2. Частотний аналіз

Існує багато досліджень, метою яких є встановлення частот, з якими букви зустрічаються у текстах. Різні дослідження дають різні частоти букв українського алфавіту: вони залежать від специфічного авторського стилю та змісту або жанру твору (в технічних текстах частоти можуть відрізнятися від відповідних частот в літературних текстах на 10%). В таблиці 1 наведено результат одного з досліджень стосовно частот букв українського алфавіту.

Таблиця 1. Частоти букв українського алфавіту

А	Б	В	Г	Ґ	Д	Е	Є	Ж	З	И
0,064	0,015	0,053	0,015	0,000	0,031	0,048	0,005	0,008	0,023	0,064
І	Ї	Й	К	Л	М	Н	О	П	Р	С
0,052	0,011	0,010	0,039	0,032	0,034	0,068	0,100	0,029	0,050	0,043
Т	У	Ф	Х	Ц	Ч	Ш	Щ	Ь	Ю	Я
0,052	0,032	0,004	0,013	0,012	0,012	0,006	0,004	0,018	0,009	0,021

Справжня частота букви Ґ в українських текстах становить $0,00006$. Дані у наведеній таблиці не враховують частоту пробілів між словами (символ $\sqcup$), яка насправді дорівнює 17%, що перевищує частоту будь-якої букви.

Найбільш уживані букви та їхні частоти наведено в таблиці 2. Як видно з цієї таблиці, 60% символів у текстах, написаних українською мовою, є однією з букв О, Н, А, И, В, І, Т, Р, Е, С.

Таблиця 2. 10 найбільш уживаних букв

О	Н	А	И	В	І	Т	Р	Е	С
0,100	0,068	0,064	0,064	0,053	0,052	0,052	0,050	0,048	0,043

Наведені таблиці зручно використовувати для дешифрування лінійних шифрів.

Приклад 4. Повідомлення

ЛЇ ЬМФЬ ШР ТРБРСНИШЩ
МЩОЩ ОН МРУҐКЕ
ЦЩФЩЧ ЦШЩТЬ ЄҐФРЇРУР
ОН СЇФНЖОЕ МҐКЕИ

було зашифровано за допомогою лінійного шифру. Знайти оригінал повідомлення.

Щоб висунути обґрунтовану ґіпотезу стосовно відповідності букв їхнім кодам, підрахуємо кількість появ у цьому повідомленні кожної з десяти найбільш уживаних букв з таблиці 2:

(2)

Р	Щ	О	Н	Ф	У	Е	Ш	С	Ц
7	6	4	4	4	3	3	3	2	2

Повідомлення складається з 61 символа, а букви, для яких підраховано частоти, входять в повідомлення 36 разів, тобто 59%, що добре узгоджується з таблицями 1 та 2.

Частіше за інших у тексті зустрічається буква Р, тому доцільно зробити припущення, що $\mathcal{C}_{\mathtt{О}} = \mathcal{P}_{\mathtt{Р}}$, тобто

$$a\mathcal{P}_{\mathtt{О}} + b \equiv \mathcal{P}_{\mathtt{Р}} \pmod{33} \quad \text{або} \quad 19a + b \equiv 21 \pmod{33}.$$

Ми знаємо, що розв'язання значно спрощується, якщо зробити друге припущення. Оскільки частота букв, вказана в таблиці 2, є майже однаковою, то друге припущення не є таким очевидним, як перше. Ми зробимо друге припущення згодом, а зараз переведемо повідомлення у числовий формат:

16-13 31-17-25-31 29-21 23-21-2-21-22-18-11-29-30
17-30-19-30 19-18 17-21-24-5-15-7
27-30-25-30-28 27-29-30-23-31 8-5-25-21-13-21-24-21
19-18 22-13-25-18-9-19-7 17-5-15-7-11

Для кращого сприйняття тексту ми до кожного числа додаємо справа символ "-".

Зробимо тепер друге припущення згідно таблиці частот: другою за частотою в таблиці (2) є буква Щ, тому з огляду на таблицю 2 робимо припущення $\mathcal{C}_{\text{Н}} = \mathcal{P}_{\text{Щ}}$. Оскільки $\mathcal{P}_{\text{Н}} = 18$ та $\mathcal{P}_{\text{Щ}} = 30$, то

$$18a + b \equiv 30 \pmod{33}.$$

Як і у прикладі 3, звідси випливає, що

$$a \equiv -9 \pmod{33} \quad \text{або} \quad a = 24.$$

Оскільки $(24, 33) \neq 1$, то цей шифр треба відкинути.

Ми можемо зробити інше припущення стосовно другої букви. Найчастіше за інші букви після Щ в повідомленні зустрічається О. Зробимо припущення про те, що $\mathcal{C}_{\text{Н}} = \mathcal{P}_{\text{О}}$. Оскільки $\mathcal{P}_{\text{О}} = 19$, то

$$18a + b \equiv 19 \pmod{33}.$$

Тоді $a = 2$. ⑧ Тому $b = 16$. ⑨

Обчислимо $a^{-1} \pmod{33} = 17$, $a^{-1}b = 272$ та застосуємо $L_{17,-272}$ шифр, ⑩ який є еквівалентним $L_{17,25}$ шифру. ⑪ Отримуємо

33-15 24-17-21-24 23-19 20-19-26-19-3-1-14-23-7

17-7-18-7 18-1 17-19-4-11-16-12

22-7-21-7-6 22-23-7-20-24 29-11-21-19-15-19-4-19

18-1 3-15-21-1-13-18-12 17-11-16-12-14

або

ЯК УМРУ ТО ПОХОВАЙТЕ
МЕНЕ НА МОГИЛІ
СЕРЕД СТЕПУ ШИРОКОГО
НА ВКРАЇНІ МИЛІЙ

3. Надійність лінійних шифрів

Ми підрахували кількість різних лінійних шифрів в розділі 6.2: виявилось, що таких шифрів існує 627. У цих підрахунках ми виходили з того, що алфавіт складається з 33 букв. Як ми бачили в §3.5, глава 3, алфавіт можна розширити, включивши інші символи клавіатури. Іншим (і більш ефективним) способом розширити алфавіт є групування символів у вихідному тексті (див. §3.5.2, глава 3). Таким чином, можна вважати, що лінійні шифри залежать від трьох параметрів: множника a, зсуву b та модуля для конгруенцій n. Ми позначаємо такі шифри через $L_{a,b,n}$.

Приклад 5. Відомо, що повідомлення було закодовано за допомогою $L_{a,b,31}$ шифра. Чи легко знайти a та b, щоб дешифрувати повідомлення?

Оцінимо спочатку кількість таких шифрів. Оскільки 31 є простим числом, існує 30 взаємно простих з n чисел a. Параметр b задовольняє умові $b \leq 31$ й тому існує 930 різних $L_{a,b,31}$ шифрів, що на 50% більше, ніж шифрів для звичайного українського алфавіту.

На сучасному комп'ютері знадобиться приблизно 1 хвилина для того, щоб перевірити всі 31 параметрів зсуву для фіксованого мультиплікативного параметру. Тому в середньому необхідно 15 хвилин для того, щоб зламати $L_{a,b,n}$ шифр при відомому n. ⑫

3.1. Принцип Керкхоффса. В усіх прикладах, які ми розглядали вище, припускалось, що відомим є принцип шифрування: приклад 5 починається словами "*Відомо, що шифрування здійснено за допомогою лінійного шифру*". Проте при дешифруванні цей факт не може бути відомим й здається, що надійність кодів від цього тільки виграє.

Проте криптологи дотримуються принципу Керкхоффса, згідно з яким стійкість криптографічного алгоритму не має залежати від принципу шифрування, але має залежати тільки від ключів. Іншими словами, при оцінці надійності шифрування необхідно вважати, що супротивник знає все про систему шифрування, крім ключів. Ключем для лінійного шифра є трійка (a, b, n).

3.2. Принцип складності обчислень. Може здатися, що згідно до принципу Керкхоффса жоден з шифрів не є надійним (стійким), оскільки вважається відомим принцип шифрування і єдине, що залишається — це перебрати усі

можливі варіанти. Це дійсно так, якщо існує лише обмежена кількість ключів. Але якщо ключів настільки багато, що метод грубої сили може дати результат тільки через кілька днів чи навіть років, то можливо відповідний шифр можна вважати досить стійким.

Нагадаємо (див. розділ 6.3), що $\phi(n)$ — це кількість чисел $a \leq n$, для яких $(a, n) = 1$ (взаємно простих з n). Тоді кількість різних лінійних кодів для алфавіту $\mathscr{A}_n$ дорівнює

$$n\phi(n). \tag{3}$$

До речі, одним з цих кодів є тотожній, тобто такий, що $\mathcal{C}_X = \mathcal{P}_X$, $X \in \mathscr{A}_n$.

3.3. Лист Джона Неша. Ідея використання складності обчислень у задачах криптографії вперше була висловлена Джоном Нешем в 1955 році у листі до Агенства національної безпеки США, який було розсекречено лише в 2012 році.

У своєму листі Неш пропонував оцінювати безпеку криптосистем базуючись на обчислювальній складності, тобто саме на тому принципі, який через 20 років потому ліг в основу сучасної криптографії.

В 1955 році Неш не був настільки відомим, як тепер,* тому здається, що керівництво АНБ не звернуло особливої уваги на його лист, можливо через молодий вік кореспондента, а можливо через особливості його особистості. Неш писав:

> "*Моя загальна гіпотеза виглядає наступним чином: майже для всіх досить складних типів шифрування ... середня складність обчислення ключа зростає експоненціально з довжиною ключа.*"

*В 1994 році Джон Неш отримав Нобелевську премію; історію його життя висвітлено у знаменитому художньому фільмі "Ігри розуму".

Вираз "експоненціально зростає" можна розуміти, наприклад, таким чином: при зміні ключа, який складається з n параметрів, на ключ з $n+1$ параметром, складність обчислень цих параметрів зростає удвічі. Д. Неш розумів значення своєї гіпотези:

> "*Важливість цієї загальної гіпотези, якщо припустити її істинність, очевидна. Вона означає, що цілком ймовірним стає створення шифрів, які фактично неможливо зламати. Зі зростанням складності шифру змагання між командами шифрувальників та дешифрувальників, стане надбанням історії.*"

3.4. Найбільш загадковий текст в історії. На противагу принципу Керкхоффса існують підходи, основані на збереженні в секреті самого способу шифрування. Один з відомих прикладів — це єгипетська ієрогліфічна система, яку змогли зрозуміти лише в XIX сторіччі. Іншим є загадка Тайлера, яку опублікував в 1841 р. Е. По (див. [По], стор. 35). Лише в 2016 р. молодий програміст Джил Броза з Канади зміг відновити оригінальний текст Тайлера. Проте не всі загадки, які дійшли до людства з стародавніх часів, нам вдалося розгадати.

В бібліотеці Єльського університету (США) зберігається манускрипт, який називають "*найбільш загадковим текстом*", відомим людству. Цей текст, який складається з 240 пергаментних сторінок і містить приблизно 170000 символів, створений невідомим автором. Засобами радіовуглецевого аналізу в 2011 році встановлено, що манускріпт було створено у період з 1404 по 1438. За призвіщем букініста, який на початку XX сторіччя відкрив людству цей зразок криптографічної майстерності, манускріпт називають *руко-*

писом Войнича. Саме цю книгу протягом XX століття називали "*святим Граалем криптографії*".

За характером ілюстрацій, вміщених в рукопис, можна віднести його до ботаніки або фармацевтики. З таким же успіхом можна вважати його текстом з астрономії або космології. Статистичний аналіз тексту виявив, що його структура є характерною для для природних мов. Проте принцип шифрування досі невідомий і тому ми до цього часу не знаємо зміст цього тексту.

Безліч теорій було висунуто з приводу мови, яка використана у манускрипті. Фактично лише гіпотеза про україномовне походження рукопису дозволяє отримати реальні прочитання фрагментів рукопису. Проте й ця гіпотеза багатьма спеціалістами вважається необґрунтованою.

Гіпотеза про україномовне походження рукопису належить Джону Стойко, який в 1978 році запропонував дешифрацію 9 його сторінок. Необхідно відзначити, що дану версію прочитання не можна вважати єдиним текстом, оскільки сторінки були узяті в різнобій. Навіть в Україні, як серед фахівців, так і читачів, дешифрування Стойко й, одночасно і сам підхід, запропонований ним, розглядається багатьма украй критично, аж до позначень "маячня". З іншого боку, у 2010 р. з'явилося декілька нових версій прочитання окремих сторінок рукопису Войнича, в яких саме підхід Стойко брався за основу методу реконструкції тексту.

3.5. Час, потрібний для зламу лінійного шифру. Ми розглянемо лише кілька ілюстративних прикладів оцінки часу, потрібного для зламу лінійних шифрів методом грубої сили.

Приклад 6. Відомо, що повідомлення було зашифровано

за допомогою лінійного $L_{a,b,231}$ шифру. В найгіршому випадку, скільки шифрів треба перебрати, що дешифрувати повідомлення?

В найгіршому випадку знадобиться перевірка $231 \cdot \phi(231)$ шифрів (див. (3)). Оскільки $231 = 3 \cdot 7 \cdot 11$, то

$$\phi(231) = 3{\cdot}7{\cdot}11{\cdot}\left(1 - \frac{1}{3}\right){\cdot}\left(1 - \frac{1}{7}\right){\cdot}\left(1 - \frac{1}{11}\right) = 2{\cdot}6{\cdot}10 = 120.$$

(див. властивість 6.5). Таким чином, у найгіршому випадку знадобиться перевірка $231 \cdot 120 = 27,720$ шифрів.

Приклад 7. Супротивник перехопив повідомлення, яке було закодовано за допомогою $L_{a,b,221}$ шифру. Без комп'ютера вдається перевірити 7 шифрів за 5 хвилин. Скільки необхідно часу, щоб дешифрувати повідомлення без комп'ютера?

У найгіршому випадку необхідно перевірити всі шифри, число яких $221 \cdot \phi(221)$ (див. (3)). Оскільки $221 = 13 \cdot 17$, то існує $221 \cdot 12 \cdot 16 = 42,432$ шифрів. ⑬ Таким чином, в найгіршому випадку знадобиться

$$\frac{42432}{7} \cdot 5 \approx 30,308$$

хвилин, щоб дешифрувати повідомлення. Зауважимо, що це відповідає більше, ніж 21 добі неперервних обчислень.

Приклад 8. Розвідка перехопила повідомлення, яке було зашифровано за допомогою лінійного $L_{a,b,440}$ шифра. Досвід свідчить, що спеціалізована комп'ютерна програма здатна перевірити за 2 хвилини всі лінійні шифри при фіксованому параметрі a та різних параметрах b. Через який

час можна очікувати, що перехоплене повідомлення буде розшифровано?

Загалом існує $440 \cdot \phi(440)$ шифрів (див. (3)). Оскільки $440 = 2^3 \cdot 5 \cdot 11$, то $\phi(440) = \left(2^3 - 2^2\right) \cdot 4 \cdot 10 = 160$. Це означає, що комп'ютер здатен обробити всі варіанти за $2 \cdot 160 = 320$ хвилин, що дорівнює 5 годин та 20 хвилин. Саме за такий час повідомлення буде дешифровано напевно.

4. Ще раз про знаходження оберненого за модулем

Критично важливим для дешифрування лінійних шифрів є вміння знаходити обернене число за модулем. Правило для знаходження оберненого за модулем наведено в теоремі 4.3, яка фактично є наслідком розширеного алгоритма Евкліда (див. алгоритм 4.3).

Для знаходження числа, оберненого за модулем, необхідні не тільки остачі $\{r_i\}$, які обчислюються у звичайному алгоритмі Евкліда (див. алгоритм 4.2), але й дільники $\{q_i\}$, які визначаються формулою (4.2). Умовою закінчення алгоритмів Евкліда є рівність (4.3). Основною для знаходження оберненого у модульній арифметиці є формула (4.12) (нагадаємо, що члени послідовності $\{u_i\}$ обчислюються у зворотному порядку, тобто числа u_2 та u_1 обчислюються останніми).

Для ілюстрації розглянемо дуже простий приклад з малими числами a та n.

Приклад 9. Для знаходження $(20, 7)$ алгоритм Евклі-

да 4.2 обчислює $r_i \equiv r_{i-2} \pmod{r_{i-1}}$:

i	-1	0	1	2	3
r_i	20	7	6	1	0

Розширений алгоритм Евкліда 4.3 додатково знаходить q_i за формулою $r_{i-2} = r_{i-1}q_i + r_i$:

i	-1	0	1	2	3
r_i	20	7	6	1	0
q_i			2	1	6

Згідно з теоремою 4.3 тепер необхідно заповнити другий рядок таблиці (4.11). Числа $\{u_i\}$ обчислюються за формулою (4.13). В нашому випадку обчислення є такими:

$$\begin{pmatrix} - & - & q_2 & q_1 \\ 0 & 1 & - & - \end{pmatrix} = \begin{pmatrix} - & - & 1 & 2 \\ 0 & 1 & - & - \end{pmatrix} \longrightarrow \begin{pmatrix} - & - & 1 & 2 \\ 0 & 1 & 1 & 3 \end{pmatrix}$$

Тому $20 \cdot 1 - 7 \cdot 3 = -1$, звідки $3 = 7^{-1} \pmod{20}$. ⑭

5. Контрольні питання

1. Отримати конгруенцію $b \equiv 23 - 3a \pmod{33}$. (стор. 144).

2. Пояснити, чому $(c, 33) = 1$? (стор. 144).

3. Поясніть, чому саме 20 пар задовольняють умову $\mathcal{C}_{\mathtt{B}} = \mathcal{P}_{\mathtt{T}}$. (стор. 144).

4. Перевірити обчислення у першій таблиці прикладу 2. (стор. 145).

5. Перевірити обчислення у другій таблиці прикладу 2. (стор. 145).

6. Чому конгруенції можна віднімати? (стор. 146).

7. Перевірити, що такий же результат отримуємо, якщо підставити a в першу конгруенцію. (стор. 146).

8. Перевірити, що $a = 2$. (стор. 149).
9. Чому $b = 16$? (стор. 149).
10. Чому саме $L_{17,-272}$ шифр? (стор. 149).
11. Чому шифри $L_{17,-272}$ та $L_{17,25}$ є еквіалентними? (стор. 149).
12. Поясніть чому необхідно 15 хвилин для того, щоб зламати $L_{a,b,n}$ шифр при відомому n? (стор. 151).
13. Як було підраховано, що існує 42,432 шифрів? (стор. 155).
14. Чому з $20 \cdot 1 - 7 \cdot 3 = -1$ випливає, що $3 = 7^{-1} \pmod{20}$? (стор. 157).

6. Задачі для самостійної роботи

Задача 1. *Довести, що якщо*

a) *відомий параметр a лінійного шифру $L_{a,b}$, то його дешифрація еквівалентна дешифрації шифру Цезаря*;
b) *відомий параметр b лінійного шифру $L_{a,b}$, то його дешифрація еквівалентна дешифрації мультиплікативного шифру.*

Задача 2. *Ви отримали повідомлення*

ІАУЛЬО ЗЯЛЯРЇ ЄУРОБФ ЯЩЯРЇІ АУЛЬОЗ ЯЛЯРЇЯ РЇБФЯЩ

яке було зашифровано лінійним шифром з параметром $a = 17$. Дешифрувати це повідомлення.

Задача 3. *Припустимо, що вам стало відомим місце, на якому в тексті, зашифрованому лінійним шифром $L_{a,b}$, стоїть код комбінації* АБ. *Як без обчислень визначити параметри a та b?*

Задача 4. *Припустимо, що вам випадково стало відомим, яким буквам в повідомленні відповідає комбінація* АБ *у тексті, отриманому застосуванням лінійного шифру. Як без обчислень визначити параметри лінійного шифру?*

Задача 5. *Повідомлення* ФЕРМА *зашифровано лінійним шифром. Зашифрованим текстом є* ИҐЧІЙ. *Визначити параметри шифру.*

Задача 6. *Повідомлення* ЕВКЛІД *зашифровано лінійним шифром. Зашифрованим текстом є* ЗТМСБҐ. *Визначити параметри шифру.*

Задача 7. *Повідомлення* ОЙЛЕР *зашифровано лінійним шифром. Зашифрованим текстом є* РИКЩФ. *Визначити параметри шифру.*

Задача 8. *Повідомлення* ГАУСС *зашифровано лінійним шифром. Зашифрованим текстом є* ЬЗДФФ. *Визначити параметри шифру.*

Задача 9. *За допомогою частотного аналізу дешифрувати повідомлення українською мовою*

БЩЬФХИЙЬ КЦГХИІДИ ТМИАНДЧЮ УЗСХГХДФ ЗСХКТЦИБ
ТЗЛЗБЗВД ГУЧМИАНЩ ІГХИЕГУЗ ЙЗБЗЛЗШЇ ГСХЗХДЗЛ
ЗГДГЬКЕЩ ЕГМИАНЗІ ГДЗЛЗХЧЦ СХЩ

яке було зашифровано мультиплікативним шифром $M_{a,33}$.

Задача 10. *У повідомленні, зашифрованому шифром* $L_{a,b}$, *найбільш уживаними буквами є* А *та* Ц. *Знайти параметри* a *та* b.

Задача 11. *Повідомлення можна спочатку зашифрувати лінійним шифром* L_{a_1,b_1}, *а потім отриманий результат зашифрувати лінійним шифром* L_{a_2,b_2}. *В результаті повідомлення буде зашифровано так званим продакт шифром. Знайти продакт шифр для комбінації* $L_{5,3}$ *та* $L_{17,3}$.

Задача 12. *Відомим в історії криптографії є випадок, який трапився під час II світової війни. Кожного дня радист німецької армії в пустелі Сахара надсилав в Берлін одне і те ж повідомлення* НІЧОГО НЕ ТРАПИЛОСЬ (*кожного дня зашифроване за допомогою нового ключа*). *Оскільки текст самого повідомлення був відомий англійським криптографам, вони кожного дня обчислювали ключ і за його допомогою дешифровували інші, часом важливі повідомлення від німецької армії в Сахарі.*

Припустимо, що ви знаєте, що текст НІЧОГО НЕ ТРАПИЛОСЬ *відповідає повідомленню* ДЦХЄИЄДМЛІҐЗФБЄЙЮ, *зашифрованому* $L_{a,b}$ *шифром з невідомими параметрами* a *та* b. *Знайти параметри цього шифру та дешифрувати інше повідомлення*: ДҐЙНЗЄЖЙЮГЦЬ.

Задача 13. *Доведіть, що для будь-яких цілих чисел* a *та* b, $b > 0$, *існують цілі числа* q *та* r, $-b/2 < r \le b/2$, *для яких* $a = bq + r$. *Цей спосіб представлення одного числа через інше є іншим способом ділення з остачею.*

Задача 14. *Довести, що* $a \pmod n = b \pmod n$ *тоді і тільки тоді, коли* $b - a$ *ділиться на* n.

Задача 15. *Нехай* $(a, b) = 1$. *Довести, що*

a) $(a + b, a - b) = 1$ *або* 2;
b) $(2a + b, a + 2b) = 1$ *або* 3;
c) $(a + b, a^2 + b^2) = 1$ *або* 2;
d) $(a + b, a^2 + -ab + b^2) = 1$ *або* 3.

Задача 16. *Нехай* a *та* b *є ненулевими цілими числами. Довести, що наступні три умови є еквівалентними*:

a) $a \mid b$;
b) $(a, b) = |a|$;
c) $[a, b] = |b|$.

Задача 17. *Нехай* a, b *та* $m > 0$ — *цілі числа. Довести, що якщо*

a) $a \equiv b \pmod m$, *то* $a \pmod m = b \pmod n$;
b) $a \pmod m = b \pmod n$, *то* $a \equiv b \pmod m$.

Задача 18. *Знайти контрприклад до твердження*: *якщо* $m > 2$ *є цілим, то*

a) $(a + b) \pmod m = a \pmod m + b \pmod m$ *для будь-яких цілих чисел* a *та* b;
b) $ab \pmod m = (a \pmod m) \cdot (b \pmod m)$ *для будь-яких цілих чисел* a *та* b.

Задача 19. *В турнірі приймають участь* $N = 2m$ *команд. Кожна команда має грати з іншою лише один раз. У кожному раунді повинні грати всі команди. Як можна скласти графік для такого турніру*?

Один з методів складання графіка турніру, який ми зараз опишемо, базується на властивостях конгруенцій: *команда* i *грає з командою* j *в раунді* k, *якщо* $(i + j) \equiv k \pmod{N - 1}$. *Це правило не стосується команди* N, *яка грає з такою командою* i, *для якої* $2i \equiv k \pmod{N - 1}$.

a) *Показати, що у кожному раунді* k *існує тільки одна команда* i, *для якої* $2i \equiv k \pmod{N - 1}$.

b) *Показати, що для кожної команди i в кожному раунді k існує тільки одна команда j, для якої* $(i+j) \equiv k \pmod{N-1}$.
c) *Показати, що кожна команда грає з іншою тільки один раз протягом турніру.*

Задача 20. *Прочитайте уважно умови задачі* 19.

a) *Як скласти графік турніру, у якому приймають участь непарна кількість команд?*
b) *Складіть графік турніру для п'яти команд.*

Задача 21. *Нехай $\sigma(n)$, $n > 1$, — це сума всіх дільників натурального числа включно з* 1 *та n. Покладемо також $\sigma(1) = 1$. Довести, що якщо p є простим числом, то*

a) $\sigma(p) = p + 1$;
b) $\sigma(p^k) = (p^{k+1} - 1)/(p - 1)$ *для* $k \geq 1$;
c) $\sigma(pq) = \sigma(p)\sigma(q)$ *для простого числа* $q > 1$;
d) $\sigma(p^k q^l) = \sigma(p^k)\sigma(q^l)$, *якщо* $q > 1$ *є простим числом, а* $k, l \geq 1$.

Задача 22. *Довести, що функція $\sigma(n)$, означена у задачі* 21, *є мультиплікативною, тобто*

$$\sigma(mn) = \sigma(m)\sigma(n),$$

якщо $(m, n) = 1$.

Задача 23. *Число n називається досконалим, якщо сума його дільників (без n) дорівнює цьому числу, тобто якщо $\sigma(n) - n = n$ або $\sigma(n) = 2n$ (означення функції $\sigma(n)$ див. в задачі* 21). *Довести теорему Евкліда: якщо $2^k - 1$ є простим числом, то $2^{k-1}(2^k - 1)$ є досконалим числом.*

Задача 24. *Нехай n є досконалим числом (означення досконалого числа див. в задачі* 23). *Довести, що*

$$\sum_{d|n} \frac{1}{d} = 2.$$

Задача 25. *Число n називається k-досконалим, якщо $\sigma(n) = kn$ (означення функції $\sigma(n)$ див. в задачі 21). Доведіть, що жодне з чисел $2^k 3^l$ не є досконалим.*

Задача 26. *Число n називається супердосконалим, якщо $\sigma(\sigma(n)) = 2n$ (означення функції $\sigma(n)$ див. в задачі 21). Доведіть, що число $n = 2^k$ є супердосконалим, якщо $2^{k+1} - 1$ є простим.*

Задача 27. *Нехай m — просте число; a та b — натуральні числа, $(a, m) = 1$. Для розв'язання рівняння*

$$ax \equiv b \pmod{m} \tag{4}$$

можна використати метод, який базується на наступних діях.

a) *Покажіть, що якщо x є розв'язком рівняння (4), то x також є розв'язком рівняння*

$$a_1 x \equiv -b[m/a] \pmod{m}$$

для $a_1 \equiv m \pmod{a}$. Нова конгруенція є такого ж типу, як і початкова, але з меншим коефіцієнтом у лівій частині.

b) *Повторюючи процедуру з* a), *отримуємо послідовність коефіцієнтів $a = a_0 > a_1 > a_1 > \dots$. Показати, що знайдеться n, при якому $a_n = 1$, тобто на цьому кроці рівняння має вигляд $x \equiv B \pmod{m}$.*

c) *Застосувати метод, описаний в* b), *для розв'язання рівняння $6x \equiv 7 \pmod{23}$.*

Задача 28. *Астроном знає, що період обертання супутника навколо Землі є кратним 1 годині і є меншим 1 дня. Астроном помітив, що супутник здійснює 11 обертань за час, який починається у момент, коли годинник показує 0 годин і закінчується, коли годинник показує 17 годин. Яким є період обертання супутника навколо Землі?*

Задача 29. *В таблиці, наведеній нижче, записано кількість днів у кожному з місяців високосного року, починаючи з грудня*:

	XII	*I*	*II*	*III*	*IV*	*V*	*VI*	*VII*	*VIII*	*IX*	*X*	*XI*
D_i	31	31	29	31	30	31	30	31	31	30	31	30
d_i	3	3	1	3	2	3	2	3	3	2	3	2

У третьому рядку обчислено значення $d_i \equiv D_i \pmod 7$, *де* D_i — *це кількість днів у місяці* i, $1 \le i \le 12$. *Кожному дню тижню припишемо такі числа:*

день	понеділок	вівторок	середа	четвер	п'ятниця	субота	неділя
w	1	2	3	4	5	6	0

Відомо, що 29.12.2015 припав на вівторок, для якого $w = 2$. *Тому 29.01.2016 припаде на* $(w + d_1) \pmod 7 = 5$, *тобто на п'ятницю.*

a) *Знайти правило, аналогічне тому, що було наведено вище для 29.01.2016, за яким можна визначати день тижня для кожної дати протягом 2016 року якщо знати на які дні тижня припадають дні довільного місяця.*
b) *Визначити скільки разів число 13 припаде на п'ятниці в 2016 році.*

Задача 30. *Прочитайте уважно текст задачі* 29. *Знайдіть правило, аналогічне тому, що було наведено у задачі* 29 *для 29.01.2016, за яким можна визначати день тижня для кожної дати протягом*

a) *невисокосного року*;
b) *будь-якого року, як завгодно далекого від 2015.*

Задача 31. *Історія математики зберігає багато задач про конгруенції, які вважались складними у свій час. Розв'яжіть три наступні задачі-головоломки.*

a) (*задача Махавіракарайя, 850 р.*) *Є* 7 *окремих бананів та* 63 *зв'язок по однаковій кількості бананів у кожній. Всі банани розділили порівну між* 23 *гостями. Скільки бананів було у кожній зв'язці*?
b) (*задача Йен Кунга, 1372 р.*) *Є кілька монет. Їх можна розкласти порівну у* 78 *стовпчиках. Якщо ж їх розкласти у* 77 *стовпчиках так, щоб кожен містив однакову кількість, то ще залишиться* 27 *монет. Скільки є монет*?
c) (*задача Ойлера, 1770 р.*) *Розбити число* 100 *на два доданки так, щоб один з них ділився на* 7, *а інший на* 11.

7. БІОГРАФІЇ

Керкхоффс, *Огюст* (1835–1903), нідерландський криптограф, лінгвист, історик, математик. Автор фундаментальної праці "*Військова криптографія*" ("*La Cryptographie Militaire*"), у якій він сформулював загальні вимоги до криптосистем. Одним з висновків цієї праці є висновок про те, що тільки криптоаналіз є єдино вірним способом оцінити надійність шифрів.

Своє знайомство з криптографією почав з вивчення телеграфних військових шифрів. Він особливо підкреслював, що на відміну від листування старого часу, телеграф значно збільшив обсяги інформації, якою обмінюються кореспонденти, що породжує принципово нові вимоги до шифрів.

"*Військова криптографія*" вперше була опублікована двома частинами в журнальному варіанті в січні і лютому 1883 року, а пізніше в тому ж році була перевидана у вигляді окремої брошури. Незважаючи на безсумнівну фундаментальність, праця була невеликою за обсягом — всього 64 сторінки. Запропоновані ним рішення нових криптографічних проблем були розумними і добре обґрунтованими. Керкхоффс сформулював шість загальних вимог до криптостійкості систем:

(1) система повинна бути фізично незламною;
(2) потрапляння системи в руки ворога не повинно завдавати проблем її автору;
(3) зберігання та передача ключа повинні здійснюватись без паперових записів; кореспонденти повинні мати можливість міняти ключ за своїм розсудом;
(4) система повинна бути придатною для передачі повідомлень телеграфом;
(5) система повинна легко адаптуватись при зміні місця; для роботи з нею не вимагається участь кількох осіб одночасно;
(6) нарешті, система повинна бути простою у використанні й не вимагати значного розумового напруження або дотримання

великої кількості правил.

Неш, *Джон* (1928–2015), американський математик, який працював у галузі теорії ігор та диференціальної геометрії.

Лауреат Нобелівської премії з економіки 1994 року (разом з Райнхардом Зелтеном та Джоном Харсані), а також Абелівської премії 2015 року (разом з Луїсом Ніренбергом). Найбільших досягнень Неш здобув у теорії ігор, яка вразила його уяву ще у віці 20 років. Неш зумів створити основи наукового методу, що зіграв величезну роль у розвитку світової економіки. У 1949 році 21-річний учений написав дисертацію у галузі теорії ігор, а через сорок п'ять років він отримав за цю роботу Нобелівську премію з економіки. У рішенні Нобелівського комітету записано, що Неш отримує нагороду "*за фундаментальний аналіз рівноваги в теорії некооперативних ігор*".

1998 року професор журналістики Колумбійського університету Сильвія Назар опублікувала біографічну книгу "*A Beautiful Mind*". У книзі вона змалювала багатогранне життя Джона Неша, описала проблеми впливу його тяжкої хвороби на світ особистих і професійних стосунків. 2001 року, за мотивами книги "*A Beautiful Mind*", історію Джона Неша покладено в основу голлівудського фільму "*Ігри розуму*", який пізніше отримав 4 премії Оскар.

Джон Неш загинув 23 травня 2015 р. разом зі своєю дружиною при поверненні з Норвегії із церемонії нагородження Абелівською премією. Трагедія сталася у штаті Нью-Джерсі: при перелаштуванні з лівої до правої смуги водій таксі втратив керування машиною і зіткнувся з огорожею та ще одним авто. Поліція встановила, що подружжя не було пристебнуте ременями безпеки, через це смерть настала практично миттєво.