Міністерство освіти і науки України
Чорноморський національний університет імені Петра Могили

Кулаковська І. В.

ДИСКРЕТНА МАТЕМАТИКА.
Частина 1. Множини, відношення та математичні основи криптографії.

Методичні вказівки для виконання лабораторних робіт з дисципліни «Дискретна математика» студентами спеціальностей 121 «Інженерія програмного забезпечення», 122 «Комп'ютерні науки», 124 «Системний аналіз»

Випуск 362

Методичні вказівки

ЧНУ
ВИДАВНИЦТВО
Миколаїв – 2021

УДК 519, 854(076)
К 90

Рекомендовано вченою радою Чорноморського національного університету імені Петра Могили (протокол № 4 від 13 травня 2021 р.).

Рецензент:
Махровська Н. А., кандидат фізико-математичних наук, доцент кафедри теорії й методики природничо-математичної освіти та інформаційних технологій МОІППО.

К 90

Кулаковська І. В. Дискретна математика. Частина 1. Множини, відношення та математичні основи криптографії. Методичні вказівки для виконання лабораторних робіт з дисципліни «Дискретна математика» студентами спеціальностей 121 «Інженерія програмного забезпечення», 122 «Комп'ютерні науки», 124 «Системний аналіз» : методичні вказівки / І. В. Кулаковська. – Миколаїв : Вид-во ЧНУ ім. Петра Могили, 2021. – 100 с. – (Методична серія ; вип. 362).

Методичні вказівки містять теорію та завдання для самостійного виконання студентами лабораторних робіт під час вивчення основ теорії множин, відношень та математичних основ криптографії. Поряд із теоретичними відомостями наводяться приклади виконання завдань, програмно-алгоритмічні рішення, вимоги до оформлення звітів та контрольні запитання.

Методичні вказівки призначені для бакалаврів спеціальностей 121 «Інженерія програмного забезпечення», 122 «Комп'ютерні науки», 124 «Системний аналіз», які вивчають дисципліни «Дискретна математика» або «Дискретні структури та дискретна математика».

УДК 519, 854(076)

ISSN 1811-492X

Зміст

ВСТУП

Студенти факультета комп'ютерних наук вивчають «Дискретну математику» протягом перших двох семестрів. Майбутні фахівці в галузі інформаційних технологій вивчають актуальність основних концепцій та принципів дискретної математики. Методичні вказівки охоплюють матеріал 1 семестру. Оскільки основні способи подання та обробки інформації в інформаційних системах мають дискретний характер, тому вони є важливою частиною інформаційних технологій. Навчальний процес передбачає розвиток у студентів розуміння та використання сучасних моделей, дискретних методів обробки, аналізу та трансформації інформації.

Методичні вказівки містять відомості з теорії бінарних відношень, теорії множин та основ математичної криптографії, якій присвячено 11–15 лабораторні роботи. На початку кожної роботи є основні символи та визначення, які є важливими для успішного засвоєння предмета. Важливі поняття та терміни, які вперше з'являються в тексті, виділено курсивом. Більшість теоретичних концепцій проілюстровано на значущих прикладах.

Варто зазначити, що ці вказівки мають чітке практичне спрямування. Його основним завданням є розвиток навичок вирішення проблем з дискретними даними. Водночас пріоритет надається графічним та програмним методам вирішення проблеми, які, на думку автора, є більш очевидними та легшими для розуміння матеріалу.

Введення теорії дуже стисле. Читачі можуть знайти більше теоретичної інформації, перевірки тверджень та детальних міркувань щодо відповідних частин дискретної математики.

Практична робота № 1

Тема: Операції над множинами. Геометричне місце точок на площині. Декартів добуток множин

Мета: навчитися виконувати операції над множинами та представляти декартів добуток та ГМТ розв'язку задач на площині засобами програмного забезпечення Advanced Grapher.

Теоретичні відомості

Операції над множинами

Для множин можна ввести низку операцій ***(теоретико-множинних операцій)****, результатом виконання яких будуть також множини.*

Нехай A і B деякі множини.

А. Об'єднанням *множин A або B (позначається* $A \cup B$*) називається сукупність тих елементів, які належать хоча б одній з множин A або B. Символічно операція об'єднання множин записується так*:

$$A \cup B = \{ x \mid x \in A \text{ або } x \in B \}.$$

Б. Перетином *множин A і B (позначається* $A \cap B$*) називається множина, що утворена з тих і тільки тих елементів, які одночасно належать обом множинам. Тобто:*

$$A \cap B = \{ x \mid x \in A \text{ і } x \in B \}.$$

Множини A і B ***не перетинаються****, якщо вони не мають спільних елементів, або* $A \cap B = \varnothing$.

Операції об'єднання та перетину множин можуть бути поширені на випадок довільної кількості множин $\{A_i | i \in N\}$. *Так, об'єднання множин* A_i *(записується* $\bigcup_{i \in I} A_i$*) складається з тих елементів, які належать хоча б одній з множин* A_i *цієї сукупності. Перетин множин* A_i *(записується* $\bigcap_{i \in I} A_i$*) містить ті й тільки ті елементи, які одночасно належать кожній з множин* A_i.

В. Різницею *множин A без B (записується* $A \backslash B$*) називається множина тих елементів, які належать множині A та не входять до множини B. Отже,*

$$A \backslash B = \{ x \mid x \in A \text{ і } x \notin B \}.$$

Г. Симетричною різницею *множин A і B (записується* $A \Delta B$, $A \oplus B$, *або* $A \div B$*) називається множина, яка складається з усіх елементів множини A, які не містяться у B, а також усіх елементів множини B, які не містяться в A. Тобто:*

$$A \Delta B = \{x \backslash A | B \cup B | A\} = \{ x \mid x \in A \text{ і } x \notin B \text{ або } x \in B \text{ і } x \notin A \}.$$

Теоретико-множинні операції представимо **діаграмою Венна** (рис. 1).

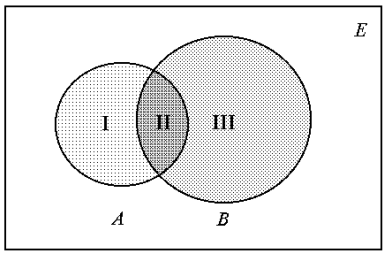


Рис. 1. Множини А, В

Тут множини А і В – це множини точок двох кругів. Тоді:

$A \cup B$ – складається з точок областей **I, II, III;**

$A \cap B$ – це область **II;**

$A \setminus B$ – область **I;**

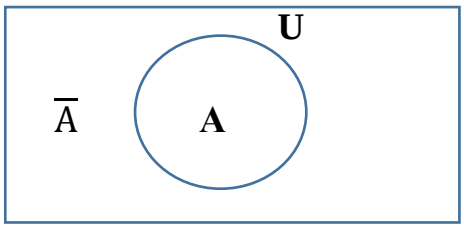
$B \setminus A$ – область **III;**

$A \Delta B$ – області **I** і **III**.

Д. У **математичній теорії** зручно припустити, що всі розглянуті множини є підмножинами певної фіксованої множини, яка називається ***універсальною*** і позначається ***E*** (або ***U***). Наприклад, в елементарній алгебрі такий повний набір можна розглядати як набір дійсних чисел ***R***, у вищій алгебрі – набір комплексних чисел ***C***, в арифметиці – набір цілих чисел ***Z***, у планіметрії – набір усіх точок площини або сукупність усіх геометричних об'єктів, множина прямих – набір точок на площині тощо.

Якщо універсальна множина ***U*** фіксована, існує доповнення множини $\overline{A}$ (***A*** це підмножина універсальної множини ***U***) – усі елементи універсальної множини, які не належать множині А. Тобто $\overline{A} = \{ x \mid x \in E \; i \; x \notin A \}$.

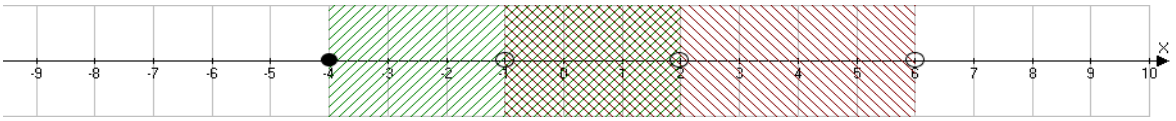
Неважко помітити, що $\overline{A} = U \setminus A$.



Завдання 1. Знайдіть множинні операції: об'єднання, переріз, різницю, доповнення та симетричну різницю множин:

а) $A = \{x \mid x \in R, -4 \le x < 2\}$; $B = \{x \mid x \in R, -1 < x < 6\}$.

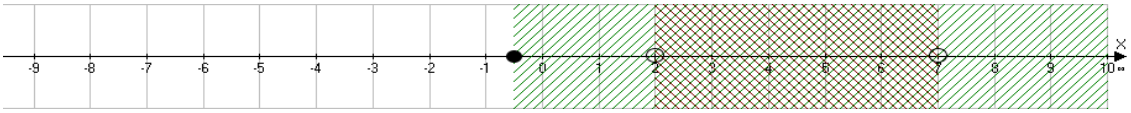
Зобразимо множини на числовій прямій.



$$A\cup B=[-4;6);\ A\cap B=(-1;2);\ A\setminus B=[-4;-1];\ B\setminus A=[2;6);$$
$$A\Delta B=[-4;-1]\cup[2;6);\ A'=(-\infty;-4)\cup[2;\infty);\ B'=(-\infty;-1]\cup[6;\infty).$$

б) $A=\left(-\frac{1}{2};\infty\right);\ B=(2;7).$

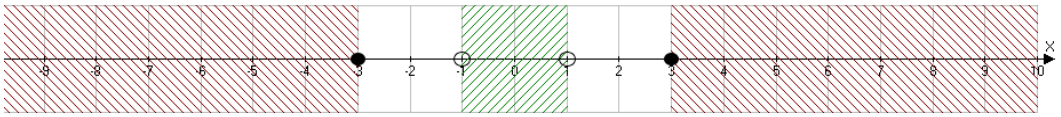
Зобразимо множини на числовій прямій.



$$A\cup B=\left(-\frac{1}{2};\infty\right);\ A\cap B=(2;7);\ A\setminus B=\left(-\frac{1}{2};2\right]\cup[7;\infty);\ B\setminus A=\varnichts;$$
$$A\Delta B=\left(-\frac{1}{2};2\right]\cup[7;\infty);\ A'=\left(-\infty;-\frac{1}{2}\right);\ B'=(-\infty;2]\cup[7;\infty).$$

в) $A=\{x\mid x\in R,|x|<1\},\ B=\{x\mid x\in R,|x|\geq 3\}.$

Зобразимо множини на числовій прямій.



Операції над цими множинами виконайте самостійно.

Представлення декартового добутку та ГМТ

Декартовим (прямим) добутком множин A і B (записується $A\times B$) називається множина всіх пар (a,b), у яких перший компонент належить множині A ($a\in A$), другий – множині B ($b\in B$).

Тобто $A\times B=\{(a,b)\mid a\in A \text{ і } b\in B\}$ або $(a,b)\in A\times B \Leftrightarrow \begin{cases}a\in A,\\ b\in B.\end{cases}$ (1.1)

Декартів добуток узагальнюється на випадок скінченної кількості множин. Якщо $A_1, A_2,..., A_n$ – множини, то декартовим добутком $A_1\times A_2\times...\times A_n$ називається множина $D=\{(a_1,a_2,...,a_n)\mid a_1\in A_1, a_2\in A_2,..., a_n\in A_n\}$, (1.2) яка складається з усіх наборів $(a_1,a_2,...,a_n)$, в кожному з яких i-й елемент називається ***і-ю координатою***, належить множині A_i, $i=1,2,...,n$.

Набір $(a_1,a_2,...,a_n)$, щоб відрізнити його від множини, яка складається з елементів $a_1,a_2,...,a_n$, записують не у фігурних, а в круглих дужках і називають ***кортежем***, ***вектором*** або ***впорядкованим набором***.

Операція декартового добутку неасоціативна і некомутативна, тобто множини $(A\times B)\times C$ і $A\times(B\times C)$, а також множини $A\times B$ і $B\times A$ нерівні між собою. Формули для застосування декартового добутку з іншими множинними операціями задаються тотожностями:

$$
\begin{aligned}
(A \cup B) \times C &= (A \times C) \cup (B \times C);\\
(A \cap B) \times C &= (A \times C) \cap (B \times C);\\
A \times (B \cup C) &= (A \times B) \cup (A \times C);\\
A \times (B \cap C) &= (A \times B) \cap (A \times C).
\end{aligned}
\qquad (1.3)
$$

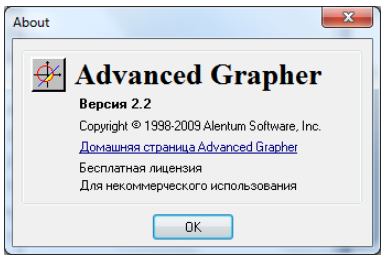
Методичні вказівки

Advanced Grapher представляє потужний і простий у використанні інструмент, що дозволяє виводити 8 типів графіків.

Програма Advanced Grapher підтримує побудову графіків функцій виду ***Y(x), X(y),*** у полярних координатах, заданих параметричними рівняннями, графіків таблиць, неявних функцій (рівнянь) і нерівностей.

Побудувати множину точок площини, що задовольняють співвідношенням:

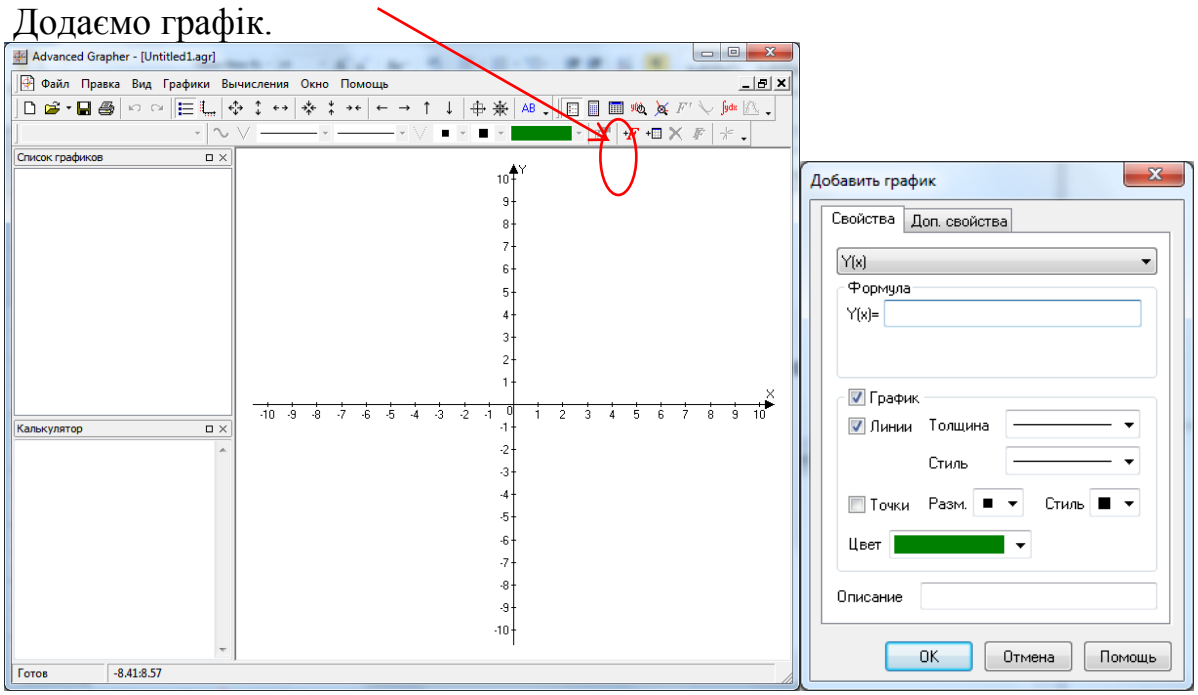
1. $\begin{cases} x^2 + y^2 \le 9; \\ x + 1 \ge 0; \\ x - 2 < 0. \end{cases}$



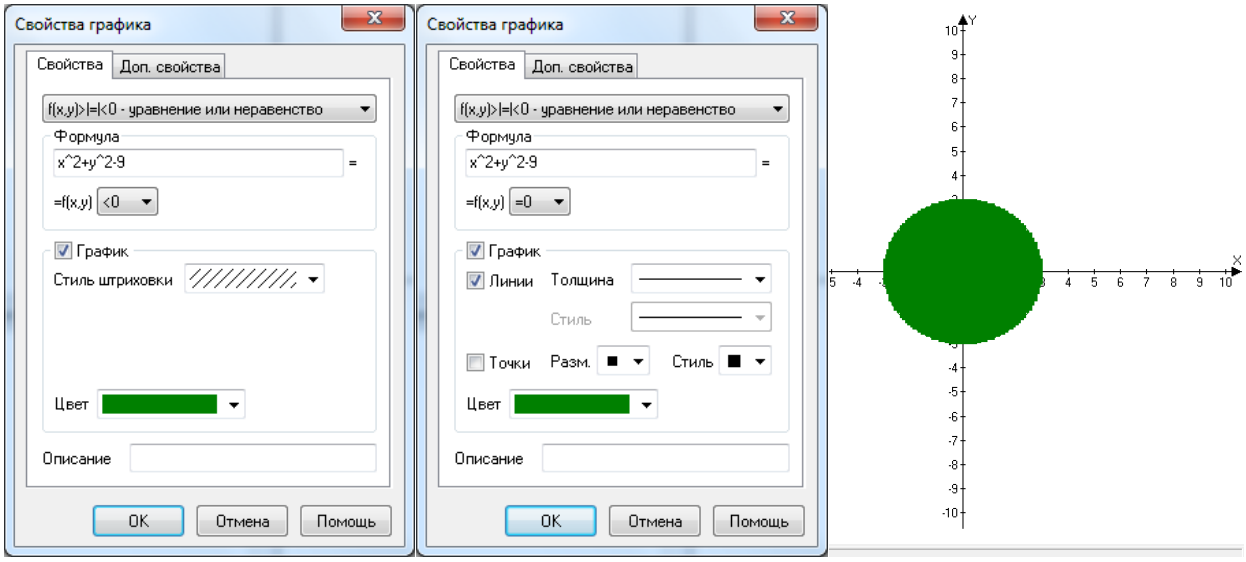
Запускаємо програму.

Детальніше: https://pro-spo.ru/winnauka/497-advanced-grapher-211.

Додаємо графік.

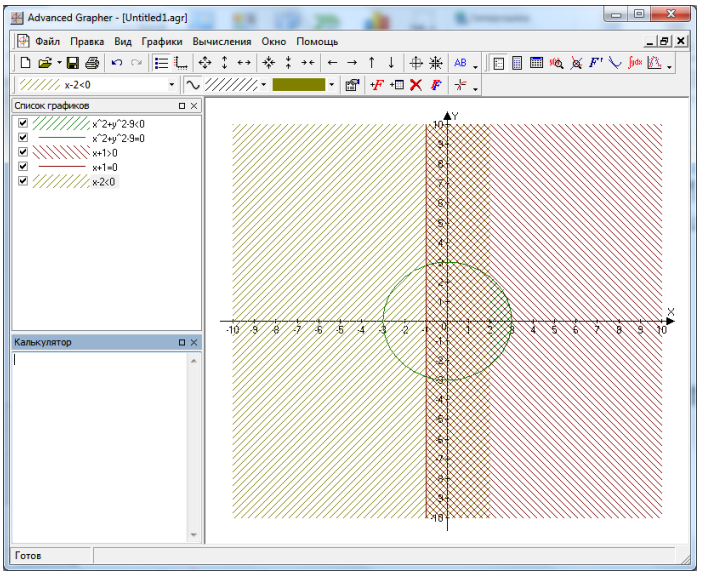


Нестрогі нерівності задаються двічі. Результат має вигляд:



Аналогічно задаються $x+1\geq 0$, $x-2<0$.

У результаті отримали ГМТ, відповіддю буде область, де є всі види штриховок, тобто:



Креслення можна зберегти як файл, або як малюнок.

Запис функцій аналогічний запису в мовах програмування або інструкцію далі.

2. $\begin{cases} x-2y\leq 2; \\ 2x+y\leq 1; \\ y\leq 2; \\ x\geq 3. \end{cases}$

Спочатку потрібно нерівності привести до стандартного виду (праворуч 0), внесемо їх границі, побудуємо відповідні прямі та знайдемо множину точок площини, які задовольняють цій системі нерівностей.

$$\begin{cases} y \ge \dfrac{x}{2} - 1; \\ y \le -2x + 1; \\ y \le 2; \\ x \ge 3. \end{cases}$$ Границі $$\begin{cases} y = \dfrac{x}{2} - 1; \\ y = -2x + 1; \\ y = 2; \\ x = 3. \end{cases}$$

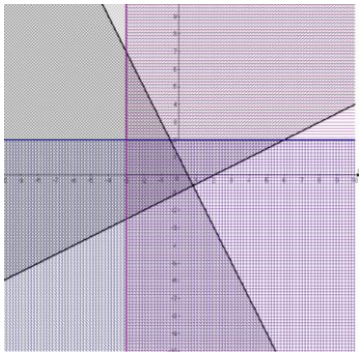


Рис. 2. Графік розв’язку

Шукану множину зображено на рис. 2)

3. $\begin{cases} x^2 + y - 1 \le 0 \\ x^2 - 2x - y - 3 < 0 \end{cases}$

Приводимо нерівності до стандартного виду, вносимо їх границі, побудуємо відповідні параболи та знайдемо множину точок площини, які задовольняють цій системі.

$$\begin{cases} y \le -x^2 + 1 \\ y > x^2 - 2x - 3 \end{cases} \qquad \begin{cases} y = -x^2 + 1 \\ y = x^2 - 2x - 3 \end{cases}$$

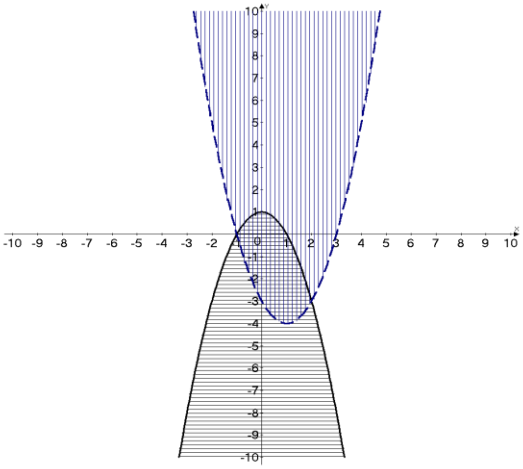


Рис. 3. Графік розв’язку

Відповідну множину зображено на рис. 3.

4. $$\begin{cases} \dfrac{x}{y} \le 0 \\ |y - x| \le 2 \end{cases} \rightarrow \left[\begin{cases} x \le 0 \\ y > 0 \\ |y - x| \le 2 \end{cases} \begin{cases} x \ge 0 \\ y < 0 \\ |y - x| \le 2 \end{cases} \right. \left[\begin{cases} x \le 0 \\ y > 0 \\ y - x \le 2 \\ y - x \ge -2 \end{cases} \begin{cases} x \ge 0 \\ y < 0 \\ y - x \le 2 \\ y - x \ge -2 \end{cases} \right. \left[\begin{cases} x \le 0 \\ y > 0 \\ y \le x + 2 \\ y \ge x - 2 \end{cases} \begin{cases} x \ge 0 \\ y < 0 \\ y \le x + 2 \\ y \ge x - 2 \end{cases} \right.$$

Перетворення. Система рівносильна сукупності систем.

Множину, точки якої задовольняють системі покажемо на рис. 4.

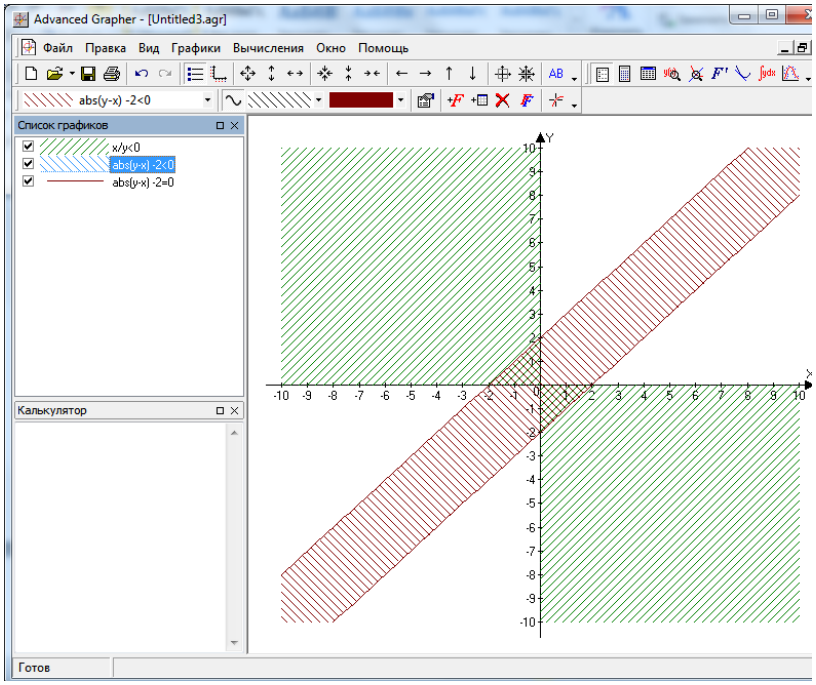


Рис. 4. Графік розв'язку

Як бачите, використання програми Advanced Grapher значно спрощує побудову графіків.

Інструкція

Вирази в Advanced Grapher складаються зі змінних, констант, чисел та функцій від них, з'єднаних операторами.

Функції. Під час використання функцій необхідно застосовувати синтаксис,

<Ім'я функції>(<Аргумент>).

Приклад: sin(x+2); ln(ln(1/x)); sin(x)^3.

Advanced Grapher підтримує наступні функції:

sin – синус;
cos – косинус;
tan – тангенс;
cot – котангенс;
asin – арксинус;
acos – арккосинус;
atan – арктангенс;
abs – модуль числа;
sqrt – квадратний корінь;
ln – натуральний логарифм;
lg – десятковий логарифм;
exp – експонента (exp(x) = e в степені x);
exp(1) = e=2,7182
int – ціла частина числа;
Pi = 3,1415;
round – округлення.
frac – дробова частина числа;
sign – знак числа,
sign(x)=1 при x>0,
sign(x)=0 при x=0 и
sign(x)=-1 при x<0;
sinh – гіперболічний синус;
cosh – гіперболічний косинус;
tanh – гіперболічний тангенс;
coth – гіперболічний котангенс;
asinh – гіперболічний арксинус;
acosh – гіперболічний арккосинус;
atanh – гіперболічний арктангенс;
acoth – гіперболічний арккотангенс;
random – random(x)=rnd(x);
rnd є випадкові значення, 0<=rnd<1.

Можна пропускати знак множення.
Приклад: xy, (x+1)(5y+x), xx, xsin(x).

Контрольні питання

1. Способи задання множин. Потужності.
2. Основні операції: перетин, об’єднання, симетрична різниця.
3. Діаграми Ейлера та діаграми Венна на універсумі. Основні закони.
4. Декартовий добуток. Перерізи.

Практична робота № 2

Тема: Підмножини. Булеан. Потужність множин

Мета: навчитися оцінювати потужність множин зважаючи на умови задачі, використовування діаграм Ейлера–Венна.

Теоретичні відомості

Для графічного зображення множини використовують спеціальні конструкції − діаграми Ейлера-Венна, які зображують сукупність елементів, що утворюють множину, овалами, а універсум − прямокутником. Відношення включення графічно зображено на рис. 1.

Скінчені власні підмножини певної множини можуть утворювати різноманітні сполучення з одного, двох, трьох тощо елементів цієї множини.

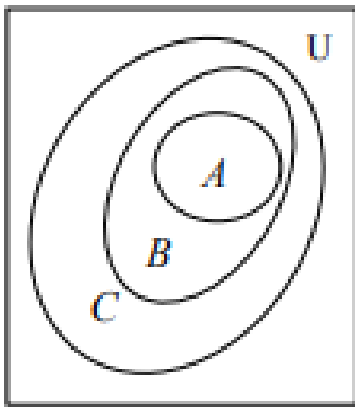


Рис. 1. Відношення включення $A \subset B \subset C \subset U$

Визначення. *Множиною всіх підмножин (булеаном) певної основної множини E називають множину, елементами якої є всі підмножини множини E. Позначається булеан через P(E) або* 2^E .

Він включає до свого складу також елементи $\emptyset$ та множину E.

Приклад. Якщо E = {a, b, c};
тоді, P(E) = {∅ , {a}, {b}, {c}, {a, b}, {a, c},{b, c}, {a, b, c}}.

УВАГА!

1. Порядок запису елементів у множині $P(E)$ є несуттєвий.
2. Якщо множина E включає n елементів, то множина $P(E)$ утворюється 2^n множинами, звідси й позначення множини P(E) як 2^E .
3. Відношення належності ∈ (елемент в множину) та включання ⊂ (множина в множину) − різні поняття.

Наприклад, множина А може бути власною підмножиною множини А($A \subset A$), але вона не може бути власним елементом цієї множини ($A \notin A$).

Метод включення і виключення

Для будь-яких скінченних двох множин А та В виконується рівність:

$$|A \cup B| = |A| + |B| - |A \cap B|.$$

Самостійно доведіть для випадку трьох множин рівність:

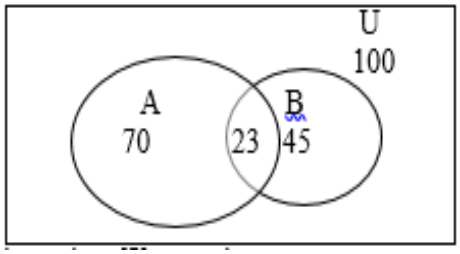
$$|A \cup B \cup C| = |A| + |B| + |C| - |A \cap B| - |A \cap C| - |B \cap C| + |A \cap B \cap C|.$$

Ці рівності є частковими випадками принципу включення-виключення.

Методичні вказівки

І тип

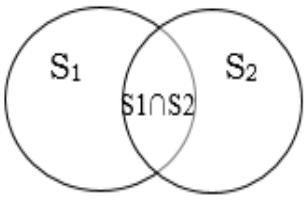
1. У групі що складається зі 100 туристів 70 осіб знає англійську мову, 45 – знають французьку і 23 туриста знають обидві мови. Скільки туристів у групі не знають ні англійської ні французької мови? Розв’язати за допомогою діаграм Ейлера–Вена.



n(AUB)=n(A)+n(B)–n(A∩B),
n(A∩B)= 70+45–23= 92
(туристи, які знають хоча б одну мову),
Не знають жодної іноземної мови:
100–92= 8 (туристів).

Відповідь: жодної іноземної мови не знають 8 туристів.

2. Відстань між містами 440 км. З цих міст назустріч одне одному виїхало 2 автомобілі зі швидкістю 50 км/год. і 60 км/год. Яка відстань буде між ними через 5 год.?

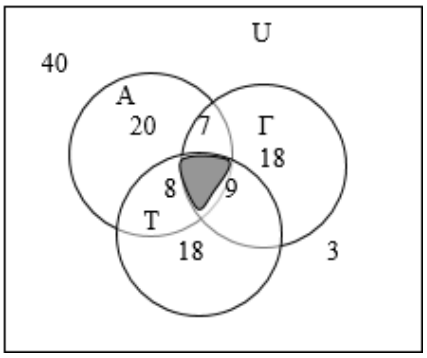


n(S1US2)=n(S1)+n(S2)–n(S1∩S2),
n(S1US2)= 440 (км) – весь шлях,
S1 = 50*5= 250 (км),
S2 = 60*5= 300 (км)
n(S1∩S2)= 250+ 300–440=110 (км)

Відповідь: через 5 год. відстань між автомобілями буде 110 км.

3. В олімпіаді з математики брали участь 40 учнів. Їм було запропоновано розв’язати одну задачу з алгебри, одну з геометрії, одну з тригонометрії. Результати перевірки розв’язання внести у таблицю:

Розв'язані задачі:	Правильно розв'язали:
з алгебри	20
з геометрії	18
з тригонометрії	18
з алгебри і геометрії	7
з алгебри і тригонометрії.	8
з геометрії і тригонометрії	9



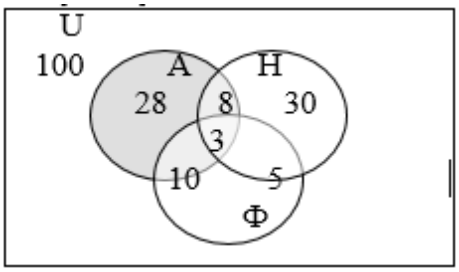
Троє учнів не розв'язали жодної із запропонованих задач. Скільки учнів розв'язали всі три задачі? Скільки учнів розв'язали рівно дві задачі?

$$n(A\cup\Gamma\cup T) = n(A)+ n(\Gamma)+ n(T)–n(A\cap\Gamma)–n(A\cap T)–n(\Gamma\cap T)+n(A\cap\Gamma\cap T),$$
$$40–3=20+18+18–7–8–9+n(A\cap\Gamma\cap T),$$
$$n(A\cap\Gamma\cap T)=5 \text{ (учнів)}.$$

Рівно 2 задачі розв'язали $n(X\cap У)–n(A\cap\Gamma\cap T)$ з алгебри і геометрії: 7–5=2, з алгебри і тригонометрії: 8–5= 3, з геометрії і тригонометрії: 9–5= 4.

Відповідь: усі три задачі розв'язали 5 учнів, рівно 2 задачі розв'язали 9 учнів.

4. Зі 100 студентів англійську мову вивчають 28, німецьку – 30, французьку – 42, англійську і німецьку – 8, англійську і французьку – 10, німецьку і французьку – 5, англійську, німецьку і французьку – 3. Скільки студентів не вивчають жодної мови? Скільки студентів вивчають тільки одну іноземну мову?



$n(AUHUФ)=n(A)+n(H)+n(Ф)–n(A\cap H)–n(A\cap Ф)–n(H\cap Ф)+n(A\cap H\cap Ф)$,
$n(AUHUФ)=28+30+42–10–8–5+3=80$,
Не вивчає жодної мови 100–80=20.
Тільки англійську (штрихова).

$$n(A)–n(A\cap H)–n(A\cap Ф)+n(A\cap H\cap Ф)= 28–10–8+3=13$$

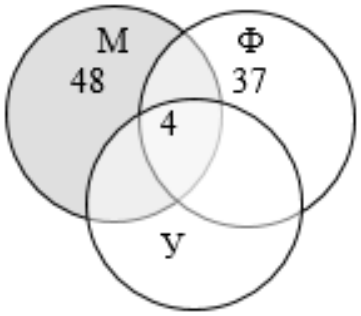
Тільки німецьку: $n(H)–n(A\cap H)–n(H\cap Ф)+n(A\cap H\cap Ф)= 30–5–8+3=20$,
тільки французьку: $n(Ф)–n(Ф\cap H)–n(H\cap Ф)+n(A\cap H\cap Ф)= 42–10–5+3=30$.
Тільки одну мову вивчають відповідно 13+20+30=63 (студенти).

Відповідь: не вивчають жодної мови 20 студентів, тільки одну мову вивчають 63 студенти.

II тип

5. Серед абітурієнтів зарахованих після іспитів до ЗВО оцінку «відмінно» отримали: з математики – 48 абітурієнтів, з фізики – 37, з української мови – 42, з математики або фізики – 75, з математики або української мови – 76, з фізики або української мови – 66, з усіх трьох предметів – 4. Скільки абітурієнтів

отримали хоча б одну «5»? Скільки серед них отримали тільки одну «5»? (немає універсальної множини!).



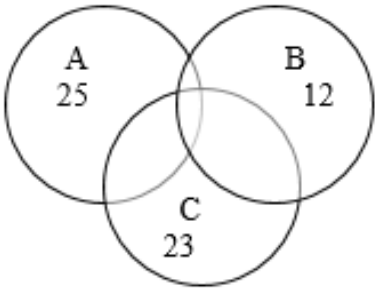
n(MUФ)=n(M)+n(Ф)–n(M∩Ф),
n(M∩Ф)= 48+37–75=10.
Аналогічно:
n(M∩У)= 48+42–46=14,
n(У∩Ф)= 37+42–66=13.
Хоча б одна оцінка «відмінно»,
n(MUФUУ)=n(M)+n(Ф)+n(У)–n(M∩Ф)–n(M∩У)–
n(Ф∩У)+n(M∩Ф∩У)–
n(MUФUУ)=48+37+42–10–14–13+4=–94.

Тільки одну «5» з математики: 48–10–14+4=28.
Тільки одну «5» з фізики: 37–10–13+4=18.
Тільки одну «5» з української мови: 42–14–13+4=19.
«Відмінно» тільки з одного предмета: 28+18+19=65 (абітурієнтів).
Відповідь: хоча б одна оцінка «5» у 94, а тільки одна у 65 абітурієнтів.

ІІІ тип (задачі з деякими неявними даними)

6. Кожен з учнів класу на зимових канікулах рівно двічі був у театрі, спектаклі А, В і С відвідали відповідно 25, 12 і 23 учні. Скільки учнів у класі? Скільки з них бачили спектаклі А і В, А і С, В і С.

Усього відвідувань театру більше ніж учнів у класі рівно в два рази.



(25 +12 +23) :2= 30 (учнів в класі).
n(AUC)= n(A)+ n(C)+ n(A∩C),
n(A∩C)= 25 +23 –30= 18 (учнів).
n(AUB)= n(A)+ n(B)+ n(A∩B),
n(A∩B)= 25 +12 –30= 7 (учнів).
n(BUC)= n(B)+ n(C)+ n(B∩C),
n(B∩C)= 23 +12 –30= 5 (учнів).

Відповідь: усього в класі 30 учнів. Спектаклі А і В відвідали 7, А і С – 18, В і С – 5 учнів.

Для розв'язування в аудиторії

7. У кондитерському відділі магазину покупці вибирають або одну коробку цукерок, або один торт, чи торт і коробку цукерок. Одного дня було продано 57 тортів і 36 коробок цукерок. Скільки було покупців, якщо 12 осіб купили і торт і коробку цукерок.

8. У дитячому садку 52 дитини. Кожній з них подобається або торт, або морозиво. Половина дітей вибрала торт, а 20 – морозиво і торт. Скільки дітей вибрали морозиво?

9. На аркуші накреслили круг площею 78 см² і квадрат площею 55 см². Площа перетину круга і квадрата дорівнює 30 см². Вільна від круга і квадрата частина аркуша має площу 150 см². Знайти площу аркуша.

10. У бригаді працює 25 робітників. Серед них 20 робітників мають вік до 30 років і 15 робітників більше 20 років. Чи можливо таке?

11. У класі 40 чоловік. Грають у баскетбол 26, у волейбол – 25, у футбол – 27, одночасно займаються баскетболом і волейболом – 15, баскетболом і футболом – 16, волейболом і футболом – 18. Один з учнів звільнений від фізкультури. Скільки чоловік займаються всіма видами спорту? Скільки чоловік займається тільки одним видом спорту?

12. У звіті про опитування 100 студентів повідомлялось, що кількість студентів, які вивчають різні мови така: всі три мови – 3, французьку і англійську – 8, німецьку і англійську – 10, німецьку і французьку – 20, англійську – 30, німецьку – 23, французьку – 50. Звіт не був затверджений. Чому?

13. Зі 100 студентів лише німецьку мову вивчають 18, німецьку, але не англійську – 23, німецьку і французьку – 8, німецьку – 26, французьку – 48, англійську і французьку – 8, ніякої мови не вивчають – 24. Скільки студентів вивчають англійську мову? Скільки вивчають англійську і німецьку мови, але не французьку? Скільки студентів вивчають французьку мову в тому і тільки в тому випадку, якщо вони не вивчають англійську?

14. Зі 160 студентів І курсу кулінарного технікуму 120 уміють готувати і 80 уміють сервірувати стіл. Скільки студентів уміють і готувати і сервірувати, якщо не вміють нічого 15 студентів?

15. У школі 1000 учнів, 830 з них уміють грати в шашки, 650 – в шахи. Ні в шашки, ні в шахи не вміють грати 40 осіб. Скільки учнів не вміють грати ані в шахи, ані в шашки?

16. Із 25 учнів 12 цікавляться математикою, 8 – фізикою. Яким може бути число учнів які цікавляться двома предметами? Скільки учнів цікавляться хоча б одним предметом?

17. З 90 школярів 50 грають у футбол, а 55 – у волейбол. Яким може бути число школярів які грають в обидві гри? Скільки хоча б в одну з цих ігор?

18. На уроці літератури вчитель вирішив дізнатися, хто із 40 учнів класу читав книги A, B і C. Результати опитування виявилися такими: книгу A читали 25 учнів, книгу B – 22, книгу C також 22. Книгу A або B – 33 учні, A або C – 32, B або C – 31, всі три книги прочитали 10 учнів. Скільки учнів прочитали тільки одну книгу? Скільки учнів не читали жодної з цих книг?

19. Вибрана деяка множина натуральних чисел. Серед них 150 чисел кратних «2», 100 кратних «3», 115 кратних «5», 55 кратних «6», 42 кратних «10», 30 кратних «15», 20 кратних «30». Скільки елементів у заданій множині?

20. У школі 1400 учнів. 1250 учнів уміють кататися на ковзанах, 952 – на лижах, не вміють кататися ні на ковзанах, ні на лижах 60 учнів. Скільки учнів уміють кататися і на лижах і на ковзанах?

21. **Задача Льюїса Керрола.** У жорстокому бою 70 зі 100 піратів втратили одне око, 75 – одне вухо, 80 – одну руку і 85 – одну ногу. Яке мінімальне число тих, хто втратив одночасно око, руку, вухо, ногу? Відповідь: мінімально 10 осіб.

22. Із 40 програмістів 18 володіють мовою Pascal, 19 – мовою C++, 21 – мовою Java. Відомо, що 10 програмістів знають одночасно Pascal і C++, 7 – Pascal і Java, 8 – C++ і Java. Троє програмістів не володіють жодною із мов Pascal, C++, Java. Знайти кількість програмістів, які одночасно знають усі три мови програмування.

23. Нехай A – множина трикутників, B – множина чотирикутників, C – множина правильних многокутників, D – множина многокутників, які мають принаймні один прямий кут, E – множина рівносторонніх многокутників.

Вказати множини: 1) $\big((D \cap A)\Delta E\big)(A \cap C)$; 2) $\overline{B \cap (C \cup D)} \cap E \cap B$.

Контрольні питання

1. Способи задання множин. Потужності.
2. Основні операції: перетин, об’єднання, симетрична різниця.
3. Круги Ейлера, діаграми Венна на універсумі. Основні закони.
4. Декартовий добуток. Перерізи.
5. Формули включення виключення для двох та трьох множин.

Практична робота № 3
Тема: Відношення та їх властивості

Мета: навчитися аналізувати множини у яких реалізовані зв'язки між об'єктами, визначати сюр'єкцію, ін'єкцію та бі'єкцію, вивчити властивості відношень: порядку, еквівалентності та ін.

Теоретичні відомості

Підмножина R декартового степеня M^n деякої множини M називається ***n-місним*** *або* ***n-арним відношенням на множині M.*** Елементи $a_1,a_2,...,a_n \in M$ знаходяться у відношенні *R*, якщо $(a_1,a_2,...,a_n) \in R$.

Якщо $n=1$ відношення $R \subseteq M$ називають **одномісним** або **унарним**.

Найбільш популярними у математиці є **двомісні** або **бінарні** відношення. Далі скрізь під словом «відношення» розумітимемо бінарне відношення. Якщо елементи $a,b \in M$ знаходяться у відношенні *R*, тобто $(a,b) \in R$, то це часто записують також у вигляді *aRb*.

Відношення можна задавати такими ж самими способами, що й звичайні множини. Крім того, зручним способом задання бінарного відношення *R* на скінченній множині $M=\{a_1,a_2,...,a_n\}$ є задання за допомогою так званої **матриці бінарного відношення**. Це квадратна матриця *C* порядку *n*, у якій елемент c_{ij}, що стоїть на перетині *i*-го рядка і *j*-го стовпчика, визначається так: $c_{ij} = 1$, якщо a_iRa_j, $c_{ij} = 0$ в іншому разі.

Відношення можна задавати також за допомогою графіків і діаграм. **Графік відношення** визначається й будується так само, як і графік відповідності. Поняття діаграми (або графа) відношення також можна визначити аналогічно до відповідності. Однак частіше **діаграма** (або граф) **відношення** R на скінченній множині $M=\{a_1,a_2,...,a_n\}$ визначається таким чином. Поставимо у взаємно однозначну відповідність елементам множини M деякі точки площини. З точки a_i до точки a_j проводимо напрямлену лінію (стрілку) у вигляді відрізка або кривої тоді і тільки тоді, коли a_iRa_j. Зокрема, якщо a_iRa_i, то відповідна стрілка, що веде з a_i в a_i, називається **петлею.**

Оскільки відношення на M є підмножинами множини M^2, то для них визначені всі відомі теоретико-множинні операції. Наприклад, перетином відношень «більше або дорівнює» і «менше або дорівнює» є відношення «дорівнює», об'єднанням відношень «менше» і «більше» є відношення «не дорівнює», доповненням відношення «ділиться на» є відношення «не ділиться на» тощо. Аналогічно відповідностям для відношень можна визначити поняття оберненого відношення і композиції відношень.

Відношення R^{-1} *називається* ***оберненим*** *до відношення R, якщо* $bR^{-1}a$ *тоді і тільки тоді, коли aRb.* Очевидно, що $(R^{-1})^{-1}=R$. Наприклад, для відношення «більше або дорівнює» оберненим є відношення «менше або дорівнює», для відношення «ділиться на» – відношення «є дільником».

Композицією *відношень R_1 і R_2 на множині M (позначається $R_1 \circ R_2$) називається відношення R на M таке, що aRb тоді і тільки тоді, коли існує елемент $c \in M$, для якого виконується aR_1c і cR_2b.*

Для відношення R на множині M через $R^{(k)}$ позначено відношення R°R°...°R (k разів). Вважаємо, що $R^{(0)}=i_M$ і $R^{(1)}=R$.

Наведемо список властивостей, за якими класифікують відношення.

Нехай R – деяке відношення на множині M .

*1. Відношення R називається **рефлексивним**, якщо для всіх $a \in M$ має місце aRa.*

*2. Відношення R називається **антирефлексивним (іррефлексивним)**, якщо для жодного $a \in M$ не виконується aRa.*

*3. Відношення R називається **симетричним**, якщо для всіх $a,b \in M$ таких, що aRb маємо bRa.*

*4. Відношення R називається **антисиметричним**, якщо для всіх $a,b \in M$ таких, що aRb і bRa маємо a=b.*

*5. Відношення R називається **транзитивним**, якщо зі співвідношень aRb і bRc випливає aRc.*

Відношення R* називається **транзитивним замиканням** відношення R на M, якщо для $a,b \in M$ aR*b тоді і тільки тоді, коли у множині M існує послідовність елементів $c_1,c_2,...,c_n$ така, що $c_1=a$, $c_n=b$ і $c_1Rc_2,c_2Rc_3,...,c_{n-1}Rc_n$. Вважаємо, що $i_M \subseteq R^*$.

Відношення R на множині M називається **толерантним** (відношенням толерантності або просто толерантністю), якщо воно рефлексивне і симетричне.

Приклад. Наведемо приклади бінарних відношень на різних множинах.

1. Відношення на множині N натуральних чисел:

R_1 – відношення «менше або дорівнює», тоді $4R_19$, $5R_15$, $1R_1m$ для будь-якого $m \hat{I} N$;

R_2 – відношення «ділиться на», тоді $4R_23$, $49R_27$, mR_21 для будь-якого $m \hat{I} N$;

R_3 – відношення «є взаємно простими», тоді $15R_38$, $366R_3121$, $1001R_3612$;

R_4 – відношення «складаються з однакових цифр», тоді $127R_4721$, $230R_4302$, $3231R_43213311$.

2. Відношення на множині точок координатної площини R^2:

R_5 – відношення «знаходяться на однаковій відстані від початку координат», тоді $(3,2)\ R_5\ (\ ,-\ )$, $(0,0)R_5(0,0)$;

R_6 – відношення «симетричні відносно осі ординат», тоді $(1,7)R_6(-1,7)$ і взагалі $(a,b)R_6(-a,b)$ для будь-яких $a,b \hat{I} R$;

R_7 – відношення «менше або дорівнює». Вважаємо, що $(a,b)R_7(c,d)$, якщо $a \pounds c$ і $b \pounds d$. Зокрема, $(1,7)R_7(20,14)$, $(-12,4)R_7(0,17)$.

3. Відношення на множині студентів цього закладу:

R_8 – відношення «є однокурсником»,

R_9 – відношення «є молодшим за віком від»,

R_{10} – відношення «бути другом».

Відношення еквівалентності

Відношення R на множині M називається ***відношенням еквівалентності*** *(або просто еквівалентністю), якщо воно рефлексивне, симетричне і транзитивне, тобто:*

а) aRa для всіх a ∈ M (рефлексивність);

б) якщо aRb, то bRa для a,b ∈M (симетричність);

в) якщо aRb і bRc, то aRc для a,b,c ∈M (транзитивність).

Сукупність множин $\{ B_i | i \in I \}$ називається **розбиттям множини** A, якщо $\bigcup_{i \in I} B_i = A$ і $B_i \cap B_j = \varnothing$ *для* $i \neq j$. Множини B_i, $i \in I$ є підмножинами множини A і називаються **класами**, **суміжними класами**, **блоками** або **елементами** розбиття. Очевидно, що кожен елемент $a \in A$ належить одній і тільки одній множині B_i, $i \in I$.

Припустимо, що на множині M задано відношення еквівалентності R. Виконаємо таку побудову. Виберемо деякий елемент $a \in M$ і утворимо підмножину $S_a^R = \{ x \mid x \in M \text{ і } aRx \}$, яка складається з усіх елементів множини M еквівалентних елементу k. Відтак, візьмемо другий елемент $b \in M$ такий, що $b \notin S_a^R$ і утворимо множину $S_b^R = \{ x | x \in M \text{ і } bRx \}$ з елементів еквівалентних b і т. д. Таким чином одержимо сукупність множин (можливо, нескінченну) $\{ S_a^R, S_b^R, \ldots \}$.

Побудована сукупність множин $\{ S_i^R | i \in I \}$ називається **фактор-множиною** множини M за еквівалентністю R і позначається M/R. Очевидно, що будь-які два елементи з одного класу еквівалентні між собою, тоді, як будь-які два елементи з різних класів фактор-множини M/R нееквівалентні. Класи S_i^R називають **класами еквівалентності** за відношенням R. Клас еквівалентності, який містить елемент x, часто позначають $[x]_R$.

Потужність фактор-множини |M/R| називається **індексом розбиття**, або **індексом** відношення еквівалентності R.

Нехай R відношення еквівалентності на множині M. Відображення множини M на фактор-множину M/R, яке кожному елементу $x \in M$ ставить у відповідність клас еквівалентності $[x]_R$, якому належить елемент x, називається **канонічним** або **природним відображенням** множини M на фактор-множину M/R.

Відношення часткового (нестрогого) порядку.

Відношення R на множині M називається відношенням ***часткового (нестрогого) порядку****, якщо воно рефлексивне, антисиметричне і транзитивне, тобто:*

а) aRa для всіх a ∈M (рефлексивність);

б) якщо aRb і bRa, то a=b (антисиметричність);

в) якщо aRb і bRc, то aRc (транзитивність).

Множина M, на якій задано деякий частковий порядок, називається **частково впорядкованою** множиною. Елементи $a,b \in M$ назвемо **порівню-ваними** за відношенням R, якщо виконується aRb або bRa.

Частково впорядкована множина M, у якій будь-які два елементи є порівнюваними між собою, називається **лінійно впорядкованою** множиною або **лан-**

цюгом. Відповідне відношення R, задане на лінійно впорядкованій множині, називається **лінійним (досконалим) порядком**. Таким чином, відношення R на множині M називається відношенням лінійного порядку, якщо воно рефлексивне, антисиметричне, транзитивне і для будь-якої пари елементів $a,b \in M$ виконується aRb або bRa.

Для позначення відношень порядку будемо використовувати знаки ≤ і ≥. Тобто для відношення порядку R замість aRb будемо записувати $a \le b$ або $b \ge a$ і читати «a менше або дорівнює b» або «b більше або дорівнює a» відповідно. Очевидно, що ≤ є оберненим відношенням до відношення ≥. Порядок ≥ іноді називають **двоїстим** порядком до ≤.

За кожним відношенням часткового порядку ≤ на довільній множині M можна побудувати інше відношення < на M, припустимо $a < b$ тоді і лише тоді, коли $a \le b$ і $a \ne b$. Це відношення називається відношенням **строгого порядку** на множині M.

Зрозуміло, що відношення строгого порядку антирефлексивне, транзитивне, а також задовольняє умову так званої **сильної антисиметричності** або **асиметричності**, тобто для жодної пари $a,b \in M$ не може одночасно виконуватися $a < b$ і $b < a$.

Зафіксуємо строгий порядок розташування символів у довільному скінченному алфавіті $A=\{a_1,a_2,...,a_n\}$, наприклад, припустимо, що $a_1<a_2<...<a_n$. Тоді природним чином визначається так званий **лексикографічний порядок** на множині A^m усіх слів довжини m в алфавіті A, а саме: вважаємо $a_{j1}a_{j2}...a_{jm} \le a_{l1}a_{l2}...a_{lm}$ тоді і тільки тоді, коли $a_{js}=a_{ls}$ при $s=1,2,...,k-1$ і $a_{jk}<a_{lk}$ для певного $k=1,2,...,m$.

Лексикографічний порядок можна поширити на множину A* всіх слів в алфавіті A, якщо доповнити алфавіт A додатковим («порожнім») символом p і вважати, що $p<a_i$, $i=1,2,...,n$. Під час порівнювання двох слів різної довжини спочатку слово меншої довжини доповнюється з правої сторони такою кількістю «порожніх» символів p, щоб зрівнятися за довжиною з другим словом, після чого обидва слова порівнюються за правилом порівнювання слів однакової довжини.

Нехай $A=\{a,b,c\}$ і $a<b<c$, тоді $aac<aba$, $abbc<abcb$, $ab<abab$, $b<cba$ тощо.

Лексикографічний порядок лежить в основі упорядкування всіх словників, енциклопедій, індексів (предметних або іменних покажчиків), довідників, списків, таблиць тощо.

Методичні вказівки

Приклад. Нехай задано множину $A=\{1,2,3,4,5\}$. До якого типу належить відношення і вкажіть його властивості.

$$R=\{(1,1),(2,2),(3,3),(4,4),(5,5),(1,3),(1,5),(3,1),(3,5),(5,1),(5,3)\}.$$

Розв’язок. Представимо відношення у вигляді таблиці.

	1	2	3	4	5
1	1		1		1
2		1			
3	1		1		1
4				1	
5	1		1		1

1. Головна діагональ – всі 1 – відношення R рефлексивне.
2. Для всіх пар (a,b)=><=(b,a): (1,3)=(3,1), (1,5)=(5,1), (3,5)=(5,3) – відношення R симетричне. Відношення не є антисиметричним, тому що наприклад з (1,3) *є R та* (3,1) *є R* не випливає що 1=3.
3. Відношення R транзитивне, оскільки:

Випадок	***(a,b) є R***	***(b,c) є R***	***(a,c) є R***	***(a,b)є R***
1	(1,3)	(3,1)	(1,1)	так
2	(1,3)	(3,5)	(1,5)	так
3	(3,1)	(1,3)	(3,3)	так
4	(3,1)	(1,5)	(3,5)	так
5	(5,1)	(1,3)	(5,3)	так
6	(5,1)	(1,5)	(5,5)	так
7	(5,3)	(3,1)	(5,1)	так
8	(5,3)	(3,5)	(5,5)	так

Приклад. Нехай маємо множину M={a, b, c, d}. Відношення на M задане за допомогою матриці R. Визначити властивості цього відношення та його тип.

R:

	a	b	c	d
a			1	1
b				1
c	1			
d	1	1		

Побудувати діаграму. Визначити тип відношення.

Контрольні питання

1. Відношення. Властивості відношень.
2. Обернене відношення. Композиції відношень. Приклади.
3. Рефлексивність, антирефлексивність. Граф.
4. Симетричність, асиметричність. Антисиметричність.
5. Транзитивність. Приклад.
6. Відношення еквівалентності. Приклад.
7. Відношення нестрогого порядку. Граф.

Практична робота № 4
Тема: Алгоритм Евкліда

Мета: повторення методів знаходження найбільшого спільного дільника і найменшого спільного кратного та їх використання.

Теоретичні відомості

Якщо кожне з цілих чисел $a_1,a_2,\ldots,a_n$ ділиться на ціле число d, то число d називають *спільним дільником* чисел $a_1,a_2,\ldots,a_n$ Найбільший із спільних дільників чисел $a_1,a_2,\ldots,a_n$ називається *найбільшим спільним дільником* (НСД) цих чисел і позначається символом $a_1,a_2,\ldots,a_n$.

Якщо найбільший спільний дільник чисел $a_1,a_2,\ldots,a_n$ дорівнює 1, то ці числа називають *взаємно простими.*

Нехай $a_1,a_2,\ldots,a_{n-1},a_n$ – будь-які цілі числа, серед яких хоч одне відмінне від нуля. Нехай $(a_1,a_2)=d_2$, $(d_2,d_3)=d_3,\ldots,(d_{n-2},a_{n-2})=d_{n-1}$, $(d_{n-1},a_n)=d_n$. Тоді $a_1,a_2,\ldots,a_n=(((a_1,a_2),a_3),\ldots)$. На основі цього факту можна дати визначення найбільшого спільного дільника.

Найбільшим спільним дільником чисел $a_1,a_2,\ldots,a_n$ називають невід'ємний спільний дільник цих чисел, який ділиться на будь-який їхній спільний дільник.

Якщо $a \vdots b$, то $(a,b)=|b|$.

Якщо $a=bq+r$, де a,b,q,r – цілі числа, то $(a,b)=(b,r)$.

Якщо a,b,m – цілі числа, то $(am,bm)=(a,b)\cdot|m|$.

Якщо a,b – цілі числа, а k – який-небудь їхній спільний дільник, то $\left(\frac{a}{k},\frac{b}{k}\right)=\frac{(a,b)}{|k|}$ (при цьому хоч одне з чисел a чи b відмінне від нуля).

Якщо $(a,b)=d$, то $\left(\frac{a}{d},\frac{b}{d}\right)=1$.

Якщо $d\mid a \wedge d\mid b$ і $\left(\frac{a}{d},\frac{b}{d}\right)=1$, то $|d|=(a,b)$.

Для знаходження найбільшого спільного дільника двох чисел користуються способом послідовного ділення, який називають алгоритмом Евкліда.

Розглянемо цей спосіб. Якщо a і b натуральні числа, то за теоремою про ділення з остачею послідовно знаходимо:

$$a = bq_1 + r_1, \quad \text{де } 0 < r_1 < b,$$
$$b = r_1 q_2 + r_2, \quad \text{де } 0 < r_2 < r_1,$$
$$r_1 = r_2 q_3 + r_3, \quad \text{де } 0 < r_3 < r_2,$$
$$\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots$$
$$r_{n-2} = r_{n-1} q_n + r_n, \quad \text{де } 0 < r_n < r_{n-1}, \ \mathbf{r_n} - \textbf{НСД}$$
$$r_{n-1} = r_n q_{n-1}, \quad \text{де } r_{n+1} = 0.$$

Остання відмінна від нуля остача r_n і є найбільшим спільним дільником чисел a і b.

Згідно з алгоритмом Евкліда, якщо $(a,b)=d$, то існують такі цілі числа x і y, що $d=ax+by$, і навпаки (лінійне зображення найбільшого спільного дільника).

Нехай $a_1,a_2,\ldots,a_n$ – відмінні від нуля цілі числа. Ціле число k, яке ділиться на всі цілі числа $a_1,a_2,\ldots,a_n$, називають *спільним кратним* цих чисел. Найменше з додатних спільних кратних чисел $a_1,a_2,\ldots,a_n$ називають *найменшим спільним кратним* (НСК) цих чисел і позначають символом $[a_1,a_2,\ldots,a_n]$.

Відомо, що $\left[a,b\right] = \dfrac{ab}{\left(a,b\right)}$, де a, b – довільні цілі числа, з яких хоча б одне відмінне від нуля. Ця формула лежить в основі першого способу знаходження найменшого спільного кратного двох чисел. Зокрема, найменше спільне кратне взаємно простих чисел дорівнює їхньому добутку.

Нехай $[a_1,a_2]=m_2$, $[m_2,a_3]=m_3$, …, $[m_{n-2},a_{n-1}]=m_{n-1}$, $[m_{n-1},a_n]=m_n$. Тоді $[a_1,a_2,\ldots,a_n]=m_n$. Це дає змогу звести питання знаходження НСК кількох чисел до питання знаходження НСК двох чисел:$[a_1,a_2,\ldots,a_n]=[\ldots[[a_1,a_2],a_3],\ldots]$.

Другий спосіб знаходження НСД і НСК цілих чисел $a_1,a_2,\ldots,a_n$ ґрунтується на канонічному зображені цих чисел. Нехай числа a і b мають такі канонічні розклади: $a = r_1^{l_1} r_2^{l_2} \ldots r_m^{l_m}$, $b = q_1^{s_1} q_2^{s_2} \ldots q_t^{s_t}$.

Позначимо символами $p_1,p_2,\ldots,p_n$ усі різні прості множники, кожен з яких входить до розкладу хоч одного з чисел a і b. Якщо водночас простий множник p_i не міститься в розкладі якого-небудь з чисел a і b, то вважатимемо, що він входить до цього розкладу в нульовому степені. За цієї умови канонічні розклади a і b можна записати так: $a = p_1^{k_1} p_2^{k_2} \ldots p_n^{k_n}$, $b = p_1^{m_1} p_2^{m_2} \ldots p_n^{m_n}$ (це узагальнені канонічні форми запису чисел a і b), де кожен з показників k_i і m_i, $i=1,2,\ldots,n$ є ціле невід'ємне число. Тоді справедливі такі рівності:

$$\left(a,b\right) = p_1^{d_1} p_2^{d_2} \ldots p_n^{d_n},$$

де $d_i=\min(k_1,m_1)$, $i=1,2,\ldots,n$.

$$\left[a,b\right]\left[a,b\right] = p_1^{f_1} p_2^{f_2} \ldots p_n^{f_n},$$

де $f_i=min(k_i,m_i)$, $i=1,2,\ldots,n$.

Методичні вказівки

Приклад 1. *Знайти найбільший спільний дільник і найменше спільне кратне чисел* 504 і 816.

Розв'язання.

І спосіб. Знайдемо канонічні розклади чисел 816 і 504:

$$816=2^4\cdot 3\cdot 17,\ 504=2^3\cdot 3^2\cdot 7.$$

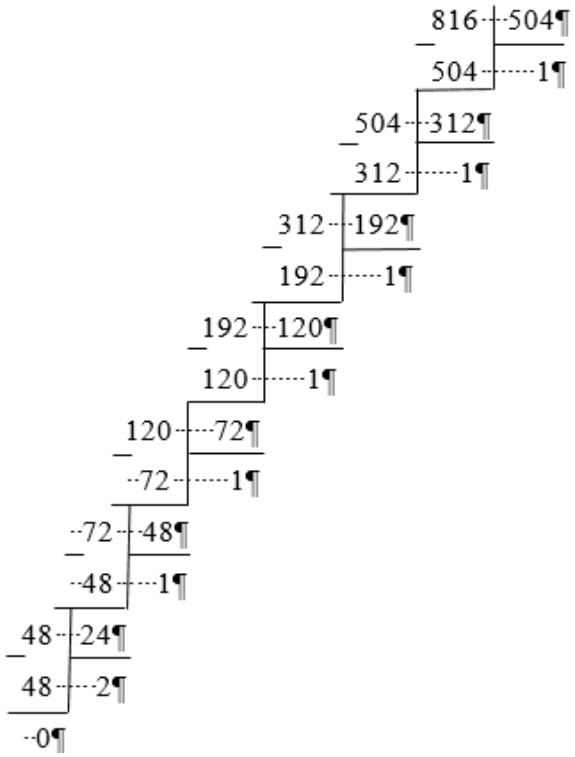
Запишемо ці числа в узагальнених канонічних формах:

$$816=2^4\cdot 3\cdot 7^0\cdot 17,\ 504=2^3\cdot 3^2\cdot 7\cdot 17^0.$$

Тоді $\text{НСД}(816,504)=2^3\cdot 3=24$, а $\text{НСК}[816,504]=2^4\cdot 3^2\cdot 7\cdot 17=17136$.

Зауваження. Цей спосіб доцільно застосовувати у тих задачах, де треба знайти НСД і НСК в канонічній формі.

ІІ спосіб. Скористаємося алгоритмом Евкліда для знаходження найбільшого спільного дільника.



1) ділимо 816 на 504, знаходимо частку 1 і першу остачу 312;
2) ділимо 504 на 312, знаходимо частку 1 і другу остачу192;
3) ділимо 312 на 192, знаходимо частку 1 і третю остачу 120;
4) ділимо 192 на 120, знаходимо частку 1 і четверту остачу 72;
5) ділимо 120 на 72, знаходимо частку 1 і п'яту остачу 48;
6) ділимо 72 на 48, знаходимо частку 1 і шосту остачу24;
7) ділимо 48 на 24, знаходимо частку 2 і сьому остачу 0.

Остання відмінна від 0 остача 24. Отже, $(504,816)=24$.

Наведені обчислення записуються так:

816=504*1+312;
504=312*1+192;
312=192*1+120;
192=120*1+72;
120=72*1+48;
72=48*1+**24 – НСД**
48=24*2+0.

Найменше спільне кратне цих чисел дорівнює їхньому добутку поділеному на їх НСД, тобто,

$$[816,504]=\frac{816\cdot 504}{(816,504)}=\frac{816\cdot 504}{24}=17136.$$

Приклад 2. Знайти найбільший спільний дільник d чисел 2737 і 943, а також цілі числа x і y, за допомогою яких число d лінійно виражається через числа 2737 і 943, тобто $d=x\cdot 2737+y\cdot 943$.

Розв'язання. Скористаємося алгоритмом Евкліда для знаходження НСД:

	2737	943
–	1886	2
943	851	
–	851	1
851	92	
–	828	9
92	23	
–	92	4
	0	

Маємо: $2737=943\cdot 2+851$, $943=851\cdot 1+92$, $851=92\cdot 9+23$, $92=23\cdot 4+0$.

Починаючи з передостанньої рівності, знаходимо остачі:

$$23=851-92\cdot 9 \qquad (1^*)$$
$$92=943-851\cdot 1 \qquad (2^*)$$
$$851=2737-943\cdot 2 \qquad (3^*)$$

Замінюватимемо послідовно остачі в цих рівностях, допоки не залишаться числа 2737 і 943. Остачу 23 у виразі (1^*) замінимо виразом (2^*) і зведемо подібні члени 851 і 943:

$$23=851-92\cdot 9=851-(943-851\cdot 1)\cdot 9=10\cdot 851-9\cdot 943.$$

У цій рівності замість множника 851 підставляємо вираз (3^*) і знову зводимо подібні члени 2737 і 943:

$$23=10\cdot 851-9\cdot 943=10(2737-943\cdot 2)-9\cdot 943=10\cdot 2737-29\cdot 943.$$

Отже, $23=10\cdot 2737-29\cdot 943$, звідси $x=10$, $y=-29$.

Приклад 3. *Довести, що* $(a,b)=(5a+3b,13a+8b)$ *для довільних цілих чисел* a і b.

Розв'язання. Введемо позначення $(a,b)= d_1$, $5a+3b$, $13a+8b$. Доведемо, що $d_1=d_2$. Оскільки d_1 і d_2 – натуральні числа, то досить показати, що $d_1 \mid d_2$ і $d_2 \mid d_1$.

Покажемо, що $d_2 \mid d_1$. Виразимо числа $5a+3b$ і $13a+8b$ через d_2. Отримуємо $5a+3b=d_2x$, $13a+8b=d_2y$;
де x і y – деякі цілі числа.

Помноживши першу рівність на 8, а другу на 3 і віднявши від першої рівності другу, знайдемо $a = d_2(8x-3y)$. Аналогічно отримуємо $b = d_2(5y-13x)$. Отже, $d_2 \mid a$ і $d_2 \mid b$. З означення числа d_1 випливає, що $d_2 \mid d_1$, що й треба було довести.

Зауваження. З доведення цього твердження випливає, що $(a,b)=(m_1a+m_2b,\ n_1a+n_2b)$, якщо $|m_1n_2-m_2n_1|=1$;
де m_1, m_2, n_1, n_2 – цілі числа.

Приклад 4. *Знайти* $[232,460,280]$.

Розв'язання. Знаходимо спочатку $[232,280]$. Для цього за допомогою алгоритму Евкліда визначаємо $(232,280)=8$, а тому:

$$[232,280]=\frac{232\cdot 280}{8}=8120.$$

Тепер знайдемо $[232,280,460]=[8120,460]$. Для цього обчислюємо $(8120,460)=20$, а тому $[8120,460]=\frac{8120\cdot 460}{20}=186760$.

Отже, маємо: $[232,460,280]=186760$.

Приклад 5. *Знайти натуральні числа* a і b, *якщо*:

$$\begin{cases} \dfrac{a}{(a,b)}+\dfrac{b}{(a,b)}=39, \\ [a,b]=4004. \end{cases}$$

Розв'язання. Використаємо факт: якщо $(a,b)=d$ і $a=d\cdot n$, $b=d\cdot k$, то $(n,k)=1$, а $[a,b]=\frac{a\cdot b}{d}=n\cdot k\cdot d$.

У цьому разі:

$$\frac{a}{(a,b)}+\frac{b}{(a,b)}=\frac{dn}{d}+\frac{dk}{d}=n+k=39,\ [a,b]=\frac{a\cdot b}{(a,b)}=\frac{dn\cdot dk}{d}=dnk=4004.$$

Оскільки натуральні числа n і k взаємно прості, то розглядаючи всі можливі випадки $dnk=2^2\cdot 11\cdot 7\cdot 13$, отримуємо, що n і k набувають значень 28 і 11, і навпаки. Тоді $d=13$. Отже, числа n і k дорівнюють $28\cdot 13$ і $11\cdot 13$, тобто, 364 і 147, і навпаки.

Приклад 6. *Чи можна розміняти 100 карбованців, маючи купюри вартістю 1 крб., 3 крб. та 5 крб., так, щоб всього в розмінюванні брало участь 29 купюр?*

Розв'язання. Нехай у розмінюванні беруть участь x купюр вартістю 1 крб., y купюр вартістю 3 крб. та z купюр вартістю 5 крб. Тоді можна скласти таке рівняння:

$$x+3y+5z=100 \Rightarrow (x+y+z)+(2x+4z)=100.$$

Зауважимо, що $x+y+z=29$ – кількість купюр. Оскільки $100 \vdots 2 \wedge (2x+4z) \vdots 2$., тоді перший доданок 29 має бути парне число, отримали протиріччя. Отже, розміняти 100 крб. за допомогою 29 купюр вартістю 1 крб., 3 крб. та 5 крб. неможливо.

Задачі рекомендовані для розв'язування в аудиторії

1. *Знайти НСД чисел:*

а) 1066 і 1970; д) 3059, 2737 і 943;
б) 1173 і 323; е) 2737, 9163 і 9639;
в) 3763 і 3337; є) 299, 391 і 667;
г) 2091 і 1681; ж) 588, 2058 і 2849.

2. *Знайти НСК чисел:*

а) –2520 і 6600; б) 279 і 372; в) 252 і 468; г)1058, 1403 і 3266;
д) 91, 252 і 462; е) 71004і 154452; є) 232, 460 і 280;

3. *Знайти лінійне зображення НСД чисел:*

а) 822 і 1734; в) 1786 і 705;
б) –26 і 174; г) –3791 і 3291.

4. *Знайти натуральні числа* a *і* b*, якщо:*

а) $\begin{cases} a+b=144, \\ (a,b)=24; \end{cases}$ б) $\begin{cases} ab=8400, \\ (a,b)=20; \end{cases}$ в) $\begin{cases} \dfrac{a}{b}=\dfrac{11}{7}, \\ (a,b)=45; \end{cases}$

г) $\begin{cases} (a,b)=4, \\ [a,b]=24; \end{cases}$ д) $\begin{cases} (a,b)=24, \\ [a,b]=2496; \end{cases}$ е) $\begin{cases} ab=168, \\ (a,b)=14. \end{cases}$

Контрольні питання

1. Канонічний розклад чисел.
2. НСД, НСК у канонічному розкладі.
3. Алгоритм Евкліда. НСК.
4. НСД, НСК для трьох чисел.
5. Лінійне представлення НСД.

Практична робота № 5

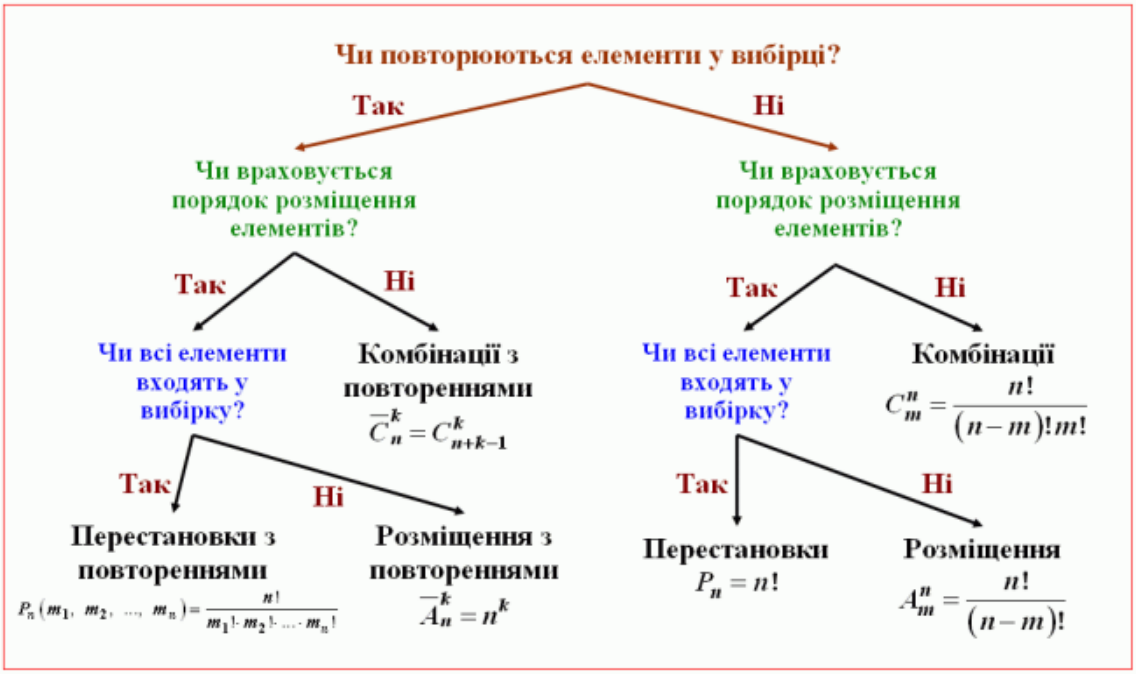
Тема: Комбінаторика та біном Ньютона

Мета: Повторити: означення упорядкованої множини, факторіала, перестановки з n елементів, розміщення з m елементів по k; сформулюйте правило суми та добутку; формули за якими знаходиться A_m^k; формули за якими знаходиться C_n^m; основні властивості формули Бінома Ньютона.

Теоретичні відомості

Під комбінаторикою зазвичай розуміють розділ дискретної математики, присвячений розв'язуванню задач про вибір та розміщення елементів скінченної множини згідно з заданими правилами. У результаті створюються необхідні комбінаторні об'єкти чи конфігурації. Характерними властивостями цих об'єктів є те, що вони відповідають деяким обмеженням щодо них, і тому завжди можна розпізнати дозволений комбінаторний об'єкт, який відповідає правилам його побудови, і недозволений, який не відповідає цим правилам.

Схема визначення виду комбінації



Методичні вказівки

Розміщення без повторень.

Задача 1. Розклад на день містить 5 уроків. Визначити кількість можливих розкладів під час вибору із 11 дисциплін, за умови, що жоден предмет не стоїть у розкладі двічі на день.

Розв'язання. Зрозуміло, що таких розкладів буде,

$$A_{11}^5 = 11(11-1)(11-2)...(11-(5-1)) = 11\cdot 10\cdot 9\cdot 8\cdot 7 = 55440.$$

Задача 2. Комісія складається з голови, його заступника і ще п'яти чоловік. Скількома способами 7 членів комісії можуть розподілити між собою обов'язки?

Розв'язання. Очевидно, що на кількість способів впливає лише вибір голови та його заступника, бо інші члени комісії «визначаються» автоматично. Отже, всього розподіл обов'язків може відбутися $A_7^2 = 7\cdot 6 = 42$ способами.

Задача 3. Із групи в 15 чоловік вибирають чотирьох учасників естафети 800х400х200х100 м. Скількома способами можна розставити спортсменів на етапах такої естафети?

Розв'язання. $A_{15}^4 = 32760$ способами.

Задача 4. Скільки різних правильних дробів можна скласти з чисел 3, 5, 7, 11, 13, 17, 19, 23 так, щоб в кожен дріб входило два числа ?

Розв'язання. Дробів, у яких чисельник не дорівнює знаменнику, можна скласти A_8^2 штук, але лише половина з них правильні. Отже, маємо $\frac{1}{2}A_8^2 = \frac{7\cdot 8}{2} = 28$ дробів.

Задача 5. Скільки можна скласти різних неправильних дробів, чисельниками і знаменниками яких є числа 3, 5, 7, 13, 17?

Розв'язання. Дробів, у яких чисельник не дорівнює знаменнику, можна скласти A_5^2 штук, але лише половина з них неправильні. До цих дробів треба ще додати дроби, у яких чисельник дорівнює знаменнику, тобто дроби, рівні одиниці; їх 5. Остаточно маємо $\frac{1}{2}A_5^2 + 5 = \frac{5\cdot 4}{2} + 5 = 15$ дробів.

Задача 6. Скільки різних натуральних чисел можна скласти з цифр 0, 1, 2, 3, 4, щоб у кожне таке число кожна з цих цифр входила не більше одного разу?

Розв'язання. Різних одноцифрових натуральних чисел буде $A_4^1 = 4$. Число різних двоцифрових виразів з такими умовами дорівнює A_5^2, а різних двоцифрових чисел буде на A_4^1 менше, а саме: $A_5^2 - A_4^1 = 5\cdot 4 - 4 = 16$. Розмірковуючи аналогічно, отримаємо, що за такими умовами можна скласти $A_5^3 - A_4^2 = 5\cdot 4\cdot 3 - 4\cdot 3 = 48$ трицифрових чисел, $A_5^4 - A_4^3 = 96$ чотирицифрових чисел, $A_5^5 - A_4^4 = 5! - 4! = 96$ п'ятицифрових чисел. Отже, всього можна утворити $4 + 16 + 48 + 96 + 96 = 260$ чисел.

Задача 7. Скільки різних чотирицифрових чисел можна скласти з цифр 0,1,2,3,4,5,6,7 так, щоб у кожному числі була цифра 1? (Цифри в числі не повинні повторюватися).

Розв'язання. Чисел, у яких одиниця стоїть на першому місці, буде A_7^3. Чисел, у яких одиниця стоїть на другому (третьому, четвертому) місці, теж було б по A_7^3, якби в цей набір цифр не входив би нуль. Тому варто виключити ті числа, де нуль стоїть на першому місці, а їх по A_6^2. Остаточно маємо: $A_7^3 + 3 \cdot \left(A_7^3 - A_6^2 \right) =$ =750 чисел.

Перестановки без повторень

Задача 8. Учасники шахового турніру грають у залі, де є 8 столів. Скількома способами можна розмістити шахістів, якщо учасники всіх партій відомі?

Розв'язання. За умовою пари шахістів відомі. Тому досить розподілити столи між 8 парами, а це можна зробити $P_8 = 8!$ способами.

Задача 9. Скільки різних п'ятицифрових чисел можна скласти з цифр 0,1,2,3,4 , якщо у кожному числі жодна з цифр не повторюється?

Розв'язання. З даних п'яти цифр можна утворити $P_5 = 5!$ п'ятицифрових виразів. Але оскільки серед цифр є нуль, то треба виключити числа, що починаються з нього; тобто P_4 чисел. Отже, таким чином можна отримати $P_5 - P_4 =$ $= 5! - 4! = 120 - 24 = 96$ чисел.

Задача 10. Скількома способами можна розставити 4 книжки з алгебри і 3 з геометрії, щоб усі книжки з геометрії стояли поруч?

Розв'язання. Об'єднаємо книжки з геометрії умовно в одну. Тоді маємо 5 книг і P_5 розстановок. Книги з геометрії можна розставляти «всередині» нової книги P_3 способами. Усього, за правилом добутку, $P_5 \cdot P_3 = 5! \cdot 3! = 120 \cdot 6 = 720$ способів.

Задача 11. Скільки п'ятицифрових чисел можна утворити з цифр 1,2,3,4,5 (без повторення) так, щоб парні цифри не стояли поруч?

Розв'язання. З цих цифр будується P_5 п'ятицифрових чисел. Серед них є і такі, що містять 2 і 4 поруч; їх буде $P_4 P_2$. Остаточно маємо $P_5 - P_4 P_2 = 72$ числа.

Сполучення (комбінації) без повторень

Задача 12. Скількома способами можна вибрати трьох чергових із класу, в якому 20 учнів?

Розв'язання. $C_{20}^3 = \frac{20!}{17!\cdot 3!} = \frac{20\cdot 19\cdot 18}{1\cdot 2\cdot 3} = 1140$ способами.

Задача 13. Скількома способами можна роздати 6 різних предметів трьом особам так, щоб кожна отримала по 2 предмета?

Розв'язання. Перша особа може вибрати довільні два предмети з шести C_6^2 способами; друга може вибрати два предмети з чотирьох, що залишилися, C_4^2 способами; а третя візьме два останніх предмета C_2^2=1 способом. За правилом добутку всього $C_6^2 \cdot C_4^2 \cdot 1 = 90$ способів.

Задача 14. Скількома способами можна вибрати 2 олівця і 3 ручки з 6 різних олівців і 8 різних ручок?

Розв'язання. Олівці можна вибрати C_6^2 способами, а ручки C_8^3 способами. Отже, всього є $C_6^2 \cdot C_8^3 = 840$ способів.

Задача 15. Скільки різних звукосполучень можна взяти на десяти вибраних клавішах рояля, якщо кожне звукосполучення може містити від трьох до десяти звуків ?

Розв'язання. Очевидно, що нам потрібно знайти суму $C_{10}^3 + C_{10}^4 + C_{10}^5 + C_{10}^6 + C_{10}^7 + C_{10}^8 + C_{10}^9 + C_{10}^{10}$. Застосуємо властивість комбінації. Маємо: $C_{10}^3 = C_{10}^3$, $C_{10}^4 = C_{10}^6$, $C_{10}^8 = C_{10}^2$, $C_{10}^9 = C_{10}^1$. Тому шукана кількість звукосполучень дорівнює $2C_{10}^3 + 2C_{10}^4 + C_{10}^5 + C_{10}^2 + C_{10}^1 + C_{10}^{10} = 968$ способів.

Задача 16. У колоді 36 карт, з них 4 тузи. Скількома способами можна вибрати 6 карт так, щоб серед них було рівно 2 тузи ?

Розв'язання. Виберемо два тузи з чотирьох C_4^2 способами, а ще чотири карти виберемо з 32, що залишилися, C_{32}^4 способами. За правилом добутку остаточно маємо, що способів вибору буде $C_4^2 \cdot C_{32}^4 = 215760$.

Задача 17. У вазі стоять пронумеровані 10 червоних і 5 рожевих гвоздик. Скількома способами можна вибрати з вази: а) три квітки; б) три квітки одного кольору; в) три квітки так, щоб серед них були як червоні, так і рожеві гвоздики?

Розв'язання.

а) C_{15}^3=455 способами;

б) можна вибрати три червоних гвоздики C_{10}^3 способами, або три рожевих C_5^3 способами. За правилом суми маємо $C_{10}^3 + C_5^3 = 130$ способів вибору;

в) можна вибрати дві червоні і одну рожеву гвоздики $C_{10}^2 \cdot C_5^1$ способами, або одну червону і дві рожеві гвоздики $C_{10}^1 \cdot C_5^2$ способами. Отже, усього способів буде $C_{10}^2 \cdot C_5^1 + C_{10}^1 \cdot C_5^2 = 325$.

Задача 18. З групи, у яку входять 7 хлопчиків і 4 дівчинки, треба скласти команду з 6 чоловік так, щоб вона містила не менше двох дівчаток. Скільки є способів скласти таку команду?

Розв'язання. Якщо в команді 2 дівчинки і 4 хлопчика, то маємо $C_4^2 \cdot C_7^4$ способів; якщо по 3 дівчинки і хлопчика, то $C_4^3 \cdot C_7^3$ способів; якщо ж 4 дівчинки і 2 хлопчика, то $C_4^4 \cdot C_7^2$ способів. За правилом суми усього маємо $C_4^2 \cdot C_7^4 + C_4^3 \cdot C_7^3 + C_4^4 \cdot C_7^2 = 371$ спосіб.

Задача 19. Скільки різних добутків, кратних 10, можна отримати з чисел 2, 3, 5, 7, 11, 13?

Розв'язання. Будемо складати добутки, кратні 10 , у вигляді $2 \cdot 5 \cdot n$, де *n* всі можливі добутки з чисел 3,7,11,13. У число *n* можуть включатися від 0 до 4 множників. Отже, всіх можливих добутків, що задовольняють умови, буде $C_4^0 + C_4^1 + C_4^2 + C_4^3 + C_4^4 = 16$.

Задача 20. Скільки різних дільників має число 2310?

Розв'язання. Оскільки $2310 = 2 \cdot 3 \cdot 5 \cdot 7 \cdot 11$, то число *d* буде дільником 2310, якщо *d* – добуток чисел з набору 2,3,5,7,11. Будемо складати всі можливі добутки з цих чисел (вони містять від 1 до 5 множників) і число –1. Отримаємо, що число 2310 має $1 + C_5^1 + C_5^2 + C_5^3 + C_5^4 + C_5^5 = 32$ дільника.

Задачі на використання основних формул комбінаторики

Розглянемо задачі, в розв'язанні яких використовуються основні формули комбінаторики.

Задача 21. На футбольний турнір треба послати збірну команду в складі: тренер, його помічник, 2 асистента, 20 футболістів, лікар і 2 масажиста. Тренерський склад може бути відібраний з 10 спеціалістів, футболісти – з 25 спортсменів, лікаря треба вибрати одного з трьох, а масажистів двох з п'яти. Скількома способами може бути укомплектована така команда?

Розв'язання. Тренер і його помічник можуть бути вибрані з 10 спеціалістів A_{10}^2 способами (оскільки вони займають різні посади). З 8 спеціалістів, що залишилися, два асистента можуть бути вибрані C_8^2 способами (оскільки вони

займають однакові посади). Футболісти можуть бути вибрані C_{25}^{20} способами, лікар C_3^1 способами і масажисти C_5^2 способами. Використовуючи правило добутку, отримаємо, що всього можливо $A_{10}^2 \cdot C_8^2 \cdot C_{25}^{20} \cdot C_3^1 \cdot C_5^2 = 4016628000$ способів.

Задача 22. Із цифр 1, 2, 3, 4, 5, 6, 7, 8, 9 утворюються всілякі шестицифрові числа, що не містять однакових цифр. Визначити кількість таких чисел, у яких є цифри 1,2,3 одночасно.

Розв'язання. Щоб скласти таке шестицифрове число, до заданих цифр 1, 2, 3 треба додати три з шести цифр, що залишилися. Це можна зробити C_6^3 способами. У кожному отриманому наборі з шести цифр, шляхом P_6 перестановок, утворимо потрібні шестицифрові числа. Тому всього таких чисел за правилом добутку буде $C_6^3 \cdot P_6 = 14400$.

Задача 23. З 8 тенісистів і 6 тенісисток утворюють 3 змішані пари (у пару входять по одному тенісисту і одній тенісистці). Скількома способами це можна зробити ?

Розв'язання. Пронумеруємо три пари: № 1, № 2, № 3. З урахуванням нумерації тенісистів можемо розставити по парах A_8^3 способами, а тенісисток A_6^3 способами. Усього буде $A_8^3 \cdot A_6^3$ способів. Але порядок пар не враховується, тобто шукане число буде в P_3 раз менше. Отже, всього способів буде $\dfrac{A_8^3 \cdot A_6^3}{P_3} = 6720$.

Біном Ньютона

1. Трикутник Паскаля.

Повна таблиця чисел $C_m^n = \dfrac{m!}{n!\cdot(m-n)!}$.

m \ n	0	1	2	3	4	5	6	7	8
0	1								
1	1	1							
2	1	2	1						
3	1	3	3	1					
4	1	4	6	4	1				
5	1	5	10	10	5	1			
6	1	6	15	20	15	6	1		
7	1	7	21	35	35	21	7	1	
8	1	8	28	56	70	56	28	8	1

$$C_m^n + C_m^{n+1} = C_{m+1}^{n+1}; \qquad C_0^0 = C_m^0 = C_m^m = 1.$$

1
1 1
1 2 1
1 3 3 1
1 4 6 4 1
1 5 10 10 5 1
1 6 15 20 15 6 1
1 7 21 35 35 21 7 1
1 8 28 56 70 56 28 8 1

Властивості трикутника Паскаля:

1) числа кожного рядка є C_m^n;

2) сума чисел $m-$го рядка дорівнює 2^m;

3) сума чисел будь-якого рядка в два рази більша від суми чисел попереднього рядка;

4) числа, розміщені на однаковій відстані від кінців рядка, рівні між собою, бо $C_m^n = C_m^{m-n}$.

2. Біном Ньютона.

Двочлен $(a+b)$ називається біномом.

$$(a+b)^0 = 1;$$

$$(a+b)^1 = 1\cdot a + 1\cdot b;$$

$$(a+b)^2 = 1\cdot a^2 + 2ab + 1\cdot b^2;$$

$$(a+b)^3 = 1\cdot a^3 + 3a^2b + 3ab^2 + 1\cdot b^3;$$

$$(a+b)^4 = 1\cdot a^4 + 4a^3b + 6a^2b^2 + 4ab^3 + 1\cdot b^4.$$

Неважко помітити, що коефіцієнти розкладу степенів бінома збігаються з відповідними рядками трикутника Паскаля. Для будь-якого натурального показника n справджується рівність:

$$\boxed{(a+b)^n = C_n^0 a^n + C_n^1 a^{n-1}b + \ldots + C_n^m a^{n-m}b^m + \ldots + C_n^n b^n} - \textbf{\textit{біном Ньютона.}}$$

Коефіцієнти правої частини формули бінома Ньютона називаються біноміальними коефіцієнтами.

Якщо $a = 1\ i\ b = x,$ то формула бінома записується: $(1+x)^n = C_n^0 + C_n^1 x + C_n^2 x^2 + \ldots + C_n^n x^n$.

$\boxed{T_{k+1} = C_n^k a^{n-k} b^k}$ – формула загального члена розкладу степеня бінома.

Методичні вказівки

Завдання 24. Запишіть розклад бінома $\left(\frac{1}{2}a + b\right)^7$.

$$\left(\frac{1}{2}a + b\right)^7 = \frac{1}{128}a^7 + \frac{7}{64}a^6b + \frac{21}{32}a^5b^2 + \frac{35}{16}a^4b^3 + \frac{35}{2}a^3b^4 + \frac{21}{4}a^2b^5 + \frac{7}{2}ab^6 + b^7$$

Завдання 25. Знайти середній член розкладу $\left(\sqrt[3]{x}-\frac{1}{\sqrt{x}}\right)^{12}$.

Розв'язання. Розклад має 13 членів. Тому середнім є T_7 – сьомий член. Маємо $T_7 = C_{12}^6 \cdot \left(-\frac{1}{\sqrt{x}}\right)^6 \cdot \left(\sqrt[3]{x}\right)^6 = 924 \cdot \frac{1}{x^3} \cdot x^2 = \frac{924}{x}$.

Завдання 26. Знайти середній член розкладу бінома $\left(\frac{1}{\sqrt{x}}+x\right)^n$, якщо сума біноміальних коефіцієнтів цього розкладу дорівнює 256.

Розв'язання. Використавши властивість бінома, що сума біноміальних коефіцієнтів розкладу дорівнює $2^n = 256$. Розв'язавши показникові рівняння знайдемо $n = 8$. Отже біном прийме вид $\left(\frac{1}{\sqrt{x}}+x\right)^8$. Розклад має 9 членів, а тому T_5 буде середнім. $T_5 = C_8^4 \cdot \left(\frac{1}{\sqrt{x}}\right)^4 \cdot x^4 = 70x^2$.

Завдання 27. Знайти *x,* якщо п'ятий член розкладу бінома $\left(\sqrt{x}+x^{-1}\right)^6$ дорівнює $\frac{5}{9}$.

Розв'язання. Зауважимо, що $x > 0$. Маємо $T_5 = C_6^4\left(\sqrt{x}\right)^2 \cdot \left(x^{-1}\right)^4 = 15x \cdot x^{-4} = \frac{15}{x^3}$; $\frac{15}{x^3} = \frac{5}{9}$, $x^3 = 27$, $x = 3$.

Завдання 28. Знайдіть член розкладу $\left(\frac{1}{\sqrt[3]{x^2}}+\sqrt[4]{x^3}\right)^{17}$, який не містить x.

Розв'язання. $T_{k+1} = C_{17}^k \left(x^{-\frac{2}{3}}\right)^{17-k} \cdot \left(x^{\frac{3}{4}}\right)^k = C_{17}^k x^{\frac{3}{4}k+\frac{2}{3}k-\frac{34}{3}}$.

За умовою $\frac{3}{4}k+\frac{2}{3}k-\frac{34}{3}=0$, звідки $k = 8$.

Отже шуканий член дорівнює $T_9 = C_{17}^8 = 24310$.

Завдання 29. Знайти тринадцятий член розкладу $\left(9x-\frac{1}{\sqrt{3x}}\right)^m$ біноміальний коефіцієнт третього члена дорівнює 105.

Розв'язання. За умовою $C_m^2 = 105$, тобто $\frac{m(m-1)}{2} = 105$, або $m^2 - m - 210 = 0$. Оскільки $m \in N, m \geq 2$, то $m = 15$. Маємо розклад $\left(9x - \frac{1}{\sqrt{3x}}\right)^{15}$. Тоді $T_{13} = C_{15}^{12} \cdot \left(-\frac{1}{\sqrt{3x}}\right)^{12} \cdot (9x)^3 = 455 \cdot \frac{1}{3^6 x^6} \cdot 9^3 x^3 = \frac{455}{x^3} \cdot$

Завдання 30. Знайти коефіцієнт при x^4 в розкладі виразу $\left(1 + 2x + 3x^2\right)^{10}$.

Розв'язання. Перетворимо цей вираз так:

$$\left(1+2x+3x^2\right)^{10} = \left((1+2x)+3x^2\right)^{10} = (1+2x)^{10} + 10 \cdot 3x^2 \cdot (1+2x)^9 + 45 \cdot 9x^4 \cdot (1+2x)^8 + \ldots.$$

Останні члени не виписані, бо вони містять *x* в степені вище четвертої. Випишемо коефіцієнти при x у кожному доданку правої частини і додамо їх. Маємо $C_{10}^4 \cdot 2^4 + 10 \cdot 3 \cdot C_9^2 \cdot 2^2 + 45 \cdot 9 = 8085$.

Завдання 31. Знайти суму коефіцієнтів у біноміальному розкладі $(3x - 2y)^n$ при довільному натуральному *n* .

Розв'язання. $(3x-2y)^n = (3x)^n + C_n^1 \cdot (3x)^{n-1} \cdot (-2y) + \ldots + (-2y)^n$. Суму коефіцієнтів отримаємо, якщо в розклад підставимо *x*=*y*=1. Отже, шукана сума коефіцієнтів у розкладі дорівнює $3^n + C_n^1 \cdot 3^{n-1} \cdot (-2) + \ldots + (-2)^n = (3 \cdot 1 - 2 \cdot 1)^n = 1^n = 1$.

Завдання 32. Скільки є раціональних членів у розкладі біному $\left(\sqrt[5]{3} + \sqrt[10]{8}\right)^{100}$.

Необхідно, щоб число k/5 було цілим. Тепер знайдемо число (100-k)/10, яке буде теж цілим. Таким числами є {0,10,20…,100}. Їх десять.

Завдання 33. Знайти раціональні члени в розкладі $\left(\sqrt[3]{3} + \sqrt{2}\right)^5$.

Розв'язання. Загальний член розкладу дорівнює $T_{k+1} = C_5^k \left(\sqrt{2}\right)^k \left(\sqrt[3]{3}\right)^{5-k} =$.

$= C_5^k \cdot 2^{\frac{k}{2}} \cdot 3^{\frac{5-k}{3}} \left(0 \leq k \leq 5\right)$. Необхідно, щоб число $\frac{k}{2}$ було цілим, тобто k – парне. Тепер серед парних чисел, менших п'яти, знайдемо таке, щоб число $\frac{5-k}{3}$ було цілим. Єдиним таким числом є двійка. Отже, $k = 2$, тобто існує єдиний раціональний член цього розкладу $T_3 = C_5^2 \cdot 2^1 \cdot 3^1 = 60$.

Завдання 34. За яких значень *x* четвертий доданок розкладу $(5 + 2x)^{16}$ більший за два сусідніх з ним доданки?

Розв'язання. $T_3 = 120 \cdot 4 \cdot x^2 \cdot 5^{14}$, $T_4 = 560 \cdot 8 \cdot x^3 \cdot 5^{13}$, $T_5 = 1820 \cdot 16 \cdot x^4 \cdot 5^{12}$. За умовою $T_4 > T_5, T_4 > T_3$. Маємо систему нерівностей:

$$\begin{cases} 560 \cdot 8 \cdot x^3 \cdot 5^{13} > 120 \cdot 4 \cdot x^2 \cdot 5^{14}; \\ 560 \cdot 8 \cdot x^3 \cdot 5^{13} > 1820 \cdot 16 \cdot x^4 \cdot 5^{12}. \end{cases}$$

Враховуючи, що $x \neq 0$, розділимо обидві нерівності на x^2, маємо $\begin{cases} x > 1,3x^2; \\ 28x > 15. \end{cases}$

Звідси $\frac{15}{28} < x < \frac{10}{13}$.

Контрольні питання

1. Перестановки. Перестановки з повтореннями.
2. Розміщення. Розміщення з повтореннями.
3. Комбінації. Комбінації з повтореннями.
4. Біном Ньютона. Властивості коефіцієнтів.

Практична робота № 6

Тема: Числові функції

Теоретичні відомості

Функція $f(x)$ називається *числовою,* якщо вона визначена за всіма натуральними значеннями аргумента x.

Через $\tau(n)$ позначають числову функцію, значення якої для будь-якого натурального числа n дорівнює числу всіх його натуральних дільників.

Через $\sigma(n)$ позначають числову функцію, значення якої для будь-якого натурального числа n дорівнює сумі всіх його натуральних дільників.

Через $\varphi(n)$ позначають числову функцію, значення якої для будь-якого натурального числа n дорівнює кількості натуральних (цілих невід'ємних) чисел, взаємно простих з n, які не перевищують n. Функцію $\varphi(n)$ називають *функцією Ейлера.*

Через $[x]$ позначають числову функцію, значення якої для будь-якого дійсного числа x дорівнює найбільшому цілому числу, яке не перевищує x. Функцію $[x]$ називають *цілою частиною від* x.

Через $\{x\}$ позначають числову функцію, значення якої для будь-якого дійсного числа x дорівнює різниці $x-[x]$. Функція $\{x\}$ називається *дробовою частиною від* x.

Числова функція $f(n)$ називається *мультиплікативною*, якщо для кожного n функція $f(n)\neq 0$ і для будь-яких взаємно простих натуральних чисел n і m виконується рівність $f(n\cdot m)=f(n)\cdot f(m)$.

Мультиплікативні функції мають такі властивості:

$f(1)=1$.

1. Добуток мультиплікативних функцій є мультиплікативна функція.

2. Якщо $n_1, n_2,\ldots, n_k$ попарно взаємно прості, то $f(n_1\cdot n_2\cdot\ldots\cdot n_k)=f(n_1)\cdot f(n_2)\cdot\ldots\cdot f(n_k)$.

3. Числові функції $\tau(n)$, $\sigma(n)$, $\varphi(n)$ мультиплікативні. Якщо $n=p_1^{\alpha_1}\cdot p_2^{\alpha_2}\cdot\ldots\cdot p_k^{\alpha_k}$ – канонічний розклад натурального числа n, то

$$\tau(n)=(\alpha_1+1)(\alpha_2+1)\ldots(\alpha_k+1), \qquad (1)$$

$$\sigma(n)=\frac{p_1^{\alpha_1+1}-1}{p_1-1}\cdot\frac{p_2^{\alpha_2+1}-1}{p_2-1}\cdot\ldots\cdot\frac{p_k^{\alpha_k+1}-1}{p_k-1}, \quad (2)$$

$$\varphi(n)=n\cdot\left(1-\frac{1}{p_1}\right)\left(1-\frac{1}{p_2}\right)\ldots\left(1-\frac{1}{p_k}\right), \quad (3)$$

Зрозуміло, що $\tau(1)=\sigma(1)=\varphi(1)=1$, згідно з означенням цих функцій.

Сума значень функції Ейлера для всіх дільників d_i числа n дорівнює n:

$$\sum_{d_i|n}\varphi(d_i)=n \text{ (формула Гаусса).} \quad (4)$$

Зауваження.

1. $\varphi(1)=\varphi(2)=1$. В усіх інших випадках $\varphi(a)$ може бути тільки парним числом 4;
2. $\varphi(2\cdot a)=\varphi(a)$, якщо $(2,a)=1$;
3. $\varphi(p^\alpha)=(p-1)\cdot p^{\alpha-1}$;
4. $\varphi(a\cdot b)=\varphi(a)\cdot\varphi(b)$, якщо $(a,b)=1$.

Якщо $x\in R,\ x>0\wedge n\in N$, то $\left[\frac{[x]}{n}\right]=\left[\frac{x}{n}\right]$.

Показник a простого числа p, яке входить до канонічного розкладу натурального числа $n!$ обчислюється за формулою:

$$\alpha=\left[\frac{n}{p}\right]+\left[\frac{n}{p^2}\right]+\left[\frac{n}{p^3}\right]+\ldots+\left[\frac{n}{p^s}\right], \text{ де } p^s\le n<p^{s+1}. \quad (5)$$

$\forall_{x\in R}$, $p_1,p_2,\ldots p_k$ – прості числа.

Кількість цілих додатних чисел, які не перевищують x і не діляться на жодне з простих чисел $p_1, p_2,\ldots, p_k$, обчислюється за формулою:

$$B[x;p_1,p_2,\ldots,p_k]=[x]-\left[\frac{x}{p_1}\right]-\left[\frac{x}{p_2}\right]-\left[\frac{x}{p_3}\right]-\ldots-\left[\frac{x}{p_k}\right]+\left[\frac{x}{p_1p_2}\right]+$$
$$+\left[\frac{x}{p_1p_3}\right]+\ldots+\left[\frac{x}{p_{k-1}p_k}\right]-\left[\frac{x}{p_1p_2p_3}\right]-\left[\frac{x}{p_1p_2p_4}\right]\ldots\left[\frac{x}{p_{k-2}p_{k-1}p_k}\right]+ \quad (6)$$
$$+\ldots+(-1)^k\left[\frac{x}{p_1p_2\ldots p_k}\right]$$

Властивості цілої та дробової частини числа.

$\forall x\in R$ виконуються властивості:

1. $x=[x]+\{x\}$;

2. $0 \le \{x\} < 1;$
3. Якщо $[x] = n$, $n \in Z$, то $n \le x < n+1;$
4. $[x] \le x < [x]+1;$
5. $x-1 < [x] \le x;$
6. $[x+m] = [x]+m$, якщо $m \in Z;$
7. $\{x+m\} = \{x\}$, якщо $m \in Z;$
8. $[x+y] = \big[[x]+[y]+\{x\}+\{y\}\big]$ і $[x+y] = [x]+[y]+\big[\{x\}+\{y\}\big];$
9. $[x]+[y] \le [x+y] \le [x]+[y]+1;$
10. Для будь-якої кінцевої кількості доданків:

$$[x_1]+[x_2]+\ldots+[x_n] \le [x_1+x_2+\ldots+x_n] \le [x_1]+[x_2]+\ldots+[x_n]+n-1$$

11. Якщо $[x] = [y]$, то $|x-y| < 1.$
12. Якщо $n \in N$, то $\left[\dfrac{[x]}{n}\right] = \left[\dfrac{x}{n}\right];$
13. $\forall x \in R \ \ \forall n \in N;$

$$[x]+\left[x+\frac{1}{n}\right]+\left[x+\frac{2}{n}\right]+\ldots+\left[x+\frac{n-1}{n}\right] = [nx].$$

14. $\forall x \in R \ \ \forall n \in N \Rightarrow n[x] \le [nx] \le n[x]+n-1.$

Методичні вказівки

Приклад 1. *Знайти число і суму всіх натуральних дільників числа* 3500.

Розв'язання. Знаходимо канонічний розклад числа 3500. $350=2^5 \cdot 5^3 \cdot 7$. Тоді

$$\tau(3500) = (2+1)(3+1)(1+1) = 24,$$

$$\sigma(3500) = \frac{2^{2+1}-1}{2-1} \cdot \frac{3^{3+1}-1}{3-1} \cdot \frac{7^{1+1}-1}{7-1} = 7 \cdot 40 \cdot 8 = 2240.$$

Відповідь: $\tau(3500) = 24$, $\sigma(3500) = 2240.$

Приклад 2. *Знайти натуральне число n, якщо:*

а) n *має тільки два простих дільники,* $\tau(n) = 12$, $\sigma(n) = 5200;$

б) $n = 2^x \cdot 3^y \cdot 5^z$; $\tau(5n) = \tau(n)+8$; $\tau(3n) = \tau(n)+12$; $\tau(8n) = \tau(n)+18.$

Розв'язання. а) оскільки $n = p^\alpha q^\beta$, то $\tau(n) = (\alpha+1)(\beta+1) = 12 \Rightarrow \alpha = 3, \beta = 2.$

$$\sigma(n)=\sigma\left(p^3\cdot q^2\right)=\frac{p^4-1}{p-1}\cdot\frac{q^3-1}{q-1}=\left(p^3+p^2+p+1\right)\left(q^2+q+1\right)=$$

$$=2^4\cdot5^2\cdot13.$$

Рівність $\left(p^3+p^2+p+1\right)\left(q^2+q+1\right)=2^4\cdot5^2\cdot13$ можлива тільки коли $p=7$ і $q=3.$

Тоді: $n=7^3\cdot3^2=3087.$

б) якщо $n=2^x\cdot3^y\cdot5^z$, то

$$\tau(n)=(x+1)(y+1)(z+1),\ \tau(5n)=(x+1)(y+1)(z+2);$$
$$\tau(3n)=(x+1)(y+2)(z+1),\ \tau(8n)=(x+4)(y+1)(z+1).$$

Складемо систему рівнянь і розв'яжемо її:

$$\begin{cases}(x+1)(y+1)(z+2)=(x+1)(y+1)(z+1)+8,\\(x+1)(y+2)(z+1)=(x+1)(y+1)(z+1)+12,\\(x+4)(y+1)(z+1)=(x+1)(y+1)(z+1)+18.\end{cases}\Rightarrow$$

$$\Rightarrow\begin{cases}(x+1)(y+1)=8,\\(x+1)(z+1)=12,\\(y+1)(z+1)\cdot3=18.\end{cases}\Rightarrow\begin{cases}(x+1)(y+1)=2\cdot2\cdot2,\\(x+1)(z+1)=2\cdot2\cdot3,\\(y+1)(z+1)=2\cdot3.\end{cases}\Rightarrow$$

Останні рівності можливі тільки коли $x=3;\ y=1;\ z=2.$

Тоді, $n=2^3\cdot3\cdot5^2=600.$

Відповідь: а) $n=3087$; б) $n=600.$

Приклад 3. *Нехай n – натуральне число. Знайти $\tau\left(n^3\right)$, якщо $\tau\left(n^2\right)=105$ і n має тільки три простих дільники.*

Розв'язання. За умовою $n=p_1^{\alpha_1}\cdot p_2^{\alpha_2}\cdot p_3^{\alpha_3}$, де p_1, p_2, p_3 – прості числа.

Тоді: $n^2=p_1^{2\alpha_1}\cdot p_2^{2\alpha_2}\cdot p_3^{2\alpha_3}$, а $n^3=p_1^{3\alpha_1}\cdot p_2^{3\alpha_2}\cdot p_3^{3\alpha_3}$.

$$\tau\left(n^2\right)=(2\alpha_1+1)(2\alpha_2+1)(2\alpha_3+1)=3\cdot5\cdot7\Rightarrow\alpha_1=1,\alpha_2=2,\alpha_3=3.$$

Отже, $\tau\left(n^3\right)=(3\alpha_1+1)(3\alpha_2+1)(3\alpha_3+1)=(3\cdot1+1)(3\cdot2+1)(3\cdot3+1)=280.$

Відповідь: 280.

Приклад 4. *Знайти функцію Ейлера для чисел:*

а) 780;

б) 75·172.

Розв'язання.

а) знайдемо канонічний розклад числа 780:

$$n = 780 = 2^2 \cdot 3 \cdot 5 \cdot 13.$$

Тоді:

$$\varphi(780) = 780 \cdot \left(1-\frac{1}{2}\right)\left(1-\frac{1}{3}\right)\left(1-\frac{1}{5}\right)\left(1-\frac{1}{13}\right) = 780 \cdot \frac{1}{2} \cdot \frac{2}{3} \cdot \frac{4}{5} \cdot \frac{12}{13} = 192.$$

б) $n = 75 \cdot 172 = n_1 \cdot n_2 = 3 \cdot 5^2 \cdot 2^2 \cdot 43.$

$$\varphi(n) = \varphi(75 \cdot 172) = \varphi(75) \cdot \varphi(172) = \left[75 \cdot \left(1-\frac{1}{3}\right)\left(1-\frac{1}{5}\right)\right] \times$$

$$\times \left[172 \cdot \left(1-\frac{1}{2}\right)\left(1-\frac{1}{43}\right)\right] = \left[75 \cdot \frac{2}{3} \cdot \frac{4}{5}\right] \cdot \left[172 \cdot \frac{1}{2} \cdot \frac{42}{43}\right] = 40 \cdot 84 = 3360.$$

Відповідь: а) 192; б) 3360.

Приклад 5. *Знайти кількість натуральних чисел, які менші від числа* 300 *і мають з ним найбільший спільний дільник d*=20.

Розв'язання. За умовою $(300, x) = 20$, всі значення $x < 300$. Поділимо 300 та x на d=20 $\Rightarrow (15, y) = 1$, де всі значення y<15 і взаємно прості з 15. Кількість значень y обчислимо за формулою:

$$\varphi(15) = 15 \cdot \left(1-\frac{1}{3}\right)\left(1-\frac{1}{5}\right) = 8,\ y = 1,2,4,7,8,11,13,14 \Rightarrow$$

$$\Rightarrow x = 20\ \ y = 20,40,80,140,160,220,260,280.$$

Відповідь: Існує 8 чисел менших 300, які мають з 300 найбільший спільний дільник 20.

Приклад 6. *Розв'язати рівняння* $\varphi(x) = 8.$

Розв'язання. Нехай x – просте число.

Тоді: $\varphi(x) = x\left(1-\frac{1}{x}\right) = x-1.$

$x-1=8,\ x=9$, а 9 – складене число.

Висновок: x – складене число.

Нехай $x = p_1^{\alpha_1} \cdot p_2^{\alpha_2} \cdot \ldots \cdot p_i^{\alpha_i}$, де p_i – прості числа менші 8. Отже, p_i можуть набувати значень $2,3,5,7$.

Якщо $x = 2^4$, то $\varphi(2^4) = 2$;

якщо $x = 2^3 \cdot 3$, то $\varphi(2^3 \cdot 3) = 8$;

якщо $x = 2^2 \cdot 5$, то $\varphi(2^2 \cdot 5) = 8$;

якщо $x = 2 \cdot 3 \cdot 5$, то $\varphi(2 \cdot 3 \cdot 5) = 8$;

якщо $x = 3 \cdot 5$, то $\varphi(3 \cdot 5) = 8$.

Відповідь: x може набувати значень $16,20,24,15,30$.

Приклад 7. *Знайти натуральне число* n, *якщо* $n = p^k q^l$, *де* p, q – *різні прості числа,* $k, l \in N$ *і* $\varphi(n) = 120$.

Розв'язання. $\varphi(n) = p^k \cdot q^l \left(1 - \frac{1}{p}\right)\left(1 - \frac{1}{q}\right) = p^{k-1}(p-1)q^{l-1}(q-1) = 120 = 2^3 \cdot 3 \cdot 5 \cdot$

Способом підбору знаходимо декілька розв'язків цієї задачі. Числа p і q повинні бути меншими 120.

1) $n = 2^3 \cdot 31$, $\varphi(n) = 120$;

2) $n = 2^2 \cdot 61$, $\varphi(n) = 120$;

3) $n = 3^2 \cdot 5^2$, $\varphi(n) = 120$;

4) $n = 11 \cdot 13$, $\varphi(n) = 120$;

5) $n = 3 \cdot 61$, $\varphi(n) = 120$.

Відповідь: $143, 183, 225, 244, 248$.

Приклад 8. *Розв'язати рівняння* $\varphi(10^x) = 4000$.

Розв'язання. $\varphi(10^x) = 10^x \cdot \left(1 - \frac{1}{2}\right)\left(1 - \frac{1}{5}\right) = 10^x \cdot \frac{1}{2} \cdot \frac{4}{5} = 10^{x-1} \cdot 4.$

$10^{x-1} \cdot 4 = 400$;

$10^{x-1} \cdot 4 = 4 \cdot 1000$;

$10^{x-1} \cdot 4 = 1000$;

$x - 1 = 3$;

$x = 4$.

Відповідь: $x = 4$.

Приклад 9. *Скількома нулями закінчується число* $1996!$?

Розв'язання. Відповіддю має бути максимальний степінь числа 10, на який ділиться число 1996! Але $10 = 2 \cdot 5$. Число 2 входить множником у 1996! значно частіше, ніж 5. Тому розв'язком буде максимальний степінь числа 5, на який ділиться 1996!. Використавши формулу (5), отримаємо, що:

$$\alpha = \left[\frac{1996}{5}\right] + \left[\frac{1996}{5^2}\right] + \left[\frac{1996}{5^3}\right] + \left[\frac{1996}{5^4}\right] = 399 + 79 + 15 + 3 = 496.$$

Відповідь: число 1996! закінчується 496-и нулями.

Задачі рекомендовані для розв'язування в аудиторії

1. Знайти число і суму всіх натуральних дільників таких чисел:

а) 375;

б) 720;

в) 990;
г) 1542;
д) 3500.

2. Знайти всі натуральні дільники чисел:
а) 24;
б) 50;
в) 100;
г) 360;
д) 375.

3. Знайти натуральне число n, якщо:
а) n – найменше натуральне число, для якого $\tau(n)=14$;
б) n має тільки два простих дільники, $\tau(n)=12$, $\sigma(n)=1240$;
в) $n=2^x3^y5^z$, $\sigma\left(\frac{1}{2}n\right)=\sigma(n)-30$, $\sigma\left(\frac{1}{3}n\right)=\sigma(n)-35$;

$\sigma\left(\frac{1}{5}n\right)=\sigma(n)-42$.

4. Нехай n – натуральне число. Знайти $\tau(n^3)$, якщо $\tau(n^2)=15$ і n має тільки два простих дільники.

5. Два натуральних числа m і n називаються **дружніми**, якщо $\sigma(m)=m+n$. Довести, що дружніми є такі пари чисел:
а) 220 і 284;
б) 1184 і 1210;
в) 2620 і 2924.

6. Знайти кількість натуральних чисел, які менші від числа n і мають з ним найбільший спільний дільник d, якщо:
а) n=1176, d=41;
б) n=1665, d=37.

7. Розв'язати рівняння:
а) $\varphi(x)=12$; б) $\varphi(x)=\frac{x}{2}$; в) $\varphi(x)=\frac{4x}{5}$; г) $\varphi\left(6^x\right)=72$.

8. Знайти натуральне число n, якщо:
а) $n=3^k5^l7^s$, $k, l, s\in\mathrm{N}$ і $\varphi(n)=3600$;
б) $n=p^k$, де p – просте число, $k\in\mathrm{N}$, $\varphi(n)=6p^{k-2}$.

9. Знайти показник степеня простого числа p, яке міститься в добутку $n!$, якщо:
а) p=11, n=1000; б) p=7, n=81561.

10. Побудувати графіки функцій:
а) $y=[x]$; б) $y=2[x]$; в) $y=\left[\frac{1}{2}x\right]$; г) $y=\frac{1}{2}[x]$; д) $y=\frac{1}{2}[2x]$;

е) $y=\left[x\right]+x$; є) $y=\dfrac{1}{\left[x\right]}$; ж) $y=\dfrac{x}{\left[x\right]}$; з) $y=\left[x^2-7x+6\right]$.

11. Довести, що:

а) $288!\vdots(16!)^{18}$; б) $288!\vdots(18!)^{16}$.

12. Знайти число і суму всіх натуральних дільників таких чисел: а) 60; б) 100; в) 957; г) 988; д) 1200; е) 1000.

13. Знайти натуральне число n, якщо:

а) n ділиться тільки на два простих числа і $\tau(n)=6$, а $\sigma(n)=42$;

б) n – найменше натуральне число, для якого $\tau(n)=18$;

в) n має тільки два простих дільники, $\tau(n)=12$, $\sigma(n)=465$;

г) n – найменше натуральне число виду $2^x p_1 p_2$ де p_1 і p_2 – різні непарні прості числа і $\sigma(n)=3n$ (задача Ферма).

14. Нехай n – натуральне число. Знайти $\tau(n^3)$, якщо $\tau(n^2)=81$ і n має тільки два простих дільники;

15. Натуральне число n називається **досконалим**, якщо $\sigma(n)=2n$. Довести, що:

а) 6, 28, 496, 8128 – досконалі числа;

б) парне число n є досконалим тоді і тільки тоді, коли $n=2^{k-1}\cdot(2^k-1)$, де $k\geq 2$, а $p=2^k-1$ – просте число (теорема Евкліда-Ейлера).

16. Знайти кількість натуральних чисел, які менші від числа n і мають з ним найбільший спільний дільник d, якщо:

а) $n=1075$, $d=8$; б) $n=2500$, $d=50$.

17. Знайти показник степеня простого числа p, яке міститься в добутку $n!$, якщо: а) $p=3$, $n=100$; б) $p=13$, $n=10000$.

18. Знайти канонічний розклад чисел: а) 11!; б) 18!; в) 40!; г) 75!.

19. Побудувати графіки функцій:

а) $y=2\left[\dfrac{1}{2}x\right]$; б) $y=\dfrac{x^2}{\left[x\right]}$; в) $y=\left\{x^2-4\right\}$; г) $y=\left\{x\right\}^2-4\left\{x\right\}-5$.

Контрольні питання

1. Дайте означення числової функції. Функції ціла частина та дробова.
2. Кількість дільників натурального числа.
3. Сума дільників натурального числа.
4. Функція Ейлера. Властивості.

Практична робота № 7
Тема: Системи числення

Мета: опрацювати методи переведення в різні системи числення, проведення операцій додавання, віднімання, множення та ділення в різних СЧ.

Теоретичні відомості

У позиційній системі числення один і той самий знак може позначати різні числа залежно від місця (позиції), займаного цим знаком в записі числа.

Загальноприйнятою (для ручних обчислень і обчисленьза допомогою механічних або електромеханічних рахункових машин) є *десяткова позиційна система*, що бере свій початок від рахункуна пальцях. Вона була винайдена в Індії, запозичена арабами і вже через арабські країни прийшла до Європи.

У цій системі для запису будь-якого числа використовується лише десять знаків (цифр):

{0, 1, 2, 3, 4, 5, 6, 7, 8, 9},

множина яких складає алфавіт цієї системи числення.

Довільна послідовність цифр алфавіту – слово цієї мови – позначає число, умовним, коротким записом складнішого виразу, складеного за певним правилом, що відображає позиційний принцип, за якого значення кожної цифри визначається як нею самою, так і займаним нею місцем (позицією).

Наприклад, слово «3785» позначає число, отримане як результат виконання всіх операцій у виразі

$3*1000 + 7*100 + 8*10 + 5$, або

$3*10^3 + 7*10^2 + 8*10^1 + 5*10^0$.

Тобто є коротким записом суми добутків послідовних степенів числа 10 (основи системи числення) на числа, кожне з яких 10.

Ці числа і позначаються цифрами, з яких утворюється короткий (умовний) запис числа у вигляді слова «3785» (у результаті опускання знаків + і · і послідовних степенів числа 10).

Тобто, якщо довільне число l записане в десятковій системі числення. за допомогою слова «$a_n a_{n-1} \ldots a_1 a_0$», де кожна a_l – цифра, тобто $0 \le a_i \le 9$ (мається на увазі, що $a_n \ne 0$), то

$$l = a_n \cdot 10^n + a_{n-1} \cdot 10^{n-1} + \ldots + a_1 \cdot 10 + a_0.$$

У такому докладному розгорненому записі числа наглядно виступає особлива роль числа 10 – основи системи числення (десяткової).

Кожне число розбивається на розряди, які вважаються з правої сторони на ліву (одиниці, десятки, сотні, тисячі, десятки тисяч і т. д.). Під час читання слова «3785» ми не читаємо назви цифр («три, сім, вісім, п’ять»), а читаємо числа, що позначаються цими цифрами, з урахуванням їх місця у записі числа, опускаючи лише знаки, які маються на увазі («три тисячі сімсот вісімдесят п’ять»).

Одиниця кожного наступного розряду (з правої сторони на ліву) вдесятеро більше одиниці попереднього (1, 10, 100, 1000, 10000, ...), тобто відношення сусідніх розрядів рівне основі системи.

Природно, можливі позиційні системи числення і з основами відмінними від 10.

Тобто, якщо довільне число l записане в системі числення з основою p за допомогою слова «$a_n a_{n-1}$ ... $a_1 a_0$», де a_l – цифри з алфавіту цієї мови що позначають числа від 0 до $p–1$ ($0 \le a \le p–1$) і $a_n 0$, то це означає, що

$$l = a_n p^n + a_{n-1} p^{n-1} + ... + a_1 p^1 + a_0 .$$

У разі $p=10$ одержуємо запис числа в десятковій системі.

У разі $p = 5$ отримуємо:

$$l = a_n \cdot 5^n + a_{n-1} \cdot 5^{n-1} + ... + a_1 \cdot 5 + a_0 ,$$

тобто запис числа в пятірковій системі числення, $0 \le a \le 4$, а алфавіт цієї мови складається з п'яти цифр: {0,1,2,3,4}.

У разі $p = 8$, очевидно:

$$l = a_n \cdot 8^n + a_{n-1} \cdot 8^{n-1} + ... + a_1 \cdot 8 + a_0,$$

запис числа l у вісімковій системі числення, у якій $0 \le a \le 7$ і алфавіт – {0, 1, 2, 3, 4, 5, 6, 7}.

У разі $p=2$ одержуємо запис числа в двійковій системі числення,

$$l = a_n \cdot 2^n + a_{n-1} \cdot 2^{n-1} + ... + a_1 \cdot 2 + a_0,$$

у якій $a_i = 0$ або 1, тобто алфавіт складається всього з двох знаків {0,1}.

Запис числа в системі числення з основою p називають також p-числом. Тобто, «десяткове», «п'ятіркове», «вісімкове», «двійкове» число, ми маємо на увазі запис числа відповідно в десятковій, п'ятірковій, вісімковій, двійковій системі числення.

Для запису числа в позиційній системі числення, як видно, потрібно стільки різних знаків (цифр), скільки одиниць в основі системи. Іншими словами, алфавіт позиційної системи числення з основою p повинен містити різні знаки, для позначення чисел,

$$0, 1, 2, ... p–1.$$

Теорема про запис будь-якого цілого числа в системі числення

Теорема. Будь-яке ціле число l може бути записано в системі числення з основою p.

Арифметичні операції над системними числами

Число, записане в певній системі числення, називають *системним числом.* Щоб розрізняти, в якій системі числення записане зазначене число, ми будемо вказувати основу системи числення, записуючи її (в десятковій системі числення!) праворуч внизу від числа у вигляді індекса.

Наприклад, 372_{10} – це запис числа у звичайній десятковій системі числення, а 372_8 – у вісімковій системі.

Під час виконання арифметичних операцій над числами, записаними в десятковій системі числення, ми користуємося правилами додавання, віднімання і

множення чисел «стовпцем» і ділення – «кутом». За цими ж правилами виконують операції й над числами, записаними в будь-якій іншій позиційній системі числення. Грунтуються ці правила на п’яти основних законах додавання і множення цілих чисел: асоціативності й комутативності додавання, асоціативності й комутативності множення, дистрибутивності множення відносно додавання.

Наприклад, під час складання формуються відповідні розряди, починаючи з молодших. Якщо у цьому розряді утворюється сума, що вже не поміщається в ньому, то відповідне перевищення переноситься в наступний старший розряд. Таким чином, фактично доводиться використовувати таблицю складання для однозначних чисел.

Розглянемо **додавання** у вісімковій і двійковій системах складання.

1. Таблиця складання однозначних чисел в двійковій системі має вид табл. 1.

Таблиця 1

$+_{(2)}$	0	1
0	0	1
1	1	10

Додавання двох багатозначних двійкових чисел виглядає так:

$$\begin{array}{r} 11011001011 \\ + \quad 111011101 \\ \hline 100010101000 \end{array}$$

Розглянемо **множення** в двійковій системі числення.

2. Таблиця множення в двійковій системі числення має вид табл. 2.

Таблиця 2

(2)	0	1
0	0	0
1	0	1

$$\begin{array}{r} 11011 \\ \times \quad 1101 \\ \hline 11011 \\ + \ 11011 \\ \quad 11011 \\ \hline 101011111 \end{array}$$

Оскільки множення на нуль завжди (у будь-якій системі числення) дає нуль, можна вважати, що таблиця множення складається лише з одного рядка $1 \cdot 1 = 1$.

3. Запишемо таблицю складання однозначних чисел у вісімковій системі числення (табл. 3).

Таблиця 3

+	0	1	2	3	4	5	6	7
0	0	1	2	3	4	5	6	7
1	1	2	3	4	5	6	7	10
2	2	3	4	5	6	7	10	11
3	3	4	5	6	7	10	11	12
4	4	5	6	7	10	11	12	13
5	5	6	7	10	11	12	13	14
6	6	7	10	11	12	13	14	15
7	7	10	11	12	13	14	15	16

Складання двох багатозначних вісімкових чисел виглядає так:

$$\begin{array}{r} 623175 \\ +\ 172034 \\ \hline 1015231 \end{array}$$

Тут під час складання в кожному розряді ми користувалися табл. 3.

Але множення на одиницю не змінює числа. Тому множення багатозначних двійкових чисел зводиться лише до зсуву і складання.

Так само просто виконуються в двійковій системі числення і зворотні дії – віднімання і ділення:

$$\begin{array}{r} 1101001 \\ -\ 11100 \\ \hline 1001101 \end{array} \qquad \begin{array}{r|l} 101011111 & 11011 \\ -\ 11011 & \hline 1101 \\ \hline 100001 & \\ -\ 11011 & \\ \hline 11011 & \\ -\ 11011 & \\ \hline 0 & \end{array}$$

Переведення цілих чисел з однієї позиційної системи числення в іншу

У процесі розв'язування задач доводиться переводити цілі числа з однієї позиційної системи числення в іншу. Як же перевести число *a,* записане в системі числення з основою *p,* в систему числення з основою g? Як відомо, записати число *a* в системі числення з основою *g* – це означає зобразити його у вигляді суми:

$$a = a_k g^k + a_{k-1} g^{k-1} + \ldots + a_1 g + a_0.$$

Отже, щоб записати число *a* в системі числення з основою *g,* треба знайти коефіцієнти $a_0, a_1, a_2, \ldots, a_k$. Ці коефіцієнти знаходимо наступним чином. Поділимо в системі числення з основою *p* число *a* на g, отримаємо $a=b_0 g + a_0$. Далі поділимо b_0 на g, отримаємо $b_0 = b_1 g + a_1$. Звідси,

$$a = b_0 g + a_0 = (b_1 g + a_1) g + a_0 = b_1 g^2 + a_1 g + a_0.$$

Потім поділимо b_1 на g і т. д. Цей процес продовжуватимемо допоки не отримаємо частку, яка дорівнює нулю. Унаслідок цього матимемо:

$$a = a_k g^k + a_{k-1} g^{k-1} + \ldots + a_1 g + a_0.$$

Оскільки за теоремою число a можна подати в такому вигляді єдиним способом, то $a_0, a_1, a_2, \ldots a_k$ є цифри числа a в системі числення з основою g.

Таким чином, *цифрами $a_0, a_1, \ldots, a_k$ числа a в системі числення з основою g є остачі, що утворюються шляхом послідовного ділення a на g.*

Представимо у двійковій системі число 23, для цього розкладемо його на суму степенів 2 (16,8,4,2,1), тобто:

$23=16+7=16+4+3=16+4+2+1=2^4+2^2+2^1+2^0=\underline{1}*2^4+\underline{0}*2^3+\underline{1}*2^2+\underline{1}*2^1+\underline{1}*2^0=10111_2$.

Хід послідовного ділення числа a на g скорочено записують так:

a	g
$\underline{a_0}$	b_0

	b_0	g
	$\underline{a_1}$	b_1

	b_1	g
	$\underline{a_2}$	b_2

…

$\underline{a_{k-2}}$	b_{k-2}	g
	$\underline{a_{k-1}}$	b_{k-1}

	b_{k-1}	g
	$\underline{a_k}$	0

Стрілка показує напрям від вищих до нижчих розрядів числа, записаного в системі числення з основою g, цифри числа a у цій системі підкреслено (або взято в кружечок).

Послідовне ділення числа a на g провадиться в системі числення з основою p. Якщо $g<p$, то дільник g, а отже, і всі остачі $a_0, a_1, \ldots, a_k$ є одноцифрові числа і ми відразу дістаємо потрібні нам цифри числа a. Якщо ж $g>p$, то в системі числення з основою p дільник g і, можливо, деякі остачі міститимуть більш як одну цифру. У системі числення з основою g ці остачі варто записати новими цифрами, яких у системі числення з основою p немає.

Приклад:

Знайдемо запис десяткового числа 1766 в п’ятірковій системі числення. Оскільки $5^4<1766<5^5$, то найбільший степіньчисла 5, який міститься в 1766, – 5^4.

Розділивши це число на 625, знайдемо у частці 2 і в 516, тобто,

$$1766 = 2\cdot 5^4 + 516.$$

Важливо відзначити, що частка повинна бути менше 5, інакше 5^4 не було б найвищим степенем 5, що міститься в числі 1766, а залишок як завжди, менше дільника.

Тепер ми можемо виділити наступну степінь 5^3, із залишку:

$$516 = 4\cdot 5^2+16,$$

(тут знову частка повинна бути менше 5). Отже

$$1766 = 2\cdot 5^4 + 4\cdot 5^3+16.$$

Наступна степінь п’яти, 5^2, не міститься в залишку 16 або міститься у ньому 0 разів: $16=0\cdot5^2+16$, тобто,

$$1766 = 2\cdot5^4 +4\cdot5^3 + 0\cdot5^2 + 16.$$

Наступна степінь п’яти, 5^1, міститься в залишку 16 три рази:

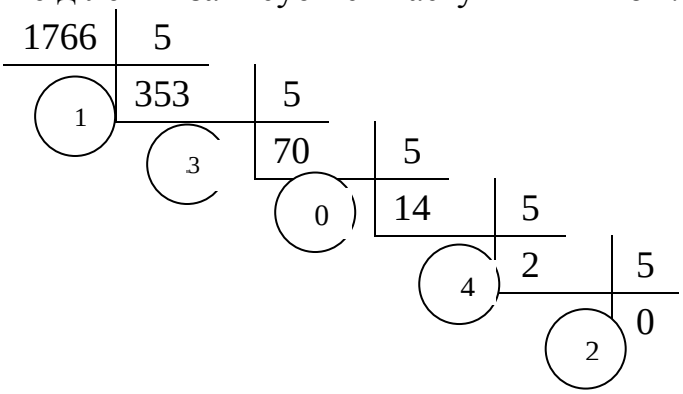
$16 = 3\cdot5^1+1$, і, нарешті, ми одержуємо$1766=2\cdot5^4 +4\cdot5^3 + 0\cdot5^2 + 3\cdot5^1 +1$.

Таким чином, десяткове число 1766 запишеться на мові п’ятіркової системи числення у вигляді слова «24031», тобто $1766 = 24031_{(5)}$.

(Індекс $_{(5)}$ вказує, що це запис числа в п’ятірковій системі числення; у десятковому числі індекс опускається.)

Розглянутий приклад, хоч і не є доказом можливості представлення будь-якого числа у будь-якій системі числення, містить всі елементи такого доказу, і проведене дослідження може бути відповідним чином узагальнено на випадок будь-якого числа і будь-якої системи числення.

Це послідовне ділення записується наступним чином:



Послідовність залишків від останнього до першого і є словом «24031», що зображає це десяткове число 1766 в п’ятірковій системі числення. Дійсно, відповідно до послідовного ділення одержуємо$1766 = 353\cdot5 +1$;

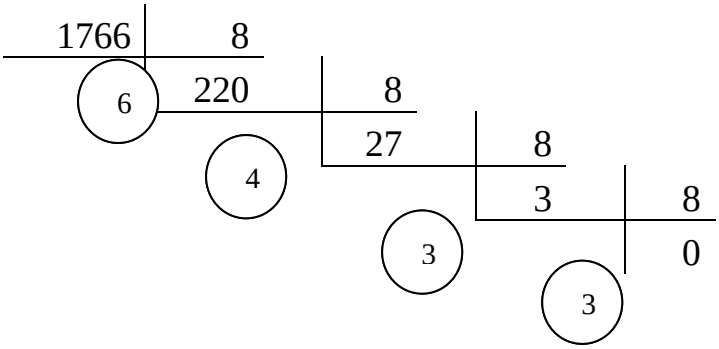
$=(70\cdot5 + 3)\cdot5+1$;

$= ((14\cdot5 + 0) \cdot5 + 3)\cdot5+1$;

$=(((2\cdot5+4)\cdot5 + 0)\cdot5 + 3)\cdot5+1$;

$=2\cdot54 + 4\cdot53+0\cdot52 + 3\cdot5+1$.

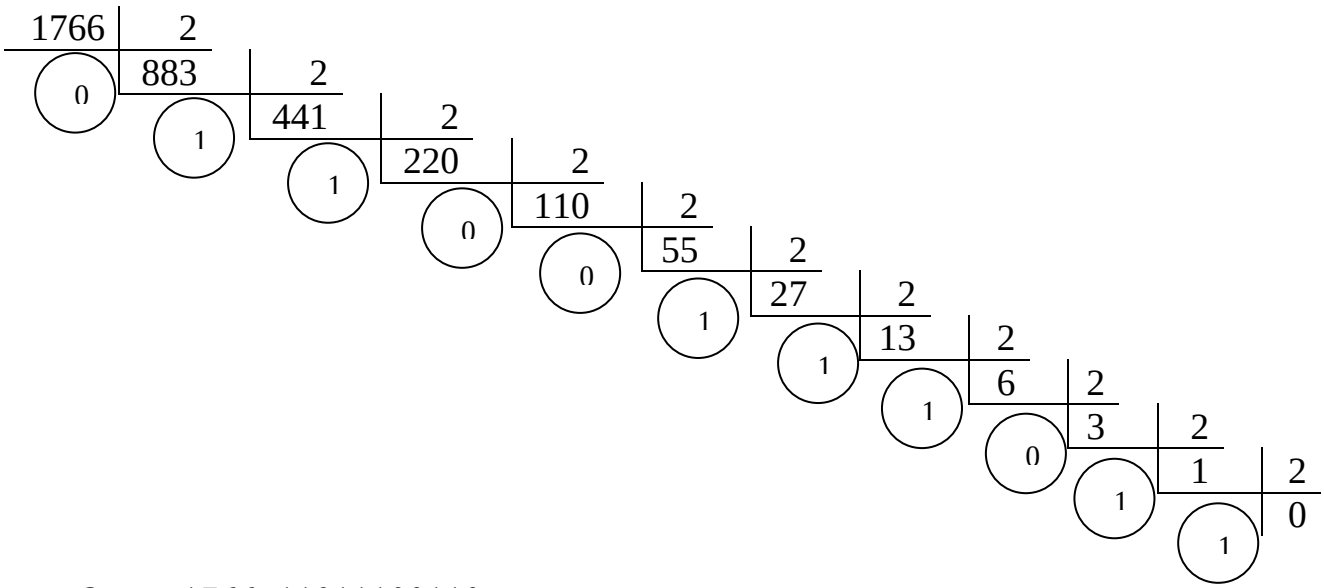
Тепер переведемо це ж десяткове число (1766) у вісімкову систему числення.



Отже, $1766 = 3346_{(8)}$.

Під час цього основа 8 дає змогу записати вже в десятковій системі числення, тобто потрібно перевести $3346_{(8)}$ у десяткову систему числення.
$3346_{(8)} = 3\cdot83+3\cdot82 + 4\cdot8 + 6;$
$= 3\cdot512 + 3\cdot64+32 + 6;$
$= 1536 + 192 + 32 + 6;$
$= 1766.$

Тепер переведемо це саме число (1766) у двійкову систему числення і одержане двійкове число назад в десяткову систему числення.



Отже, $1766=11011100110_{(2)}$.

Зворотнє двійкового числа в десяткове:
$11011100110_{(2)}=1\cdot2^{10}+1\cdot2^{9}+0\cdot2^{8} + 1\cdot2^{7} + 1\cdot2^{6} + 1\cdot2^{5} +0\cdot2^{4}+0\cdot2^{3}+1\cdot2^{2}+1\cdot2^{1} +0;$
$= 210+ 29+ 27 + 26 + 25 + 22+ 21;$
$= 1024+512+128+64+32+ 4+2= 1766.$

Алгоритми переведення чисел з однієї позиційної системи числення в іншу

1. Для переведення чисел із системи числення з основою p в систему числення з основою q, використовуючи арифметику нової системи числення з основою q, потрібно записати коефіцієнти розкладу, основи степенів і показники степенів у системі з основою q і виконати всі дії в цій самій системі. Очевидно, що це правило зручне під час переведення до десяткової системи числення.

2. Для переведення чисел із системи числення з основою p у систему числення з основою q з використанням арифметики старої системи числення з основою p потрібно:

- для переведення цілої частини:

– послідовно число, записане в системі основою p ділити на основу нової системи числення, виділяючи остачі. Останні записані у зворотному порядку, будуть утворювати число в новій системі числення;

- для переведення дробової частини:

– послідовно дробову частину множити на основу нової системи числення, виділяючи цілі частини, які й будуть утворювати запис дробової частини числа в новій системі числення.

Цим самим правилом зручно користуватися в разі переведення з десяткової системи числення, тому що її арифметика для нас зрозуміліша.

Приклади: $999{,}35_{10}=1111100111{,}01011_2$

для цілої частини:

999	2	
1	499	2
	1	249	2
		1	124	2
			0	62	2
				0	31	2
					1	15	2
						1	7	2
							1	3	2
								1	1

для дробової частини:

0,	35
	2
0,	70
	2
1,	40
	2
0,	80
	2
1,	60
	2
1,	20

Методичні вказівки

1. Обчислити:

а) $202332_4 + 22222_4$; б) $220111_4 – 32323_4$; в) $23230301_4 : 113_4$.

Розв'язання. У четвірковій системі числення цифрами є: {0, 1, 2, 3}. Складемо для них таблиці додавання і множення (табл. 4 і 5).

Таблиця 4

+	0	1	2	3
0	0	1	2	3
1	1	2	3	10
2	2	3	10	11
3	3	10	11	12

Таблиця 5

x	0	1	2	3
0	0	0	0	0
1	0	1	2	3
2	0	2	10	12
3	0	3	12	21

Тепер виконуємо дії:

а) $\begin{array}{r} 202332_4 \\ + \\ 22222_4 \\ \hline 231220_4 \end{array}$

Перевірка: $\begin{array}{r} 231220_4 \\ - \\ 22222_4 \\ \hline 202332_4 \end{array}$

б) $\begin{array}{r} 220111_4 \\ - \\ 32323_4 \\ \hline 121122_4 \end{array}$

Перевірка: $\begin{array}{r} 121122_4 \\ + \\ 32323_4 \\ \hline 220111_4 \end{array}$

в) $202332_4 \mid \frac{113_4}{200203_4}$

232

303

232

1101

1011

30_4 (остача)

Перевірка:

200203_4

$\times$

113_4

1211221

$+\ 200203$

200203

23230211_4

$23230211_4 + 30_4 = 2323301_4$

2. Перевести з однієї системи в іншу:

а) $138_{10} \rightarrow x_4$;

б) $1340_{10} \rightarrow x_{15}$;

в) $10032_4 \rightarrow x_3$;

г) $2032_4 \rightarrow x_{10}$.

Розв'язання.

а) $138_{10} \rightarrow x_4$;

$138_{10} \mid \frac{4_{10}}{34_{10}} \mid \frac{4_{10}}{8_{10}} \mid \frac{4_{10}}{2_{10}} \mid \frac{4_{10}}{0}$

12 32 8 0

18 16 2 0

16 2 2

2

Оскільки $4<10$, то всі остачі є цифрами в новій системі числення.

Отже, $138_{10}=2022_4$.

б) $1340_{10} \rightarrow x_{15}$;

У 15-ковій системі числення число 14 є цифрою і позначається (14).

$1340_{10} \mid \frac{15_{10}}{89_{10}} \mid \frac{15_{10}}{5_{10}} \mid \frac{15_{10}}{0}$

120 75 0

140 135 14 5

135 5

5

Отже, $1340_{10}=5(14)5_{15}$

в) $10032_4 \rightarrow x_3$

Число 3 в четвірковій системі числення записують так само.

Тоді,

$10032_4 \mid \frac{3_4}{1122_4} \mid \frac{3_4}{132_4} \mid \frac{3_4}{22_4} \mid \frac{3_4}{3_4} \mid \frac{3_4}{1_4} \mid \frac{3_4}{0}$

3 22 12 21 3 0

10 21 12 12 0 1

3 12 12 1

13 12 0

12 12

12 0

12

0

Отже, $10032_4 \rightarrow 101000_3$.

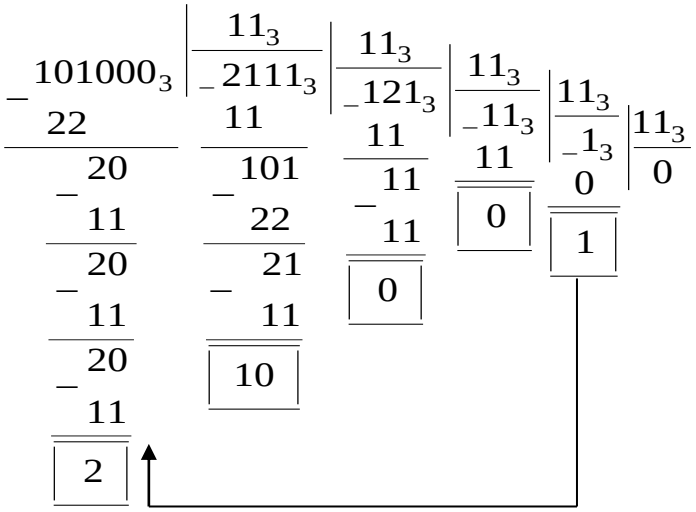
Перевірка: число 4 у трійковій системі числення записують як 11_3. Використовуючи таблиці додавання і множення одноцифрових чисел у трійковій системі числення (табл. 6, 7) матимемо:

Таблиця 6

+	0	1	2
0	0	1	2
1	1	2	10
2	2	10	11

Таблиця 7

x	0	1	2
0	0	0	0
1	0	1	2
2	0	2	11

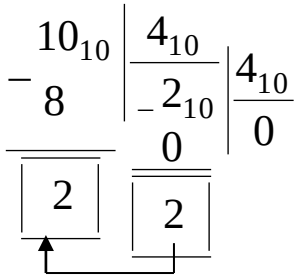


Отже, $101000_3=100(10_3)2_4=10032_4$, оскільки $10_3=3_4$.

г) $2032_4 \rightarrow x_{10}$.

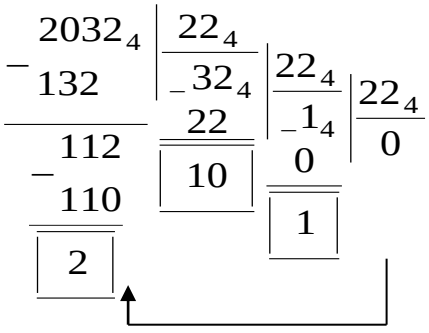
І спосіб.

Число 10 в четвірковій системі числення записують так:



$10_{10}=22_4$.

Тоді,



Отже, $2032_4=1(10_4)2_{10}=142_{10}$.

ІІ спосіб. $2032_4=2\cdot4^3+3\cdot4^1+2\cdot4^0=2\cdot64+0+12+2=142_{10}$.

Як бачимо, результати однакові.

Приклад. Варіант 0

1. Обчислити: $23015_7+14304_5->X_7$

$14304_5=1*5^4+4*5^3+3*5^2+4=1204_{10}=3340_7$.

1204	7			
1204	172	7		
0	168	24	7	
	4	21	**3**	
		3		

g=7

2	3	0	1	5
+	3	3	4	0
2	6	3	5	5

Відповідь: $23015_7+3340_7->26355_7$.

2. Обчислити: $46141_7-12334_5->X_7$

$12334_5=1*5^4+2*5^3+3*5^2+3*5+4=969_{10}=2553_7$.

969	7			
966	138	7		
3	133	19	7	
	5	14	**2**	
		5		

g=7 (–1 → +7)

4	6	1	4	1
-	2	5	5	3
3	3	2	5	5

Відповідь: $23015_7+2553_7->33255_7$.

3. Обчислити: $20322_4*401_5->X_5$.

$20322_4=2*4^4+0*4^3+3*4^2+2*4+2=570_{10}=4240_5$

570	5				
570	114	5			
0	110	22	5		
	4	20	**4**		$16_{10}=31_5$
		2			$11_{10}=21_5$
g=5					$18_{10}=33_5$
		4	2	4	0
*			4	0	1
		4	2	4	0
	0	0	0	0	
33	1	1	0		
33	2	0	2	4	0

Відповідь: $4240_5*401_5->3320240_5$.

4. Обчислити: $15240500_6/230304_4 \to X_6$

$230304_4=2*4^5+3*4^4+0*4^3+3*4^2+0*4+4=2852_{10}=21112_6$

2852	6				21112	*1
2850	475	6			42224	*2
2	474	79	6		103340	*3
	1	78	**13**	6	124452	*4
		1	12	**2**	150004	*5
g=6			**1**			

15240500	21112
150004	51
24011	
21112	
2455	

Відповідь: $15240500_6/21112_6 \to 51_6+2455/21112$.

Завдання 1.

Обчислити: $205315_6 + 15326_9 \to x_9$.

Переведемо число 205315_6 у x_9 систему:

$205315_6 = 2 \cdot 6^5 + 0 \cdot 6^4 + 5 \cdot 6^3 + 3 \cdot 6^2 + 1 \cdot 6^1 + 5 \cdot 6^0 = 16751_{10} = 24872_9$.

	16751	9			
	16749	1861	9		
	2	1854	206	9	
		7	198	22	9
			8	18	2
				4	
	g=9				
	2	4	8	7	2
+	1	5	3	2	6
2	2	1	6	4	2

Відповідь: $205315_6 + 15326_9 = 221642_9$.

Завдання 2.

Обчислити: $43434_5 - 22222_4 \to x_5$.

Переведемо число 22222_4 у x_5 систему:

$22222_4 = 2 \cdot 4^4 + 2 \cdot 4^3 + 2 \cdot 4^2 + 2 \cdot 4^1 + 2 \cdot 4^0 = 682_{10} = 10212_5$.

	682	5			
	680	136	5		
	2	135	27	5	
		1	25	5	5
			2	5	1
				0	

Продовження табл.

	g = 5				
	4	3	4	3	4
+	1	0	2	1	2
	3	3	2	1	2

Відповідь: $43434_5 - 22222_4 = 33212_5$.

Завдання 3.

Обчислити $3405_6 \cdot 1032_4 \to x_6$.

Переведемо число 1032_4 у x_6 систему:

$1032_4 = 1 \cdot 4^3 + 0 \cdot 4^2 + 3 \cdot 4^1 + 2 \cdot 4^0 = 78_{10} = 210_6$.

	78	6					
	78	13	6				
	0	12	2				
		1					
	g = 6						
				3	4	0	5
×					2	1	0
				0	0	0	0
			3	4	0	5	
	1	1	2	1	4		
	1	1	5	5	4	5	0

Відповідь: $3405_6 \cdot 1032_4 = 1155450_6$.

Завдання 4.

Обчислити: $2022101_6/122_3 \to x_6$.

Переведемо число 122_3 у x_6 систему:

$122_3 = 1 \cdot 3^2 + 2 \cdot 3^1 + 2 \cdot 3 = 17_{10} = 25_6$.

17	6										
12	2										
5											
g = 6											
2	0	2	2	1	0	1	2	5			
1	5	2					4	2	1	2	5
	1	0	2								
		5	4								
			4	1							
			2	5							
			1	2	0						
				5	4						
				2	2	1					
				2	2	1					
						0					

Відповідь: $2022101_6/122_3 = 42125_6$.

Контрольні питання

1. Теорема про запис будь-якого цілого числа в системі числення.
2. Арифметичні операції над системними числами.
3. Алгоритми переведення чисел з однієї позиційної системи числення в іншу.
4. Алгоритми переведення чисел з основами 2,8,16 з однієї позиційної системи числення в іншу.

Практична робота № 8

Тема: Контрольна робота з систем числення

Мета: закріпити та перевірити засвоєння методів переведення в різні системи числення, проведення операцій додавання, віднімання, множення та ділення в різних СЧ.

Методичні вказівки

1. Обчислити: $x = \frac{ab+c}{(d+k)m-p}$. Усі дії виконати в g-ній системі числення.

a = $153_6 = 69_{10} = 153_6$
b = $144_5 = 126_{10} = 121_6$
c = $1211_3 = 49_{10} = 121_6$
d = $362_8 = 242_{10} = 1042_6$
k = $31_4 = 13_{10} = 21_6$
m = $110_3 = 12_{10} = 20_6$
p = $55_7 = 40_{10} = 104_6$
g = 6

$$x = \frac{153_6 \cdot 121_6 + 121_6}{(1042_6 + 21_6)20_6 - 104_6} = \frac{23353_6 + 121_6}{1103_6 * 20_6 - 104_6} = \frac{23514_6}{22100_6 - 104_6} = \frac{23514_6}{21552_6} = 1\frac{1522_6}{21552_6}$$

Відповідь: $1\frac{1522_6}{21552_6}$.

2. Обчислити: $x = \frac{a*b+c}{(d+k)*m-p}$. Усі дії виконати в g-ній системі числення.

a=111001_4=1345_{10}=111001_4
b=12253_7=3223_{10}=302113_4
c=43021_8=17937_{10}=10120101_4
d=31_8=25_{10}=121_4
k=11011_3=112_{10}=1300_4
m=115_6=47_{10}=233_4
p=24532_7=6442_{10}=1210222_4
g=4

$$x = \frac{a * b + c}{(d + k) * m - p} = \frac{111001 * 302113 + 10120101}{(121 + 1300) * 233 - 1210222} = \frac{100202111113 + 10120101}{2021 * 233 - 1210222} = \frac{100212231220}{1210213 - 1210222} == \frac{100212231220}{-3} = = -11202033031\frac{1}{3}$$

Відповідь: $(-11202033031\frac{1}{3})_4$.

Завдання КР.

Обчислити X, всі дії виконати в g-ній системі числення. Результат записати в g-ній та десятковій системах числення.

$$X = \frac{a*b+c}{(d+k)*m-p}.$$

№	*a*	*b*	*c*	*d*	*k*	*m*	*p*	*g*
1.	321_4	642_7	57_8	121_3	45_6	54_7	12_4	2
2.	232_5	421_6	43_7	210_4	120_3	46_7	17_8	3
3.	423_6	215_7	51_6	320_4	210_3	110_2	25_6	4
4.	121_3	432_5	103_4	401_5	102_3	101_2	21_3	5
5.	567_8	142_5	315_6	113_4	211_3	111_2	101_2	6
6.	744_8	213_4	502_6	312_4	125_6	103_4	33_4	7
7.	625_7	452_6	321_4	121_3	30_4	53_6	15_6	8
8.	242_5	377_8	155_6	222_3	124_5	103_4	25_6	2
9.	153_6	710_8	440_5	331_4	210_3	401_5	12_5	3
10.	442_5	215_6	123_4	461_7	52_6	102_3	71_8	4
11.	245_6	546_7	320_5	603_7	22_5	51_6	35_6	5
12.	126_7	144_5	121_6	362_8	31_4	110_3	55_7	6
13.	662_7	411_5	270_8	223_4	17_8	34_5	43_6	7
14.	771_8	325_6	321_4	144_5	72_8	231_4	120_3	8
15.	615_7	504_6	102_3	413_6	241_5	133_5	211_3	2
16.	504_6	444_5	215_8	332_4	115_6	212_4	14_5	3
17.	325_7	326_8	112_4	211_3	510_6	421_5	105_6	4
18.	114_6	214_7	715_8	235_6	314_5	214_6	102_3	5
19.	154_6	511_7	322_5	301_4	502_6	321_4	143_6	6
20.	455_6	313_4	621_8	125_6	304_5	220_3	125_6	7
21.	774_8	213_4	502_6	312_4	125_6	103_4	33_4	7
22.	134_8	18_9	2200_3	30_4	8_{10}	7_8	23_4	5
23.	423_6	215_7	51_6	320_4	210_3	110_2	25_6	4
24.	111_4	25_6	320_4	2_{10}	46_8	121_5	11001_2	5
25.	625_7	123_4	22_5	34_5	51_6	34_5	35_6	6
26.	126_7	546_7	331_4	320_5	125_6	53_6	55_7	7
27.	567_8	142_5	315_6	113_4	211_3	111_2	101_2	6
28.	327_8	326_8	112_4	211_3	510_6	421_5	105_6	4
29.	321_4	421_6	43_7	121_3	31_4	101_2	15_8	4
30.	154_6	313_6	215_8	144_5	72_8	212_4	143_6	5

Номер варіанта КР вказується викладачем на парі.

Контрольні питання

1. Теорема про запис будь-якого цілого числа в системі числення.
2. Арифметичні операції над системними числами.
3. Алгоритми переведення чисел з однієї позиційної системи числення в іншу.
4. Алгоритми переведення чисел з основами 2,8,16 з однієї позиційної системи числення в іншу.

Практична робота № 9

Тема: Застосування конгруенції, їх властивостей та теорем Ейлера і Ферма

Мета: навчитися розв'язувати Діофантові рівняння першого ступеня, визначати остачу від ділення, розв'язувати лінійні конгруенції та використовувати їх в прикладних задачах цілочисельного розв'язку.

Теоретичні відомості

Означення 1. *Цілі числа* a і b *називають конгруентними за модулем* m*, де* m *– ціле число, якщо їхня річниця* $a - b$ *ділиться на* m*.* Позначення:

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

Якщо a і b не конгруентні за модулем m, то пишуть,

$$a \not\equiv b \pmod{m}.$$

Означення 2. *Цілі числа* a і b *називають конгруентними за модулем* m*, де* $m \in Z$*, якщо вони під час ділення на* m *дають однакові остачі.*

Означення 3. *Цілі числа* a і b *називають конгруентними за модулем* m*, де* $m \in Z$*, якщо існує таке ціле число* q*, що* $a=b+mq$*.*

Означення 1, 2, 3 рівносильні.

Основні властивості конгруенцій

2. Відношення конгруентності за цим модулем є бінарне відношення еквівалентності на множині цілих чисел. Класи еквівалентності називають **класами лишків за даним модулем.**

3. Конгруенції за одним модулем можна почленно додавати, віднімати і множити.

4. До обох частин конгруенції можна додати будь-яке ціле число (це дає змогу переносити будь-який доданок з однієї сторони в другу з протилежним знаком).

5. До будь-якої частини конгруенції можна додати довільне ціле число, кратне модулю.

6. Обидві частини конгруенції можна помножити на ціле число.

7. Обидві частини конгруенції можна поділити на їхній спільний дільник, якщо він взаємно простий за модулем.

8. Якщо у виразі $f(a_1,a_2,...,a_k)\sum Aa_1^{n1},a_2^{n2},...,a_k^{nk}$, усі коефіцієнти A і числа $a_1,a_2,...,a_k$ замінити на конгруентні їм за модулем m коефіцієнти B і числа $b_1,b_2,...,b_k$ відповідно, то вираз:

$$g(b_1, b_2,..., b_k) = \sum Bb_1^{n_1}\ b_2^{n_2}...b_k^{n_k},$$

буде конгруентний заданому за модулем m:

$$f\left(a_1, a_2, ..., a_k\right) \equiv g\left(b_1, b_2, ..., b_k\right)\left(\mathrm{mod}\, m\right).$$

9. Обидві частини конгруенції і модуль можна множити на ціле число.

10. Обидві частини конгруенції і модуль можна скорочувати на їхній спільний дільник.

11. Якщо конгруенція має місце за кількома модулями, то вона має місце і за модулем, який дорівнює спільному найменшому кратному цих модулів.

12. Якщо конгруенція має місце за модулем *m,* то вона має місце за модулем *d,* де *d* – довільний дільник числа *m.*

13. Якщо одна частина конгруенції і модуль діляться на деяке число, то й друга частина конгруенції ділиться на те саме число.

14. Якщо a≡b(mod*m)*, то (a,m)≡(b,m).

Теорема Ейлера. *Якщо* $m > 1$ і $\left(a, m\right) = 1$, то $a^{\varphi(m)} \equiv 1\left(\mathrm{mod}\, m\right)$.

Теорема Ферма (мала теорема Ферма). *Якщо число p просте,*

$$\left(a, p\right) = 1 \text{ то } a^{p-1} \equiv 1\left(\mathrm{mod}\, p\right).$$

Унаслідок. *Якщо p – просте число, a – будь-яке ціле число, то* $a^p \equiv a\left(\mathrm{mod}\, p\right)$.

Методичні вказівки

Приклад 1. Які з чисел 234, 634, 104 конгруентні числу 9 за модулем 25.

Розв'язання. Віднімемо від зазначених чисел число 9. Отримуємо:

234–9=225, 634–9=625, 104–9=95. Числа 225 і 625 діляться на 25, тому числа 234 і 634 конгруентні числу 9 за модулем 25, тобто:

$$234 \equiv 9\left(\mathrm{mod}\, 25\right),\ 634 \equiv 9\left(\mathrm{mod}\, 25\right).$$

Приклад 2. Довести, що $11 \cdot 13 \cdot 18 \cdot 2322 \equiv -3\left(\mathrm{mod}\, 7\right)$.

Розв'язання. Скористуємося другою властивістю конгруенцій за одним і тим самим модулем. Розглянемо почленно конгруенції:

$11 \equiv 4\left(\mathrm{mod}\, 7\right); 13 \equiv 6\left(\mathrm{mod}\, 7\right) \equiv -1\left(\mathrm{mod}\, 7\right); 18 \equiv 4\left(\mathrm{mod}\, 7\right); 2322 \equiv 5\left(\mathrm{mod}\, 7\right)$,

помножимо всі одержані конгруенції,

$$11 \cdot 13 \cdot 18 \cdot 2322 \equiv 4 \cdot \left(-1\right) \cdot 4 \cdot 5\left(\mathrm{mod}\, 7\right) \equiv -3\left(\mathrm{mod}\, 7\right).$$

Отже, $11 \cdot 13 \cdot 18 \cdot 2322 \equiv -3\left(\mathrm{mod}\, 7\right)$.

Приклад 3. Знайти остачу від ділення $13^{1054} - 23 \cdot 16^{285} + 22^{17}$ на 15.

Розв'язання. Скористаємося властивостями конгруенцій за модулем 15. Нам треба знайти таке ціле невід'ємне число x, що $x \equiv 13^{1054} - 23 \cdot 16^{285} + 22^{17}\left(\mathrm{mod} 15\right)$ і $x < 15$. Оскільки $\left(13 + 2\right) \vdots 15$, то $13 \equiv -2\left(\mathrm{mod} 15\right)$, тобто $13^4 \equiv \left(-2\right)^4\left(\mathrm{mod} 15\right) \equiv 1\left(\mathrm{mod} 15\right)$.

За властивостями $(13^4)^{263} \equiv 1^{263} (\mathrm{mod} 15) \Rightarrow 13^{1054} \equiv 1 (\mathrm{mod} 15)$.

$$13^{1054} \equiv 4 (\mathrm{mod} 15). \qquad (*)$$

$23 \equiv 8 (\mathrm{mod} 15);\ 16 \equiv 1 (\mathrm{mod} 15) \Rightarrow 16^{285} \equiv 1 (\mathrm{mod} 15) \Rightarrow 23 \cdot 16^{285} \equiv 8 \cdot 1 (\mathrm{mod} 15) \equiv 8 (\mathrm{mod} 15)$ (**)

$$23\equiv 7(\mathrm{mod}15);22^2\equiv 7^2(\mathrm{mod}15)\equiv 4(\mathrm{mod}15);$$
$$22^4\equiv 4^2(\mathrm{mod}15)\equiv 1(\mathrm{mod}15)\Rightarrow 22^{16}\equiv 1(\mathrm{mod}15);\ 22^{17}\equiv 1\cdot 7(\mathrm{mod}15)\qquad (\overset{*}{**})$$

Виконаємо дії додавання та віднімання над конгруенціями (*),(**),($\overset{*}{**}$).

$$(*)-(**)+(\overset{*}{**}),$$
$$13^{1054}\equiv 4(\mathrm{mod}15)\cdot -23\cdot 16^{285}\equiv 8(\mathrm{mod}15)+22^{17}\equiv 7(\mathrm{mod}15)\Rightarrow 13^{1054}-23\cdot 16^{285}+22^{17}\equiv$$
$$\equiv 4-8+7(\mathrm{mod}15)\equiv 3(\mathrm{mod}15)$$

Отже, число $13^{1054}-23\cdot 16^{285}+22^{17}$ під час ділення на 15 дає остачу 3.

Приклад 4. Розв'язати конгруенцію: $ax\equiv b(mod\ m)$.

Нехай (a, m), нехай P_{n-1} – чисельник передостаннього підхідного дробу $\frac{P_{n-1}}{Q_{n-1}}$ для числа $\frac{m}{a}$, $\frac{m}{a}=\frac{P_n}{Q_n}$. Оскільки $\frac{m}{a}$ нескоротний дріб, то $m=P_n,\ a=Q_n$. За властивостей підхідних дробів маємо $a\cdot(-1)^n P_{n-1}\equiv 1(\mathrm{mod}\,m)$.

Розглянемо приклад $7x\equiv 1(mod\ 20)$ маємо таблицю, де m=20, $a=7$, n=2, $P_{n-1}=P_1$=3. Тоді $\frac{m}{a}=\frac{20}{7}$;

k	−1	0	1	2
q_k	–	2	1	6
P_k	1	2	3	20
Q_k	0	1	1	7

$$7x*(-1)^2*3\equiv 1*(-1)^2*3(mod\ 20);$$
$$x*7*3\equiv 3(mod\ 20);$$
$$x\equiv 3(mod\ 20).$$

Приклад 5. Розв'язати конгруенцію: $501x\equiv 1(mod\ 1993)$.

Розв'язання. (1993,501)=1.

Розкладемо дріб $\frac{1993}{501}$ у ланцюговий дріб і знайдемо P_{n-1} та m.

За алгоритмом Евкліді отримаємо:

1993=501***3**+490; n=0;
501=490***1**+11; n=1;
490=11***44**+6; n=2;
11=6***1**+5; n=3;
6=5***1**+1; n=4;
5=1***5**+0; n=5;

Отже, $\frac{1993}{501}=[3;1,44,1,1,5],\ n=5$.

Для обчислення P_{n-1}, складемо таблицю.

k	–1	0	1	2	3	4	5
q_k	///////	**3**	**1**	**44**	**1**	**1**	**5**
P_k	1						
Q_k	0	1					

k	-1	0	1	2	3	4	5
q_k	–	3	1	44	1	1	5
P_k	1	3	4	179	183	362	1993

Звідси $P_{n-1} = P_4 = 362$.

$$501 * 362 \equiv 181362 \equiv 90 * 1993 + 1992 \equiv -1(mod 1993).$$

Відповідь: $x \equiv (-1)^5 * 362(mod\ 1993)$.

Приклад 6. Знайти остачу від ділення на 8.

$$3^{345} + 7^{199}(mod 8) \equiv$$

$$\varphi(8) = 8 * \left(1 - \frac{1}{2}\right) = 4;\ a^4 \equiv 1(mod 8);$$

$$345 = 4 * 86 + 1; 199 = 4 * 49 + 3;$$

$$3^{345} \equiv 3^1(mod 8);\ 7^{199} \equiv 7^3(mod 8);$$

$$3^{345} + 7^{199}(mod 8) \equiv 3 + 343 = 346(\text{mod}8) = 43 * 8 + 2 = 2(\text{mod}8).$$

Остача від ділення $3^{345} + 7^{199}$ на 8 дорівнює 2.

Приклад 7. Розв'язати лінійну конгруенцію $64\text{x} \equiv 5(mod\ 13)$.

Обчислимо ланцюговий дріб $\frac{m}{a} = \frac{13}{64} = [0; 4,1,12]$.

13=64*0+13
64=13*4+12
13=12*1+1
12=1*12+0

k	–1	0	1	2	3
q_k	///////	**0**	**4**	**1**	**12**
P_k	1	**0**	1	1	13
Q_k	0	1	4	5	64

$64\text{x} * (-1)^3 * 1 \equiv -64\text{x} \equiv -5(mod\ 13);\ x \equiv -5 + 13(mod\ 13) \equiv 8(mod\ 13);$

Перевірка: $64 * 8 \equiv 512(mod\ 13) \equiv 39 * 13 + 5 \equiv 5(mod 13)$.

Контрольні питання

1. Означення конгруенції. Властивості.
2. Операції з конгруенціями.
3. Лінійні конгруенції та способи їх розв'язку.
4. Підхідні дроби та їх табличне обчислення.
5. Теорема Ейлера та теорема Ферма.

Практична робота № 10

Тема: Діофантові рівняння в прикладних задачах цілочисельного розв'язку

Мета: навчитися розв'язувати Діофантові рівняння першого ступеня, визначати остачу від ділення, розв'язувати лінійні конгруенції та використовувати їх в прикладних задач цілочисельного розв'язку.

Теоретичні відомості

Рівняння виду $P(x,y,...z)=0$, де $P(x,y,...z)$ – многочлен декількох змінних з цілими коефіцієнтами для яких потрібно знайти цілі розв'язки, називають діофантовими рівняннями. Названі вони ім'ям грецького математика Діофанта, який жив у III ст. н. е. Його книга «Арифметика» містила 189 задач з цілими числами, для кожної з яких наводилося один або декілька розв'язків.

Розв'язати діофантове рівняння означає:

а) з'ясувати, чи має рівняння хоча б один ненульовий розв'язок в цілих числах;

б) якщо рівняння має розв'язок в цілих числах, то з'ясувати скінченна чи нескінченна множина його розв'язків;

в) знайти всі цілі розв'язків рівняння.

Лінійні діофантові рівняння виду $ax+by=c$ навчилися розв'язувати ще до Діофанта. Стародавні греки знали, що якщо це рівняння має один цілий розв'язок $(x_0;y_0)$, то його буде задовольняти нескінченна множина пар $(x;y)$ виду $x=x_0+bk; y=y_0-bk$, де k – будь яке ціле число.

Математики Стародавньої Греції та Стародавньої Індії знали методи розв'язання деяких рівнянь другого степеня виду $ax^2+bxy+cy^2=dz^2$. Зокрема їм були відомі всі піфагорові трійки натуральних чисел x,y,z, що задовольняють рівняння $x^2+y^2=z^2$. Усі трійки взаємно простих піфагорових чисел стародавні математики знаходили за формулами $x=m^2-n^2$, $y=2mn$, $z=m^{2+}n^2$, m,n – натуральні числа причому $n>m$.

Особливе місце серед діофантових рівнянь займає рівняння $x^n+y^n=z^n$, де n– натуральне число. Французький математик П'єр Ферма довів, що у разі $n>2$ рівняння $x^n+y^n=z^n$ не має розв'язків у натуральних числах x,y,z.

Діофантові рівняння першого степеня

Рівняння виду $ax+by=c$ де a,b,c – числа, а x,y– змінні, називають діофантовим рівнянням першого степеня з двома змінними. Для розв'язання рівняння застосовують наступні теореми.

Теорема 1. Якщо *a* і *b* – взаємно прості числа, то для будь-якого цілого *c*, рівняння *ax+by=c* має хоча б один розв'язок у цілих числах.

Теорема 2. Якщо *a* і *b* мають спільний натуральний дільник $d \neq 1$, а ціле число c не ділиться на *d*, то рівняння *ax+by=c* не має розв'язків у цілих числах.

Теорема 3. Якщо *a* і *b* взаємно прості числа, то рівняння *ax+by=c* має нескінченну кількість розв'язків $x = x_0 + bk; y = y_0 - ak$, які знаходять за формулами, де $(x_0; y_0)$ – будь-який цілий розв'язок цього рівняння, $k \in Z$.

Частинний розв'язок $(x_0; y_0)$ можна знайти підбором, для малих *a* і *b*, а у випадку коли числа $a\,i\,b$ великі, то користуємось наступною теоремою.

Теорема 4. НСД(a,b)=d може бути записаний у вигляді *d=am+bn*, де *m, n* цілі числа, *d* знаходимо за алгоритмом Евкліда.

Методичні вказівки

Приклад 1. Розв'язати в цілих числах рівняння. $13x + 21y = 55$.

Оскільки *НСД(13,21)=1,* то таке рівняння має безліч розв'язків. Підбором встановлюємо частинний розв'язок $(x_0; y_0) = (1;2)$.

Тоді загальний розв'язок має вигляд: $x = 1 + 21k; y = 2 - 13k; k \in Z$.

Відповідь: $x = 1 + 21k; y = 2 - 13k; k \in Z$.

Приклад 2. Розв'язати в цілих числах рівняння. $45x - 37y = 25$

Оскільки *НСД(45;37)=1,* то рівняння має безліч розв'язків.

Щоб знайти $(x_0; y_0)$ застосуємо алгоритм Евкліда:

45=37·1+8;37=8·4+5;8=5·1+3;5=3·1+2;3=2·1+1. Отже *d*=1. Запишемо алгоритм Евкліда у зворотному напрямку (лінійне представлення):

$$1 = 3 - 2 \cdot 1 = 3 - 1(5 - 3 \cdot 1) = 3 - 5 + 3 \cdot 1 = 2 \cdot 3 - 5 = 2 \cdot (8 - 5 \cdot 1) - 5 =$$
$$= 2 \cdot 8 - 2 \cdot 5 - 5 = 2 \cdot 8 - 3 \cdot 5 = 2 \cdot 8 - 3 \cdot (37 - 8 \cdot 4) = 2 \cdot 8 - 3 \cdot 37 + 12 \cdot 8 =$$
$$= 14 \cdot 8 - 3 \cdot 37 = 14 \cdot (45 - 37 \cdot 1) - 3 \cdot 37 = 14 \cdot 45 - 14 \cdot 37 - 3 \cdot 37 =$$
$$= 45 \cdot 14 - 37 \cdot 17.$$

Отже (14;17) частинний розв'язок рівняння $45x - 37y = 1$.

Тоді, $25 = 45 \cdot (14 \cdot 25) - 37 \cdot (17 \cdot 25); 25 = 45 \cdot 350 - 37 \cdot 425,$ тобто, $(x_0; y_0) = (350;425)$.

Отже всі розв'язки знайдемо за формулами $x = 350 - 37k; y = 425 - 45k, k \in Z$.

Відповідь: $x = 350 - 37k; y = 425 - 45k, k \in Z$.

Приклад 3. Розв'язати в цілих числах рівняння. 2183*x*–1961*y*=6327.

Знайдемо *НСД(2183;1961)=d*для цього скористаємося алгоритмом Евкліда.

$$2183 = 1961 \cdot 1 + 222; 1961 = 222 \cdot 8 + 185; 222 = 185 \cdot 1 + 37; 185 = 37 \cdot 5 + 0.$$

Отже, d=(2183;1961)=37.

Запишемо алгоритм Евкліда в зворотному напрямку:

$$37 = 222 - 185 \cdot 1 = 222 - (1961 - 222 \cdot 8) = 222 - 1961 + 222 \cdot 8 = 222 \cdot 9 - 1961 =$$
$$= (2183 - 1961 \cdot 1) \cdot 9 - 1961 = 2183 \cdot 9 - 1961 \cdot 9 - 1961 = 2183 \cdot 9 - 1961 \cdot 10$$

Отже (9;10) – частинний розв'язок рівняння 2183*x*–1961*y*=37.

Тоді, $6327 = 2183\cdot(9\cdot171) - 1961\cdot(10\cdot171) = 2183\cdot1539 - 1961\cdot1710$, тобто (1539; 1710) частинний розв'язок рівняння 6327=2183x–1961y.

Загальний розв'язок має вигляд: $x = 1539 - 1961k; y = 1710 - 2183k, k \in Z$.

Відповідь: $x = 1539 - 1961k; y = 1710 - 2183k, k \in Z$.

Приклад 4. 5x+7y=11; $5x \equiv 11(mod7)$;

$$5x \equiv 11 + 7 * 2(mod7) \equiv 25;$$

$$5x \equiv 25(mod7);\quad nsd(5,7) = 1;\ \vdots 5,\quad x \equiv 5(mod7);\quad \mathbf{x=7t+5;}$$

$$5(7t + 5) + 7y = 11;\quad 35t + 25 + 7y = 11; 7y = 11 - 25 - 35t;$$

$$7y = -14 - 35t; \boldsymbol{y = -2 - 5t};$$

$$\begin{cases} x = 7t + 5; \\ y = -2 - 5t; \end{cases}$$

t	– 2	– 1	0	1	2	3
x	– 9	– 2	5	12	19	– 9
y	8	3	– 2	– 7	– 12	8

Відповідь: (–9,8),(–2,3),(5,–2),(12,–7),(19,–12),(–9,8),…

Приклад 5. 102x–37y=408;

$$102x \equiv 408(mod37); 28x \equiv 1(mod37);$$

37/28=[1;3,9];
37=28*__1__+9;
28=9*__3__+1;
9=1*__9__+0;

k	–1	0	1	2
q_k	///////	**1**	**3**	**9**
P_k	1	**1**	4	37
Q_k	0	1	3	28

$$28 * (-1)^2 * 4 * x \equiv (-1)^2 * 4 * 1(mod37)$$

$$112x \equiv 4(mod37); 112 \equiv 1(mod37);$$

$$x \equiv 4(mod37);\ \mathbf{x=37t+4;}$$

$$102(37t + 4) - 37y = 408;\quad 102 * 37t + 408 - 37y = 408;$$

$$102 * 37t = 37y;$$

$$\boldsymbol{y = 102t};$$

$$\begin{cases} x = 37t + 4; \\ y = 102t; \end{cases}$$

t	– 2	– 1	0	1	2	3
x	– 70	– 33	4	41	78	– 70
y	– 204	– 102	0	102	204	– 204

Відповідь: (–70,–204),(–33,–102),(4,0),(41,102),(78,204),(–70,–204),….

Приклад 6. Для настилання підлоги завширшки 4,5 м є дошки шириною 12 та 17 см. Скільки треба взяти дошок того та другого розміру, якщо вважати, що довжина дошок і кімнати однакова.

$$4.5m=450cm;$$
$$12x+17y=450;$$
$$12x\equiv 450(mod17);$$
$$12x\equiv 26*17+8(mod17);$$
$$12x\equiv 8(mod17);$$

$\langle nsd(17,4)=1,\vdots 4,\rangle;$

$$3x\equiv 2(mod17);$$
$$3x\equiv -15(mod17);$$

$\langle nsd(3,17)=1,\vdots 3\rangle;$

$$x\equiv -5(mod17)\equiv 12(mod17);$$
$$\boldsymbol{x=17t+12};$$
$$2x+17y=450;\qquad 12*(17t+12)+17y=450;$$
$$17y=450-144-12*17t;$$
$$y=\frac{306-12*17*t}{17};$$
$$\boldsymbol{y=18-12t};$$
$$\begin{cases}x=17t+12;\\y=18-12t;\end{cases}$$

t	– 2	– 1	0	1	2	3
x	– 22	– 5	12	29	46	63
y	42	30	18	6	– 6	– 18

Відповідь: *Оскільки від'ємної кількості дошок не може бути, тоді відповідь має міститися в додатних розв'язках (12,18) або (29,6).*

Контролі питання

1. Підхідні дроби та їх табличне обчислення.
2. Теорема Ейлера та теорема Ферма для обчислення конгруенції.
3. Діофантові рівняння та використання конгруенцій до їх розв'язку.

Практична робота № 11

Тема: Використання теорії множин до аналізу текстів та підбору здвигу в шифрі Цезарі (одноалфавітної заміни)

Мета: опрацювати методи аналізу множин на прикладі статистичного аналізу текстів у процесі одноалфавітної заміни.

Теоретичні відомості

У теорії множин є два основних первісних неозначуваних поняття: Множина і елемент, а основні неозначувані відношення між ними описуються словами: належить, відповідає, передує, отже, поняття множина приймаємо без означення, тому пояснимо його прикладами.

Можна говорити про множину букв в алфавіті, про множину розв'язків, множину студентів І курсу і т. д. У повсякденному житті замість терміну множина вживають сукупність, череда, табун, зграя, екіпаж, колекція, клас, трупа і т. д.

У математиці під множиною розуміють сукупність, зібрання деяких предметів, об'єктів, які об'єднуються між собою характеристичною ознакою.

Математичний зміст терміну «множина» відрізняють від повсякденного, де його зв'язують з великою кількістю об'єктів. У математиці розглядаються множини, які складаються з декількох елементів або їх немає.

Об'єкти будь-якої природи (літери, числа, книги), з яких складається множина називається елементами.

Завдання. Які літери використовуються в записі слова «м а т е м а т и к а»? Яка їх потужність (кількість елементів)?

М={ *м, а, т, е, и, к*}.

Зауваження:

1) у множині кожен елемент зустрічається лише один раз.
2) порядок запису елементів множин немає значення.

літери	м	а	т	е	и	к
потужн.	2	3	2	1	1	1

Такий спосіб можна використовувати для аналізу шифрів. Наприклад.

Шифри одноалфавітної заміни є найпростішими серед інших шифрів заміни. Принцип їхньої дії побудований на тому, що кожній букві відкритого тексту ставиться у відповідність інша, але детермінована (незмінна) буква деякого алфавіту (алфавіту заміни). Через те, що кожній букві відкритого тексту відповідає єдина буква алфавіту заміни, всьому відкритому алфавіту відповідає єдиний незмінний алфавіт заміни, тому шифри цього класу називають шифрами одноалфавітної заміни.

Розглянемо шифр одноалфавітної заміни на прикладі так званого шифру Цезаря. Щоб розібрати і прочитати його тексти, потрібно всякий раз читати четверту букву замість першої відповідно до алфавіту, наприклад Д замість А, у цьому разі алфавіт представлявся як кільце – наступним за символом Я вважався символ А. Ми розглянемо узагальнений шифр Цезаря, у якому будемо зсовувати символи початкового алфавіту на довільну кількість позицій. Знак пробілу між словами не враховується.

Алфавіт для шифрування

АБВГДЕЄЖЗИІЇЙКЛМНОПРСТУФХЦЧШЩЬЮЯ

Алф.	А	Б	В	Г	Д	Е	Є	Ж	З	И
Зам.	Е	Є	Ж	З	И	І	Ї	Й	К	Л

І	Ї	Й	К	Л	М	Н	О	П	Р	С
М	Н	О	П	Р	С	Т	У	Ф	Х	Ц

Т	У	Ф	Х	Ц	Ч	Ш	Щ	Ь	Ю	Я
Ч	Ш	Щ	Ь	Ю	Я	А	Б	В	Г	Д

Зашифруємо текст шифром Цезаря з ключем К=5:

Відкритий текст:

МНОЖИНА – ОДНЕ З ОСНОВНИХ ПОНЯТЬ СУЧАСНОЇ МАТЕМАТИКИ. СТРОГО ВОНО НЕ ВИЗНАЧАЄТЬСЯ, АЛЕ МОЖЕ БУТИ ДАНО ІНТУЇТИВНЕ ВИЗНАЧЕННЯ МНОЖИНИ ЯК СУКУПНОСТІ ПЕВНИХ І РІЗНИХ ОБ'ЄКТІВ ДОВІЛЬНОЇ ПРИРОДИ, ЯКА РОЗГЛЯДАЄТЬСЯ ЯК ОДНЕ ЦІЛЕ. ОБ'ЄКТИ, ЯКІ СКЛАДАЮТЬ МНОЖИНУ, НАЗИВАЮТЬСЯ ЇЇ ЕЛЕМЕНТАМИ. НАПРИКЛАД, МОЖНА ГОВОРИТИ ПРО МНОЖИНУ УСІХ КНИГ У ПЕВНІЙ БІБЛІОТЕЦІ, МНОЖИНУ ЛІТЕР УКРАЇНСЬКОГО АЛФАВІТУ АБО ПРО МНОЖИНУ ВСІХ КОРЕНІВ ПЕВНОГО РІВНЯННЯ.

Усього літер у тексті – 360.

Шифротекст:

СТУЙЛТЕУИТІКУЦТУЖТЛЬФУТДЧВЦШЯЕЦТУНСЕЧІСЕЧЛПЛЦЧХУЗУЖУТУТІЖЛКТ ЕЯЕЇЧВЦДЕРІСУЙІЄШЧЛИЕТУМТЧШНЧЛЖТІЖЛКТЕЯІТТДСТУЙЛТЛДПЦШПШФТУ ЦЧМФІЖТЛЬМХМКТЛЬУЄЇПЧМЖИУЖМРВТУНФХЛХУИЛДПЕХУКЗРДИЕЇЧВЦДДПУ ИТІЮМРІУЄЇПЧЛДПМЦПРЕИЕГЧВСТУЙЛТШТЕКЛЖЕГЧВЦДННІРІСІТЧЕСЛТЕФХЛП РЕИСУЙТЕЗУЖУХЛЧЛФХУСТУЙЛТШШЦМЬПТЛЗЖФІЖТМОЄМЄРМУЧІЮМСТУЙЛТ ШРМЧІХШПХЕНТЦВПУЗУЕРЩЕЖМЧШЕЄУФХУСТУЙЛТШЖЦМЬПУХІТМЖФІЖТУЗ УХМЖТДТТД

Побудуємо діаграму розподілу частот символів відкритого і шифротексту:

Відкритий текст:

А	Б	В	Г	Д	Е	Є	Ж	З	И	І	Ї	Й	К	Л	М
23	6	17	6	8	18	4	8	6	25	18	6	1	14	10	12

Н	О	П	Р	С	Т	У	Ф	Х	Ц	Ч	Ш	Щ	Ь	Ю	Я
43	37	9	13	13	19	12	1	5	2	3	0	0	7	2	12

Шифротекст:

А	Б	В	Г	Д	Е	Є	Ж	З	И	І	Ї	Й	К	Л	М
0	0	7	2	12	23	6	17	6	8	18	4	8	6	25	18

Н	О	П	Р	С	Т	У	Ф	Х	Ц	Ч	Ш	Щ	Ь	Ю	Я
6	1	14	10	12	43	37	9	13	13	19	12	1	5	2	3

З двох приведених діаграм розподілу частот, ми бачимо, що рядок чисел для відкритого тексту складається з чисел:

23, 6, 17, 6, 8, 18, 4, 8, 6, 25, 18, 6, 1, 14, 10, 12 , 43, 37, 9, 13, 13, 19, 12, 1, 5, 2, 3, 0, 0, 7, 2, 12,

а рядок чисел для шифротексту складається з чисел:

0, 0, 7, 2, 12, 23, 6, 17, 6, 8, 18, 4, 8, 6, 25, 18, 6, 1, 14, 10, 12 , 43, 37, 9, 13, 13, 19, 12, 1, 5, 2, 3

Іншими словами, починаючи з шостого символу, числовий рядок для шифротексту ідентичний початку рядка для відкритого тексту, перші п’ять членів рядка повторюють останні п’ять членів рядка. Побудувавши діаграму, побачимо це в більш наглядній формі:

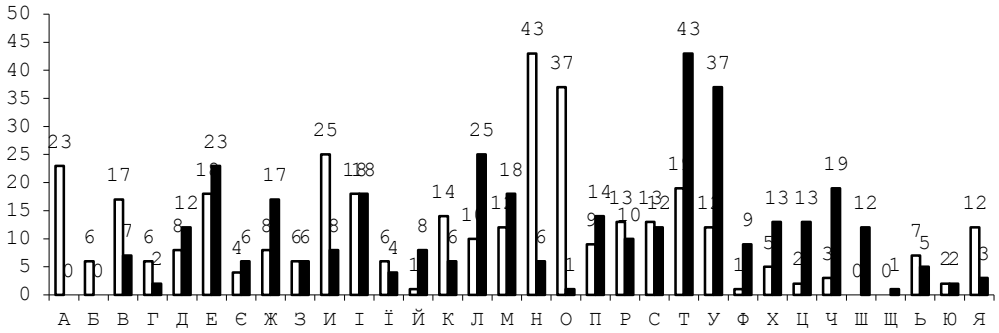


Рис. 1. Діаграма розподілу частот відкритого і шифрованого текстів, де □ – відкритий текст; ■ – шифротекст

Причому порівнювати можна як окремі елементи (О–У (37)), так і групи символів (И, І – Л, М).

Перейдемо до аналізу шифру Цезаря тільки на основі шифротексту. Для цього ми повинні:

- побудувати діаграми розподілу частот для відкритого і шифрованого текстів у процентному відношенні, оскільки довжина відкритого і шифрованого текстів може відрізнятися;
- розташувати частоти у порядку зростання;
- знайти можливі значення ключа як різницю між відповідними значеннями частот.

Приведемо приклад:

Таблиця 3

Ранжовані частоти використання букв української мови

О	0,0942	р	0,0448	я	0,0248	ж	0,0093
А	0,0807	с	0,0424	з	0,0232	ю	0,0093
Н	0,0681	л	0,0369	б	0,0177	ц	0,0083
И	0,0626	к	0,0354	ь	0,0177	ш	0,0076
І	0,0575	д	0,0338	г	0,0155	ї	0,0065
В	0,0535	у	0,0336	ч	0,0141	є	0,0061
Т	0,0535	м	0,0303	й	0,0138	щ	0,0056
Е	0,0495	п	0,0290	х	0,0119	ф	0,0028

Рис. 2. Гістограма частот використання букв алфавіту української мови

Методичні вказівки

Приклад виконання роботи.

1. Проаналізувати текст згідно варіанту за наступним алгоритмом.

Шифротекст:

СТУЙЛТЕУИТІКУЦТУЖТЛЬФУТДЧВЦШЯЕЦТУНСЕЧІСЕЧЛПЛЦЧХУЗУЖУТУТІЖЛКТ
ЕЯЕЇЧВЦДЕРІСУЙІЄШЧЛИЕТУМТЧШНЧЛЖТІЖЛКТЕЯІТТДСТУЙЛТЛДПЦШПШФТУ
ЦЧМФІЖТЛЬМХМКТЛЬУЄЇПЧМЖИУЖМРВТУНФХЛХУИЛДПЕХУКЗРДИЕЇЧВЦДДПУ
ИТІЮМРІУЄЇПЧЛДПМЦПРЕИЕГЧВСТУЙЛТШТЕКЛЖЕГЧВЦДННІРІСІТЧЕСЛТЕФХЛП
РЕИСУЙТЕЗУЖУХЛЧЛФХУСТУЙЛТШШЦМЫПТЛЗЖФІЖТМОЄМЄРМУЧІЮМСТУЙЛТ
ШРМЧІХШПХЕНТЦВПУЗУЕРЩЕЖМЧШЕЄУФХУСТУЙЛТШЖЦМЫПУХІТМЖФІЖТУЗ
УХМЖТДТТД

Визначаємо потужність множин:

Шифротекст:

А	**Б**	**В**	**Г**	**Д**	**Е**	**Є**	**Ж**	**З**	**И**	**І**
0	0	7	2	12	23	6	17	6	8	18
Ї	**Й**	**К**	**Л**	**М**	**Н**	**О**	**П**	**Р**	**С**	**Т**
4	8	6	25	18	6	1	14	10	1	43
У	**Ф**	**Х**	**Ц**	**Ч**	**Ш**	**Щ**	**Ь**	**Ю**	**Я**	**Разом**
37	9	13	13	19	12	1	5	2	3	360

1. Сортуємо за потужністю входження літер у шифротекст, будуємо діаграму (необов'язково, але наглядно).

Рис. 3. Діаграма розподілу літер шифротексту

Визначаємо ключ (зазначена діаграма для всіх варіантів!!!):

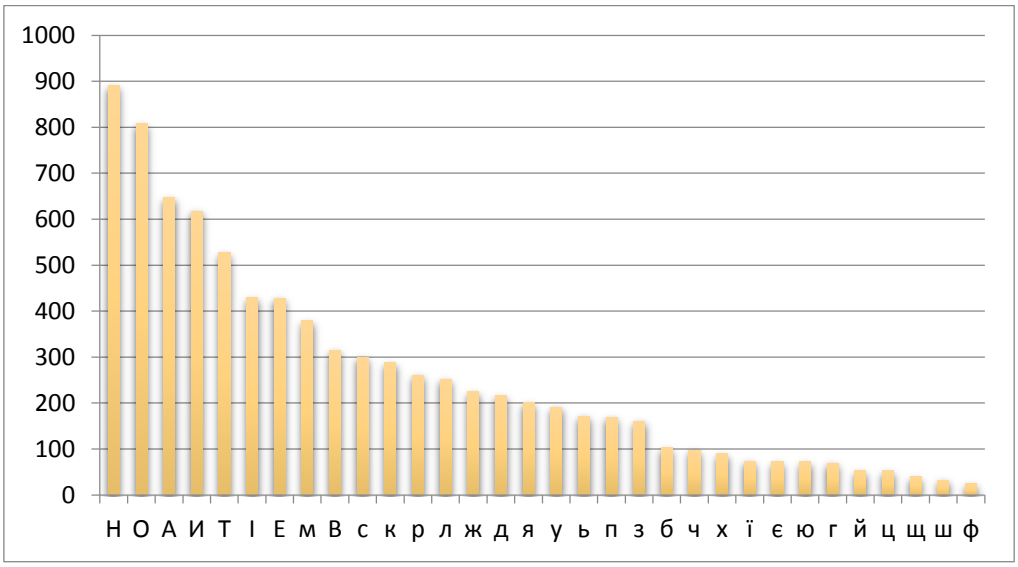


Рис. 4. Діаграма розподілу літер тексту прикладу

2. Повинна існувати взаємно однозначна відповідність між літерами із найчастішим входженням. Для цього потрібно врахувати номер відповідної літери в алфавіті.

А	Б	В	Г	Д	Е	Є	Ж	З	И	І	Ї	Й	К	Л	М
1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16

Н	О	П	Р	С	Т	У	Ф	Х	Ц	Ч	Ш	Щ	Ь	Ю	Я
17	18	19	20	21	22	23	24	25	26	27	28	29	30	31	32

Між елементами діаграм немає постійної різниці. Це відбувається через те, що шифротекст має досить малу довжину (360 символів) і обчислення потужності входження символів було не таким точним. Тому вибираємо п’ять перших елементів і розраховуємо їх різницю у будь-яких сполученнях:

текст	Н	О	А	И	Т	або–>	А	И	
№	17	18	1	10	22		1	10	
шифр	т	у	л	е	ч		е	л	
№	22	23	15	6	27		6	15	
різниця	5	5	10	4	5		5	5	

Ураховуючи невелику кількість літер в тексті можливі різні комбінації.

3. Найчастіше значення, як ми бачимо, дорівнює 5, тому можна з досить великою імовірністю казати, що ключ дорівнює 5. До того ж різниця між найчастішими символами дорівнює також 5 але це може бути 32–5=27.

Методичні вказівки

Порядок виконання завдання.

1. Вивчити відомості з криптоаналізу.
2. Усі тексти зашифровані шифром Цезаря ключем, не перевищуючим 32. Алфавіт для шифрування:
3. АБВГДЕЄЖЗИІЇЙКЛМНОПРСТУФХЦЧШЩЬЮЯ.
4. Номер завдання добирається відповідно номера студента у журналі.
5. Дешифрувати поданий текст, вказати відповідний йому відкритий текст, знайдений ключ. Студент повинен навести таблицю потужності входження літер відкритого і шифрованого текстів.
6. Скласти звіт, у якому вказати всі результати виконання лабораторної роботи і відповідний дешифрований текст.

Приклад виконання завдання.

Визначити тип шифротексту:

- Алфавіт: АБВГДЕЄЖЗИІЇЙКЛМНОПРСТУФХЦЧШЩЬЮЯ.
- Шифротекст:

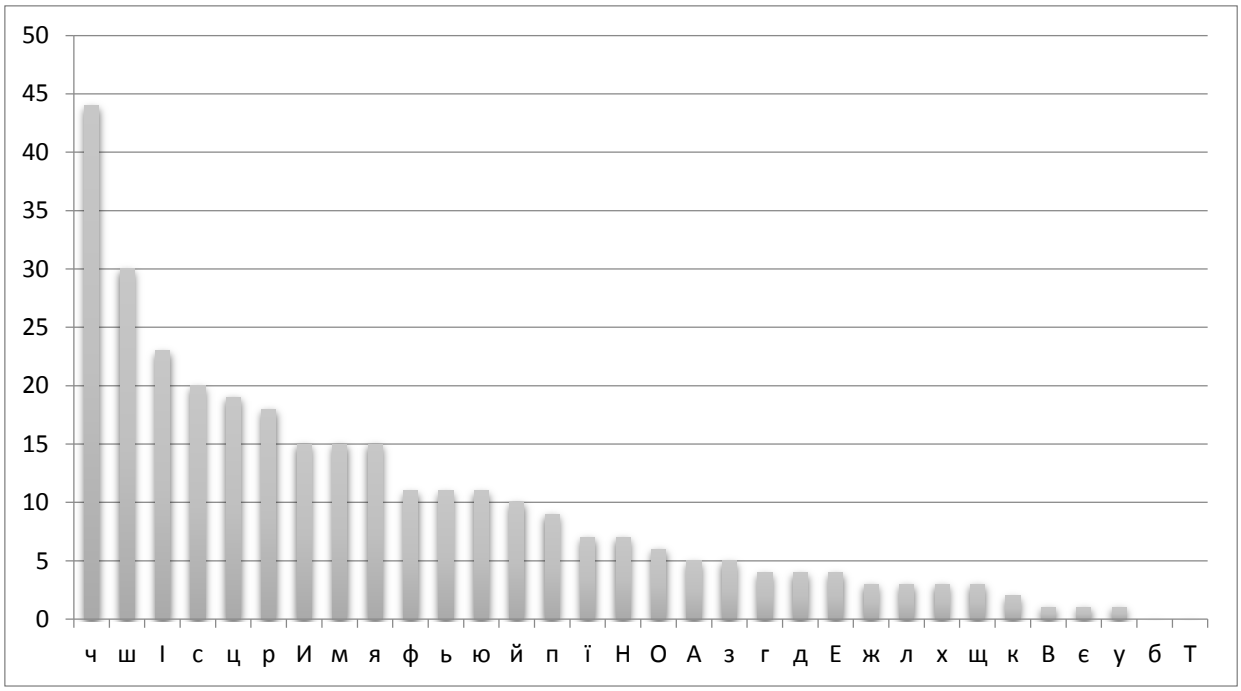
ФІЧЯШЬСЙЮЖФРУЙРЫПЦЧШОРЧІГМПСЇЫЧЧИЙНЛРЧМГСХМЙРПЧІДМЧРВШЇ
НФЯСЙИФСДСЯФШЬШПЬСПЧИЗЯЖЮИЧІЕШЗСЧЯАСГСНЗІЇШЧІЕШЗЛАЦФШЗЇМПА
ЦШЙЧШЧМЦШОМЙЙЮІЯРЮИЮЯЬШКРЦЦІЯМЦІЯРДЧРЦШПЧІДМЧЧИЦІНЮФШЬС
ЕМЩЦШИЮЧМЧЧИЦЩЦШЧИЯЯИЦЧШОРЧРИФМПЦСЧИНЯМЬЦСЧЦЧШОРЧІЧІЯМЬЦС
ЧПСЇЫЧЧИСЧЕРЦРЮРЧШЧСЦЦРШЮЧШЙЧШКШЮХШЙЦЧШОРЧІНЮАФАЩЧСЮ
ЯЖЧЇЇСЬФШХМФГСИШЇНЛЧІЧЧИЯШЄШ

Статистика

Шифротекст: Значущих для кодування =310

А	Б	В	Г	Д	Е	Є	Ж	З	И	І	Ї	Й	К	Л	М
5	0	1	4	4	4	1	3	5	15	23	7	10	2	3	15

Н	О	П	Р	С	Т	У	Ф	Х	Ц	Ч	Ш	Щ	Ь	Ю	Я
7	6	9	18	20	0	1	11	3	19	44	30	3	11	11	15

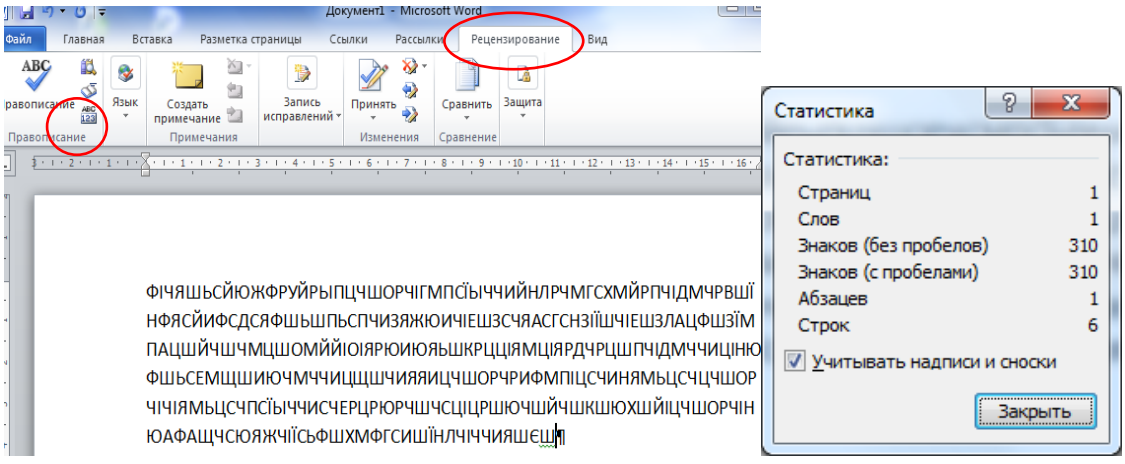


текст	Н	О	А	И	Т	або–>	А	И	Т
	17	18	1	10	22		1	10	22
шифр	ч	ш	і	є	ц				і
	27	28	12	21	26				12
	10	10	11	11	4				10

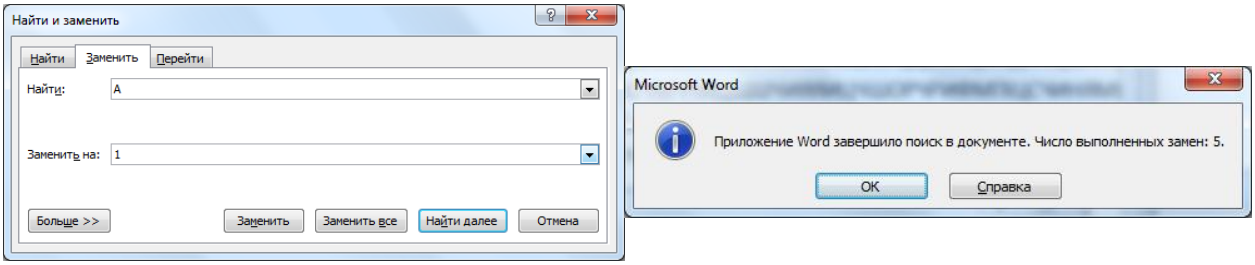
У результаті криптоаналізу шифротекста можливий ключ 10, 11, 22, 21.

Перевірка: ФІЧЯШЬС-10 – канторі; або ФІЧЯШЬС-11 – йаьснпи.

Очевидно, перший ключ є відповіддю. Програма для дешифрування на свій вибір. Це можна зробити у Word 2010 використовуючи статистику та режим заміни.



Зауваження. Під час заміни літери вводити краще цифру, а після отримання результату відміняти.



Коли обчислено значення зсуву (10) і є таблиця для підстановок перші заміни бажано теж зробити цифровими «А–И» на «0–9» і продовжувати з заміни «І–Р» на «А–И» і так далі, в кінці потрібно повернути «0–9» на «У–Я».

Крок 1.

шифр	**А**	**Б**	**В**	**Г**	**Д**	**Е**	**Є**	**Ж**	**З**	**И**
код	0	1	2	3	4	5	6	7	8	9
код	У	Ф	Х	Ц	Ч	Ш	Щ	Ь	Ю	Я

Крок 2.

шифр	**І**	**Ї**	**Й**	**К**	**Л**	**М**	**Н**	**О**	**П**	**Р**
код	А	Б	В	Г	Д	Е	Є	Ж	З	И

Крок 3.

шифр	**С**	**Т**	**У**	**Ф**	**Х**	**Ц**	**Ч**	**Ш**	**Щ**	**Ь**
код	І	Ї	Й	К	Л	М	Н	О	П	Р

Крок 4.

шифр	**Ю**	**Я**								
код	С	Т								

Крок 5.

шифр										
код	0	1	2	3	4	5	6	7	8	9
код	У	Ф	Х	Ц	Ч	Ш	Щ	Ь	Ю	Я

Вигляд таблиці підстановок у загальному виді.

шифр	**А**	**Б**	**В**	**Г**	**Д**	**Е**	**Є**	**Ж**	**З**	**И**	**І**	**Ї**	**Й**	**К**	**Л**	**М**
код	У	Ф	Х	Ц	Ч	Ш	Щ	Ь	Ю	Я	А	Б	В	Г	Д	Е
	5	0	1	4	4	4	1	3	5	15	23	7	10	2	3	15

	Н	О	П	Р	С	Т	У	Ф	Х	Ц	Ч	Ш	Щ	Ь	Ю	Я
	Є	Ж	З	И	І	Ї	Й	К	Л	М	Н	О	П	Р	С	Т
	7	6	9	18	20	0	1	11	3	19	44	30	3	11	11	15

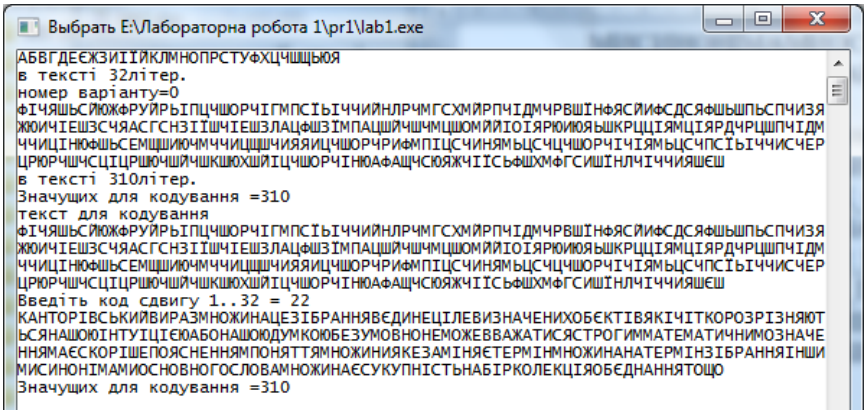
Відкритий текст:

КАНТОРІВСЬКИЙВИРАЗМНОЖИНАЦЕЗІБРАННЯВЄДИНЕЦІЛЕВИЗНАЧЕНИХОБЄКТІВЯКІЧІТКОРОЗРІЗНЯЮТЬСЯНАШОЮІНТУІЦІЄЮАБОНАШОЮДУМКОЮБЕЗУМОВНОНЕМОЖЕВВАЖАТИСЯСТРОГИММАТЕМАТИЧНИМОЗНАЧЕННЯМАЄСКОРІШЕПОЯСНЕННЯМПОНЯТТЯМНОЖИНИЯКЕЗАМІНЯЄТЕРМІНМНОЖИНАНАТЕРМІНЗІБРАННЯІНШИМИСИНОНІМАМИОСНОВНОГОСЛОВАМНОЖИНАЄСУКУПНІСТЬНАБІРКОЛЕКЦІЯОБЄДНАННЯТОЩО

Розставити пробіли. Отриманий текст має вигляд.

КАНТОРІВСЬКИЙ_ВИРАЗ_МНОЖИНА_ЦЕ_ЗІБРАННЯ_В_ЄДИНЕ_ЦІЛЕ_ВИЗНАЧЕНИХ_ОБЄКТІВ_ЯКІ_ЧІТКО_РОЗРІЗНЯЮТЬСЯ_НАШОЮ_ІНТУІЦІЄЮ_АБО_НАШОЮ_ДУМКОЮ_БЕЗУМОВНО_НЕ_МОЖЕ_ВВАЖАТИСЯ_СТРОГИМ_МАТЕМАТИЧНИМ_ОЗНАЧЕННЯМ_МАЄ_СКОРІШЕ_ПОЯСНЕННЯМ_ПОНЯТТЯ_МНОЖИНИ_ЯКЕ_ЗАМІНЯЄ_ТЕРМІН_МНОЖИНА_НА_ТЕРМІН_ЗІБРАННЯ_ІНШИМИ_СИНОНІМАМИ_ОСНОВНОГО_СЛОВА_МНОЖИНА_Є_СУКУПНІСТЬ_НАБІР_КОЛЕКЦІЯ_ОБЄДНАННЯ_ТОЩО

За бажанням можна скласти програму на будь-якій мові програмування.

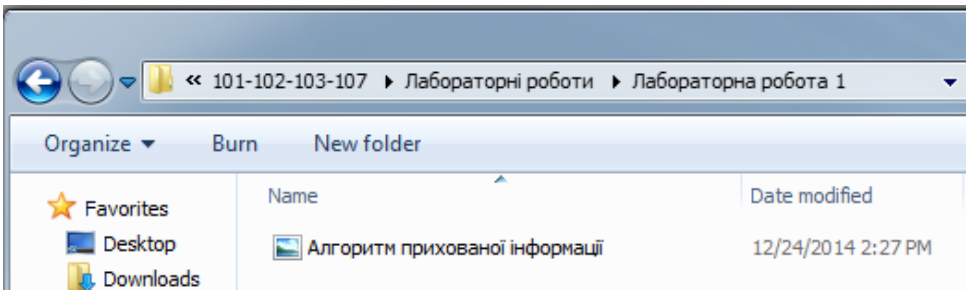


Цікавинка

Стеганографія – це наука про приховану передачу інформації шляхом збереження в таємниці самого факту передачі. На відміну від криптографії, яка приховує зміст секретного повідомлення, стеганографія приховує сам факт його існування. Стеганографії зазвичай використовують спільно з методами криптографії, таким чином, доповнюючи її.

Перевага стеганографії над чистою криптографією полягає у тому, що повідомлення не привертають до себе уваги. Повідомлення, факт шифрування яких не прихований, викликають підозру і можуть бути самі по собі викривають у тих країнах, у яких заборонена криптографія. Таким чином, криптографія захищає зміст повідомлення, а стеганографія захищає сам факт наявності будь-яких прихованих послань.

Приклад конкретної стеганосистеми (на основі зображень JPEG) і схему її реалізації можна прочитати в



Контрольні питання

1. До якого класу шифрів належить шифр Цезаря? Чому цей клас шифрів отримав таку назву?
2. Поясніть принцип дії шифрів одноалфавітної заміни взагалі і особисто узагальненого шифру Цезаря.
3. На чому засновується принцип частотного криптоаналізу одноалфавітної заміни?
4. Чому під час аналізу досить важко однозначно визначити ключ? Як подолати ці труднощі?
5. У чому слабкість шифрів одноалфавітної заміни?

Практична робота № 12

Тема. Одиночна перестановка по ключу, подвійна перестановка по ключу, шифр решіток, магічні квадрати

Мета: відпрацювати навички шифрування перестановкою символів початкового тексту, відпрацювати шифрування методами: одиночної перестановки ключем, подвійної перестановки ключем, шифри решіток та магічних квадратів.

Теоретичні відомості

У цій роботі ми познайомимося із найпростішими шифрами перестановки. Це ручні шифри, які може використовувати широке коло людей. Види шифрів мають дуже малу крипостійкість, тому використовуються в поєднанні з більш новими шифрами.

1. Одиночна перестановка ключем. У цьому методі шифрування як ключ використовується слово. Пронумерувавши букви які складають слово у алфавітному порядку, і розташувавши їх після цього у порядку зростання, одержуємо шифровану фразу.

Використавши у виді ключа слово ПОРЯДКИ одержимо таблицю.

П	О	Р	Я	Д	К	И
5	4	6	7	1	3	2
Р	Ю	О	К	Н	Е	Р
О	Т	Е	О	Я	Т	Е
З	Ь	К	Р		И	С
Р	С	Т	И	Е	Ч	У
О	Я	И	С	Н	Н	Р
Б			Т	Е	И	С
Л	П	В	А	Р	Х	І
Я	Р	И	Н	Г		В

До перестановки

Д	И	К	О	П	Р	Я
1	2	3	4	5	6	7
Н	Р	Е	Ю	Р	О	К
Я	Е	Т	Т	О	Е	О
	С	И	Ь	З	К	Р
Е	У	Ч	С	Р	Т	И
Н	Р	Н	Я	О	И	С
Е	С	И		Б		Т
Р	І	Х	П	Л	В	А
Г	В		Р	Я	И	Н

Після перестановки

У верхньому рядку таблиці записаний ключ, а під ключем – номера відповідних букв ключа в алфавіті. Якщо в ключі зустрілися однакові букви, вони нумерувалися з лівої сторони на праву. Виходить шифровка [2]:

НРЕЮР ОКЯЕТ ТОЕО_ СИЬЗК РЕУЧС РТИНР НЯОИС ЕСИ_Б _ТРІХ ПЛВАГ В_РЯИН. [1]

2. Шифрування подвійною перестановкою ключів.

Для додаткової скритності шифру одиночної перестановки можна повторно шифрувати повідомлення, які вже були зашифровані. Цей спосіб відомий під назвою *подвійна перестановка.* Для цього розмір таблиці підбирають так, щоб довжина її рядків і стовпців була іншою, ніж у першій таблиці. Найкраще, якщо вони будуть взаємно простими. Крім того, в першій таблиці можна переставляти

стовпці, а в іншій рядки. Можна заповнювати таблицю зиґзаґом, змійкою, спіраллю, або якимось іншим способом. Такі способи заповнення таблиці не підсилюють стійкість шифру, але роблять процес шифрування набагато більш цікавим [4].

У таблицю вписується текст і переставляються стовпці, а потім рядки. Під час розшифровки порядок перестановок зворотний. Наскільки просто виконується це шифрування показує наступний приклад:

	2	4	1	3
4	П	Р	И	Ї
1	З	Д	Ж	А
2	Ю	Ш	О	С
3	Т	О	Г	О

Початкова таблиця

	1	2	3	4
4	И	П	Ї	Р
1	Ж	З	А	Д
2	О	Ю	С	Ш
3	Г	Т	О	О

Перестановка стовпців

	1	2	3	4
1	Ж	З	А	Д
2	О	Ю	С	Ш
3	Г	Т	О	О
4	И	П	Ї	Р

Перестановка строк

Отримуємо шифровку ЖЗАДОЮСШГТООИПЇР. Ключем до цього шифру служать номери стовпців 2413 і номери рядків 4123 вихідної таблиці. Число варіантів подвійної перестановки теж велике: для таблиці 3×3 їх 36, для 4×4 їх 576, а для 5×5 їх вже 14400. Однак подвійна перестановка дуже слабкий вид шифру, що читається легко за будь-якого розміру таблиці шифрування [1].

Примітка: під час рішення прямої і зворотної задачі варто враховувати наступні особливості:

- після заповнення таблиці, якщо залишилися порожні клітини, можна заповнити їх послідовністю букв, що не змінюють змісту повідомлення, наприклад буквами А;
- довжина ключа дорівнює числу стовпців таблиці;
- для зашифровки таблиця заповнюється стовпцями, а читається рядками;
- перший ключ у завданні – номера стовпців, а другий рядків [2].

Клас шифрів перестановок, названих решітками

Цей клас шифрів являє собою квадратні таблиці, де чверть осередків прорізана так, що у ході чотирьох поворотів вони покривають весь квадрат. Вписування в прорізані осередки (тобто осередки, у які заносяться літери шифрованого повідомлення) тексту і повороти решітки продовжуються допоки, весь квадрат не буде заповнений. Наприклад, на малюнку нижче показаний процес шифровки решітками 4х4. Зірочками позначені не прорізані осередки, а повороти здійснюються за годинниковою стрілкою на зазначений нижче кут. А саме, у перший квадрат вписані перші чотири букви першого рядка таблиці таким чином, щоб під час повороту на 270° ці букви прорізали всі осередки квадрату. Переконавшись, що це розміщення букв, під час чергового повороту на 90° прорізає нові осередки, потрібно вписувати в них букви наступного рядка таблиці (вниз, якщо прорізаних осередків по одній в кожному рядку, як у першому прикладі). Якщо прорізаних осередків в одному рядку небагато, то їх заповнення здійснюється праворуч, як у другому і третьому прикладах. Потім усі букви квадратів заносяться у нову таблицю, причому зберігається їхнє положення у рядку та у стовпці. У кінці, всі букви виписуються в один рядок і, таким чином, виходить шифровка [5].

Приклади шифрування методом решіток:

Приклад № 1.

Текст шифровки: ВИПРОБОВУВАТИ_НА.

В	И	П	Р
О	Б	О	В
У	В	А	Т
И	__	Н	А

*	*	В	*
*	*	*	И
*	П	*	*
Р	*	*	*

О	*	*	*
*	Б	*	*
*	*	*	О
*	*	В	*

*	*	*	У
*	*	В	*
А	*	*	*
*	Т	*	*

*	И	*	*
_	*	*	*
*	*	Н	*
*	*	*	А

О	И	В	У
_	Б	В	И
А	П	Н	О
Р	Т	В	А

0°, 90°, 180°, 270°.

Таким чином, одержали шифровку: ОИВУ_БВИАПНОРТВА.

Приклад № 2.

Зверніть увагу на особливість, приведену в цьому прикладі: під час першого повороту на 90° букви вписані построково (праворуч).

Текст шифровки: КЛЕПАТИ_ ЯЗИКАМИ_.

К	Л	Е	П
А	Т	И	_
Я	З	И	К
А	М	И	_

К	*	*	*
*	Л	*	*
Е	*	*	*
*	П	*	*

*	А	*	Т
И	*	_	*
*	*	*	*
*	*	*	*

*	*	Я	*
*	*	*	З
*	*	И	*
*	*	*	К

*	*	*	*
*	*	*	*
*	А	*	М
И	*	_	*

К	А	Я	Т
И	Л	_	З
Е	А	И	М
И	П	_	К

0° 90° 270° шифр.

Таким чином, одержали шифровку: КАЯТИЛ_ЗЕАИМИП_К.

Приклад № 3.

Текст шифровки: ПУСТІ_МРІЇ_МАРНІ.

П	У	С	Т
І	_	М	Р
І	Ї	_	М
А	Р	Н	І

П	*	*	*
У	*	С	*
Т	*	*	*
*	*	*	*

*	І	_	М
*	*	*	*
*	*	Р	*
*	*	*	*

*	*	*	*
*	*	*	І
*	Ї	*	_
*	*	*	М

*	*	*	*
*	А	*	*
*	*	*	*
Р	Н	І	*

П	І	_	М
У	А	С	І
Т	І	Р	_
Р	Н	І	П

0° 90° 270° шифр.

Таким чином, одержали шифровку: ПІ_МУАСІТІР_РНІП

Число подібних решіток з їхнім розміром швидко росте. Так, решітка 2х2 єдина, решіток 4х4 вже 256, а решіток розміром 6х6 – понад сто тисяч. Незважаючи на велику складність, шифри типу решітки досить просто розкриваються і не можуть використовуватися у вигляді самостійного шифру. Однак вони дуже зручні і довго використовувалися в практиці для посилення шифрів заміни.

Клас шифрів, названих магічними квадратами.

Магічними квадратами називаються квадратні таблиці з вписаними в їхні клітинки послідовними натуральними числами від 1, які дають у сумі за кожним стовпцем, кожного рядка і кожної діагоналі те саме число. Побудувавши такий квадрат, вписуємо у нього відповідно букви шифрованого повідомлення. Наприклад, перша буква нашого повідомлення П – заносимо її в клітинку з числом 1, і в такий же спосіб вписуємо всі інші букви нашого тексту.

Ось приклад магічного квадрату та його шифровки:

16	3	2	13
5	10	11	8
9	6	7	12
4	15	14	1

А	П	И	И
О	В	А	В
У	Б	О	Т
Р	Н	_	В

Отримана, шифровка АПИИОВАВУБОТРН_В з тексту ВИПРОБОВУВАТИ_НА представляється досить складною. На перший погляд здається, начебто магічних квадратів дуже мало. Проте їхнє число дуже швидко зростає зі збільшенням розміру квадрата. Так, існує лише один магічний квадрат розміром 3х3, якщо не брати до уваги його повороти. Магічних квадратів 4х4 нараховується вже 880, а число магічних квадратів розміром 5х5 близько 250000. Звернемо увагу на наступні особливості під час складання магічного квадрату 4х4:

1. Сума чисел в усіх стовпцях і всіх рядках, а також і в двох діагоналях, є одне і теж число, рівне 34. Причому сума всіх чисел від 1 до 16 дорівнює 136, а 136/4=34.

2. Сума чисел, розташованих у кутах на одній діагоналі, дорівнює сумі чисел розташованих на кутах іншої діагоналі, причому ця сума дорівнює 17. Розглядаючи приведений вище приклад, можемо простежити, що 16 і 1 розташовано на одній діагоналі, а 13 і 4 розташовані на іншій діагоналі, і сума їхніх чисел дорівнює 17, а загальна їхня сума дорівнює 34.

16			13
4			1

	10	11	
	6	7	

3. Сума чисел, розташованих у центрі квадрата на одній діагоналі, дорівнює сумі чисел, розташованих у центрі квадрата на іншій діагоналі, причому ця сума дорівнює 17. Розглядаючи приклад, можна простежити, що 10 і 7 розташовані на одній діагоналі, а 11 і 6 на іншій, і сума їхніх чисел дорівнює 17, а загальна їхня сума дорівнює 34.

4. Аналогічним чином, можна показати:

	3	2	
	15	14	

5			8
9			12

	3		
5			
			12
		14	

		2	
			8
9			
	15		

5. Сума чисел, утворюючих квадрат 2х2, дорівнює 34.

16	3		
5	10		

Методичні вказівки

Порядок виконання завдання.

1. Вивчити основні принципи побудови простих шифрів.
2. Взяти ключі та відкриті тексти відповідно до номера студента в журналі.
3. Здійснити ручне шифрування одиночною перестановкою за ключем.
4. Здійснити ручне шифрування подвійною перестановкою за ключем.
5. Здійснити ручне шифрування шифром решіток.
6. Здійснити ручне шифрування шифром магічних квадратів.
7. Взяти ключ та шифртекст відповідно до номера студента. Розшифрувати шифртекст, який було зашифровано методом подвійної перестановки за ключем.
8. Скласти звіт, у який включити початкові дані, опис послідовності дій шифрування, кінцевий результат.

Контрольні питання

1. Одиночна перестановка за ключем, принцип шифрування.
2. Клас шифрів, названих решітками, принцип шифрування.
3. Клас шифрів магічні квадрати, принцип шифрування.
4. Де знайшли застосування шифри перестановки?
5. Які недоліки шифрів перестановки?

Практична робота № 13

Тема: Шифр Playfair і шифр подвійного квадрата

Мета: відпрацювати шифрування за допомогою біграм (шифри Playfair та подвійного квадрата).

Теоретичні відомості

Найбільш відомий шифр біграмами називається Playfair. Він застосовувався Великобританією у Першу світову війну. Відкритий текст розбивався на пари букв (біграми) і текст шифровки будувався з нього за наступними двома дуже простим правилам (наводяться нижче).

Для шифрування ключ вписувався у таблицю, а потім усі останні літери вписувалися у цю таблицю за алфавітом.

Наприклад:

П	Р	И	К	Л	А	Д	Б
В	Г	Е	Є	Ж	З	І	Ї
Й	М	Н	О	С	Т	У	Ф
Х	Ц	Ч	Ш	Щ	Ь	Ю	Я

Для шифрування використовуються наступні правила:

1. Якщо обидві букви біграми вихідного тексту належали одному стовпчикові таблиці, то буквами шифру вважалися букви, що лежали під ними. Так біграма ИН давала текст шифровки ЕЧ. Якщо буква відкритого тексту знаходилася у нижньому рядку, то для шифру бралася відповідна буква з верхнього рядка і біграма ЇЯ давала шифр ФБ. (Біграма з однієї букви чи пари однакових букв теж підкорялася цьому правилу і текст ЕЕ давав шифр НН).

2. Якщо обидві букви біграми вихідного тексту належали одному рядку таблиці, то буквами шифру вважалися букви, що лежали праворуч від них. Так біграма ВЄ давала текст шифровки ГЖ. Якщо буква відкритого тексту знаходилася у правому стовпчику, то для шифру бралася відповідна буква з лівого стовпчика і біграма ФТ давала шифр ЙУ.

Якщо обидві букви біграми відкритого тексту лежали в різних рядах і колонках, то замість них бралися такі дві букви, щоб уся четвірка їх представляла прямокутник. Під час цього послідовність букв у шифрі була дзеркальною відносно вихідної пари. Наприклад, РШ шифрувалося як КЦ, а ЙБ шифрувалося як ФП.

Розберемо цей алгоритм на прикладі:

У ході шифрування фрази НЕХАЙ КОНСУЛИ БУДУТЬ УВАЖНІ за біграмами виходить така шифровка:

НЕ	ХА	ЙК	ОН	СУ	ЛИ	БУ	ДУ	ТЬ	УВ	АЖ	НІ
ЧН	ЬП	ОП	СО	ТФ	КА	ДФ	ІЮ	ЬА	ЙІ	ЛЗ	УЕ

Шифрування біграмами різко підсилило стійкість, шифрів до розкриття. [2]

Шифр подвійного квадрату

Зазначений шифр, на перший погляд, дещо відрізняється від шифру Playfair, для шифрування він використовує дві таблиці, однак, ці, здавалося б і не настільки значні зміни привели до появи на світ нової криптографічної системи ручного шифрування. Вона виявилася така надійна і зручна, що застосовувалася німцями навіть у роки Другої світової війни. Шифрування методом подвійного квадрата дуже просте. Приведемо приклад використання шифру подвійний квадрат для російських текстів. Маються дві таблиці з випадково розташованими в них алфавітами:

Ч		В	І	П
О	К	Й	Д	У
Г	Ш	З	Є	Ф
Л	Ї	Х	А	,
Ю	Р	Ж	Щ	Н
Ц	Б	И	Т	Ь
.	С	Я	М	Е

Е	Л	Ц	Й	П
.	Х	Ї	А	Н
Ш	Д	Є	К	С
І		Б	Ф	У
Я	Т	И	Ч	Г
М	О	,	Ж	Ь
В	Щ	З	Ю	Р

Для шифрування повідомлення розбивають на біграми. Перша буква біграми знаходиться в лівій таблиці, а друга в правій. Потім, наочно в таблиці будується прямокутник так, щоб букви біграми лежали в його протилежних вершинах. Інші дві вершини цього прямокутника дають букви шифровки. Припустимо, що шифрується біграма тексту ОЖ. Буква О знаходиться у першій колонці другого рядка лівої таблиці. Буква Ж в четвертій колонці шостого рядка правої таблиці. Виходить прямокутник утворений рядками 2 і 6, а також колонками 1 і 4 правої таблиці. Отже, шифровці відповідають букви, що лежать у першій колонці шостого рядка лівої таблиці Ц і в четвертій колонці другого рядка правої таблиці А – отримуємо біграму АЦ. Так парами букв шифрується все повідомлення:

Повідомлення:	ПР	ИЇ	ЗД	ЖА	Ю	ШО	СТ	ОГ	О
Шифровка:	ПЕ	,Й	ЄШ	ЧЙ	ЛТ	ДБ	ЩР	НЮ	ХЛ

Якщо обидві букви біграми повідомлення лежать в одному рядку, то і букви шифровки беруться з цього ж рядка. Перша буква біграми шифровки береться з лівої таблиці у стовпці, що відповідає другій букві біграми повідомлення. Друга буква з правої таблиці в стовпці, що відповідає першій букві біграми повідомлення. Так, за приведеним вище таблицями біграма повідомлення ТО перетворюється в біграму шифровки ЖБ.

Безсумнівно, що шифрування біграмами дає дуже стійкий до розкриття і простий шифр, а це було в свій час великим успіхом. Злам шифровки подвійного квадрата вимагає великих зусиль і довжини повідомлення більше тридцяти рядків.

Методичні вказівки

1. Вивчити схеми алгоритмів Playfair та подвійного квадрата.
2. Вибрати завдання відповідно до номера студента в журналі.
3. Зашифрувати поданий текст алгоритмом Playfair.
4. Розшифрувати поданий шифротекст, який було зашифровано алгоритмом Playfair.
5. Зашифрувати поданий текст алгоритмом подвійного квадрата.
6. Розшифрувати поданий шифр текст, який було зашифровано алгоритмом подвійного квадрата.
7. Скласти звіт, у який включити початкову інформацію, опис послідовності дій шифрування, кінцевий результат.

Контрольні питання

1. Шифр Playfair, принцип шифрування.
2. Шифр подвійного квадрата, принцип шифрування.
3. Де знайшли застосування біграмні шифри?
4. Які недоліки біграмних шифрів?

Практична робота № 14

Тема: Шифрування за допомогою таблиці Віженера

Мета: відпрацювати навички шифрування з використанням системи Віженера.

Теоретичні відомості

Шифр Віженера належить до шифрів багатоалфавітної заміни. Завдяки цьому він має значно більшу криптостійкість порівняно з шифрами одноалфавітної заміни.

Розглянемо на прикладі: Шифруємо текст : «Захист інформації», з ключем ЗАЯЦЬ.

Для шифрування тексту складається таблиця Віженера. Кожна строчка є українським алфавітом, в котрий входить пробіл. Кожна наступна строчка отримується з попередньої зсувом праворуч на один символ.

А	Б	В	Г	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	_
_	А	Б	В	Г	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
Я	_	А	Б	В	Г	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
Ю	Я	_	А	Б	В	Г	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
Ь	Ю	Я	_	А	Б	В	Г	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
Щ	Ь	Ю	Я	_	А	Б	В	Г	Д	Е	Є	Ж	З	И	І	Ї	Й	К	Л	М	Н	О	П	Р	С	Т	У	Ф	Х	Ц	Ч	Ш
Ш	Щ	Ь	Ю	Я	_	А	Б	В	Г	Д	Е	Є	Ж	З	И	І	Ї	Й	К	Л	М	Н	О	П	Р	С	Т	У	Ф	Х	Ц	Ч
Ч	Ш	Щ	Ь	Ю	Я	_	А	Б	В	Г	Д	Е	Є	Ж	З	И	І	Ї	Й	К	Л	М	Н	О	П	Р	С	Т	У	Ф	Х	Ц
Ц	Ч	Ш	Щ	Ь	Ю	Я	_	А	Б	В	Г	Д	Е	Є	Ж	З	И	І	Ї	Й	К	Л	М	Н	О	П	Р	С	Т	У	Ф	Х
Х	Ц	Ч	Ш	Щ	Ь	Ю	Я	_	А	Б	В	Г	Д	Е	Є	Ж	З	И	І	Ї	Й	К	Л	М	Н	О	П	Р	С	Т	У	Ф
Ф	Х	Ц	Ч	Ш	Щ	Ь	Ю	Я	_	А	Б	В	Г	Д	Е	Є	Ж	З	И	І	Ї	Й	К	Л	М	Н	О	П	Р	С	Т	У
У	Ф	Х	Ц	Ч	Ш	Щ	Ь	Ю	Я	_	А	Б	В	Г	Д	Е	Є	Ж	З	И	І	Ї	Й	К	Л	М	Н	О	П	Р	С	Т
Т	У	Ф	Х	Ц	Ч	Ш	Щ	Ь	Ю	Я	_	А	Б	В	Г	Д	Е	Є	Ж	З	И	І	Ї	Й	К	Л	М	Н	О	П	Р	С
С	Т	У	Ф	Х	Ц	Ч	Ш	Щ	Ь	Ю	Я	_	А	Б	В	Г	Д	Е	Є	Ж	З	И	І	Ї	Й	К	Л	М	Н	О	П	Р
Р	С	Т	У	Ф	Х	Ц	Ч	Ш	Щ	Ь	Ю	Я	_	А	Б	В	Г	Д	Е	Є	Ж	З	И	І	Ї	Й	К	Л	М	Н	О	П
П	Р	С	Т	У	Ф	Х	Ц	Ч	Ш	Щ	Ь	Ю	Я	_	А	Б	В	Г	Д	Е	Є	Ж	З	И	І	Ї	Й	К	Л	М	Н	О
О	П	Р	С	Т	У	Ф	Х	Ц	Ч	Ш	Щ	Ь	Ю	Я	_	А	Б	В	Г	Д	Е	Є	Ж	З	И	І	Ї	Й	К	Л	М	Н
Н	О	П	Р	С	Т	У	Ф	Х	Ц	Ч	Ш	Щ	Ь	Ю	Я	_	А	Б	В	Г	Д	Е	Є	Ж	З	И	І	Ї	Й	К	Л	М
М	Н	О	П	Р	С	Т	У	Ф	Х	Ц	Ч	Ш	Щ	Ь	Ю	Я	_	А	Б	В	Г	Д	Е	Є	Ж	З	И	І	Ї	Й	К	Л
Л	М	Н	О	П	Р	С	Т	У	Ф	Х	Ц	Ч	Ш	Щ	Ь	Ю	Я	_	А	Б	В	Г	Д	Е	Є	Ж	З	И	І	Ї	Й	К
К	Л	М	Н	О	П	Р	С	Т	У	Ф	Х	Ц	Ч	Ш	Щ	Ь	Ю	Я	_	А	Б	В	Г	Д	Е	Є	Ж	З	И	І	Ї	Й
Й	К	Л	М	Н	О	П	Р	С	Т	У	Ф	Х	Ц	Ч	Ш	Щ	Ь	Ю	Я	_	А	Б	В	Г	Д	Е	Є	Ж	З	И	І	Ї
Ї	Й	К	Л	М	Н	О	П	Р	С	Т	У	Ф	Х	Ц	Ч	Ш	Щ	Ь	Ю	Я	_	А	Б	В	Г	Д	Е	Є	Ж	З	И	І
І	Ї	Й	К	Л	М	Н	О	П	Р	С	Т	У	Ф	Х	Ц	Ч	Ш	Щ	Ь	Ю	Я	_	А	Б	В	Г	Д	Е	Є	Ж	З	И
И	І	Ї	Й	К	Л	М	Н	О	П	Р	С	Т	У	Ф	Х	Ц	Ч	Ш	Щ	Ь	Ю	Я	_	А	Б	В	Г	Д	Е	Є	Ж	З
З	И	І	Ї	Й	К	Л	М	Н	О	П	Р	С	Т	У	Ф	Х	Ц	Ч	Ш	Щ	Ь	Ю	Я	_	А	Б	В	Г	Д	Е	Є	Ж
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	_	А	Б	В	Г	Д	Е	Є
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	_	А	Б	В	Г	Д	Е

Продовження табл.

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	_	А	Б	В	Г	Д
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	_	А	Б	В	Г
Г	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	_	А	Б	В
В	Г	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	_	А	Б
Б	В	Г	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	_	А

Для шифрування тексту встановлюється ключ, що представляє собою деяке слово або набір букв. Далі з повної матриці вибирається підматриця шифрування, що включає, наприклад, перший рядок і рядки матриці, початковими буквами яких є послідовно букви ключа , наприклад рядки, що починаються з букв З, А, Я, Ц, Ь.

А	Б	В	Г	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	_
З	И	І	Ї	Й	К	Л	М	Н	О	П	Р	С	Т	У	Ф	Х	Ц	Ч	Ш	Щ	Ь	Ю	Я	_	А	Б	В	Г	Д	Е	Є	Ж
А	Б	В	Г	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	_
Я	_	А	Б	В	Г	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
Ц	Ч	Ш	Щ	Ь	Ю	Я	_	А	Б	В	Г	Д	Е	Є	Ж	З	И	І	Ї	Й	К	Л	М	Н	О	П	Р	С	Т	У	Ф	Х
Ь	Ю	Я	_	А	Б	В	Г	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

Процес шифрування включає наступну послідовність дій:

1) під кожною буквою шифрованого тексту записуються букви ключа, причому ключ повторюється необхідну кількість разів;

2) кожна буква шифрованого тексту замінюється на букву, розташовану на перетині стовпця тексту, що починається з букви тексту і рядка, що починається з букви ключа який знаходиться під буквою тексту.

Так, під першою буквою З шифрованого тексту виявилася буква Ж ключа. На перетині стовпця, що починається з З, і рядка, що починається з Ж, знаходиться буква О. Буква О буде першою буквою шифрованого тексту.

Текст шифровки	З	А	Х	И	С	Т	_	І	Н	Ф	О	Р	М	А	Ц	І	Ї
Ключ	З	А	Я	Ц	Ь	З	А	Я	Ц	Ь	З	А	Я	Ц	Ь	З	А
Шифрограма	Н	А	У	Б	Н	Ь	_	З	З	Р	Ц	Р	К	Ц	Т	П	Ї

Шифрований текст поділяється на групи, наприклад чотири букви в кожній.

Для дешифрування тексту необхідно знати ключ. Розшифровка тексту виконується в наступній послідовності:

1) над буквами шифрованого тексту послідовно записуються букви ключа;

2) у рядку підматриці Віженера, що починається з букви ключа, відшукується буква шифрованого тексту, буква першого рядка, що знаходиться у відповідному стовпці, буде буквою розшифрованого тексту;

3) отриманий текст групується в слова за змістом [15].

Ключ	З	А	Я	Ц	Ь	З	А	Я	Ц	Ь	З	А	Я	Ц	Ь	З	А
Шифртекст	Н	А	У	Б	Н	Ь	_	З	З	Р	Ц	Р	К	Ц	Т	П	Ї
Початковий текст	З	А	Х	И	С	Т	_	І	Н	Ф	О	Р	М	А	Ц	І	Ї

Методичні вказівки

1. Вивчити схему алгоритму Віженера.
2. У додатку № 1 вибрати завдання відповідно до номера студента в журналі.
3. Зашифрувати поданий текст алгоритмом Віженера.
4. Скласти звіт, у який включити початкову інфорацію, опис послідовності дій шифрування, кінцевий результат.

Контрольні питання

1. Принцип шифрування з використанням системи Віженера.
2. Де знайшла застосування система шифрування Віженера?
3. Які недоліки системи Віженера?
4. Принцип побудови таблиці Віженера.

Практична робота № 15
Тема: Системи з відкритим ключем. Криптосистема RSA

Мета: відпрацювати вміння використання криптосистеми RSA. На практиці зашифрувати текст за допомогою цього алгоритму шифрування.

Теоретичні відомості

Концепцію систем з відкритим ключем запропонували у 1976 році Діффі і Хеллман [19]. Криптосистеми з відкритим ключем засновуються на використанні особливих властивостей шифрування, що являє собою розрахунок оберненої величини від якоїсь функції, що не може бути реалізована числовими методами.

У сучасній криптографії стандартом де-факто на системи з відкритим ключем є система RSA, спроєктована Рівестом, Шаміром та Адлеманом.

Розглянемо математичні результати, покладені в основу алгоритму RSA.

Теорема 1. (Мала теорема Ферма.)

Якщо p – просте число, то

$$x^{p-1} = 1 \ (mod\ p); \qquad (1)$$

для будь-якого x, простого відносно p, і

$$x^{p} = x \ (mod\ p); \qquad (2)$$

для будь-якого x[1].

Визначення. Функцією Эйлера $\varphi(n)$ називається число позитивних цілих, менших n і простих відносно n.

n	2	3	4	5	6	7	8	9	10
$\varphi(n)$	1	2	2	3	2	6	4	6	4

Теорема 2. Якщо $n=pq$, (p і q – відмінні одне від одного прості числа), то

$$\varphi(n)=(p-1)(q-1).$$

Теорема 3. Якщо $n=pq$, (p і q – відмінні одне від одного прості числа) і x – просте відносно p и q, то

$$x^{\varphi(n)} = 1 \ (mod\ n).$$

Унаслідок . Якщо $n=pq$, (p і q – відмінні одне від одного прості числа) і є просте відносно $\varphi(n)$, то відображення

$$E_{e,n}: x \to x^{e} \ (mod\ n)$$

є взаємно однозначним на $\mathbf{Z}_n$.

Очевидний і той факт, що якщо e – просте відносно (n), то існує ціле d, таке, що

$$ed = 1 \ (mod\ \varphi(n)); \qquad (3)$$

На цих математичних фактах і заснований популярний алгоритм RSA [4].

Нехай $n=pq$, де p і q – різні прості числа. Якщо e і d задовольняють рівнянню (3), то відображення $E_{e,n}$ і $E_{d,n}$ є інверсіями на Z_n. Як $E_{e,n}$, так і $E_{d,n}$ легко розраховуються, коли відомі e, d, p, q. Якщо відомі e і n, але p і q невідомі, то $E_{e,n}$ являє собою однобічну функцію; перебування $E_{d,n}$ за заданим n рівнозначно розкладанню n. Якщо p і q – досить великі прості, то розкла-дання n практично не здійсненне. Це і закладено в основу системи шифрування RSA.

Користувач i вибирає пару різних простих p_i і q_i і розраховує пари цілих (e_i, d_i), що є простими відносно $\varphi(n_i)$, де $n_i=p_i\ q_i$. Довідкова таблиця містить публічні ключі $\{(e_i, n_i)\}$[20].

Припустимо, що вихідний текст

$$x =(x_0, x_1, ..., x_{n-1}),\ x \in Z_n\ ,\ 0 \le i < n,\ Z_n$$ – безліч цілих чисел

спочатку представлений по підставі n_i :

$$N = c_0+c_{i\ ni}+....$$

Користувач i зашифровує текст, під час передачі його користувачу j, застосовуючи до n відображення Ed_i,n_i :

$$N \rightarrow Ed_i,n_i\ n = n'.$$

Користувач j робить розшифрування n', застосовуючи Ee_i,n_i :

$$N' \rightarrow Ee_i,n_i\ n' = Ee_i,n_i\ Ed_i,n_i\ n = n\ .$$

Очевидно, для того щоб знайти інверсію Ed_i,n_i стосовно Ee_i,n_i, потрібно знання множників $n=p_i\ q_i$. Час виконання найкращих з відомих алгоритмів розкладання при $n=10^{100}$ на сьогодні виходить за межі сучасних технологічних можливостей [1].

Розглянемо кілька прикладів, що ілюструють застосування алгоритму RSA.

Приклад 1. Зашифруємо повідомлення «САВ». Для простоти будемо використовувати маленькі числа (на практиці застосовуються набагато більші).

Виберемо p=3 і q=11.

Визначимо n=3*11=33.

Знайдемо (p–1)(q–1)=20. Отже, у якості d, взаємно простої з 20, приймемо наприклад, d=3.

Виберемо число e. Як таке число може бути узяте будь-яке число, для якого задовольняється співвідношення (e*3) (mod 20) = 1, наприклад 7.

Примітка: для простого знаходження числа e досить вирішити в цілих числах рівняння $e = \frac{a \cdot 20 + 1}{3}$, де a=1,2..n (перебираючи значення n до першого цілого e).

Представимо повідомлення як послідовність цілих чисел за допомогою відображення: А→1, У→2, З→3. Тоді повідомлення приймає вид (3,1,2). Зашифруємо повідомлення за допомогою ключа {7,33}.

C[1] = (3^7) (mod 33) = 2187 (mod 33) = 9;

C[2] = (1^7) (mod 33) = 1 (mod 33) = 1;

C[3] = (2^7) (mod 33) = 128 (mod 33) = 29.

Розшифруємо отримане зашифроване повідомлення C{9,1,29} на основі закритого ключа {3,33}:

M[1] = (9^3) (mod 33) = 729 (mod 33) = 3;

M[2] = (1^3) (mod 33) = 1 (mod 33) = 1;

M[3] = (29^3) (mod 33) = 24389 (mod 33) = 2.

Приклад 2. Шифруємо слово БІГ . Коефіцієнти p=3, q=7.

Визначимо $n=p*q=3*7=21$. Знайдемо $(p–1)(q–1)=12$. Виберемо d=5. Знайдемо число e, для якого справедливо $ed \bmod ((p–1)(q–1)) = 1$ (вирішуємо рівняння $e=\frac{a\cdot 12+1}{5}$, де a=1,2...n;) виберемо з безлічі рішень відмінне від числа d число, e = 17.

Представимо шифроване слово у вигляді послідовності чисел 2 6 4 (порядковий номер букв у алфавіті).

Шифрування відкритим ключем (17,21):

$C_1=2^{17}$ mod(21) = 131032 mod (21) =11;

$C_2 = 6^{17}$mod (21) = 16926659444736 mod (21) = 6;

$C_3 = 4^{17}$mod(21) = 17179869184 mod (21) = 16.

Отримане зашифроване повідомлення: 11 6 16.

Розшифруємо зашифроване повідомлення за секретним ключем (5,21)

$M_1= 11^5$mod (21) = 161051 mod (21) = 2;

$M_2 = 6^5$ mod (21) = 7776 mod (21) = 6;

$M_3 = 16^5$ mod (21) = 1048576 mod (21) = 4.

У підсумку одержуємо вихідне повідомлення БІГ.

Отже, у реальних системах алгоритм RSA реалізується у такий спосіб: кожен користувач вибирає два великих простих числа, і відповідно до описаного вище алгоритму вибирає два простих числа e і d. Як результат множення перших двох чисел (p і q) установлюється n.

{e,n} утворить відкритий ключ, а *{d,n}* – закритий (хоча можна взяти і навпаки).

Відкритий ключ публікується і доступний кожному, хто бажає послати власнику ключа повідомлення, що зашифровується зазначеним алгоритмом. Після шифрування, повідомлення неможливо розкрити за допомогою відкритого ключа. Власник закритого ключа легко може розшифрувати прийняте повідомлення [20].

Особливості методу накладають деякі обмеження на значення деяких змінних. *Наприклад*: змінна D має бути взаємно простою відносно M, тобто ці числа не повинні мати спільних дільників, а змінна E повинна бути такою, щоб залишок від ділення (D*E) на M дорівнював 1.

Методичні вказівки

1. Вивчити опис криптосистеми RSA та відомості з елементарної теорії чисел.
2. Розібрати схему шифрування алгоритмом RSA.

3. Зашифрувати повідомлення алгоритмом RSA за ключами поданими у додатку 1. Передостання цифра номера студентського квитка означає номер варіанту відкритого тексту, остання цифра номера студентського квитка означає ключі шифрування.

4. Повідомлення шифрується вручну посимвольно з використанням алфавіту: _АБВГДЕЄЖЗИІЇЙКЛМНОПРСТУФХЦЧШЩЬЮЯ.

5. Після ручного шифрування для перевірки результату необхідно розшифрувати отриманий шифртекст (також посимвольно).

6. Скласти звіт, у якому необхідно вказати свою ключову пару, шифртекст та поновлений текст і відповіді на контрольні запитання.

Алгоритм RSA.

i:	j:
0. КРИПТОГРАФІЯ	P=7;Q=17;D=119;E=167;
1. РЕФЛЕКСИВНІСТЬ	P=5;Q=7;D=23;E=191;
2. СІНХРОФАЗОТРОН	P=3;Q=11;D=19;E=179;
3. АПРОКСИМАЦІЯ	P=11;Q=13;D=119;E=239;
4. ІНДЕФЕРЕНТНІСТЬ	P=13;Q=17;D=191;E=191;
5. КОНФІДЕНЦІЙНІСТЬ	P=11;Q=7;D=59;E=239;
6. НЕОБОРОТНІСТЬ	P=5;Q=11;D=41;E=161;
7. ТРАНЗИТИВНІСТЬ	P=7;Q=13;D=71;E=143;
8. КРИПТОАНАЛІЗ	P=11;Q=17;D=157;E=213;
9. МАРШРУТИЗАТОР	P=5;Q=13;D=47;E=95;

Контрольні питання

1. У чому полягає сутність систем з відкритим ключем (СВК)?
2. За допомогою яких ключів шифрується і розшифровується повідомлення в СВК?
3. Що таке необоротні функції? Які типи необоротних перетворень використовуються в СВК?
4. Які головні вимоги пред’являються до СВК?
5. Як можна використовувати алгоритми криптосистем з відкритим ключем?
6. На яких математичних фактах заснований алгоритм RSA?
7. Як вибираються числа P і Q алгоритму RSA?
8. Які значення користувач, що генерує ключі RSA, повідомляє іншим користувачам, а які зберігає у таємниці?
9. Чи можна розшифрувати повідомлення за допомогою відкритого ключа?
10. Як обчислюється значення функції Ейлера? Для чого воно використовується в алгоритмі RSA?
11. Чи зміниться криптограма, якщо числа P і Q поміняти місцями?

РЕКОМЕНДОВАНІ ДЖЕРЕЛА ІНФОРМАЦІЇ

Основні:

1. Кудрявцев В. Б. Теория автоматов / В. Б. Кудрявцев, С. В. Алешин, А. С. Подколзин. – 2-е изд., испр. и доп. – М. : Юрайт, 2018. – 320 с.
2. Журавчак Л. М. Дискретна математика для програмістів. Навчальний посібник. Львів : Видавництво Львівської політехніки, 2019. 420 с.
3. Коноваленко О. Є., Ткачук М. А., Грабовський А. В. Дискретна математика : навчально-методичний посібник. – Харків : Національний технічний університет «Харківський політехнічний інститут», (НТУ "ХПІ"), 2016. – 77 с.
4. Шевченко Г. В. Дискретна математика : навчально-методичний посібник. – К. : ДУТ, 2015. – 158 с.

Додаткові:

1. Дискретна математика : підручник : гриф МОН України / Ю. М. Бардачов, Н. А. Соколова, В. Є. Ходаков. – 2-ге вид., перероб. і доп. – К. : Вища школа, 2007. – 383 с.
2. Яблонский С. В. Введение в дискретную математику. – М. : Наука, 1986.
3. Биркгоф Г., Барти Т. Современная прикладная алгебра. Пер. с англ. – М. : Мир, 1976.
4. Холл М. Комбинаторика. Пер. с англ. – М. : Мир, 1970.
5. Скороход А. В. Вероятность вокруг нас. – К : Наукова думка, 1980.

ДЛЯ НОТАТОК

Навчальне видання

Інесса Василівна
Кулаковська

ДИСКРЕТНА МАТЕМАТИКА.

Частина 1. Множини, відношення та математичні основи криптографії.

Методичні вказівки для виконання лабораторних робіт
з дисципліни «Дискретна математика»
студентами спеціальностей
121 «Інженерія програмного забезпечення»,
122 «Комп'ютерні науки», 124 «Системний аналіз»

Випуск 362

Методичні вказівки

Редактор *Р. Грубкіна*.
Технічний редактор *О. Петроченко.*
Комп'ютерна верстка *Н. Кардаш.*
Друк *С. Волинець*. Фальцювально-палітурні роботи *О. Мішалкіна.*

Підп. до друку 15.09.2021
Формат 60x84$^{1}/_{16}$. Папір офсет.
Гарнітура «Times New Roman». Друк ризограф.
Ум. друк. арк. 5,81. Обл.-вид. арк. 3,03.
Тираж 5 пр. Зам. № 6320.

Видавець і виготовлювач: ЧНУ ім. Петра Могили.
54003, м. Миколаїв, вул. 68 Десантників, 10.
Тел.: 8 (0512) 50–03–32, 8 (0512) 76–55–81, e-mail: rector@chmnu.edu.ua.
Свідоцтво суб'єкта видавничої справи ДК № 6124 від 05.04.2018.