6. Задачі

Задача 1. *У книзі рекордів Гінесса написано, що найбільшим відомим простим числом є* $23021^{377} - 1$. *Довести, що*

a) *це є помилкою*;
b) *вказане число ділиться на 10.*

Задача 2. *Л. Ойлер, геніальний математик XVIII сторіччя, вважав, що значеннями полінома* $P_-(x) = x^2 - x + 41$ *при всіх натуральних* x *є прості числа.*

a) *перевірити його гіпотезу для* $x = 1, 2, \ldots, 15$ *(для цього спочатку побудувати решето Ератосфена* 16×16*).*
b) *чи вірною є гіпотеза Ойлера? (обрати* $x = 41$*)*

Задача 3. *Нехай* $P_+(x) = x^2 + x + 41$.

a) *перевірити, що* $P_+(x)$ *є простим числом для* $x = 1, 2, \ldots, 15$;
b) *довести, що серед значень* $P(x)$, $x = 1, 2, \ldots,$ *зустрічаються складені числа.* Вказівка. $1763 = 41 \cdot 43$.

Додатковий матеріал до задачі 3. *Припустимо, що всі значення поліному* $P_+(x)$ *є простими числами яким би не було натуральне* x. *Нехай* $n = 1$, $p = 43$. *Оскільки* $P_+(n) = p$, *то*

$$P_+(n + p) = n^2 + n + 41 + 2np + p^2 + p$$

ділиться на p. *За припущенням,* $P_+(n+p)$ *є простим числом, тобто* $P_+(n+p) = p$. *Аналогічним чином доводимо, що* $P_+(n+2p)$ *ділиться на* p. *Таким чином, поліном* $P_+(x) - p$ *має принаймні три корені:* p, $n+p$ *та* $n+2p$. *З іншого боку, поліном другого степеня може мати не більше двох коренів. Отримане протиріччя доводить, що не всі значення поліному* $P_+(x)$ *є простими числами.*

Задача 4. *Нехай* p *— просте число. Довести, що*

a) *обидва числа* $p - 1$ *та* $p + 1$ *є парними*;
b) *одне з чисел* $p - 1$ *або* $p + 1$ *ділиться на 3.*

Задача 5. *Нехай* p *— просте число. Довести, що або* $p = 6k + 1$, *або* $p = 6k - 1$ *для деякого натурального* k.

Задача 6. *Нехай $p > 3$ — просте число. Довести, що*

a) *одне з чисел $p-1$ або $p+1$ ділиться на 4;*
b) *невірно, що одне з чисел $p-1$ або $p+1$ ділиться на 5.*

Задача 7. *Записати слово "*`морзе`*" за допомогою азбуки Морзе.*

Додатковий матеріал до задачі 7. *Азбука Морзе — спосіб, названий за ім'ям його розробника, американського інженера Семюела Морзе (1838 р.), кодування букв комбінацією коротких (крапок) і довгих (тире) посилок. За одиницю часу приймається тривалість передачі однієї точки. Тривалість тире дорівнює трьом точкам. Пауза між елементами одного знака дорівнює одній точці, між знаками в слові — 3 точки, між словами — 7 точок. Радист середньої кваліфікації передає 60–100 знаків на хвилину. Найкращі радисти у змозі передати 220–260 знаків за хвилину.*

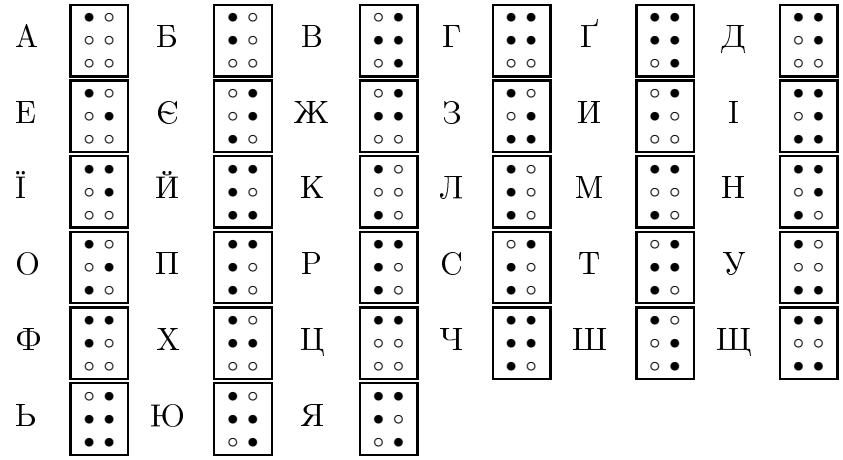
Азбука Морзе для українського алфавіту

А ·–	Б –···	В ·– –	Г ····	Ґ – –·
Д –··	Е ·	Є ··–··	Ж ···–	З – –··
И –·– –	І ··	Ї ·– – –·	Й ·– – –	К –·–
Л ·–··	М – –	Н –·	О – – –	П ·– –·
Р ·–·	С ···	Т –	У ··–	Ф ··–·
Х – – – –	Ц –·–·	Ч – – –·	Ш – – – –	Щ – – · – –
Ь –··–	Ю ··– –	Я ·–·–		

Задача 8. *Записати слово "*`брайль`*" за допомогою шифра Брайля.*

Додатковий матеріал до задачі 8. *Шрифт Брайля — рельєфно-крапковий шрифт для написання і читання сліпими, розроблений французом Луїсом Брайлем (1829 р.). Брайль осліп у віці трьох років, але у зрілому віці зміг викладати музику для сліпих. В основі шрифту (в тому числі й для музичної нотації) лежить комбінація шести опуклих/увігнутих крапок, що використовується і дотепер в усьому світі.*

Шифр Брайля для українського алфавіту



Символом • позначено опуклі точки, а символом ○ — увігнуті.

Задача 9. *Скільки існує перестановочних шифрів з параметром n? Дешифрувати секретне повідомлення*

`пчеімо унактр иаїзнф оутлбу`,

якщо ключовим словом є "`динамо`*".*

Додатковий матеріал до задачі 9. *Перестановочний шифр, відомий принаймі з часів Стародавньої Греції, визначається двома параметрами: натуральним числом n та перестановкою чисел $1, \dots, n$.*

Наприклад, якщо $n = 4$, а перестановкою є $\begin{pmatrix} 1 & 2 & 3 & 4 \\ 2 & 4 & 3 & 1 \end{pmatrix}$, то шифром слова "`кіно`*" є "*`іонк`*". Загальне правило шифрування цим методом таке: якщо перестановочний шифр визначається параметрами n та $\begin{pmatrix} 1 & 2 & \dots & n \\ i_1 & i_2 & \dots & i_n \end{pmatrix}$, то першою буквою у шифрі буде буква з номером i_1 у звичайному тексті, другою — i_2-га і так далі.*

Замість перестановки можна обрати ключове слово, яке визначає перестановку. Наприклад, перестановку $\begin{pmatrix} 1 & 2 & 3 & 4 \\ 2 & 4 & 3 & 1 \end{pmatrix}$ визначає слово "`якщо`*". Загальне правило таке: переставимо букви ключового слова*

згідно до їхнього порядку в українському алфавіті. Нехай перша буква у цій перестановці має позицію i_1 у початковому слові, друга — i_2, і так далі. Тоді послідовність $i_1, i_2, \ldots, i_n$ визначає перестановку $\begin{pmatrix} 1 & 2 & \ldots & n \\ i_1 & i_2 & \ldots & i_n \end{pmatrix}$.

Якщо необхідно зашифрувати великий текст, то його розбивають на блоки довжини n й до кожного з блоків застосовують перестановочний шифр.

Задача 10. *Скільки існує рандомізованих матричних шифрів з параметром n? Дешифрувати секретне повідомлення*

```
35 51 61 34 42 52 12 45 53 36 31 62 35 32 14 15 65 51
```

якщо другий параметр шифру наведено нижче.

Додатковий матеріал до задачі 10. *Шифр, який ми називаємо рандомізованим перестановочним, визначається двома параметрами: натуральним числом n і перестановкою букв українського алфавіту. Пояснімо процес шифрації таким шифром на прикладі $n = 6$. Для зручності розташуємо букви у матриці 6×6:*

	1	2	3	4	5	6
1	а	б	в	г	ґ	д
2	е	є	ж	з	и	і
3	ї	й	к	л	м	н
4	о	п	р	с	т	у
5	ф	х	ц	ч	ш	щ
6	ь	ю	я			

Оскільки український алфавіт складається з 33 букв, то 3 позиції в матриці залишились вільними.

Переставимо тепер букви, враховуючи й вільні місця, згідно до другогопараметру шифру (перестановки букв алфавіту). Перестановка, яку ми застосували нижче у якості приклада, отримується з попередньої матриці розташуванням її рядків у порядку 642135, тобто шостий рядок став першим, четвертий — другим і так далі.

На три вільні позиції необхідно поставити довільні букви; ми обрали "е", "и", "ї".

	1	2	3	4	5	6
1	ь	ю	я			
2	о	п	р	с	т	у
3	е	є	ж	з	и	і
4	а	б	в	г	ґ	д
5	ї	й	к	л	м	н
6	ф	х	ц	ч	ш	щ

→

	1	2	3	4	5	6
1	ь	ю	я	**е**	**и**	**ї**
2	о	п	р	с	т	у
3	е	є	ж	з	и	і
4	а	б	в	г	ґ	д
5	ї	й	к	л	м	н
6	ф	х	ц	ч	ш	щ

Таким чином, кожній букві алфавіту відповідає пара чисел (номер стовбчика-номер рядка), причому буквам "е", "и" та "ї" відповідають по дві пари.

При шифруванні кожна буква замінюється відповідною парою чисел, причому пари для "е", "и", "ї" чергуються.