\ 63,\ 65,\ 67,$$

$$69,\ 71,\ 73,\ 75,\ 77,\ 79,\ 81,\ 83,\ 85,\ 87,\ 89,\ 91,\ 93,\ 95,\ 97,\ 99.$$

На першому кроці залишимо 3 і викреслимо всі числа, які кратні 3.

$$2,\ 3,\ 5,\ 7,\ \not{9},\ 11,\ 13,\ \not{15},\ 17,\ 19,\ \not{21},\ 23,\ 25,\ \not{27},\ 29,\ 31,\ \not{33},\ 35,$$

$$37,\ \not{39},\ 41,\ 43,\ \not{45},\ 47,\ 49,\ \not{51},\ 53,\ 55,\ \not{57},\ 59,\ 61,\ \not{63},\ 65,\ 67,$$

$$\not{69},\ 71,\ 73,\ \not{75},\ 77,\ 79,\ \not{81},\ 83,\ 85,\ \not{87},\ 89,\ 91,\ \not{93},\ 95,\ 97,\ \not{99}.$$

Наступним після 3 не викресленим числом є 5. Його залишаємо і викреслимо всі числа, які кратні 5.

$$2,\ 3,\ 5,\ 7,\ \not{9},\ 11,\ 13,\ \not{15},\ 17,\ 19,\ \not{21},\ 23,\ \not{25},\ \not{27},\ 29,\ 31,\ \not{33},\ \not{35},$$

$$37,\ \not{39},\ 41,\ 43,\ \not{45},\ 47,\ 49,\ \not{51},\ 53,\ \not{55},\ \not{57},\ 59,\ 61,\ \not{63},\ \not{65},\ 67,$$

$$\not{69},\ 71,\ 73,\ \not{75},\ 77,\ 79,\ \not{81},\ 83,\ \not{85},\ \not{87},\ 89,\ 91,\ \not{93},\ \not{95},\ 97,\ \not{99}.$$

Наступним за 5 іде число 7. Залишаємо 7 і викреслюємо всі числа, які кратні 7.

$$2,\ 3,\ 5,\ 7,\ \not{9},\ 11,\ 13,\ \not{15},\ 17,\ 19,\ \not{21},\ 23,\ \not{25},\ \not{27},\ 29,\ 31,\ \not{33},\ \not{35},$$

$$37,\ \not{39},\ 41,\ 43,\ \not{45},\ 47,\ \not{49},\ \not{51},\ 53,\ \not{55},\ \not{57},\ 59,\ 61,\ \not{63},\ \not{65},\ 67,$$

$$\not{69},\ 71,\ 73,\ \not{75},\ \not{77},\ 79,\ \not{81},\ 83,\ \not{85},\ \not{87},\ 89,\ \not{91},\ \not{93},\ \not{95},\ 97,\ \not{99}.$$

Оскільки $\sqrt{100} = 10$, то наступного кроку, тобто викреслювати числа кратні 11, робити не потрібно. Виписуємо ряд не викреслених чисел.

$$2,\ 3,\ 5,\ 7,\ 11,\ 13,\ 17,\ 19,\ 23,\ 29,\ 31,\ 37,\ 41,$$

$$43,\ 47,\ 53,\ 59,\ 61,\ 67,\ 71,\ 73,\ 79,\ 83,\ 89,\ 97.$$

Всі вони будуть простими числами від 2 до 100.

Вправа 4.11. Використовуючи алгоритм решета Ератосфена знайти прості числа від 2 до 200.

4.7 Прайморіал простого числа

У 1987 році американський математик Гарві Дабнер за аналогією з факторіалом числа, $n! = 1 \cdot 2 \cdot \ldots \cdot n$, ввів поняття прайморіала.

Означення 4.6. ***Прайморіалом*** $p^{\#}$ ***простого числа*** $p > 0$ *називається добуток всіх простих чисел, менших або рівних* p.

Наприклад, $2^{\#} = 2, 5^{\#} = 2 \cdot 3 \cdot 5 = 30$. При умові, що q — наступне після p просте число, $q^{\#} = p^{\#} \cdot q$.

Якщо розглядати числа вигляду $p^{\#} + 1$, часто їх ще називають числами Евкліда, то виявляється, що

$$2^{\#} + 1 = 3, \quad 3^{\#} + 1 = 6 + 1 = 7, \quad 5^{\#} + 1 = 30 + 1 = 31,$$

$$7^{\#} + 1 = 210 + 1 = 211, \quad 11^{\#} + 1 = 2310 + 1 = 2311$$

прості числа, але

$$13^{\#} + 1 = 2 \cdot 3 \cdot 5 \cdot 7 \cdot 11 \cdot 13 + 1 = 30031 = 59 \cdot 509$$

число складене. Хоча числа $p^{\#} + 1$ не завжди прості числа, але не мають дільників менших або рівних числу p.

Маємо такий алгоритм відшукання великих простих чисел. Нехай відомі прості числа із проміжку $[0; p]$.

- з'ясовуємо, чи $p^{\#} + 1$ просте число. Якщо так, то задача розв'язана,
- якщо ні то шукаємо найменший простий дільник числа $p^{\#} + 1$, який більший за p.

Проблема також полягає в тому, що навіть при невеликих значеннях p прайморіал $p^{\#}$ — велике число.

Приклад 4.9. *Обчислити прайморіал числа числа* 19 *та з'ясувати, чи* $19^{\#}+1$ *буде простим числом.*

Розв'язання. Згідно із означенням

$$19^{\#} = 2 \cdot 3 \cdot 5 \cdot 7 \cdot 11 \cdot 13 \cdot 17 \cdot 19 = 9699690.$$

Але число

$$19^{\#} + 1 = 9699691 = 347 \cdot 27953$$

не є простим числом.

♦

Вправа 4.12. Обчислити прайморіал чисел $20, 21, 24, 25, 29, 31$.

Вправа 4.13. З'ясувати чи число $17^{\#}+1$ буде простим числом.

Вправа 4.14. Обчислити прайморіал числа числа 23 та з'ясувати, чи число $23^{\#}+1$ буде простим числом.

4.8 Основна теорема арифметики

Теорема 4. *Для будь–якого цілого числа* $m \neq 1$ *існує єдине* ***канонічне розвинення на прості множники*** *(з точністю до їх перестановок), тобто*

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

де $p_1, p_2, \ldots, p_n$ *— різні прості числа, а* $k_1, k_2, \ldots, k_n$ *— натуральні числа, що називаються* ***кратності простих чисел****.*

Наслідки з основної теореми арифметики

1. Число

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

ділиться на число b тоді і тільки тоді, коли

$$b = p_1^{t_1} \cdot p_2^{t_2} \cdot \ldots \cdot p_n^{t_n},$$

де $0 \leqslant t_1 \leqslant k_1, 0 \leqslant t_2 \leqslant k_2, \ldots, 0 \leqslant t_n \leqslant k_n$.

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

3. Кількість усіх дільників числа
$$m = p_1^{k_1} \cdot p_2^{k_2} \cdot \ldots \cdot p_n^{k_n}$$
можна обчислити за формулою
$$\tau(m) = (k_1 + 1)(k_2 + 1) \cdots (k_n + 1). \tag{4.3}$$ MPR9

4. Сума всіх дільників числа дорівнює
$$S(m) = \frac{p_1^{k_1+1} - 1}{p_1 - 1} \cdot \frac{p_2^{k_2+1} - 1}{p_2 - 1} \cdot \ldots \cdot \frac{p_n^{k_n+1} - 1}{p_n - 1}. \tag{4.4}$$ MPR10

Приклад 4.10. *Знайти канонічне розвинення числа* 16200 *на прості множники.*

Розв'язання. Послідовно виконуємо ділення на прості числа

16200	2	‖	225	3
8100	2		75	3
4050	2		25	5
2025	3		5	5
675	3		1	

Отримуємо розвинення
$$16200 = 2^3 \cdot 3^4 \cdot 5^2.$$

♦

Вправа 4.15. Знайти канонічне розвинення числа 379456 на прості множники.

Вправа 4.16. Знайти канонічне розвинення числа 29712375 на прості множники.

Приклад 4.11. *Показати, що число* 14553 *ділиться на число* 2079.

Розв'язання. Знайдемо канонічні розвинення чисел 14553 та 2079 на прості множники. Послідовно ділимо на прості числа.

14553	3
4851	3
1617	3
539	7
77	7
11	11
1	

2079	3
693	3
231	3
77	7
11	11
1	

Отримали розвинення

$$14553 = 3^3 \cdot 7^2 \cdot 11, \qquad 2079 = 3^3 \cdot 7 \cdot 11.$$

Числа розвинуті за одними і тими ж простими числами $3, 7, 11$. Згідно із першим наслідком з основної теореми арифметики число 14553 ділиться на 2079.

♦

Вправа 4.17. Показати, що число 83006 ділиться на число 539.

Вправа 4.18. Показати, що число 343343 ділиться на число 637.

Приклад 4.12. *Знайти кількість дільників та їх суму числа* 79625.

Розв'язання. Число має канонічне розвинення на прості множники

$$79625 = 5^3 \cdot 7^2 \cdot 13.$$

Згідно із формулою (4.3) маємо

$$\tau(79625) = (3+1)(2+1)(1+1) = 24.$$

За допомогою формули (4.4) знаходимо

$$S(79625) = \frac{5^4-1}{5-1} \cdot \frac{7^3-1}{7-1} \cdot \frac{13^2-1}{13-1} = 156 \cdot 57 \cdot 14 = 124488.$$

♦

Вправа 4.19. Знайти кількість дільників та їх суму числа 705551.

Вправа 4.20. Знайти кількість дільників та їх суму числа 7626125.

Як наслідок із основної теореми алгебри випливає твердження.

Теорема 5. *Нехай маємо канонічні розвинення на множники двох чисел a та b*

$$a = p_1^{k_1} \cdot p_2^{k_2} \cdot \ldots \cdot p_n^{k_n}, \quad b = p_1^{m_1} \cdot p_2^{m_2} \cdot \ldots \cdot p_n^{m_n},$$

причому деякі показники k_i і m_i можуть дорівнювати нулю. Тоді найбільший спільний дільник чисел a і b визначається за формулою

$$\boldsymbol{НСД}(a,b) = p_1^{t_1} \cdot p_2^{t_2} \cdot \ldots \cdot p_n^{t_n}, \tag{4.5}$$ MPR12

де $t_i = \min\{k_i; m_i\},\ i = 1, 2, \cdots, n$, а найменше спільне кратне цих чисел за формулою

$$\boldsymbol{НСК}(a,b) = p_1^{s_1} \cdot p_2^{s_2} \cdot \ldots \cdot p_n^{s_n}, \tag{4.6}$$ MPR14

де $s_i = \max\{k_i; m_i\},\ i = 1, 2, \cdots, n$,

Приклад 4.13. *Обчислити найбільший спільний дільник (**НСД**) та найменше спільне кратне (**НСК**) чисел $a = 7800$ та $b = 14586$.*

Розв'язання. Запишемо канонічне розвинення чисел на прості множники

$$a = 7800 = 2^3 \cdot 3 \cdot 5^2 \cdot 13, \qquad b = 14586 = 2 \cdot 3 \cdot 11 \cdot 13 \cdot 17.$$

Перепишемо розвинення у вигляді

$$a = 2^3 \cdot 3 \cdot 5^2 \cdot 11^0 \cdot 13 \cdot 17^0, \qquad b = 2 \cdot 3 \cdot 5^0 \cdot 11 \cdot 13 \cdot 17.$$

За допомогою формули (4.5) знаходимо

$$\mathbf{НСД}(7800, 14586) = 2^1 \cdot 3^1 \cdot 5^0 \cdot 11^0 \cdot 13^1 \cdot 17^0 = 78.$$

Аналогічно, згідно із формулою (4.6) маємо

$$\mathbf{НСК}(7800, 14586) = 2^3 \cdot 3^1 \cdot 5^2 \cdot 11^1 \cdot 13^1 \cdot 17^1 = 1458600.$$

♦

Вправа 4.21. Обчислити найбільший спільний дільник (**НСД**) та найменше спільне кратне (**НСК**) чисел $a = 429975$ та $b = 647360$.

Вправа 4.22. Обчислити найбільший спільний дільник (**НСД**) та найменше спільне кратне (**НСК**) чисел $a = 714420$ та $b = 1028160$.

4.9 Відношення порівняння

Нехай $m > 1$ — ціле додатне число, яке назвемо **модулем**.

Означення 4.7. *Два числа a та b називаються **порівнянними за модулем** m, якщо їх різниця $a - b$ ділиться без остачі на число m.*

Таке співвідношення між числами a та b називається **порівнянням (конгруенцією)** чисел та записують

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

В такому записі про число a кажуть, що це — **лишок числа b за модулем m**. Запис $a \mod m$ означає лишок числа a, який рівний деякому цілому числу від 0 до $m - 1$. Операція $a \mod m$ називається **зведенням числа a за модулем m**.

Властивості відношення порівняння

- рефлексивність: $a \equiv a \pmod{m}$ для будь–якого числа m;
- симетричність: якщо $a \equiv b \pmod{m}$, то $b \equiv a \pmod{m}$;
- транзитивність: якщо $a \equiv b \pmod{m}$ та $c \equiv b \pmod{m}$, то $a \equiv c \pmod{m}$;
- якщо $a \equiv b \pmod{m}$ і k — довільне ціле число, то $ka \equiv kb \pmod{m}$;
- якщо $ka \equiv kb \pmod{m}$, а k і m взаємно прості числа, то $a \equiv b \pmod{m}$;
- якщо $a \equiv b \pmod{m}$ і k — довільне натуральне число, то $ka \equiv kb \pmod{km}$;
- Якщо $a \equiv b \pmod{m}$ і $c \equiv d \pmod{m}$, то $a \pm c \equiv b \pm d \pmod{m}$;
- Будь–який доданок лівої та правої частин порівняння можна переносити з протилежним знаком в іншу частину, тобто:

  1) якщо $a \equiv b + c \pmod{m}$, то $a - b \equiv c \pmod{m}$, $a - c \equiv b \pmod{m}$;

  2) якщо $a + b \equiv c \pmod{m}$, то $a \equiv c - b \pmod{m}$;
- Якщо $a \equiv b \pmod{m}$, то $a^n \equiv b^n \pmod{m}$ для будь–якого цілого $n \geqslant 0$;

- Якщо $a \equiv b \pmod m$ і

$$f(x) = c_n x^n + c_{n-1} x^{n-1} + \cdots + c_1 x + c_0$$

довільний багаточлен із цілими коефіцієнтами, то

$$f(a) \equiv f(b) \pmod m.$$

Приклад 4.14. *Чи будуть порівняними за модулем* 29 *такі числа* $-56, -43, -27, -14, 2, 60, 89, 102, 160$.

Розв'язання. Перевіряємо, чи ділиться без остачі різниця двох чисел $a - b$ на число 29.

$$(-43 + 56)/29 = 13/29; \quad (-27 + 56)/29 = 1; \quad (-14 + 56)/29 = 42/29;$$

$$(2 + 56)/29 = 2; \quad (60 + 56)/29 = 4; \quad (89 + 56)/29 = 5;$$

$$(102 + 56)/29 = 158/29; \quad (160 + 56)/29 = 216/29;$$

$$(-27 + 43)/29 = 16/29; \quad (-14 + 43)/29 = 1; \quad (2 + 43)/29 = 45/29;$$

$$(60 + 43)/29 = 103/29; \quad (89 + 43)/29 = 132/29; \quad (102 + 43)/29 = 5;$$

$$(160 + 43)/29 = 7; \quad (-14 + 27)/29 = 13/29; \quad (2 + 27)/29 = 1;$$

$$(60 + 27)/29 = 3; \quad (89 + 27)/29 = 4; \quad (102 + 27)/29 = 129/29;$$

$$(160 + 27)/29 = 187/29; \quad (2 + 14)/29 = 16/29; \quad (60 + 14)/29 = 74/29;$$

$$(89 + 14)/29 = 103/29; \quad (102 + 14)/29 = 4; \quad (160 + 14)/29 = 6.$$

$$(60 - 2)/29 = 2; \quad (89 - 2)/29 = 3; \quad (102 - 2)/29 = 100/29;$$

$$(160 - 2)/29 = 158/29; \quad (89 - 60)/29 = 1; \quad (102 - 60)/29 = 42/29;$$

$$(160 - 60)/29 = 100/29; \quad (102 - 89)/29 = 13/29;$$

$$(160 - 89)/29 = 71/29; \quad (160 - 102)/29 = 2;$$

Отже, за модулем 29 порівняними є група чисел $\{-56, -27, 2, 60, 89\}$ та група чисел $\{-43, -14, 102, 160\}$.

♦

Вправа 4.23. Які числа множини

$$A = \{-68, -34, -31, -29, 8, 40, 43, 45, 80, 82, 114, 119, 154\}$$

будуть порівняними за модулем 37.

Приклад 4.15. *Звести числа за модулем:*
a) $123 \mod 47$*;* *b)* $-23 \mod 17$*;*

Розв'язання. a) Оскільки $123 = 2 \cdot 47 + 29$, то $123 \equiv 29 \mod 47$.
b) Аналогічно $-23 \equiv 34 - 23 \equiv 11 \mod 17$.

♦

Вправа 4.24. Звести числа за модулем. 1) $23 \mod 17$; 2) $64 \mod 31$; 3) $-23 \mod 13$; 4) $-3 \mod 7$; 5) $-67 \mod 19$.

Відношення еквівалентності розбиває множину, на якій воно визначено, на **класи еквівалентності**, які позначаються $\bar{0}, \bar{1}, \bar{2}, \ldots, \overline{m-1}$. Два класи еквівалентності або не перетинаються, або збігаються. Класи еквівалентності, які визначаються відношенням порівняння, називаються **класами лишків за модулем** m. Клас лишків, що містить число a, позначається $\bar{a}$, або $a \pmod m$ і є множиною чисел вигляду $a + km, k \in \mathbb{Z}$, число a називають **представником** цього класу:

$$\begin{aligned}
\bar{0} &= \{\ldots, -2m, -m, 0, m, 2m, \ldots\},\\
\bar{1} &= \{\ldots, -2m+1, -m+1, 1, m+1, 2m+1, \ldots\},\\
\bar{2} &= \{\ldots, -2m+2, -m+2, 2, m+2, 2m+2, \ldots\},\\
&\vdots \quad \vdots \quad \vdots \quad \vdots \quad \vdots \quad \vdots \quad \vdots \quad \vdots \quad \vdots \quad \vdots\\
\overline{m-1} &= \{\ldots, -m-1, -1, m-1, 2m-1, 3m-1, \ldots\},
\end{aligned}$$

Приклад 4.16. *Визначити до якого класу лишків за модулем* 17 *належать числа* $\{23, 38, 49, -3, -10, -24\}$.

Розв'язання. Оскільки $23 = 17+6 \equiv 6 \pmod{17}$, то число 23 належить класу $\bar{6}$. Далі маємо, що $38 = 2 \cdot 17 + 4 \equiv 4 \pmod{17}$, а тоді число 38 належить класу $\bar{4}$. Аналогічно $49 = 2 \cdot 17 + 15 \equiv 15 \pmod{17}$. Тоді число 49 належить класу $\overline{15}$. Знову, позаяк $-3 = -17 + 14 \equiv 14 \pmod{17}$, то число (-3) належить класу $\overline{14}$. Враховуючи, що $-10 = -17 + 7 \equiv 7 \pmod{17}$, то число (-10) належить класу $\bar{7}$. Насамкінець $-24 = -2 \cdot 17 + 10 \equiv 10 \pmod{17}$ і маємо, що о число (-24) належить класу $\overline{10}$.

♦

Вправа 4.25. Визначити до якого класу лишків за модулем 19 належать числа $\{21, 38, 44, -2, -8, -14\}$.

Вправа 4.26. Визначити чи належать числа $\{25, -2, 48, -21, 33, -13\}$ до одного класу лишків за модулем 23.

4.10 Обернений елемент за модулем

Множина класів лишків за модулем m позначається $\mathbb{Z}\backslash m\mathbb{Z}$, складається рівно із m елементів і відносно операцій додавання та множення є скінчене комутативне **кільцем класів лишків** за модулем m з одиницею.

Означення 4.8. *Елемент кільця $\mathbb{Z}\backslash m\mathbb{Z}$, який позначається $a^{-1} \in Z_m$ називається **оберненим** до елемента a у кільці $\mathbb{Z}\backslash m\mathbb{Z}$, а саме число a називається **оборотним**, якщо виконується рівність*

$$a \cdot a^{-1} \equiv 1 \pmod{m}, \quad \textit{або} \quad 1 \equiv a \cdot a^{-1} \pmod{m}.$$

У кільці лишків за модулем m можуть бути дільники нуля тоді і тільки тоді, коли m — складене число. Кільце лишків за простим модулем не містить дільників нуля.

Означення 4.9. *Множина елементів в $\mathbb{Z}\backslash m\mathbb{Z}$, для яких у цьому кільці існують обернені елементи відносно множення, утворюють мультиплікативну групу Z_m^*.*

Теорема 6. *Елементами групи Z_m^* будуть тільки взаємно прості за модулем m елементи a кільця $\mathbb{Z}\backslash m\mathbb{Z}$.*

4.11 Розширений евклідів алгоритм

Ідея розширеного евклідового алгоритму, який запропонований Кнутом, полягає в тому, щоб на кожному кроці алгоритму відшукання **НСД(a,b)** подати залишок r_j у вигляді комбінації діленого a і дільника b, тобто

$$\begin{aligned}
a &= bq_1 + r_1, & r_1 &= ax_1 + by_1,\\
b &= r_1q_2 + r_2, & r_2 &= ax_2 + by_2,\\
r_1 &= r_2q_3 + r_3, & r_3 &= ax_3 + by_3,\\
&\vdots & &\vdots\\
r_{j-1} &= r_jq_{j+1} + r_{j+1}, & r_{j+1} &= ax_{j+1} + by_{j+1},\\
&\vdots & &\vdots\\
r_{n-3} &= r_{n-2}q_{n-1} + r_{n-1}, & r_{n-1} &= ax_{n-1} + by_{n-1},\\
r_{n-2} &= r_{n-1}q_n, & r_n &= 0.
\end{aligned}$$

Числа x_j та y_j визначаються за рекурентними формулами

$$x_j = x_{j-2} - q_j x_{j-1}, \qquad y_j = y_{j-2} - q_j y_{j-1}, \qquad j = 1, 2, \ldots, n, \qquad (4.7)$$ MPR15

при початкові значення $x_{-1} = 1, y_{-1} = 0, x_0 = 0, y_0 = 1$.

Приклад 4.17. *За допомогою розширеного евклідового алгоритму знайти* d=***НСД***(a, b) *та числа* α *і* β *у співвідношенні* $\alpha \cdot a + \beta \cdot b = d$, *якщо* $a = 168156, b = 38925$.

Розв'язання. Скористаємося формулами (4.7).

$$\begin{array}{l} 168156 = 4 \cdot 38925 + 12456, x_1 = 1 - 4 \cdot 0 = 1, \quad y_1 = 0 - 4 \cdot 1 = -4 \\ 38925 = 3 \cdot 12456 + 1557, \quad x_2 = 0 - 3 \cdot 1 = -3, y_2 = 1 + 3 \cdot 4 = 13 \\ 12456 = 8 \cdot 1557 + 0, \end{array}$$

Отримали

$$\alpha = -3, \quad \beta = 13, \qquad -3 \cdot 168156 \cdot +13 \cdot 38925 = 1557,$$

d=**НСД**$(168156, 38925)$=1557.

♦

Вправа 4.27. За розширеним евклідовим алгоритмом знайти значення d=**НСД**(a, b) та числа α, β у рівності $\alpha \cdot a + \beta \cdot b = d$, коли $a = 116675$, $b = 90468$.

Вправа 4.28. За розширеним евклідовим алгоритмом знайти значення d=**НСД**(a, b) та числа α, β у рівності $\alpha \cdot a + \beta \cdot b = d$, коли $a = 827793$, $b = 275094$.

Якщо числа m та a взаємно прості, то **НСД**$(m, a) = 1$. Згідно із розширеним евклідовим алгоритмом існують такі числа α, β, що $\alpha \cdot m + \beta \cdot a = 1$, а це в Z_m^* еквівалентно тотожності

$$\beta \cdot a \equiv 1 \pmod{m}, \qquad \text{тобто} \quad \beta = a^{-1}.$$

Приклад 4.18. *За розширеним евклідовим алгоритмом знайти елемент, який обернений до елемента* 173 *у кільці лишків* Z_{659}^*.

Розв'язання.

За допомогою розширеного евклідового алгоритму знайдемо **НСД**$(659, 173)$ та числа α, β:

$$1)\, 659 = 173 \cdot 3 + 140, \quad x_1 = 1 - 0 = 1, \quad y_1 = 0 - 3 = -3;$$

$$2)\, 173 = 140 \cdot 1 + 33, \quad x_2 = 0 - 1 = -1, \quad y_2 = 1 + 3 = 4;$$

$$3)\, 140 = 33 \cdot 4 + 8, \quad x_3 = 1 + 4 = 5, \quad y_3 = -3 - 16 = -19;$$

$$4)\, 33 = 8 \cdot 4 + 1, \quad x_4 = -1 - 20 = -21, \quad y_4 = 4 + 76 = 80;$$

$$8 = 8 \cdot 1 + 0.$$

Отже, $\mathbf{НСД}(659, 173) = 1, \qquad (-21) \cdot 659 + 80 \cdot 173 = 1,$
$\beta = 80 \Rightarrow 80 \cdot 173 \equiv 1 \pmod{659} \Rightarrow 173^{-1} \pmod{659} = 80 \pmod{659}.$

♦

Вправа 4.29. За розширеним евклідовим алгоритмом знайти елемент, який обернений до елемента 233 у кільці лишків Z^*_{719}.

Вправа 4.30. Використовуючи розширений евклідів алгоритм знайти у кільці лишків Z^*_{761} обернений елемент до 443.

Згідно із теоремою Ойлера для будь–якого модуля m і будь–якого $a \geqslant 1$, яке взаємно просте з числом m, справедливе порівняння

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

а звідки

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

Приклад 4.19. *За допомогою теореми Ойлера знайти обернений елемент до елемента 7 у кільці лишків* Z^*_{13}.

Розв'язання. Оскільки модуль 13 — просте число, то

$$\varphi(13) = 13 - 1 = 12, \qquad \text{звідки} \quad 7^{-1} \pmod{13} \equiv 7^{11} \pmod{13} =$$

$$\equiv 7^{11} = 1977326743 \pmod{13} =$$

$$= 152102057 \cdot 13 + 2 \pmod{13} = 2 \pmod{13}.$$

Отже,

$$7^{-1} \pmod{13} \equiv 2 \pmod{13}.$$

♦

Вправа 4.31. За допомогою теореми Ойлера знайти обернений елемент до елемента 9 у кільці лишків Z_{11}^*.

Вправа 4.32. За допомогою теореми Ойлера знайти до елемента 12 у кільці лишків Z_{17}^* обернений елемент.

Розділ 5

Многочлени

5.1 Операції над многочленами

Означення 5.1. ***Многочленом (багаточленом, поліномом)*** *степеня n відносно змінної x*

$$f_n(x) = a_0x^n + a_1x^{n-1} + \cdots + a_{n-1}x + a_n = \sum_{i=0}^{n} a_ix^{n-i}, \qquad (5.1)$$ MPR11

де $a_i, (0 \leqslant i \leqslant n)$ — коефіцієнти многочлена, $a_0 \neq 0$ — старший коефіцієнт, a_n — вільний член.

Відносно коефіцієнтів многочлена припускають, що вони належать деякому кільцю $\mathbf{K}$ або полю $\mathbf{F}$. Наприклад полю дійсних $\mathbb{R}$, раціональних $\mathbb{Q}$ або комплексних $\mathbb{C}$ чисел. Тоді кажуть, що многочлен заданий над полем або над кільцем.

Деколи многочлен записують не тільки за спадними степенями x, а і за зростаючими степенями:

$$f_n(x) = b_0 + b_1x + \cdots + b_{n-1}x^{n-1} + b_nx^n = \sum_{i=0}^{n} b_ix^i. \qquad (5.2)$$ MPR16

Зауваження 5.1. Многочлен (5.1) або (5.2) називається **нормованим (зведеним)**, якщо коефіцієнт при старшому степені рівний 1, тобто коли $a_0 = 1$ або $b_n = 1$.

Приклад 5.1. *Знайти нормований (зведений) многочлен для многочлена* $f_5(x) = 3x^5 + 6x^4 - 9x^3 + 7x^2 - 2x - 1$.

Розв'язання. Розділивши всі коефіцієнти многочлена $f_5(x)$ на коефіцієнт при старшому степені x, отримаємо $p_5(x) = x^5 + 2x^4 - 3x^3 + \frac{7}{3}x^2 - \frac{2}{3}x - \frac{1}{3}$.

Многочлен $p_5(x)$ буде нормованим (зведеним) многочленом, який відповідний многочлену $f_5(x)$.

♦

Вправа 5.1. Знайти нормований (зведений) многочлен для многочлена $f_6(x) = 2x^6 + x^5 - 4x^4 - 6x^3 + 3x^2 + 4x - 5$.

Вправа 5.2. Знайти нормований (зведений) многочлен для многочлена $f_7(x) = -4x^7 + 2x^6 - x^5 + 3x^4 - 5x^3 - 8x^2 + 12x - 8$.

Всяке число, яке відмінне від нуля — **многочлен нульової степені** $f_0(x) = a_0$.

Число нуль також належить до многочленів, але позаяк степінь його не визначена, то його називають **нульовим многочленом**.

Многочлен першого степеня $f_1(x) = a_0x + a_1$ називається **лінійним**, другого степеня $f_2(x) = a_0x^2 + a_1x + a_2$ — **квадратним**, третього степеня $f_3(x) = a_0x^3 + a_1x^2 + a_2x + a_3$ — **кубічним**.

Зауваження 5.2. Вигляд многочлена (5.2) називають **канонічним**. Якщо многочлен не містить якогось степеня x, то у канонічному записі коефіцієнт при такому степені x ставлять рівним 0.

Так, наприклад, многочлен $f_6(x) = x^6 - 3x^3 + 5x^2 + 1$ записують у канонічному вигляді як $f_6(x) = x^6 + 0x^5 + 0x^4 - 3x^3 + 5x^2 + 0x + 1$ і $a_0 = 1, a_1 = 0, a_2 = 0, a_3 = -3, a_4 = 5, a_5 = 0, a_6 = 1$.

Приклад 5.2. *Записати канонічний вигляд многочлена* $f_7(x) = 2x^7 + + 6x^4 + x$.

Розв'язання. В записі многочлена $f_7(x)$ відсутні коефіцієнти при степенях x^6, x^5, x^3, x^2, x^0. Коефіцієнти в канонічному записі многочлена будуть рівні $a_0 = 2, a_1 = 0, a_2 = 0, a_3 = 6, a_4 = 0, a_5 = 0, a_6 = 1, a_7 = 0$. Тоді многочлен може бути записаний в наступному канонічному вигляді

$f_7(x) = 2x^7 + 0x^6 + 0x^5 + 6x^4 + 0x^3 + 0x^2 + 1x^1 + 0x^0$.

♦

Вправа 5.3. Записати канонічний вигляд многочлена $f_8(x) = -3x^8 + 4x^5 - - 3x^2 + 5$.

Вправа 5.4. Записати канонічний вигляд многочлена $f_9(x) = x^9 - 7x^6 + + 5x^3 - 2x$.

Означення 5.2. *Два многочлени*

$$f_n(x) = a_0x^n + a_1x^{n-1} + a_2x^{n-2} + \cdots + a_{n-1}x + a_n$$

та

$$\varphi_m(x) = b_0x^m + b_1x^{m-1} + b_2x^{m-2} + \cdots + b_{m-1}x + b_m$$

називаються ***рівними****, якщо* $n = m$ *та* $a_i = b_i, i = 0, 1, 2, \ldots, n$*. Рівність многочленів записують так* $f_n(x) = \varphi_n(x)$*.*

Протилежним *для многочлена*

$$f_n(x) = a_0x^n + a_1x^{n-1} + a_2x^{n-2} + \cdots + a_{n-1}x + a_n$$

буде многочлен

$$-f_n(x) = -a_0x^n - a_1x^{n-1} - a_2x^{n-2} - \cdots - a_{n-1}x - a_n.$$

Нехай маємо многочлени

$$f_n(x) = a_0x^n + a_1x^{n-1} + a_2x^{n-2} + \cdots + a_{n-1}x + a_n \ ,$$

$$\varphi_m(x) = b_0x^m + b_1x^{m-1} + b_2x^{m-2} + \cdots + b_{m-1}x + b_m,$$

$$g_k(x) = c_0x^k + c_1x^{k-1} + c_2x^{k-2} + \cdots + c_{k-1}x + c_k \ .$$

Означення 5.3. ***Сумою*** *многочленів* $f_n(x)$ *та* $\varphi_m(x)$ *називається многочлен*

$$g_k(x) = f_n(x) + \varphi_m(x) = c_0x^k + c_1x^{k-1} + c_2x^{k-2} + \cdots + c_{k-1}x + c_k,$$

де $k = \max(n, m)$,

$$c_i = \begin{cases} a_i + b_i, & \text{для} \quad i \leqslant \min(n, m); \\ a_i, & \text{для} \quad \min(n, m) < i \leqslant n, \quad \text{якщо} \quad n > m; \\ b_i, & \text{для} \quad \min(n, m) < i \leqslant m, \quad \text{якщо} \quad n < m. \end{cases}$$

Означення 5.4. ***Різницею*** *многочленів* $f_n(x) - \varphi_m(x)$ *називається такий многочлен* $g_k(x)$*, що виконується рівність* $f_n(x) = \varphi_m(x) + g_k(x)$*.*

Означення 5.5. ***Добутком*** *многочленів* $f_n(x)$ *та* $\varphi_m(x)$ *називається многочлен*

$$g_{m+n}(x) = (a_0x^n + a_1x^{n-1} + a_2x^{n-2} + \cdots + a_{n-1}x + a_n)\times$$

$$\times(b_0x^m + b_1x^{m-1} + b_2x^{m-2} + \cdots + b_{m-1}x + b_m)$$

степеня $n + m$ *вигляду*

$$g_{m+k}(x) = a_0b_0x^{n+m} + (a_0b_1 + a_1b_0)x^{n+m-1} + (a_0b_2 + a_1b_1 + a_2b_0)x^{n+m-2} +$$

$$+ \cdots + (a_0b_k + a_1b_{k-1} + \cdots + a_kb_0)x^{n+m-k} + \cdots + (a_nb_{m-1} + a_{n-1}b_m)x + a_nb_m.$$

Приклад 5.3. *Знайти суму, різницю та добуток многочленів*

$$f_3(x) = 3x^3 - 4x^2 + 6x, \quad g_4(x) = -2x^4 + 5x^3 + 2x^2 - 8.$$

Розв'язання. Знаходимо суму

$$f_3(x) + g_4(x) = (3x^3 - 4x^2 + 6x) + (-2x^4 + 5x^3 + 2x^2 - 8) =$$

$$= (0 - 2)x^4 + (3 + 5)x^3 + (-4 + 2)x^2 + (6 + 0)x + (0 - 8) =$$

$$= -2x^4 + 8x^3 - 2x^2 + 6x - 8.$$

Різницею многочленів буде многочлен

$$f_3(x) - g_4(x) = (3x^3 - 4x^2 + 6x) - (-2x^4 + 5x^3 + 2x^2 - 8) =$$

$$= (0 + 2)x^4 + (3 - 5)x^3 + (-4 - 2)x^2 + (6 - 0)x + (0 + 8) =$$

$$= 2x^4 - 2x^3 - 6x^2 + 6x + 8.$$

Підрахуємо добуток

$$f_3(x) \times g_4(x) = (3x^3 - 4x^2 + 6x) \times (-2x^4 + 5x^3 + 2x^2 - 8) =$$

$$= (-6)x^7 + (15 + 8)x^6 + (6 - 20 - 12)x^5 + (-8 + 30)x^4 +$$

$$+(-24 + 12)x^3 + (32)x^2 + (-48)x + (0) =$$

$$= -6x^7 + 23x^6 - 26x^5 + 22x^4 - 12x^3 + 32x^2 - 48x.$$

♦

Вправа 5.5. Знайти суму, різницю та добуток многочленів

$$f_5(x) = -2x^5 - 3x^3 + 4x^2 - 8, \quad g_4(x) = 3x^4 + 4x^3 - 5x^2 + 6x - 7.$$

Вправа 5.6. Знайти суму, різницю та добуток многочленів

$$f_6(x) = 3x^6 - 4x^5 + 5x^4 - 4x^3 + 3x^2 - 2x + 1,$$

$$g_5(x) = -3x^5 + 2x^4 + 6x^3 - 7x^2 + 8x - 9.$$

5.2 Ділення многочленів

Означення 5.6. ***Часткою від ділення*** *многочлена $f_n(x)$ на многочлен $\varphi_m(x)$ називається многочлен $g_{n-m}(x)$ (при умові, що він існує), який при його множені на многочлен $\varphi_m(x)$ дає многочлен $f_n(x)$, тобто*

$$g_{n-m}(x) = \frac{f_n(x)}{\varphi_m(x)}, \qquad \textit{якщо} \quad g_{n-m}(x)\varphi_m(x) = f_n(x).$$

У цьому випадку говорять, що ***многочлен $f_n(x)$ ділиться на многочлен $\varphi_m(x)$ без остачі,*** *а множники $\varphi_m(x), g_{n-m}(x)$ називаються* ***дільниками многочлена $f_n(x)$.***

Якщо многочлен $f_n(x)$ не ділиться на многочлен $\varphi_m(x)$, то вводять операцію **ділення многочленів з остачею**.

Для будь–яких многочленів $f_n(x)$ та $\varphi_m(x)$ існують і визначаються єдиним способом многочлени $q_{n-m}(x)$ та $r_k(x)$, для яких

$$f_n(x) = q_{n-m}(x)\varphi_m(x) + r_k(x), \qquad \text{де} \quad k < m. \tag{5.3}$$ MPR17

Багаточлен $q_{n-m}(x)$ називається **часткою**, а многочлен $r_k(x)$ — **остачею від ділення** многочлена $f_n(x)$ на $\varphi_m(x)$.

На практиці многочлен ділять на многочлен (з остачею чи без остачі), використовуючи або метод "ділення кутиком", що аналогічний методу ділення чисел, або метод невизначених коефіцієнтів. Проілюструємо кожен із них на прикладах.

Приклад 5.4. *Розділити без остачі многочлен $f_5(x) = 2x^5 - 3x^4 + 5x^3 + + x^2 + 3x + 28$ на многочлен $\varphi_3(x) = 2x^3 + 3x^2 + 6x + 7$.*

Розв'язання.

$$\begin{array}{rl|l}
2x^5-3x^4+5x^3+ & x^2+\ 3x+28 & 2x^3+3x^2+6x+7 \\ \cline{3-3}
-\underline{2x^5+3x^4+6x^3+\ 7x^2} & & x^2-3x+4 \\
-6x^4-\ x^3-\ 6x^2+\ 3x & & \\
-\underline{-6x^4-9x^3-18x^2-21x} & & \\
8x^3+12x^2+24x+28 & & \\
-\underline{8x^3+12x^2+24x+28} & & \\
0 & &
\end{array}$$

♦

Вправа 5.7. Розділити без остачі многочлен $f_6(x) = 3x^6 + 5x^5 - 16x^4 + 2x^3 + 27x^2 - 28x + 10$ на многочлен $\varphi_2(x) = 3x^2 - 4x + 2$.

Вправа 5.8. Розділити без остачі многочлен $f_7(x) = -5x^7 + 7x^6 - 5x^5 - 13x^4 - 33x^3 - 37x^2 + 41x - 10$ на многочлен $\varphi_3(x) = 5x^3 + 3x^2 - 4x + 1$.

Приклад 5.5. *За допомогою методу "ділення кутом" розділити з остачею многочлен* $f_6(x) = x^6 - x^5 + x^4 + 3x^3 + x - 8$ *на многочлен* $g_3(x) = x^3 + 2x^2 + 3x + 4$.

Розв'язання. Аналогічно виконуємо дії.

$$\begin{array}{r|l}
x^6 - x^5 + x^4 + 3x^3 + 0x^2 + x - 8 & x^3 + 2x^2 + 3x + 4 \\
\cline{2-2}
-\underline{x^6 + 2x^5 + 3x^4 + 4x^3} & x^3 - 3x^2 + 4x \\
\cline{1-1}
-3x^5 - 2x^4 - x^3 + 0x^2 & \\
-\underline{3x^5 - 6x^4 - 9x^3 - 12x^2} & \\
\cline{1-1}
4x^4 + 8x^3 + 12x^2 + x & \\
-\underline{4x^4 + 8x^3 + 12x^2 + 16x} & \\
\cline{1-1}
-15x - 8 &
\end{array}$$

Отримали частку $q_3(x) = x^3 - 3x^2 + 4x$ і остачу $r_1(x) = -15x - 8$. Має місце рівність

$x^6 - x^5 + x^4 + 3x^2 + x - 8 = (x^3 + 2x^2 + 3x + 4)(x^3 - 3x^2 + 4x) - 15x - 8.$

♦

Вправа 5.9. За допомогою методу "ділення кутом" розділити многочлен $f_7(x) = x^7 + 6x^5 - 3x^3 + 4x^2 + 9$ на многочлен $g_4(x) = x^4 - 5x^3 - 4x^2 + 7x + 3$.

Вправа 5.10. За допомогою методу "ділення кутом" розділити многочлен $f_8(x) = -5x^8 + 4x^7 - 3x^5 + 2x^3 - 3x^2 + 5x + 9$ на многочлен $g_3(x) = 2x^3 + 3x^2 - 6x + 5$.

Приклад 5.6. *За допомогою методу "невизначених коефіцієнтів" розділити з остачею многочлен* $f_5(x) = x^5 + 4x^3 - 5x^2 + x - 7$ *на многочлен* $g_3(x) = x^3 - 6x^2 + 8x - 4$.

Розв'язання. Згідно із (5.3) маємо, що

$$f_5(x) = q_2(x)g_3(x) + r_2(x),$$

де коефіцієнти многочленів $q_2(x), r_2(x)$ потрібно знайти, тобто

$$x^5 + 4x^3 - 5x^2 + x - 7 = (Ax^2 + Bx + C)(x^3 - 6x^2 + 8x - 4) +$$

$$+Dx^2 + Ex + F.$$

У правій частині зведемо коефіцієнти при однакових степенях x. Отримуємо

$$x^5 + 0x^4 + 4x^3 - 5x^2 + x - 7 = Ax^5 + (-6A + B)x^4 + (8A - 6B + C)x^3 +$$

$$+(-4A + 8B - 6C + D)x^2 + (-4B + 8C + E)x + (-4C + F).$$

Прирівняємо коефіцієнти при однакових степенях x в лівій та правій частинах рівності.

x^5	$1 = A$	$A = 1$
x^4	$0 = -6A + B$	$B = 6$
x^3	$4 = 8A - 6B + C$	$C = 32$
x^2	$-5 = -4A + 8B - 6C + D$	$D = 143$
x	$1 = -4B + 8C + E$	$E = -231$
x^0	$-7 = -4C + F$	$F = 121$

Отримали, що частка від ділення $q_2(x) = x^2+6x+32$ і остача від ділення $r_2(x) = 143x^2 - 231x + 121$.

♦

Вправа 5.11. За допомогою методу "невизначених коефіцієнтів" розділити многочлен $f_6(x) = x^6 + 5x^5 + 2x^4 - 3x^3 + 6x^2 - 4x + 9$ на многочлен $g_4(x) = x^4 - 7x^3 + 5x^2 + 3x - 8$.

Вправа 5.12. За допомогою методу "невизначених коефіцієнтів" розділити многочлен $f_7(x) = 2x^7 - 5x^6 + 4x^5 - 3x^4 + 7x^3 - 2x^2 + 5x + 3$ на многочлен $g_4(x) = x^4 + 3x^3 - 4x^2 + 6x + 9$.

Схема Горнера є наслідком методу невизначених коефіцієнтів і використовується при діленні многочлена $f_n(x)$ на двочлен $x - c$, де c — стала. Згідно із формулою (5.3), якщо

$$f_n(x) = a_0x^n + a_1x^{n-1} + a_2x^{n-2} + \cdots + a_{n-1}x^1 + a_n,$$

то

$$f_n(x) = q_{n-1}(x)(x - c) + r,$$

де

$$q_{n-1}(x) = b_0x^{n-1} + b_1x^{n-2} + b_2x^{n-3} + \cdots + b_{n-2}x + b_{n-1},\ r = \text{const}.$$

Коефіцієнти $b_0, b_1, \ldots, b_{n-1}$ та стала r визначаються за формулами:

$$b_0 = a_0; \quad b_k = a_k + cb_{k-1}; \quad k = 1, 2, \ldots, n-1; \quad r = a_n + cb_{n-1}.$$

Процес ділення за схемою Горнера записують у вигляді таблиці.

	a_0	a_1	$\ldots$	a_{n-1}	a_n
c	$b_0 = a_0$	$b_1 = a_1 + cb_0$	$\ldots$	$b_{n-1} = a_{n-1} + cb_{n-2}$	$r = a_n + cb_{n-1}$

У верхньому рядку таблиці містяться коефіцієнти многочлена, який записаний у канонічному вигляді за зростаючими степенями x, а у нижньому — коефіцієнти частки та остача.

Приклад 5.7. *За допомогою схеми Горнера знайти частку та остачу від ділення многочлена* $f_5(x) = 2x^5 + 3x^3 - 2x + 6$ *на двочлен* $x + 3$.

Розв'язання. Запишемо многочлен $f_5(x)$ у канонічному вигляді

$$f_5(x) = 2x^5 + 0x^4 + 3x^3 + 0x^2 - 2x + 6,$$

і застосуємо схему Горнера при $c = -3$

$c = -3$						
a_i	2	0	3	0	-2	6
b_i, r	2	-6	21	-63	187	-555

Отримали частку $q_4(x) = 2x^4 - 6x^3 + 21x^2 - 63x + 187$ і остачу $r = -555$.

♦

Вправа 5.13. За допомогою схеми Горнера знайти частку та остачу від ділення многочлена $f_6(x) = -3x^6 + 2x^5 - x^4 + x^2 - 7$ на двочлен $x - 2$.

Вправа 5.14. За допомогою схеми Горнера знайти частку та остачу від ділення многочлена $f_7(x) = 3x^7 - 4x^6 - 3x^5 + 4x^4 - 5x^3 + 7x^2 + 3x - 7$ на двочлен $x - 2$.

5.3 Евклідів алгоритм знаходження найбільшого спільного дільника двох многочленів

Означення 5.7. *Многочлен* $g_k(x)$ *називається* ***спільним дільником*** *многочленів* $f_n(x), \varphi_m(x)$, *якщо він — дільник кожного із них.*

Усі многочлени нульового степеня будуть спільними дільниками будь–яких двох многочленів $f_n(x)$ і $\varphi_m(x)$. Якщо ці два многочлени не мають інших спільних дільників, то вони називаються **взаємно простими**.

Означення 5.8. *Спільний дільник двох многочленів називається* ***найбільшим спільним дільником (НСД)****, якщо він ділиться на будь–який інший спільний дільник цих многочленів.*

НСД многочленів визначається з точністю до сталого множника, який відмінний від нуля, і позначається $d(f_n(x); \varphi_m(x))$ або **НСД**$(f_n(x); \varphi_m(x))$.

НСД двох многочленів можна знайти за **евклідовим алгоритмом**, який базується лише на операції ділення многочленів з остачею.

Приклад 5.8. *За евклідовим алгоритмом знайти* ***НСД*** *двох многочленів* $f_4(x) = x^4 - 2x^3 - 4x^2 + 4x - 3$ *та* $\varphi_3(x) = 2x^3 - 5x^2 - 4x + 3$.

Зауваження 5.3. НСД визначається із точністю до сталого множника, відмінного від нуля. Тому в процесі застосування евклідового алгоритму, щоб спростити обчислення, многочлени та проміжні результати при діленні будемо домножати на "зручні" коефіцієнти. Такі випадки будемо помічати подвійною рискою.

Розв'язання. Поділимо многочлен $2 \cdot f_4(x)$ на $\varphi_3(x)$:

$$\begin{array}{r|l}
2x^4 - 4x^3 - 8x^2 + 8x - 6 & 2x^3 - 5x^2 - 4x + 3 \\
\cline{2-2}
2x^4 - 5x^3 - 4x^2 + 3x & \|x + 1 \\
\cline{1-1}
x^3 - 4x^2 + 5x - 6 & \\
\cline{1-1}
2x^3 - 8x^2 + 10x - 12 & \\
2x^3 - 5x^2 - 4x + 3 & \\
\cline{1-1}
-3x^2 + 14x - 15 &
\end{array}$$

Поділимо многочлен $\varphi_3(x)$ на остачу $-3x^2 + 14x - 15$:

$$\begin{array}{r|l}
2x^3 - 5x^2 - 4x + 3 & -3x^2 + 14x - 15 \\
\cline{2-2}
6x^3 - 15x^2 - 12x + 9 & \|-2\,x - 13 \\
6x^3 - 28x^2 + 30x & \\
\cline{1-1}
13x^2 - 42x + 9 & \\
\cline{1-1}
39x^2 - 126x + 27 & \\
39x^2 - 182x + 195 & \\
\cline{1-1}
56x - 168 & \\
\cline{1-1}
x - 3 &
\end{array}$$

Тепер поділимо многочлен $3x^2 - 14x + 15$ на $x - 3$:

$$\begin{array}{r|l} 3x^2 - 14x + 15 & x - 3 \\ \cline{2-2} 3x^2 - 9x & 3x - 5 \\ \cline{1-1} -5x + 15 & \\ -5x + 15 & \\ \cline{1-1} 0 & \end{array}$$

Отже, найбільший спільний дільник многочленів

$$f_4(x) = x^4 - 2x^3 - 4x^2 + 4x - 3 \quad \text{та} \quad \varphi_3(x) = 2x^3 - 5x^2 - 4x + 3$$

буде $x - 3$, тобто

$$\textbf{НСД}(f_4(x); \varphi_3(x)) = x - 3.$$

♦

Приклад 5.9. *За евклідовим алгоритмом знайти* ***НСД*** *наступних многочленів* $f_5(x) = x^5 - 5x^2 + x - 3$ *та* $\varphi_3(x) = x^3 - x - 6$.

Розв'язання. Знайдемо неповну частку $q_2^{(1)}(x)$ та остачу $r_2^{(1)}(x)$ при діленні $f_5(x)$ на $\varphi_3(x)$ за допомогою методу невизначених коефіцієнтів.

Нехай

$$q_2^{(1)}(x) = Ax^2 + Bx + C \quad \text{і} \quad r_2^{(1)}(x) = Dx^2 + Ex + F.$$

Тоді

$$x^5 - 5x^2 + x - 3 = (Ax^2 + Bx + C)(x^3 - x - 6) + Dx^2 + Ex + F.$$

$$x^5 - 5x^2 + x - 3 = Ax^5 + Bx^4 + (-A + C)x^3 +$$
$$+(-6A - B + D)x^2 + (-6B - C + E)x + (-6C + F).$$

Прирівняємо коефіцієнти при однакових степенях

$$\begin{array}{c|l|l} x^5 & 1 = A & A = 1 \\ x^4 & 0 = B & B = 0 \\ x^3 & 0 = -A + C & C = 1 \\ x^2 & -5 = -6A - B + D & D = 1 \\ x^1 & 1 = -6B - C + E & E = 2 \\ x^0 & -3 = -6C + F & F = 3 \end{array}$$

Отримали:

$$q_2^{(1)}(x) = x^2 + 1, \quad r_2^{(1)}(x) = x^2 + 2x + 3. \quad r_2^{(1)}(x) \not\equiv 0.$$

Розділимо $\varphi_3(x)$ на $r_2^{(1)}(x)$. Маємо:

$$x^3 - x - 6 = (Ax + B)(x^2 + 2x + 3) + Cx + D.$$

Або

$$x^3 - x - 6 = Ax^3 + (2A + B)x^2 + (3A + 2B + C)x + 3B + D.$$

Тоді

x^3	$1 = A$	$A = 1$
x^2	$0 = 2A + B$	$B = -2$
x^1	$-1 = 3A + 2B + C$	$C = 0$
x^0	$-6 = 3B + D$	$D = 0$

Отже, $r_1^{(2)}(x) \equiv 0$. Тоді

НСД$(x^5 - 5x^2 + x - 3, x^3 - x - 6)$=$x^2 + 2x + 3$.

♦

Вправа 5.15. За допомогою евклідового алгоритму знайти найбільший спільний дільник многочленів

$$f_6(x) = x^6 + 3x^5 + 3x^4 + 8x^3 - 4x^2 + 3x - 14$$

та

$$\varphi_4(x) = x^4 + 3x^3 + x^2 + x - 6.$$

Вправа 5.16. За евклідовим алгоритмом знайти **НСД** многочленів

$$f_7(x) = x^7 - 2x^6 + 4x^5 - 2x^4 + 6x^3 - 5x^2 + 4x - 10$$

та

$$\varphi_4(x) = 5x^4 - 2x^3 + 4x^2 + 3x - 7.$$

Післямова

Основу методичного посібника склали типові задачі з тих розділів сучасної математики, які утворюють підґрунтя для різноманітних криптографічних алгоритмів як зі секретним (симетричним) ключем, так зі відкритим (асиметричним) ключем. Подібні задачі пропонуються студентам для розв'язання на практичних (лабораторних) заняттях. Підбір типів задач визначався теоретичним матеріалом, що вдається розглянути в наявній кількості годин. Значна кількість типів задач залишилася за межами посібника. В той же час, мета розглянути всі типи задач і не ставилася.

Бібліографія

[BHSF] [1] *Бабенко Т.В.,Гулак Г.М.,Сушко С.О.,Фомичова Л.Я.* Криптологія у прикладах, тестах і задачах: навч. посібник. Дніпропетровськ: Нац. гірн. ун–т, 2013. 318 с.

[BM] [2] *Богуш В.М.,Мухачов В.А.* Криптографічні застосування елементарної теорії чисел. Навч. посібник. Київ. ДУІКТ, 2006. 126 с.

[Verb] [3] *Вербицький О.В.* Вступ до криптології. Львів, ВНТЛ, 1998. 248 с.

[VP] [4] *Вишенський В.А.,Перестюк М.О.* Комбінаторика: перші кроки. Кам'янець–Подільський. Аксіома, 2010. 324 с.

[KFSF] [5] *Кузнецов Г.В.,Фомичов В.В.,Сушко С.О.,Фомичова Л.Я.* Математичні основи криптографії: Навч. посібник, Ч. 1. Дніпропетровськ. Нац. гірн. ун–т, 2004. 391 с.

[S] [6] *Стасюк, Марта* Елементи математичних основ криптографії. Львів, ЛДУ БЖД, 2021. 216 с.

[CM] [7] *Cozzens M.,Miller S.J.* The Mathematics of Encryption. An Elementary Introduction. AMS, 2013. 332 p.

[Kobl] [8] *Koblitz, N.* A course in number theory and cryptography. Springer Science & Business Media, 1994. 235 p.

Зміст

Предметний покажчик

Міністерство освіти і науки України
ДВНЗ "Ужгородський національний університет"
Фізичний факультет
Кафедра твердотільної електроніки та інформаційної безпеки

Мисло Юлія Михайлівна, Пагіря Михайло Михайлович
Різак Василь Михайлович

МАТЕМАТИЧНІ ОСНОВИ КРИПТОГРАФІЇ

Методичний посібник до практичних занять

Підписано до друку ??.??.20??.
Формат 60x84/16. Гарнітура Bookman Old Style
Папір офсетний. Друк офсетний. Облік.–вид. арк. 3.0
Замовлення № ??. Наклад ??? прим.

Видавництво ????
Свідоцтво про державну реєстрацію видавців, виготівників
і розповсюджувачів видавничої продукції.
Серія ?? № ??? від ? вересня 20??? року.
88000, м. Ужгород, вул.