11. Доведіть конгруенцію (8). (стор. 174).
12. Пояснити рівності $a^{kj} = up + a$ та $a^{kj} = vq + a$. (стор. 174).
13. Чому $q \mid u$, якщо $up = vq$? (стор. 174).
14. Пояснити правило 2. (стор. 174).
15. Перевірити, чи дійсно ми вже довели лему 4? (стор. 174).
16. Підрахувати $\phi(33)$. (стор. 175).
17. Перевірити рівність $27^{-1} \pmod{20} = 3$. (стор. 175).
18. Чому алгоритм 2 завжди дає $a^k \pmod{n}$? (стор. 177).
19. Пояснити, чому алгоритм 3 є правильним у загальному випадку? (стор. 179).
20. Пояснити, чому алгоритм 4 є правильним у загальному випадку? (стор. 181).

7. Задачі

Задача 1. *Знайти два різні натуральні числа $a < 29$ та $b < 29$, для яких $a^2 \equiv b^2 \pmod{29}$. Пояснити, чому не варто використовувати шифр $E_{2,29}$?*

Задача 2. *Перевірити, що $9^k \equiv 0 \pmod{27}$ для будь-якого $k \geq 2$. Чому мультиплікативний шифр з модулем $n = 27$ не варто використовувати?*

Задача 3. *Оскільки $391 = 17 \times 23$, то*

$$\phi(391) = \phi(17)\,\phi(23) = 16 \cdot 22 = 352.$$

Пояснити, що означає рівність $\phi(391) = 352$ з точки зору

a) *теорії чисел,*
b) *лінійних шифрів,*
c) *експоненціальних шифрів.*

Задача 4. *Обчислити*

a) $31^{11} \pmod{59}$;
b) $11^{41} \pmod{521}$;
c) $19^{107} \pmod{1249}$.

Задача 5. *Використовуючи конгруенцію* $29 \equiv -2 \pmod{31}$, *обчислити*

a) $29^2 \pmod{31}$;
b) $29^5 \pmod{31}$.

Задача 6. *Скільки операцій множення необхідно зробити, щоб обчислити*

a) a^{47}?
b) a^{147}?

Задача 7. *Записати* $(2015)_{10}$ *у двійковій системі числення за допомогою*

a) *алгоритму 3*;
b) *алгоритму 4*.

Задача 8. *Записати* $(988)_{10}$ *у двійковій системі числення за допомогою*

a) *алгоритму 3*;
b) *алгоритму 4*.

Задача 9. *Записати позиції букв тексту* `КІНО` *у десятковій та двійковій системах числення.*

Задача 10. *Записати позиції букв тексту* `ШИФР` *у десятковій та двійковій системах числення.*

Задача 11. *Використовуючи алгоритм 2, зашифрувати текст* `КІНО` *за допомогою експоненціального шифру з параметрами* $k = 2015$ *та* $n = 1000$.

Задача 12. *Використовуючи алгоритм 2, зашифрувати текст* `ШИФР` *за допомогою експоненціального шифру з параметрами* $k = 988$ *та* $n = 51$.

Задача 13. *Знайти* j, *при якому* $a^{7j} \equiv a \pmod{34}$.

Задача 14. *Знайти* j, *при якому* $a^{7j} \equiv a \pmod{523}$. *Зважте на те, що* 523 *є простим числом.*

Задача 15. *За допомогою експоненціального шифру $E_{7,34}$ отримано зашифрований текст* ЇАС. *Дешифрувати його (використати обчислення, зроблені у задачі 13).*

Задача 16. *За допомогою експоненціального шифру $E_{7,523}$ отримано зашифрований текст* 131 95 1. *Дешифрувати його (використати обчислення, зроблені у задачі 14).*

Задача 17. *Нехай $p \equiv 2 \pmod 3$, де p — просте число. Показати, що $(3, \phi(p)) = 1$. Це означає, що $k = 3$ можна обрати для експоненціального шифру за модулем p. Показати, що показник степеня для дешифрації такого шифру дорівнює $j = \frac{2p-1}{3}$.*

Задача 18. *Нехай $p \equiv 2 \pmod 3$ та $q \equiv 2 \pmod 3$, де p та q — прості числа. Покладемо $n = pq$. Показати, що $(3, \phi(n)) = 1$. Це означає, що $k = 3$ можна обрати для експоненціального шифру за модулем n. Знайти показник степеня для дешифрації такого шифру.*

Задача 19. *Нехай $n = p_1p_2p_3$, де p_1, p_2, p_3 — три різних простих числа. Нехай k та j є взаємно оберненими за модулем $\phi(n)$. Довести, що $a^{kj} \equiv a \pmod{\phi(n)}$ для всіх цілих a.*

Задача 20. *Використовуючи задачу 19, визначити показник j кореня з k за модулем $\phi(n)$, якщо $k = 7$, $n = p_1p_2p_3$, $p_1 = 11$, $p_2 = 13$, $p_3 = 19$.*

Задача 21. *Нехай a та m — натуральні числа, причому $(a, m) = 1$. Довести, що послідовність $r_i = a^i \pmod m$, $i \geq 0$, є періодичною.*

Задача 22. *Згідно до задачі 21, послідовність $r_i = a^i \pmod m$, $i \geq 0$, є періодичною, якщо $(a, m) = 1$. Найменший період цієї послідовності назвемо порядком числа a за модулем m і позначатимемо $\operatorname{ord}_m(a)$. Нехай натуральне число u є таким, що $a^u \equiv 1 \pmod m$. Довести, що $\operatorname{ord}_m(a) \mid u$.*

Задача 23. *Позначення $\operatorname{ord}_m(a)$ для натуральних чисел a та m пояснено у задачі 22. Довести, що якщо $(a, m) = 1$, то $\operatorname{ord}_m(a) \mid \phi(m)$.*

Задача 24. *Довести, що якщо $ab \equiv 1 \pmod m$, то $\operatorname{ord}_m(a) = \operatorname{ord}_m(b)$.*

Задача 25. *Позначимо* $e = \mathrm{ord}_m(a)$. *Нехай* k — *натуральне число. Довести, що*

$$\mathrm{ord}_m(a^k) = \frac{e}{(e,k)}.$$

Задача 26. *Натуральне число* α *називається примітивним коренем для модуля* m, *якщо* $(\alpha, m) = 1$ *та* $\mathrm{ord}_m(\alpha) = \phi(m)$. *Перевірити, що*

a) 3 *та* 5 *є примітивними коренями для модуля* 7;
b) 2 *є примітивними коренями для модуля* 9.

Довести, що не існує жодного примітивного кореня для модуля 12.

Задача 27. *Нехай* $\mathrm{ord}_m(a) = e$. *Довести, що* $a^i \equiv a^j \pmod{m}$ *тоді і тільки тоді, коли* $i \equiv j \pmod{e}$.

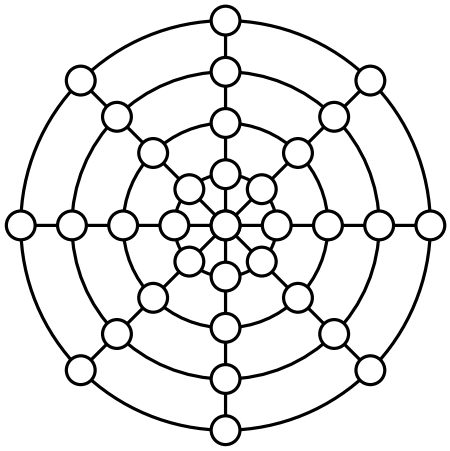
Задача 28. *Нехай* α — *це примітивний корінь для модуля* m (*ми також кажемо, що* m *має примітивний корінь* α). *Позначимо* $r_k = \alpha^k \pmod{m}$, $1 \le k \le \phi(m)$. *Довести, що* $r_1, \ldots, r_{\phi(m)}$ — *це перестановка чисел, які не перевищують* m *та є взаємно простими з ним.*

Задача 29. *Довести, що якщо число* m *має примітивний корінь, то воно має* $\phi(\phi(m))$ *примітивних коренів. Зокрема, якщо* m *є простим числом, то воно має* $\phi(m-1)$ *примітивних коренів.*

Задача 30. *Довести, що якщо просте число* $p > 3$ *має примітивний корінь, то воно має парну кількість примітивних коренів.*

Задача 31. *Нехай натуральне число* m *є таким, що* $(a, m) = 1$ *та* $\mathrm{ord}_m(a) = m - 1$. *Довести, що* m *є простим числом.*

Задача 32. *На малюнку, наведеному нижче, розташувати числа 1, 2, . . . , 33 в маленьких колах так, щоб суми чисел на усіх більших колах та на діаметрах були б однаковими.*



Цю задачу запропонував китайський математик Янг Хуу книзі "Методи обчислень", виданій у 1275 році.

БІОГРАФІЇ

Поліґ, *Стефен* (нар. 1953 р.), американський інженер-електрик, працює в Масачусетському технологічному інституті. В середині 1970-х років був аспірантом Мартіна Хеллмана в Стенфордському університеті. Саме тоді він брав участь у розробці експоненціального шифру. Отримані ним формули використовуються також і для обчислення дискретних логарифмів.

С. Поліґ

В 1978 році разом з М. Хеллманом отримав патент "*Метод для експоненціального шифрування*".

Хеллман, *Мартін* (нар. 2.10.1945), американський криптограф. Здобув популярність головним чином завдяки розробці першої асиметричною криптосистеми у співавторстві з Уітфілдом Діффі і Ральфом Меркле у 1976 році.

М. Хеллман

Проте його спільна робота з С. Поліґом стосовно експоненціальних шифрів також добре відома спеціалістам.