12. Чому з $15t_2 + 7 \equiv 3 \pmod 7$ випливає $t_2 \equiv 3 \pmod 7$? (стор. 107).

13. Перевірити, що $x = 105s + 52$ для деякого цілого s. (стор. 107).

14. Впевнитись у тому, що старовинна китайська задача має нескінчену кількість розв'язків. (стор. 107).

15. Якщо модулі конгруенцій є взаємно простими, то $(M_i, m_i) = 1$ для кожного i. Чому? (стор. 108).

16. Показати, що $M_i \equiv 0 \pmod{m_j}$ якими б не були $i \neq j$. (стор. 108).

17. Згадайте, чому конгруенція $M_i y \equiv 1 \pmod{m_i}$ має єдиний розв'язок y_i? (стор. 109).

18. Довести, що найменшим спільним кратним чисел $m_1, \ldots, m_k$ є M? (стор. 109).

19. Навіщо ототожнювати Ґ з Г? (стор. 111).

8. Задачі

Задача 1. *За допомогою шифру Хілла з матрицею* $\begin{bmatrix} 1 & 2 \\ 3 & 4 \end{bmatrix}$ *зашифрувати фразу*

(a) ДУМИ МОЇ, ДУМИ МОЇ.
(b) НЕ КИДАЙТЕ ХОЧ ВИ МЕНЕ.

Задача 2. *Дешифрувати фразу, яку зашифровано методом Хілла з матрицею* $\begin{bmatrix} 1 & 2 \\ 3 & 4 \end{bmatrix}$:

(a) ФПСЧШҐЧШЖВ
(b) ШІЗЬЩҐЕХЖСЧШЖВ

Задача 3. *Чи підходить матриця* $\begin{bmatrix} 1 & 2 \\ 3 & 4 \end{bmatrix}$ *для шифрування за Хіллом текстів англійською мовою?*

Задача 4. *Чи підходить матриця* $\begin{bmatrix} 9 & 2 \\ 17 & 5 \end{bmatrix}$ *для шифрування за Хіллом текстів українською мовою?*

Задача 5. *Для матриці A розміру 2×2, елементами якої є натуральні числа a_{ij}, $1 \le i, j \le 2$, побудуємо матрицю A', яка складається з елементів $a_{ij} \pmod n$, де $n > 1$ — довільне натуральне число.*

(a) *Довести, що* $\det(A) \pmod n = \det(A') \pmod n$.
(b) *Довести аналогічне твердження для матриць розміру* $k \times k$.

Задача 6. *Довести, що шифр Хілла з матрицею A розміру 2×2 є рівносильним шифру Хілла з матрицею A', означеної у задачі 5. Чи є ця властивість вірною для довільного розміру $k \times k$?*

Задача 7. *Шифром підстановки називається наступне правило перетворення букв алфавіту: $\mathcal{C}_{\mathtt{X}} = \sigma(\mathcal{P}_{\mathtt{X}})$ для будь-якої букви* `X`, *де $\sigma(\cdot)$ — це перестановка символів алфавіту.*

(a) *Підрахувати кількість шифрів підстановки для українського алфавіту.*
(b) *Чи є шифр Цезаря шифром підстановки?*
(c) *Ототожнімо букви* `Ґ` *та* `Г`, *щоб в алфавіті залишилось 32 символи. До кожної з 8 послідовних груп, які складаються з чотирьох букв, застосуємо підстановку: $\sigma = \left(\begin{smallmatrix} 1 & 2 & 3 & 4 \\ 4 & 3 & 2 & 1 \end{smallmatrix}\right)$. Зашифрувати текст* `ХЕЛЛОУЇН`.
(d) *Записати формулу перетворення $\mathcal{P}_{\mathtt{X}}$ в $\mathcal{C}_{\mathtt{X}}$ для шифру з (c).*

Задача 8. *Скільки існує матриць 2×2, якщо їхні елементи приймають тільки значення 0 або 1? Скільки серед них матриць, які мають обернені за* mod 2?

Задача 9. *Розглянемо множину матриць 2×2, елементи яких a_{ij}, $1 \le i, j \le 2$, приймають тільки значення 0, 1 або 2. Розглянемо дві підмножини матриць A, які визначаються умовами*

$$\begin{array}{lll} a_{11} \neq 0, & a_{22} = 0, & \det(A) \pmod 3 \neq 0, \\ a_{11} \neq 0, & a_{22} \neq 0, & \det(A) \pmod 3 = 0. \end{array}$$

Довести, що в кожній з цих двох множин міститься 36 матриць.

Задача 10. *Розглянемо множину матриць* 2×2, *елементи яких* a_{ij}, $1 \le i, j \le 2$, *приймають тільки значення* 0, 1 *або* 2. *Розглянемо підмножину матриць* A, *яка визначається умовами*

$$a_{11} \neq 0, \qquad a_{22} \neq 0.$$

Скільки існує матриць у цій підмножині? Використовуючи задачу 9, *довести, що у цій множині існує рівно 36 матриць, які мають обернену за* mod 3.

Задача 11. *Розглянемо множину матриць* 2×2, *елементи яких* a_{ij}, $1 \le i, j \le 2$, *приймають тільки значення* 0, 1 *або* 2. *Розглянемо підмножину матриць* A, *яка визначається умовами*

$$a_{11} = 0, \qquad \det(A) \pmod 3 \neq 0.$$

(a) *Довести, що таких матриць існує рівно 12.*
(b) *Використовуючи задачі* 9 *та* 10, *довести, що існує рівно 48 матриць, для яких* $\det(A) \pmod 3 \neq 0$.

Задача 12. *Число* $(abc)_{10}$ *має остачу 5 при діленні на 12. Якщо це число помножити на 2, то отримаємо число, яке має остачу 4 при діленні на 35. Знайти a, b, c.*

Задача 13. *Знайдіть всі натуральні числа між 200 та 500, які при діленні на 4, 5 та 7 дають остачі 3, 4 та 5, відповідно.*

Задача 14. *Знайдіть всі натуральні числа, які при діленні на 2, 3, 4, 5, 6, 7 дають остачі 0, 1, 2, 3, 4, 5, відповідно.*

Задача 15. *За допомогою китайської теореми про остачі знайти розв'язок системи конгруенцій*

$$\begin{cases} x \equiv 5 \pmod 7, \\ x \equiv 3 \pmod{11}, \\ x \equiv 10 \pmod{13}. \end{cases}$$

Задача 16. *За допомогою китайської теореми про остачі знайти розв'язок системи конгруенцій*

$$\begin{cases} x \equiv 1 \pmod{15}, \\ x \equiv 3 \pmod{17}, \\ x \equiv 10 \pmod{24}, \\ x \equiv 4 \pmod{19}. \end{cases}$$

Чи існує розв'язок цієї системи, якщо замість 19 в останній конгруенції обрати у якості модуля 8?

Задача 17. *Китайську теорему про остачі використовують для виконання арифметичних операцій з великими числами. Нехай, наприклад,* $m_1 = 2^{23} - 1$, $m_2 = 2^{29} - 1$, $m_3 = 2^{33} - 1$, $m_4 = 2^{34} - 1$, $m_5 = 2^{35} - 1$. *Можна перевірити, що всі ці числа є простими. Покладемо* $M = m_1 m_2 m_3 m_4 m_5$.

(a) *Чому кожне натуральне число* $x \leq M$ *можна єдиним чином представити п'ятіркою натуральних чисел* $(a_1, \ldots, a_5)$, *де* $a_i = x \pmod{m_i}$?
(b) *Скільки десяткових цифр можуть мати такі числа* x?
(c) *Як, використовуючи остачі від ділення на* $m_1, \ldots, m_5$, *можна здійснювати операції додавання та множення чисел* $x \leq M$ *та* $y \leq M$?
(d) *Якими мають бути* x *та* y, *щоб операції додавання та множення за допомогою остач від ділення на* $m_1, \ldots, m_5$, *давали коректний результат*?

Задача 18. *Можна обчислити, що* $2^{26} = 67,108,864$ *та* $2^{27} = 134,217,728$. *Калькулятор* `Casio fx 330A` *може робити точні обчислення лише для натуральних чисел, які не перевищують* $99,999,999$. *Оскільки* $2^{31} > 99,999,999$, *то при обчисленні калькулятор дає приблизну відповідь* $2^{31} \approx 2.1474836 \cdot 10^9$. *Знайдіть спосіб обчислити точно* 2^{31} *за допомогою лише* `Casio fx 330A` *та китайської теореми про остачі.*

Задача 19. *Довести, що дві конгруенції* $x \equiv a \pmod{n}$ *та* $x \equiv b \pmod{m}$ *мають спільний розв'язок тоді і тільки тоді, коли*

$a - b$ ділиться на (n, m); якщо розв'язок існує, то він є єдиним за модулем $[n, m]$.

Задача 20. *Знайти всі значення a, при яких наступна система має хоча б один розв'язок*

$$\begin{cases} 2x \equiv a \pmod 4, \\ 3x \equiv 4 \pmod{10}. \end{cases}$$

Задача 21. *Знайти хоча б одне m, при якому наступна система не має жодного розв'язку*

$$\begin{cases} x \equiv 3 \pmod 6, \\ x \equiv 7 \pmod m. \end{cases}$$

Задача 22. *Довести, що наступні системи не мають розв'язків*

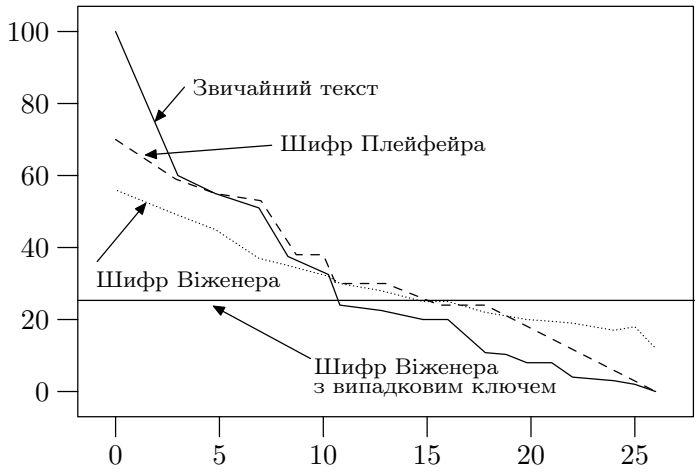
(a) $\begin{cases} x \equiv 2 \pmod 4, \\ x \equiv 3 \pmod 6; \end{cases}$ (b) $\begin{cases} x \equiv 3 \pmod 4, \\ x \equiv 4 \pmod 5, \\ x \equiv 4 \pmod 6. \end{cases}$

Задача 23. *Довести, що якщо $x \equiv a \pmod n$, то виконується одна з двох конгруенцій $x \equiv a \pmod{2n}$ або $x + n \equiv a \pmod{2n}$. Чи можуть ці дві конгруенції справджуватись одночасно?*

Задача 24. *Знайти ціле число, яке при діленні на*

(a) *2, 3, 6, 12 дає остачі 1, 2, 5, 5* (Ю Хін, пом. 717 р.);
(b) *3, 4, 5, 6 дає остачі 2, 3, 4, 5* (Бхаскара, нар. 1114 р.);
(c) *10, 13, 17 дає остачі 3, 11, 15* (Регіомонтан (1436-1476)).

Задача 25. *Наступний малюнок створено на основі аналізу статті англійською в енциклопедії Brittaniса по криптології, яка складається з більше ніж 70,000 літер.*



Для кожної букви латинського алфавіту було підраховано її відносну кількість, тобто кількість копій цієї букви у тексті, поділену на кількість букв "e" (найбільш уживана буква в англійській мові). Зрозуміло, що відносна частота букви буква "e" дорівнює. Виявилось також, що відносна частота, наприклад, "t" дорівнює приблизно 0,76. Частоти на малюнку розташовано у порядку спадання. На малюнку показано графіки відносних частот після шифрування статті про криптографію за допомогою шифрів Плайфейра та Віженера, а також за допомогою шифра Віженера з випадковим ключем.

(a) *За допомогою малюнка поясніть, чому шифр Віженера вважається найбільш стійким до дешифрування за допомогою частотного аналізу?*
(b) *Проаналізуйте стійкість інших шифрів, представлених на малюнку.*

Задача 26. *При застосуванні шифра Плейфейра в англійській мові використовують таблицю* 5×5, *а букви* `I` *та* `J` *ототожнюють. Якщо кількість букв у повідомленні є непарною, то в кінці додають букву* `X`.

(a) *Чому в англійській мові обрано таблицю* 5×5, *а в українській —* 4×8?
(b) *Для чого ототожнюють букви* `I` *та* `J`? *Чому саме їх*?
(c) *Навіщо в кінці повідомлення додають букву* `X`, *якщо кількість букв у повідомленні є непарною*?

Задача 27. *У романі англійської письменниці Дороті Сейерз "Have His Carcase" шифр Плейфейра грає визначальну роль. Повідомлення* `WE ARE DISCOVERED` *в тому романі було зашифровано за допомогою шифра Плейфейра з використанням ключового слова* `MONARCHY` *та матриці кодування*

M	**O**	**N**	**A**	**R**
C	**H**	**Y**	B	D
E	F	G	I/J	K
L	P	Q	S	T
U	V	W	X	Z

Зашифрувати це повідомлення.

Задача 28. *За допомогою тієї ж матриці кодування, що і в задачі* 27, *дешифрувати закінчення повідомлення*: `XBUF HNZMLIXE`.

Задача 29. *Запишіть наступні числа у вигляді звичайних та десяткових дробів:*

(a) $0,\underset{\text{period}}{(12)} + 0,\underset{\text{period}}{(122)}$;
(b) $0,\underset{\text{period}}{(3)} \cdot 0,\underset{\text{period}}{(4)}$;
(c) $0,\underset{\text{period}}{(9)} - 0,\underset{\text{period}}{(85)}$.

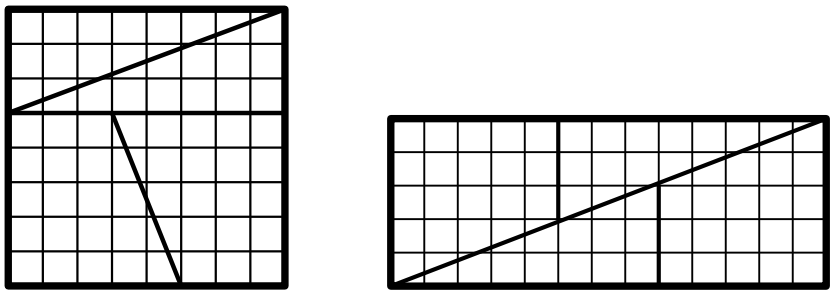
Тут за допомогою $0,\underset{\text{period}}{(xyz)}$ *позначено нескінчений десятковий дріб з періодом* xyz, *тобто* $0,xyzxyzxyz\ldots$.

Задача 30. (старовинна французька задача) *Жінка несла на базар кошик яєць. Перехожий ненавмисно штовхнув її, корзина впала і яйця розбилися. Винуватець, бажаючи відшкодувати втрату, запитав, скільки яєць було в кошику. "Точно не знаю, — відповіла жінка, — але пам'ятаю, що коли я виймала з кошика по 2, по 3, по*

4, по 5, по 6 яєць, в кошику завжди залишалося одне яйце, а коли виймала по 7, в кошику нічого не залишалося ". Яке найменше число яєць могло бути в кошику?

Задача 31. (задача Брахмагупти, VII ст.) *Якщо виймати яйця з кошику по 2, 3, 4, 5 або 6 за раз, то залишаються 1, 2, 3, 4 або 5 яєць відповідно. Якщо ж виймати по 7, то в кошику нічого не залишиться. Яке найменше число яєць могло бути в кошику?*

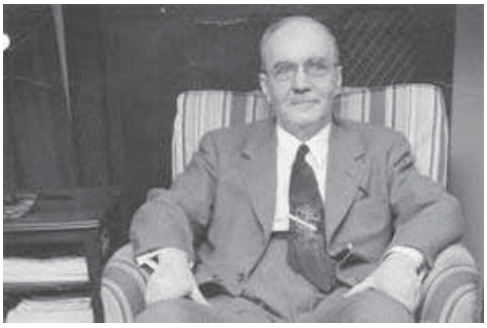
Задача 32. *Нижче наведено геометричне "доведення" рівності* $64 = 65$. *Шахівницю* 8×8 *розрізають на чотири частини, як показано на лівому малюнку, а потім з них складають іншу фігуру, зображену на правому малюнку*:



Як розташувати ті ж чотири частини шахівниці так, щоб "довести" рівність $64 = 63$?

БІОГРАФІЇ

Хілл, *Лестер* (1891–1961), американський математик та вчений у галузі шифрування, цікавився застосуваннями математики до теорії інформації та зв'язку.



Лестер Хілл

Він запропонував методи виявлення помилок у телеграфному коді. Має значні внески у розвиток криптографії та теорії кодування. За результати у цих науках відзначений урядом США під час другої світової війни.

У 1929 році він розробив шифри Хілла, які тепер відносять до класу полиграмних шифрів підстановки. Особливістю шифра Хілла було інтенсивне використання методів лінійної алгебри. Процес шифрування та дешифрування методом Хілла розмірності 6 було реалізовано за допомогою механічного пристрою, який здійснював множення матриць 6×6 за допомогою системи шестерінок та приводів. Розташування шестерінок змінювати було неможливо, що означало один і той же ключ для всіх повідомлень. З метою підвищити криптостійкість рекомендувалось послідовно трічи пропускати текст через машину Хілла. Така комбінація була дуже надійною для 1929 року, проте машина попитом не користувалась.

Зараз вважається, що шифр Хілла є вразливим, тобто нестійким до криптоатак.

Плейфейр, *Ліон* (1818–1898), шотландський вчений та політик. Ім'ям Плейфейра названо систему шифрування, застосування якої в англійській армії він домігся, хоча автором є інший англійський вчений *Чарльз Уітстен* (1802–1875).

Ліон Плейфейр

Чарльз Уітстен

Простота і надійність цього шифру зробили його надзвичайно популярним в англійській армії. Британці користувались цим шифром під час англо-бурської війни, а пізніше і під час першої світової війни. Навіть під час другої світової війни цей шифр був резервним в американській армії на випадок несподіваних подій. Відомо, що лейтенант Джон Ф. Кеннеді (пізніше став президентом США) у 1943 році використав цей метод шифрування, щоб відправити аварійне повідомлення після того, як його човен був потоплений японськими військовими кораблями поблизу Соломонових островів.

Шифр Плейфейра має значні переваги над іншими одноалфавітними шифрами через ускладнену ідентифікацію діграм у разі його застосування. Певний час його навіть вважали незламним. Проте, сучасні криптографи встановили, що цей шифр не є надійним, оскільки він все ж таки зберігає багато структурних особливостей природних текстів. Як правило, кількох сотень символів у повідомленні вистачає, щоб його дешифрувати.