7. Контрольні питання

1. показати це! (стор. 31).

2. доказать! (стор. 31).

3. впевнитись! (стор. 31).

4. чому? (стор. 33).

5. чому? (стор. 33).

6. довести! (стор. 33).

7. пояснити (стор. 33).

8. чому? (стор. 33).

9. впевнитись! (стор. 34).

10. Перевірити, що властивості 1, 2 та 3 випливають з означення 2. (стор. 35).

11. Довести, що властивості 4–5 випливають з означення 2 (стор. 36).

12. Перевірити, що доведення властивостей 7 та 8 є таким же, як і доведення властивості 6. (стор. 36).

13. Чому теорема 5 є очевидною для $n = 2$? (стор. 37).

14. Пояснити, чому знайдуться натуральні числа $a \neq 1$ та $b \neq 1$, для яких $n = ab$, якщо m є простим числом? (стор. 37).

15. Чому жодне з чисел $q_1, \ldots, q_m$ не може дорівнювати жодному з чисел $p_1, \ldots, p_k$? (стор. 39).

16. Чому кожне з чисел $q_1, \ldots, q_m$ є більшим за p? (стор. 39).

17. Пояснити чому з теореми 6 випливає, що на кожному з проміжків $[n, n! + 1]$ ряду натуральних чисел є принаймні одне просте число. (стор. 40).

18. Чому $N! + 2$ ділиться на 2? (стор. 40).

19. Довести, що $N!+k$ ділиться на k для будь-якого $k \leq N$. (стор. 40).

8. Задачі

Задача 1. *Використати шифр Цезаря з $b = 5$ й зашифрувати слово* `ЧИСЛО`.

Задача 2. *Дешифрувати фразу* `Ю І Ф Х У Ц Ч У`, *яку зашифровано за допомогою шифру Цезаря з $b = 5$.*

Задача 3. *Відомо, що текст зашифровано спочатку шифром Цезаря з параметром b_1, а потім ще раз шифром Цезаря з іншим параметром b_2. Чи є такий спосіб шифрування більш стійким, ніж спосіб, коли шифр Цезаря використовується тільки один раз?*

Задача 4. *Зашифрувати слово* `МАТЕМАТИКА` *за допомогою шифра Віженера та ключового слова* `ФІЗМАТ`.

Задача 5. *Довести, що шифр Цезаря є частковим випадком шифра Віженера й знайти відповідне ключове слово.*

Задача 6. *Нехай черговою буквою у фразі, яку необхідно зашифрувати за допомогою шифру Віженера, є* `X`, *а їй відповідає буква* `Y` *у шифр-матриці. Нехай буква* `Y` *має позицію i, в алфавіті, а* `X` *— позицію j. Довести, що елементом (i, j) в tabula recta є*

$$i + j \pmod{33}.$$

Задача 7. *Зашифрувати фразу за допомогою шифру Вернама:*

`ШИФРВЕРНАМА`

Використати наступне ключове слово:

`ТЇВХЛДШОЖЮС`

Задача 8. *Ключове слово у задачі 7 утворено за правилом:*

$$\mathtt{X}_{n+1} = \mathtt{X}_n \pmod{23},$$

тобто кожна наступна буква обчислюється через попередню за допомогою конгруенції за модулем 23. Першою буквою у ключовому слові є $\mathcal{P}_{23} = \mathtt{T}$. Перевірити це.

Задача 9. *Підрахувати суми*

$$\sum_{d|12} d, \qquad \sum_{d|12} 1, \qquad \sum_{d|18} \frac{1}{d}, \qquad \sum_{d|18} \frac{18}{d}.$$

Задача 10. *Довести, що якщо* $a|b$ *та* $b|a$*, то* $a = b$*.*

Задача 11. *Довести, що якщо* $a|b$ *та* $c|d$*, то* $ac|bd$*.*

Задача 12. *Довести, що якщо квадрат цілого числа є парним, то і саме число є парним.*

Задача 13. *Довести, що якщо квадрат цілого числа є непарним, то і саме число є непарним.*

Задача 14. *Довести, що добуток двох послідовних цілих чисел є парним.*

Задача 15. *Довести, що* $n^2 + n$ *є парним для будь-якого натурального числа* n*.*

Задача 16. *Довести, що* $2n^3 + 3n^2 + n$ *є парним для будь-якого натурального числа* n*.*

Задача 17. *Довести, що* $30|(n^5 - n)$ *для будь-якого натурального числа* n*.*

Задача 18. *Довести, що різниця квадратів двох натуральних чисел не може дорівнювати 1.*

Задача 19. *Довести, що якщо сума кубів трьох послідовних натуральних чисел є кубом* k^3*, то* $3|k$*.*

Задача 20. *Які з наступних тверджень є вірними?*

1) $(a, b) = (b, a)$ 2) $(a, b) = (a, a - b)$ 3) $(a, b) = (a, a - 2b)$
4) $(a, a + 2) = 1$ 5) $(p, p + 2) = 1$ 6) $(ac, bc) = c(a, b)$

Задача 21. *Знайти* (a, b)*, якщо*

1) $b = 1$ 2) $b = a$ 3) $b = a + 1$ 4) $b|a$
5) $b = a^2$ 5) $b = a^n$ 7) $b = na$ 8 $b = (b, a)$

Задача 22. *Нехай $a > b$. Знайти*

1) $(a+b, a^2-b^2)$ 2) (a^2-b^2, a^3-b^3) 3) (a^2-b^2, a^4-b^4)

Задача 23. *Спростувати твердження: якщо $(a,b)=1$ та $(b,c)=1$, то $(a,c)=1$.*

Задача 24. *Спростувати твердження: якщо $(a,b)=2$ та $(b,c)=2$, то $(a,c)=2$.*

Задача 25. *Довести, що $(a, a-b)=1$ тоді і тільки тоді, коли $(a,b)=1$.*

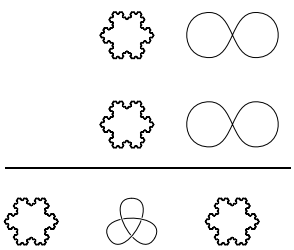
Задача 26. *Довести, що якщо $(a,b)=1$, то $(a+b, a-b)=1$ або 2.*

Задача 27. *Довести, що якщо $(a,b)=1$ та $(a,\mathrm{c})=1$, то $(a,bc)=1$.*

Задача 28. *Англійський математик де Морган, який жив у XIX сторіччі, одного разу сказав, що у році x^2 йому виповнилось x років. Коли він народився? Чи може таке ж стверджувати математик, який жив у XX сторіччі?*

Задача 29. *Цю задачу в 1968 році опублікував М. Ґарднер, відомий популяризатор математики, автор численних книг. Ми подаємо переклад оригінального формулювання задачі.*

Астронавти, які досліджують Венеру, знайшли запис домашнього завдання з математики, виконане венеріанським школяром на тему додавання двох чисел у стовбчик:



Числова система венеріанців є схожою на нашу, а основою для неї служить кількість пальців на руці венеріанців. Визначити базу венеріанської системи числення.

ДОДАТКИ

Задача 4. Шифр Віженера — це один з поліалфавітних шифрів, який у якості ключа використовує слово. При використанні цього шифру зручно створити таблицю (tabula recta), кожний наступний рядок якої є циклічно зсунутим вліво на одну позицію попереднім рядком. У першому рядку записано всі букви українського алфавіту у їхньому природному порядку.

Таблиця 5. Tabula recta для шифру Віженера

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

Утворимо тепер *шифр-матрицю* з двох рядків: перший рядок складається з фрази, що необхідно зашифрувати, а у другому ключове

слово записано стільки разів, скільки необхідно, щоб другий рядок став довшим за перший. Цю матрицю можна розглядати як послідовність стовбчиків, кожен з яких складається з двох букв. Якщо на певній позиції фрази стоїть буква X, а під нею буква Y, то відповідним стовбчиком буде $\begin{bmatrix} \mathtt{X} \\ \mathtt{Y} \end{bmatrix}$. Знаходимо букву(позначимо її Z) у tabula recta, яка стоїть на перетині рядка Y та стовбчика X. Саме вона і є шифром Віженера букви X.

Наприклад, якщо текст починається з букви Б, а першою буквою ключового слова є Г, то першим символом шифрованої фрази є буква, яка знаходиться у tabula recta на перетині рядка Г та стовбчика Б, тобто Ґ.

Задача 7. Шифр Вернама або схема одноразових блокнотів (англ. one-time pad) — система симетричного шифрування, винайдена в 1917 році співробітниками AT&T М. Моборном і Г. Вернамом. Шифр Вернама є єдиною системою шифрування, для якої доведена абсолютна криптографічна стійкість. Подамо принцип кодування за Вернамом на прикладі шифру Віженера.

В цьому випадку єдиною відмінністю між ними є принцип, за яким обирається ключове слово. Якщо у шифрі Віженера воно обирається так, щоб його легко було запам'ятати, то у шифрі Вернама ключове слово

1. має бути випадковим;
2. збігатися за довжиною з заданим відкритим текстом;
3. застосовуватися тільки один раз.

Слово "*блокнот*" у назві шифру пояснюється такою схемою утворення випадкового ключа: шифрувальник забезпечується блокнотом, кожна сторінка якого містить новий ключ. Такий же блокнот є і у приймаючої сторони. Використані сторінки знищуються.

Проблемою у застосуванні шифру Вернама є таємна передача ключового слова та збереження їйого у таємниці. Якщо існує надійно захищений канал передачі повідомлень, то шифри взагалі не потрібні: секретні повідомлення можна передавати через цей канал.

Тим не менше, схема шифроблокнотів є досить надійною при ручній шифровці.