Глава 6

ЛІНІЙНІ ШИФРИ

Як шифр Цезаря, так і мультиплікативний шифр не є стійкими до криптоатак, але їхня комбінація є більш надійною. Як ми бачили у §3.5, глава 3, розширення алфавіту може приводити до підвищення стійкості шифру. Особливо це стає помітним при групуванні символів повідомлення, яке необхідно зашифрувати. Після розширення алфавіт може складатися з довільної кількості букв, тому для загальності аналіза ми розглядаємо алфавіт $\mathscr{A}$, який складається з n букв. Таким чином можна вважати, що *алфавіт* — це сукупність n довільних *символів*.

Ми називаємо *лінійним шифром* наступне перетворення алфавіту $\mathscr{A}$

$$\mathcal{C}_{\mathtt{X}} \equiv a\mathcal{P}_{\mathtt{X}} + b \pmod{n}, \qquad X \in \mathscr{A}, \tag{1}$$

яке визначається параметрами a, b, та n і яке позначається $L_{a,b,n}$. У випадку $n = 33$ ми замість $L_{a,b,33}$ пишемо $L_{a,b}$. Лінійні шифри називають також *афінними*.

Тут a та b два параметри лінійного шифру. Дію $L_{a,b}$ шифра можна описати словами наступним чином: шифр $\mathcal{C}_{\mathtt{X}}$ кожної букви $\mathtt{X}$ дорівнює зсунутому на b добутку її позиції $\mathcal{P}_{\mathtt{X}}$ в алфавіті $\mathscr{A}$ на a та обчисленому за модулем n.

Зауваження 1. Лінійний шифр $L_{a,b}$ при $a = 1$ перетворюється в шифр Цезаря C_b, а при $b = 0$ — в мультиплікативний шифр M_a.

Приклад 1. Нижче показано процедуру перетворення повідомлення УРА за допомогою $L_{2,5}$ шифру:

УРА $\longrightarrow$ 24 21 1	перетворення букв у числа
$\longrightarrow$ 48 42 2	множення на 2
$\longrightarrow$ 53 47 7	зсув на 5
$\longrightarrow$ 20 14 7	обчислення mod 33
$\longrightarrow$ П Й Е	перетворення чисел у букви

Закодованим повідомленням є ПЙЕ.

1. Дешифрування лінійного шифру

Як і для мультиплікативних шифрів, параметри a та n повинні бути взаємно простими для того, щоб $L_{a,b}$ шифр був взаємно однозначним. ① Ми знаємо (див. §3.1, глава 3), що для дешифрування мультиплікативного шифру використовується число обернене до a за модулем n, причому $a^{-1} \pmod n$ існує, якщо $(a,n)=1$. Тому в такому випадку конгруенцію (1) можна перетворити наступним чином

$$\mathcal{P}_{\mathtt{X}} \equiv a^{-1}\mathcal{C}_{\mathtt{X}} - a^{-1}b \pmod n. \tag{2}$$

② Таким чином, дешифрування $L_{a,b}$ шифру здійснюється за допомогою лінійного шифру з параметрами $a^{-1} \pmod n$ та $-b\cdot a^{-1} \pmod n$. Щоб привести цю формулу до вигляду (1), другий параметр у рівності (2) можна записати у вигляді $n - a^{-1}b \pmod n$. ③ Таким чином,

$$\begin{gathered}\mathcal{P}_{\mathtt{X}} = u\mathcal{C}_{\mathtt{X}} + v \pmod n,\\ u = a^{-1} \pmod n,\\ v = n - a^{-1}b \pmod n.\end{gathered} \tag{3}$$

Приклад 2. Нижче показано процедуру дешифрування повідомлення ПЙЕ, закодованого за допомогою $L_{2,5}$ шифру. Нагадаємо, що $2^{-1} \pmod{33} = 17$, тому дешифрування здійснюється за правилом:

$$\mathcal{P}_{\mathtt{X}} \equiv 17\mathcal{C}_{\mathtt{X}} - 17 \cdot 5 \pmod{33}.$$

Оскільки $14 = 33 - 17 \cdot 5 \pmod{33}$, то

$$\mathcal{P}_{\mathtt{X}} \equiv 17\mathcal{C}_{\mathtt{X}} + 14 \pmod{33}.$$

Тому

ПЙЕ	⟶	20	14	7	перетворення букв у числа
	⟶	340	238	119	множення на 17
	⟶	354	252	133	зсув на 14
	⟶	24	21	1	обчислення mod 33
	⟶	У	Р	А	перетворення чисел у букви

Таким чином, закодовано було повідомлення УРА.

2. Скільки існує лінійних шифрів?

Існує 33 шифрів Цезаря та 20 однозначних мультиплікативних шифрів для українського алфавіту (див. §3.2, глава 3). ④ Тому загалом існує $33 \cdot 20 = 660$ лінійних шифрів. ⑤ Один з них, а саме $L_{1,0}$, є тотожним перетворенням, тому існує 659 нетривіальних лінійних шифрів. Чи нема серед них однакових? Однаковими ми вважаємо такі два шифри, для яких коди довільної букви є однаковими. Якщо ж коди хоча б однієї букви є різними, то ми вважаємо, що шифри є різними.

Теорема 1. *Нехай* $1 \le a_1, a_2 < n$ *та* $0 \le b_1, b_2 < n$. *Тоді, якщо для будь-якого* $0 \le m < n$

$$a_1 m + b_1 \equiv a_2 m + b_2 \pmod{n}, \tag{4}$$

то $a_1 = a_2$ *та* $b_1 = b_2$.

Таким чином, теорема 1 стверджує, що всі 659 лінійних шифрів є різними.

Доведення теореми 1. При умовах теореми, накладених на b_1 та b_2, з конгруенції (4) при $m = 0$ випливає, що $b_1 = b_2$. ⑥ Знову скористаємось конгруенцією (4), але тепер при $m = 1$, й отримаємо $a_1 = a_2$. ⑦ □

2.1. Випадок загального n. Скільки існує лінійних шифрів для алфавіту, який складається з n букв? Зрозуміло, що для такого алфавіту існує n шифрів Цезаря, але скільки існує однозначних мультиплікативних шифрів? Ми знаємо, що у випадку $n = 33$ таких шифрів рівно 20. А як обчислити їхню кількість у загальному випадку?

Означення 1. *Функцією Ойлера* $\phi(n)$ для аргументу n називається кількість натуральних чисел, менших за n та взаємно простих з n.

Таким чином, відповідь на поставлене питання визначається функцією Ойлера: існує $\phi(n)$ мультиплікативних шифрів й $n\phi(n)$ лінійних шифрів для алфавіту, який складається з n букв.

Приклад 3. Нагадаємо, що латинський алфавіт складається з 26 букв. Скільки існує лінійних шифрів для латинського алфавіту? Відповідь вже відома: існує $26 \cdot \phi(26)$

лінійних шифрів. Але чому дорівнює $\phi(26)$? Безпосередньо можна обчислити, що $\phi(26) = 12$, оскільки 1, 3, 5, 7, 9, 11, 15, 17, 19, 21, 23, 25 є взаємно простими з 26. ⑧ Тому існує 312 лінійних шифрів для латинського алфавіту.

Чи можна запропонувати алгоритм обчислення значення функції Ойлера для довільного аргумента?

3. Функція Ойлера

Зрозуміло, що $\phi(n) \leq n - 1$. ⑨ Ця оцінка є точною, оскільки $\phi(n) = n - 1$, якщо n є простим числом. ⑩

Властивість 1. *Якщо p є довільним простим числом, то $\phi(p) = p - 1$.*

Значення функції Ойлера нескладно отримати й для степеня простого числа.

Властивість 2. *Нехай p є простим числом, а $k \geq 1$. Тоді*

$$\phi\left(p^k\right) = p^k - p^{k-1}. \tag{5}$$

Доведення властивості 2. Тільки числа вигляду $p{\cdot}j$, $j \in \mathbf{N}$, не є взаємно простими з p^k. ⑪ Таких чисел, менших за p^k, існує p^{k-1}. ⑫ Звідси і випливає необхідне твердження. □

Властивість 3. *Нехай p та q є різними простими числами. Тоді*

$$\phi(pq) = (p-1)(q-1). \tag{6}$$

Доведення властивості 3. Серед чисел, що не перевищують pq, тільки ті числа не є взаємно простими з pq, які діляться або на p, або на q. ⑬ Ці дві множини мають одне спільне число pq. Тому $\phi(pq) = pq - p - q + 1$. ⑭ □

Приклад 4. На підставі формули (6) ⑮

$$\phi(33) = \phi(3 \cdot 11) = (3-1)(11-1) = 20,$$
$$\phi(26) = \phi(2 \cdot 13) = (2-1)(13-1) = 12.$$

Властивість 4. *Нехай p та q є різними простими числами, а $i, j \geq 1$. Тоді*

$$\phi\left(p^i q^j\right) = (p^i - p^{i-1})(q^j - q^{j-1}). \tag{7}$$

Доведення властивості 3. Рівно $p^{i-1}q^j$ чисел, менших за $p^i q^j$, діляться на p. ⑯ Аналогічно, рівно $p^i q^{j-1}$ чисел, що не перевищують $p^i q^j$, діляться на q, й рівно $p^{i-1}q^{j-1}$ чисел, що не перевищують $p^i q^j$, діляться на pq. Тому $\phi\left(p^i q^j\right) = p^i q^j - p^{i-1}q^j - p^i q^{j-1} + p^{i-1}q^{j-1}$. ⑰ Ця рівність є еквівалентною до рівності (7). □

Зауважимо, що властивість 3 можна записати у вигляді

$$\phi\left(p^i q^j\right) = \phi\left(p^i\right)\phi\left(q^j\right). \tag{8}$$ ⑱

3.1. Формула включення/виключення. Доведення всіх властивостей функції Ойлера, розглянутих вище, використовує одну просту, але важливу, ідею. Її можна представити наступним чином: якщо певна множина містить рівно N елементів, з яких

- рівно N_1 елементів задовольняють обмеженню V_1,
- рівно N_2 елементів задовольняють обмеженню V_2,
- рівно N_{12} елементів задовольняють обом обмеженням V_1 та V_2,

то

$$M = N - N_1 - N_2 + N_{12} \tag{9}$$

де M — це кількість елементів, які не задовольняють жодне з обмежень.

Наприклад, при доведенні властивості 4 множина елементів складається з натуральних чисел, які не перевищують $N = p^i q^j$; обмеження V_1 означає, що число з цієї множини ділиться на p, а V_2 — що ділиться на q. Тоді $N_1 = p^{i-1} q^j$, а $N_2 = p^i q^{j-1}$. В доведенні властивості 4 ми встановили, що кількість чисел, які не діляться на p та на q, дійсно дорівнює (9).

Ідея підрахунку необхідної кількості полягає в тому, що ми виключаємо з множини ті її елементи, які мають властивості V_1 та V_2, а потім включаємо туди ті елементи, які мають обидві властивості. Елементи, які залишились в множині, не мають жодного з обмежень. Через такий спосіб утворення необхідної множини, формула (9) називається *формулою включення/виключення.*

Формула включення/виключення відома й для довільної кількості обмежень, а не тільки для двох, як у випадку (9). Символічно загальну формулу можна записати наступним чином: якщо M — це кількість елементів, які не задовольняють жодному з обмежень $V_1, \ldots, V_k$, то

$$M = N - \underbrace{(N_1 + \ldots)}_{\text{одне обмеження}} + \underbrace{(N_{12} + \ldots)}_{\text{два обмеження}} - \underbrace{(N_{123} + \ldots)}_{\text{три обмеження}} + \cdots + (-1)^k \underbrace{N_{123\ldots k}}_{k \text{ обмежень}}.$$

Тут вираз з назвою “одне обмеження” дорівнює сумі всіх можливих чисел N_α, $1 \le \alpha \le k$, де N_α — це кількість

елементів, які задовольняють обмеженню V_α; вираз з назвою "два обмеження" дорівнює сумі всіх можливих чисел $N_{\alpha\beta}$, $1 \le \alpha < \beta \le k$, де $N_{\alpha\beta}$ — це кількість елементів, які задовольняють обмеженням V_α та V_β; вираз з назвою "три обмеження" дорівнює сумі всіх можливих чисел $N_{\alpha\beta\gamma}$, $1 \le \alpha < \beta < \gamma \le k$, де $N_{\alpha\beta\gamma}$ — це кількість елементів, які задовольняють обмеженням V_α, V_β та V_γ; ... . Нарешті, вираз з назвою "k обмежень" дорівнює одному числу $N_{123\ldots k}$ — кількості елементів, які задовольняють всі k обмежень.

3.2. Загальна формула для функції Ойлера. Саме варіант формули включення/виключення з довільною кількістю обмежень використовується при доведенні формули для функції Ойлера у найбільш загальному вигляді.

Властивість 5. *Нехай $p_1, \ldots, p_k$ — різні прості числа, а $i_1, \ldots, i_k \ge 1$. Тоді*

$$\phi\left(p_1^{i_1} \ldots p_k^{i_k}\right) = p_1^{i_1} \ldots p_k^{i_k} \left(1 - \frac{1}{p_1}\right) \ldots \left(1 - \frac{1}{p_k}\right). \tag{10}$$

Зауважимо, що при $k = 2$ властивість 5 є рівносильною (7). ⑲

Доведення властивості 5. Позначимо $m = p_1^{i_1} \ldots p_k^{i_k}$. Для будь-якого $1 \le j \le k$ існує рівно m/p_j чисел, які не перевищують m та діляться на p_j. Аналогічно, для будь-якої пари різних $j_1 \le k$ та $j_2 \le k$ існує рівно $m/p_{j_1}p_{j_2}$ чисел, які не перевищують m та діляться на $p_{j_1}p_{j_2}$.

Якщо $l \le k$, то для будь-яких $j_1 \le k, \ldots, j_l \le k$ існує рівно $m/p_{j_1} \ldots p_{j_l}$ чисел, які не перевищують m та діляться на $p_{j_1} \ldots p_{j_l}$. Згідно до правила включення-виключення, серед

чисел, що не перевищують m, існує рівно

$$\sum_{j=1}^{k} \frac{m}{p_j} - \sum_{j_1 \neq j_2} \frac{m}{p_{j_1} p_{j_2}} + \sum_{j_1, j_2, j_3 \text{ різні}} \frac{m}{p_{j_1} p_{j_2} p_{j_3}} - \cdots + (-1)^k \frac{m}{p_1 \ldots p_k} \tag{11}$$

таких чисел, які діляться на хоча б одне з $p_1, \ldots, p_k$. Індукцією за k нескладно довести, ⑳ що цей вираз дорівнює

$$m \left(1 - \left(1 - \frac{1}{p_1}\right) \ldots \left(1 - \frac{1}{p_k}\right)\right). \tag{12}$$

Звідси випливає, що чисел, менших за m, та взаємно простих з m існує рівно

$$m \left(1 - \frac{1}{p_1}\right) \ldots \left(1 - \frac{1}{p_k}\right),$$

що є еквівалентним (10). □

Властивість 6. *Нехай m та n є взаємно простими, тобто $(m, n) = 1$. Тоді*

$$\phi(mn) = \phi(m)\,\phi(n). \tag{13}$$

Зауваження 2. Рівність (13) не є вірною для довільних m та n. Наприклад, при $m = n = p$, де p — просте число, маємо за властивістю 1

$$\phi\left(p^2\right) = p^2 - p \neq (p-1)(p-1) = \phi(p)\,\phi(p).$$

Доведення властивості 6. Нехай $m = p_1^{i_1} \dots p_k^{i_k}$ та $n = q_1^{j_1} \dots q_k^{j_l}$ — це канонічні розклади чисел m та n в добуток простих дільників. Оскільки m та n є взаємно простими, то серед $p_1, \dots, p_k, q_1, \dots, q_l$ немає однакових чисел. ㉑ Тому з властивості (10) випливає, що

$$\begin{aligned}\phi\left(p_1^{i_1} \dots p_k^{i_k} q_1^{j_1} \dots q_k^{j_l}\right) &= p_1^{i_1} \dots p_k^{i_k} q_1^{j_1} \dots q_k^{j_l} \\ &\quad \times \left(1 - \frac{1}{p_1}\right) \dots \left(1 - \frac{1}{p_k}\right) \\ &\quad \times \left(1 - \frac{1}{q_1}\right) \dots \left(1 - \frac{1}{q_l}\right) \\ &= \phi\left(p_1^{i_1} \dots p_k^{i_k}\right) \phi\left(q_1^{j_1} \dots q_k^{j_l}\right). \qquad \square\end{aligned}$$

Означення 2. Функція f, для якої $f(mn) = f(m)f(n)$ при $(m, n) = 1$, називається *мультиплікативною.*

Згідно до властивості 6 функція Ойлера є мультаплікативною.

4. Теорема Ойлера

Ми розглянемо один з результатів Ойлера про функцію $\phi(\cdot)$, який має багаточисельні застосування у криптографії.

Теорема 2 (*Л. Ойлер*). *Якщо* $(a, m) = 1$, *то*

$$a^{\phi(m)} \equiv 1 \pmod{m}. \tag{14}$$

Доведення. Нехай $x_1, \dots, x_{\phi(m)}$ — різні натуральні числа, що не перевищують m та є взаємно простими з m. Розглянемо всі можливі добутки вигляду $x_i a$ для i від 1 до

$\phi(m)$. Оскільки a є взаємно простим з m та x_i є взаємно простим з m, то й $x_i a$ також є взаємно простим з m, тобто $x_i a \equiv x_j \pmod{m}$ для деякого $1 \leq j \leq \phi(m)$.

Зауважимо, що всі залишки від ділення чисел $x_i a$, $1 \leq i \leq \phi(m)$, на m є різними. Дійсно, якщо це не так, то існують такі $i_1 \neq i_2$, що $1 \leq i_1, i_2 \leq \phi(m)$ та

$$x_{i_1} a \equiv x_{i_2} a \pmod{m}$$

або

$$(x_{i_1} - x_{i_2})a \equiv 0 \pmod{m}.$$

Оскільки a є взаємно простим з m, то остання рівність є рівносильною тому, що

$$x_{i_1} - x_{i_2} \equiv 0 \pmod{m}$$

або

$$x_{i_1} \equiv x_{i_2} \pmod{m} \quad \Longleftrightarrow \quad x_{i_1} = x_{i_2}.$$

Це протирічить припущенню про те, що числа $x_1, \ldots, x_{\phi(m)}$ є різними натуральними числами. Тому всі числа x_j у конгруенціях $x_i a \equiv x_j \pmod{m}$, $i = 1, 2, \ldots, \phi(m)$, є різними.

Перемножимо тепер всі конгруенції $x_i a \equiv x_j \pmod{m}$. Отримуємо

$$x_1 \ldots x_{\phi(m)} a^{\phi(m)} \equiv x_1 \ldots x_{\phi(m)} \pmod{m}$$

або

$$x_1 \ldots x_{\phi(m)}(a^{\phi(m)} - 1) \equiv 0 \pmod{m}.$$

Оскільки число $x_1 \ldots x_{\phi(m)}$ є взаємно простим з m, то остання конгруенція є равносильною тому, що

$$a^{\phi(m)} - 1 \equiv 0 \pmod{m}$$

або $a^{\phi(m)} \equiv 1 \pmod{m}$. $\square$

4.1. Обчислення оберненого за модулем. Теорему Ойлера можна використати для обчислення оберненого числа $a^{-1} \pmod{n}$, якщо $(a, n) = 1$. Дійсно з (14) випливає, що $a^{\phi(n)-1} \cdot a \equiv 1 \pmod{n}$, тобто

$$a^{-1} = a^{\phi(n)-1} \pmod{n}. \tag{15}$$

Таким чином за допомогою функції Ойлера можна обчислювати числа, обернені за модулем.

Приклад 5. На підставі прикладу 4 маємо $\phi(33) = 20$. Тому (всі рівності у наступному рядку треба розуміти за модулем 33)

$$2^{-1} = 2^{19} = 2^{10} \cdot 2^9 = 1024 \cdot 512 = 1 \cdot 17 \equiv 17 \pmod{33}.$$

4.2. Мала теорема Ферма. Ще одним важливим для криптографії результатом є наступний наслідок теореми 2.

Теорема 3 (*мала теорема Ферма*)**.** *Якщо p є простим числом, то*

$$a^{p-1} \equiv 1 \pmod{p} \tag{16}$$

для будь-якого a, яке не ділиться на p.

Теорема 3 випливає з (14) та (5). ㉒

5. Таблиця перших значень функції Ойлера

Нижче наведено значення функції Ойлера $\phi(n)$ для $n = 1, 2, \ldots, 99$.

Таблиця 1. Таблиця значень функції $\phi(n)$

	0	**1**	**2**	**3**	**4**	**5**	**6**	**7**	**8**	**9**
0+		1	1	2	2	4	2	6	4	6
10+	4	10	4	12	6	8	8	16	6	18
20+	8	12	10	22	8	20	12	18	12	28
30+	8	30	16	20	16	24	12	36	18	24
40+	16	40	12	42	20	24	22	46	16	42
50+	20	32	24	52	18	40	24	36	28	58
60+	16	60	30	36	32	48	20	66	32	44
70+	24	70	24	72	36	40	36	60	24	78
80+	32	54	40	82	24	64	42	56	40	88
90+	24	72	44	60	46	72	32	96	42	60

Цю таблицю можна використати для для обчислення значень $\phi(n)$ для багатьох інших n, якщо використати властивість мультиплікативності. Наприклад,

$$\phi(100) = \phi(25 \cdot 4) = \phi(25) \cdot \phi(4) = 20 \cdot 4 = 80.$$

6. Контрольні питання

1. Пояснити чому параметри a та n повинні бути взаємно простими, щоб шифр $L_{a,b}$ був взаємно однозначним? (стор. 114).

2. Довести, що дешифрування $L_{a,b}$ шифру дійсно здійснюється за формулою (2). (стор. 114).

3. Чому другий параметр у формулі (2) можна записати у вигляді $n - b \cdot a^{-1} \pmod{n}$? (стор. 114).

4. Пояснити чому існує 33 шифрів Цезаря та 20 однозначних мультиплікативних шифрів для українського алфавіту? (стор. 115).

5. Чому існує 660 лінійних шифрів для українського алфавіту? (стор. 115).

6. Впевнитись, що за умов теореми, накладених на b_1, b_2, з конгруенції (4) при $m = 0$ випливає, що $b_1 = b_2$. (стор. 116).

7. Перевірити, що з конгруенції (4) при $m = 1$ випливає $a_1 = a_2$. (стор. 116).

8. Перевірити, що серед чисел, що не перевищують 26, тільки 1, 3, 5, 7, 9, 11, 15, 17, 19, 21, 23, 25 є взаємно простими з 26. (стор. 116).

9. Пояснити чому $\phi(n) \leq n - 1$? (стор. 117).

10. Чому $\phi(n) = n - 1$, якщо n є простим числом? (стор. 117).

11. Довести, що тільки числа вигляду $p \cdot j$, $j \in \mathbf{N}$, не є взаємно простими з p^k. (стор. 117).

12. Чому існує рівно p^{k-1} чисел, які є меншими за p^k та які мають спільний дільник з p, більший за 1? (стор. 117).

13. Впевнитись, що серед чисел, що не перевищують pq, тільки ті числа не є взаємно простими з pq, які діляться або на p, або на q. (стор. 117).

14. Перевірити, що $\phi(pq) = pq - p - q + 1$. (стор. 117).

15. Чому в прикладі 4 обрано числа 33 та 26? (стор. 117).

16. Довести, що рівно $p^{i-1}q^j$ чисел, менших за p^iq^j, діляться на p. (стор. 118).

17. Довести методом включення–виключення, що $\phi\left(p^iq^j\right) = p^iq^j - p^{i-1}q^j - p^iq^{j-1} + p^{i-1}q^{j-1}$. (стор. 118).

18. Чому властивість 3 можна записати у вигляді (8)? (стор. 118).

19. Перевірити, що властивість 5 при $k = 2$ є рівносильною (8). (стор. 120).

20. Роз'язати задачу 5. (стор. 121).

21. Показати, що якщо $m = p_1^{i_1} \dots p_k^{i_k}$ та $n = q_1^{j_1} \dots q_k^{j_l}$ є взаємно простими, то серед серед $p_1, \dots, p_k, q_1, \dots, q_l$ немає однакових чисел. (стор. 121).

22. Довести, що теорема 3 випливає з (14) та (5). (стор. 124).

7. Задачі для самостійної роботи

Задача 1. *За допомогою лінійного шифра з параметрами* $a = 23$, $b = 7$ *зашифрувати повідомлення* `СЕКРЕТ`. *Чи можна вживати параметр* $a = 21$ *для* $L_{a,b}$ *шифру*?

Задача 2. *За допомогою лінійного шифра з параметрами* $a = 23$, $b = 7$ *зашифрувати повідомлення* SECRET, *використовуючи латинський алфавіт. Чи можна вживати параметр* $a = 21$ *для* $L_{a,b}$ *шифру?*

Задача 3. *Результатом застосування лінійного шифра з параметрами* $a = 23$, $b = 7$ *отримано фразу* ЄЩХБФШАЕ. *Знайти текст, який було зашифровано.*

Задача 4. *Результатом застосування лінійного шифра з параметрами* $a = 23$, $b = 7$ *до фрази англійською отримано* TJBYREJ. *Знайти текст, який було зашифровано.*

Задача 5. *Довести, що* (12) *випливає з* (11).

Задача 6. *Проаналізувати таблицю* 1 *й висловити гіпотезу стосовно парності функції* $\phi(n)$. *Довести цю гіпотезу.*

Задача 7. *Показати, що* $\phi(5186) = \phi(5187) = \phi(5188)$.

Задача 8. *Показати, що для кожного натурального* n *виконується властивість*

$$\phi(2n) = \begin{cases} \phi(n), & \text{якщо } n \text{ непарне,} \\ 2\phi(n), & \text{якщо } n \text{ парне.} \end{cases}$$

Задача 9. *Знайти остачу від ділення* 7^{1020} *на* 15.

Задача 10. *Знайти остачу від ділення* 79^{1776} *на* 24.

Задача 11. *Визначити останню цифру числа* 17^{6666}.

Задача 12. *Розв'язати рівняння* $\phi(x) = x/3$.

Задача 13. *Розв'язати рівняння* $\phi(2x) = \phi(3x)$.

Задача 14. *Розв'язати рівняння* $\phi(x) = 2$.

Задача 15. *Довести, що* $\phi\left(n^2\right) = n\phi(n)$.

Задача 16. *Нехай* $m \mid n$. *Довести, що* $\phi(mn) = m\phi(n)$.

Задача 17. *Нехай* $d = (m, n)$. *Довести, що*

$$\phi(mn) = \phi(m)\,\phi(n)\,\frac{d}{\phi(d)}.$$

Задача 18. *Нехай* $d = (m, n)$, *а* $K = [m, n]$. *Довести, що*

$$\phi(m)\,\phi(n) = K\phi(d).$$

Задача 19. *Для* $n = 7, 10, 12, 17$ *підрахувати*

$$\sum_{d|n} \phi(d). \tag{17}$$

На основі обчислень висунути гіпотезу стосовно значення цієї суми у загальному випадку.

Задача 20. *Довести, що сума* (17) *дорівнює* n *для будь-якого* n. *Цей результат отримав Ф. Гаус.*

Задача 21. *Для* $n = 7, 10, 12, 17$ *підрахувати*

$$\sum_{d|n} (-1)^{n/d} \phi(d). \tag{18}$$

На основі обчислень висунути гіпотезу стосовно значення цієї суми у загальному випадку.

Задача 22. *Позначимо через* T_n *суму* (18). *Довести, що*

$$T_n = \begin{cases} -n, & n \text{ є непарним}, \\ 0, & n \text{ є парним}. \end{cases}$$

Задача 23. *Нехай* p *є простим числом.*

(a) *Знайти* $\phi(1) + \phi(p)$.

(b) *Нехай* $\alpha > 1$ *є натуральним числом. Знайти суму*

$$\phi(1) + \phi(p) + \cdots + \phi(p^{\alpha}).$$

Задача 24. *Нехай* $(a,b)=1$. *Розглянемо таблицю*

$$\begin{array}{ccccc} 1 & 2 & 3 & \dots & b \\ b+1 & b+2 & b+3 & \dots & 2b \\ \vdots & \vdots & \vdots & \dots & \vdots \\ (a-1)b+1 & (a-1)b+2 & (a-1)b+3 & \dots & ab. \end{array}$$

У яких стовпчиках цієї таблиці знаходяться числа, які є взаємно простими з числом b? *Скільки у кожному з цих стовпчиків чисел, які є взаємно простими з* a? *Доведіть мультиплікативність функції Ойлера на підставі відповідей на попередні два питання.*

Задача 25. *Відомо, що* $(m,n)>1$. *Яке з чисел є більшим:* $\phi(mn)$ *чи* $\phi(m)\,\phi(n)$?

Задача 26. *Коло розділено* n *точками на* n *рівних частин. Скільки існує різних замкнених ламаних з* n *рівних ланцюгів з вершинами у цих точках*?

Задача 27. *Чи існує степінь трійки, яка закінчується на 0001?*

Задача 28. *З використанням функції* $\phi(n)$ *знайти правило, за яким утворено початок послідовності* $1,2,2,4,4,4,6,8,6,\dots$.

Задача 29. *Скільки існує правильних нескоротних дробів зі знаменником 150*?

Задача 30. *Знайти кількість натуральних чисел* n, *які не перевищують 615 та мають властивість* $(n,615)=15$.

Задача 31. *Чи існує границя* $\phi(n)/n$ *при* $n\to\infty$? *Довести, що*

$$\liminf_{n\to\infty}\frac{\phi(n)}{n}=0, \qquad \limsup_{n\to\infty}\frac{\phi(n)}{n}=1.$$

Задача 32. *Нехай* $0<\delta<1$. *Довести, що*

$$\lim_{n\to\infty}\frac{\phi(n)}{n^{1-\delta}}=\infty.$$

Задача 33. *Нехай f — мультиплікативна функція. Довести, що якщо*

$$\lim_{p^m \to \infty} f(p^m) = 0$$

(тут p — просте число), то $f(n) \to 0$ при $n \to \infty$.

8. БІОГРАФІЇ

Ойлер, *Леонард* (1707–1783), швейцарський математик, вважається найвидатнішим математиком 18-го століття, а, можливо, навіть усіх часів. Вплив Ойлера на математику описує висловлювання "*Читайте Ойлера, читайте Ойлера, він є вчителем усіх нас*", яке приписується Пьєру Лапласу (також великому математику з Франції).

Леонард Ойлер

Першу наукову роботу Ойлер написав у віці 19 років. Ця робота не отримала премії на конкурсі Паризької академії в 1727 році, але, в інші роки й за інші роботи, його було нагороджено нею 72 рази. Загалом ним опубліковано більше 700 книг та статей. Половину свого творчого життя (у 1727–1741 та 1766–1783 роках) провів у Російській імперії, а іншу половину (у 1741–1766 роках) — у Прусії. Повне зібрання трудів Ойлера публікується з 1911 року Швейцарською академією наук: до цього часу вийшло 76 томів, загальна кількість має скласти 85 томів.

Досягнення Ойлера добре відомі в математичному аналізі, де він довів до досконалості використання степеневих рядів, наприклад

$$e^x = \sum_{n=0}^{\infty} \frac{x^n}{n!}.$$

Саме число e носить ім'я Ойлера. У комплексному аналізу відомою є формула Ойлера: $e^{ix} = \cos(x) + i\sin(x)$, з якої випливає тотожність

Ойлера: $e^{i\pi}+1=0$. Останню називають "*найчудовішою математичною формулою*". Загально відомою є інша математична константа γ, яку називають константою Ойлера–Маскероні:

$$\gamma=\lim_{n\to\infty}\left[\sum_{k=1}^{n}\frac{1}{k}-\ln(n)\right].$$

Ойлер також довів формулу $V-E+F=2$, що пов'язує число вершин, ребер і граней опуклого багатогранника, а отже, і планарних графів (для планарних графів $V-E+F=1$). Цю формулу він отримав при розв'язанні задачі про сім мостів у м. Кенігсберг.

Леонард Ойлер зробив значний внесок у розвиток механіки, де його ім'я носять *рівняння* руху ідеальної рідини, та *кути*, якими описується обертання твердого тіла. Основні рівняння лагранжевої механіки часто називають рівняннями Ойлера–Лагранжа.

П. Л. Чебишов (див. [Чебишов], стор. 311) писав: "*Ойлером було покладено початок всіх досліджень, які тепер складають загальну теорію чисел*". Багато ранніх робіт Ойлера з теорії чисел базувалось на роботах П'єра Ферма (див. [Ферма], стор. 30). Ойлер опрацював деякі ідеї Ферма, і спростував деякі з його припущень. Він спростував гіпотезу Ферма про те, що всі числа виду $F_n=2^{2^n}+1$ є простими; виявилося, що F_5 ділиться на 641. Дав одне з розв'язань задачі про чотири куби.* Довів, що число Мерсенна $2^{31}-1=2,147,483,647$ є простим; протягом майже ста років (до 1867 року) воно залишалося найбільшим відомим простим числом.

Ойлер створив основу теорії порівнянь і квадратичних лишків, вказавши для останніх критерій існування. Ойлер ввів поняття первісного кореня і висунув гіпотезу, що для будь-якого простого числа p існує первісний корінь за модулем p; довести це він не зумів, пізніше теорему довели Лежандр (див. [Лежандр], стор. 309) і Гаусс (див. [Гаусс], стор. 287). Велике значення в теорії мала інша гіпотеза Ойлера про квадратичний закон взаємності також доведена пізніше Гауссом. Ойлер довів Велику теорему Ферма для $n=3$ і $n=4$, створив повну теорію неперервних дробів, досліджував різні класи діофантових рівнянь.

*Полягає у розвязанні рівняння $x^3+y^3+z^3=w^3$ у натуральних числах.