2, 3, 5, 7, 11, 13, 17, 19, 23, ...

Number Theory

$n \in \mathbb{N}$

$\Downarrow$

$n = p_1^{\alpha_1} \cdots p_k^{\alpha_k}$

$\Downarrow$

$\varphi(n) = n\left(1-\frac{1}{p_1}\right)\cdots\left(1-\frac{1}{p_k}\right)$

中國剩餘定理 : $\begin{cases} x \equiv a_1 \pmod{n_1} \\ \vdots \\ x \equiv a_k \pmod{n_k} \end{cases}$

$\gcd(n_i, n_j) = 1 \Rightarrow \exists! x \pmod{n_1 \cdots n_k}$

$$1 + \cfrac{1}{1 + \cfrac{1}{1 + \cfrac{1}{1 + \ddots}}} = \frac{1+\sqrt{5}}{2}$$

$$\left(\frac{p}{q}\right)\left(\frac{q}{p}\right) = (-1)^{\frac{p-1}{2}\cdot\frac{q-1}{2}}$$

$ax + by = c$

$x^2 - dy^2 = 1$

$n \in \{1, 2, 4, p^k, 2p^k\}_{k \in \mathbb{N}}$

smallest

Yes

$\exists r : r^{\varphi(n)} \equiv 1 \pmod{n}$

$\{\pm 5, \ldots \pm 5^{2m-2}\}$

NO

$2^m, m > 3$

Yes

Зміст

1 Основи теорії чисел

1.1 Подільність

Definition 1.1.1 Задані числа $a, b \in \mathbb{Z}$, де $a \neq 0$.
Кажуть, що число a **ділить число** b, якщо

$$\exists c \in \mathbb{Z} : b = ac$$

Позначення: $a \mid b$.
Інколи кажуть, що b **ділиться націло на** a, позначають за $b \vdots a$.

Example 1.1.2 Зокрема $2 \mid 6$, тому що $6 = 2 \cdot 3$.

Remark 1.1.3 $a \mid 0$, де a – будь-яке ненульове число. Справді, $0 = 0 \cdot a$.

Remark 1.1.4 Кожне число $b \neq 0$ має скінченну кількість дільників.
Дійсно, візьмімо якийсь дільник a числа b, тобто $a \mid b$, то звідси $b = ac$, а тому $|b| = |a||c| \implies |b| \geq |a|$. Остання нерівність і підтверджує слова.

Proposition 1.1.5 Задані числа $a, b, c \in \mathbb{N}$. Тоді:
1) $a \mid a$;
2) $a \mid b, b \mid a \implies a = b$;
3) $b \mid a, c \mid b \implies c \mid a$.
Тобто ділення формує відношення нестрогого порядку.

Proof.
Маємо таке доведення:

1) $a = 1 \cdot a \implies a \mid a$.

2) Маємо $a \mid b, b \mid a$. За означенням, існують такі числа $x, y \in \mathbb{N}$, для яких $b = ax$, $a = by$. Тоді $a = axy \implies xy = 1$. Єдиний варіант – це одночасно $x = y = 1$. Підставляючи отримані значення, маємо $a = b$.

3) $b \mid a \implies a = bx$. $c \mid b \implies b = yc \implies a = bx = xy \cdot c \implies c \mid a$.

Відношення порядку доведено. ■

Example 1.1.6 Довести, що різниця послідовних кубів ніколи не ділиться на 2.
Різниця сусідніх кубів $(a+1)^3 - a^3 = 3a^2 + 3a + 1 = 3a(a+1) + 1$. Зауважимо, що $2 \mid a(a+1)$, і дійсно:
якщо $a = 2k, k \in \mathbb{Z}$, то отримаємо $2 \mid 2k(2k+1)$;
якщо $a = 2k+1, k \in \mathbb{Z}$, то отримаємо $2 \mid (2k+1)(2k+2)$.
Отже, $a(a+1) = 2x$, тоді звідси $3a(a+1) = 2 \cdot (3x) = 2u$. Тобто $(a+1)^3 - a^3 = 2u + 1$, а значить $2 \nmid (a+1)^3 - a^3$.

Lemma 1.1.7 Ділення з остачею
Для довільних $a, b \in \mathbb{Z}$, де число $a > 0$, існують єдині $q, r \in \mathbb{Z}$, для яких $b = qa + r$, де r задовольняє нерівності $0 \leq r < a$.
Число r називають **остачею** від ділення b числом a.

Proof.
I. *Існування.*
Розглянемо множину $S = \{b - qa : q \in \mathbb{Z}\} \cap \mathbb{Z}_{\geq 0}$. Ясно, що вона непорожня, оскільки там лежить число в залежності від числа b:
або $b = b - 0 \cdot a$, якщо $b \geq 0$;
або $b - b \cdot a = b(1 - a)$, якщо $b < 0$.
Також ця множина обмежена знизу, оскільки кожне число – невід'ємне. Значить, існує $\min S$. Цей мінімум позначимо за число r, яке шукали. Отже, $r \geq 0$, а також $\exists q \in \mathbb{Z} : r = b - qa$. Залшилося показати, що $r < a$.
!Якщо припустити, що $r \geq a$, то тоді $r - a \geq 0$, а число
$r - a = b - qa - a = b - (q + 1)a \overset{q+1=q^*}{=} b - q^*a$.
Таким чином, $r - a \in S$. Але ми знаємо, що r – мінімальне число цієї множини та при цьому $r - a < r$. Суперечність!

II. *Єдиність.*
!Припустімо, що окрім q, r, для яких $b = qa + r$, існує ще одна інша пара q', r', для яких $b = q'a + r'$. Ми тут вважаємо, що $r' < r$, для іншого випадку аналогічно. Тоді
$qa + r = q'a + r' \implies a(q' - q) = r - r'$.
Із цієї рівності випливає, що $a \mid (r - r')$. Але ми водночас маємо, що $0 < r - r' < r < a$, тоді єдиний варіант під час ділення – це випадок $r - r' = 0 \implies r = r'$. Тоді вже звідси $q' = q$. Суперечність! ■

Example 1.1.8 От уже $4 \nmid 14$, але за попередньою лемою, $4 = 3 \cdot 4 + 2$, де число 2 – остача.

Corollary 1.1.9 Для довільних $a, b \in \mathbb{Z}$, де число $a \neq 0$, існують єдині $q, r \in \mathbb{Z}$, для яких $b = qa + r$, де число $0 \leq r < |a|$.
Вказівка: розглянути випадок $a > 0$, а при $a < 0$ звести до першого випадку.

Оскільки тут ще буде теорія чисел з абстрактної точки зору, я вимушений залишити таку лему.

Lemma 1.1.10 Для довільних $a, b \in \mathbb{Z}$, де число $a \neq 0$, існують єдині $q, r \in \mathbb{Z}$, для яких $b = qa + r$, де число $-\frac{1}{2}|a| < r \leq \frac{1}{2}|a|$.

Proof.
Маємо $b = q'a + r'$, де $0 \leq r' < |a|$.
Якщо $0 \leq r' < \dfrac{|a|}{2}$, то тоді $r = r'$ та $q = q'$.
Якщо $\dfrac{|a|}{2} \leq r' < |a|$, то тоді $r = r' - |a|$ та $q = q' + \operatorname{sgn} a$.
У обох випадках ми знайшли r, q єдиним чином, для яких $b = qa + r$.
Причому в цьому випадку $\dfrac{-|a|}{2} < r \leq \dfrac{|a|}{2}$. ■

1.2 Найбільший спільний дільник

Definition 1.2.1 Задані числа $a, b \in \mathbb{Z} \setminus \{0\}$.
Найбільшим спільним дільником чисел a, b назвемо таке число:

$$\gcd(a, b) = \max\{c \in \mathbb{N} : c \mid a, c \mid b\}$$

Альтернативні позначення: НСД(a, b) або (a, b).
Останнє позначення частіше можна зустріти в сучасних книгах.

Example 1.2.2 Зокрема $\gcd(6, 20) = 2$.

Definition 1.2.3 Задані числа $a, b \in \mathbb{Z} \setminus \{0\}$.
Числа a, b називаються **взаємно простими**, якщо

$$\gcd(a, b) = 1$$

Example 1.2.4 Маємо $\gcd(3, 5) = 1$, тобто $3, 5$ – взаємно прості.

Remark 1.2.5 Можна визначити НСД для чисел $a_1, \ldots, a_n \in \mathbb{Z} \setminus \{0\}$ аналогічним чином:

$$\gcd(a_1, \ldots, a_n) = \max\{c \in \mathbb{Z} : c \mid a_i, i = \overline{1, n}\}$$

Також аналогічно визначається взаємна простота цих чисел:

$$\gcd(a_1, \ldots, a_n) = 1$$

Example 1.2.6 До прикладу, $\gcd(49, 35, 28, 2023) = 7$.
Також $\gcd(11, 13, 21) = 1$, тобто вони взаємно прості.

Proposition 1.2.7 Задані числа $a, b \in \mathbb{Z} \setminus \{0\}$. Тоді існують $x, y \in \mathbb{Z}$, для яких $\gcd(a, b) = x \cdot a + y \cdot b$.
Тобто НСД a, b можна розкласти як лінійну комбінацію чисел a та b.

Proof.
Розглянемо множину $S = \{xa + yb : x, y \in \mathbb{Z}\} \cap \mathbb{N}$. Вона непорожня, бо:
при $a > 0, b > 0$ можна взяти $x = a, y = b$;
при $a < 0, b > 0$ можна взяти $x = -a, y = b$;
при $a < 0, b < 0$ можна взяти $x = -a, y = -b$;
при $a > 0, b < 0$ можна взяти $x = a, y = -b$.
Також обмежена знизу, оскільки всі числа – додатні. Тому існує $\min S$, цей мінімум позначимо за c. Тоді $\exists x_0, y_0 \in \mathbb{Z} : c = ax_0 + by_0$.
А тепер покажемо, що $c = \gcd(a, b)$.
Поділимо a, c з остачею. Маємо $a = cq + r$, де число $0 \leq r < c$. Водночас $c = x_0a + y_0b$. Тоді
$r = a - cq = a - (x_0a + y_0b)q = (1 - x_0q) \cdot a - qy_0 \cdot b$.
!Якщо припустити $r \neq 0$, то маємо $r \in S$, але тоді звідси $r \geq c$. Тобто варіант $r \neq 0$ не канає!
Значить, $r = 0$, а тому звідси $a = cq \implies a \mid c$.
Поділимо b, c з остачею. Абсолютно аналогічно доводиться, що $b \mid c$.
Таким чином, c буде вже спільним дільником. Покажемо, що цей дільник – справді найбільший.
Візьмемо інший спільний дільник d чисел a, b, тобто $d \mid a$ та $d \mid b$. Тому $a = ud$, $b = vd$. А нам вже відомо, що $c = ax_0 + by_0$, тоді
$c = udx_0 + vdy_0 = (ux_0 + vy_0)d$,
а ця рівність каже про те, що $d \mid c$, а звідси $d \leq c$. Тобто кожний інший спільний дільник a, b менший за c.
А тому c – НСД, тобто $c = \gcd(a, b)$. ■

Corollary 1.2.8 Задані числа $a, b \in \mathbb{Z} \setminus \{0\}$. Припустімо, що d - якийсь спільний дільник чисел a, b. Тоді $d \mid \gcd(a, b)$.

Proof.
За щойно доведеним твердженням, $\gcd(a, b) = xa + yb$ для $x, y \in \mathbb{Z}$.
Маємо $d \mid a, d \mid b \implies d \mid xa + yb = \gcd(a, b)$. ■

Corollary 1.2.9 Задані числа $a, b \in \mathbb{Z} \setminus \{0\}$ та число $d = \gcd(a, b)$.
Тоді $\gcd(a_1, b_1) = 1$, де числа a_1, b_1 взялись від того факту, що
$a = da_1$ та $b = db_1$ – означення подільності.
Простіше кажучи, $\gcd\left(\frac{a}{d}, \frac{b}{d}\right) = 1$.

Proof.
За **Prp. 1.2.7**, $\gcd(a_1, b_1) = a_1x + b_1y$. Помножимо на d – отримаємо:
$d \gcd(a_1, b_1) = d(a_1x + b_1y) = (da_1) \cdot x + (db_1) \cdot y = ax + by = \gcd(a, b) = d$.
Отже, $\gcd(a_1, b_1) = 1$. ■

Example 1.2.10 Маємо $\gcd(a,b) = 1$ та $\gcd(a,c) = 1$. Довести, що $\gcd(a,bc) = 1$ (доволі важливий приклад).
!Припустімо, що $\gcd(a,bc) = d$, причому $d \neq 1$. За означенням, $d \mid a$ та $d \mid bc$. Але за **Prp. 1.2.7**, ми маємо:
$\gcd(a,b) = 1 = ax + by \implies c = cax + cby$.
Із цієї рівності випливає, що $d \mid c$, але тоді звідси d – спільний дільник чисел a, c. Тож отримаємо $d \mid \gcd(a,c) = 1 \implies d = 1$. Суперечність!
Аналогічними міркуваннями, розписавши $\gcd(a,c) = 1$, ми можемо отримати $d \mid b$, що так само дає суперечність $d = 1$.

1.3 Алгоритм Евкліда

Задані числа $a, b \in \mathbb{Z} \setminus \{0\}$, де число $a > 0$. Мета: знайти $\gcd(a,b)$.

Lemma 1.3.1 $\gcd(a,b) = \gcd(b, b-a)$.

Proof.
Зробимо позначення: $d_1 = \gcd(a,b)$ та $d_2 = \gcd(b, b-a)$.
Маємо $d_1 \mid a, d_1 \mid b$. Тоді звідси $d_1 \mid b - a$. Отже, d_1 – спільний дільник чисел $b, b-a$. Тоді $d_1 \mid d_2$.
Маємо $d_2 \mid b, d_2 \mid b-a$. Тоді звідси $d_2 \mid a = b-(b-a)$. Отже, d_2 – спільний дільник чисел a, b. Тоді $d_2 \mid d_1$.
Остаточно, за антисиметричністю, $d_1 = d_2$. ■

Corollary 1.3.2 $\gcd(a,b) = \gcd(b, b - xa)$, де $x \in \mathbb{Z}$.

Theorem 1.3.3 Алгоритм Евкліда
Задані числа $a, b \in \mathbb{N}$ та припустімо $b > a$. Ми послідовно використаємо ділення за остачею таким чином:

$$
\begin{aligned}
&b = aq_1 + r_1 && 0 < r_1 < a \\
&a = r_1q_2 + r_2 && 0 < r_2 < r_1 \\
&r_1 = r_2q_3 + r_3 && 0 < r_3 < r_2 \\
&\vdots \\
&r_{k-2} = r_{k-1}q_k + r_k && 0 < r_k < r_{k-1} \\
&r_{k-1} = r_kq_k.
\end{aligned}
$$

Тоді $\gcd(a,b) = r_k$ – остання ненульова остача.

Proof.
Спочатку з'ясуємо, чому кількість разів ділення за остачею – скінченна.
Маємо остачу r_1. Якщо $r_1 = 0$, то стоп. Інакше $0 < r_1 < a$.
Далі маємо остачу r_2. Якщо $r_2 = 0$, то стоп. Інакше $0 < r_2 < r_1$.
$\vdots$
В силу строгої нерівності, рано чи пізно буде $r_k = 0$.

Маємо $\gcd(b,a) \overset{\text{Crl. 1.3.2}}{=} \gcd(a, b-aq_1) = \gcd(a, r_1)$. Позначимо ще $a = r_0$. Тоді отримаємо $\gcd(b,a) = \gcd(r_0, r_1)$.
Далі припустимо, що $\gcd(a,b) = \gcd(r_n, r_{n+1})$. Доведемо звідси, що $\gcd(a,b) = \gcd(r_{n+1}, r_{n+2})$.
Дійсно, $\gcd(r_n, r_{n+1}) \overset{\text{Crl. 1.3.2}}{=} \gcd(r_{n+1}, r_n - r_{n+1}q_n) = \gcd(r_{n+1}, r_{n+2})$.
Тобто за МІ, $\gcd(b,a) = \gcd(r_n, r_{n+1})$. А тому звідси випливає, що $\gcd(b,a) = \gcd(r_k, r_{k-1}) = r_k$. ■

Example 1.3.4 Знайти $\gcd(392, 693)$.
$693 = 392 \cdot 1 + 301$
$392 = 301 \cdot 1 + 91$
$301 = 91 \cdot 3 + 28$
$91 = 28 \cdot 3 + 7$
$28 = 7 \cdot 4$.
А число 7 – остання ненульова остача. Тоді за алгоритмом Евкліда, $\gcd(392, 693) = 7$.

Example 1.3.5 Маючи той факт, що $\gcd(392, 693) = 7$ та рівняння з алгоритму Евкліда, ми можемо записати $\gcd(392, 693)$ як лінійну комбінацію цих двох чисел. Це ще називають розширеним алгоритмом Евкліда. Починаючи з першого рівняння, ми будемо виражати остачі. Кожна з остач буде в подальшому записана як лінійна комбінація $392, 693$ ось так:
$301 = 693 \cdot 1 - 392 \cdot 1$
$91 = 392 \cdot 1 - 301 \cdot 1 = 392 \cdot 1 - (693 \cdot 1 - 392 \cdot 1) \cdot 1 = 2 \cdot 392 - 1 \cdot 693$.
$28 = 301 \cdot 1 - 91 \cdot 3 = (639 \cdot 1 - 392 \cdot 1) \cdot 1 - (2 \cdot 392 - 1 \cdot 693) \cdot 3 = 4 \cdot 693 - 7 \cdot 392$.
$7 = 91 \cdot 1 - 28 \cdot 3 = (2 \cdot 392 - 1 \cdot 693) \cdot 1 - (4 \cdot 693 - 7 \cdot 392) \cdot 3 = 23 \cdot 392 - 13 \cdot 693$.
Таким чином, $7 = \gcd(392, 693) = 23 \cdot 392 - 13 \cdot 693$.

1.4 Лінійні діофантові рівняння

Розглянемо рівняння такого вигляду:

$$ax + by = c,$$

де $x, y \in \mathbb{Z}$ – невідомі; $a, b, c \in \mathbb{Z}$, причому $a, b \neq 0$. Мета: знайти роз'язок в цілих числах.

Для цього розглянемо два випадки:
I. $\gcd(a,b) \nmid c$. Тоді розв'язків нема.

!Припустімо, що $x_0, y_0 \in \mathbb{Z}$ - деякий розв'язок рівняння $ax_0 + by_0 = c$. Відомо, що $\gcd(a,b) \mid a$ та $\gcd(a,b) \mid b$, а тому звідси $\gcd(a,b) \mid ax_0 + by_0 = c$. Суперечність!

II. $\gcd(a,b) \mid c$.
Оскільки всі числа a, b, c діляться націло на $\gcd(a,b)$, то можна обидві частини поділити на це число – отримаємо:
$a_1 x + b_1 y = c_1$,
причому тут $\gcd(a_1, b_1) = 1$. Але $\gcd(a_1, b_1) = a_1 x + b_1 y = 1$ для деяких $x, y \in \mathbb{Z}$. Помножимо на число c_1 - отримаємо:
$a_1(c_1 x) + b_1(c_1 y) = c_1$
А потім ще на $\gcd(a,b)$ – отримаємо:
$a_1 x_0 + b_1 y_0 = c$.
Тобто знайшли деякий розв'язок (x_0, y_0), для яких спрацьовує рівняння.

Припустимо, що (x_1, y_1) – якийсь інший розв'язок рівняння. Тоді
$a(x_1 - x_0) + b(y_1 - y_0) = 0$.
Поділимо на $\gcd(a,b)$, буде
$a_1(x_1 - x_0) + b_1(y_1 - y_0) = 0 \implies a_1(x_1 - x_0) = b_1(y_0 - y_1)$.
Числа a_1, b_1 - взаємно прості. Тому для рівності треба вимагати, щоб $b_1 \mid (x_1 - x_0)$. Звідси $x_1 - x_0 = mb_1$ для $m \in \mathbb{Z}$. Тоді звідси $y_0 - y_1 = ma_1$.
Тобто
$\begin{cases} x_1 = x_0 + mb_1 \\ y_1 = y_0 - ma_1 \end{cases}$, де $m \in \mathbb{Z}$ – ще один розв'язок.
Підсумуємо:

Theorem 1.4.1 Рівняння $ax + by = c$, де $a, b, c \in \mathbb{Z}$, має розв'язок $\iff \gcd(a,b) \mid c$. Причому якщо (x_0, y_0) – деякий розв'язок, то
$\begin{cases} x_1 = x_0 + mb_1 \\ y_1 = y_0 - ma_1 \end{cases}$, $m \in \mathbb{Z}$ - інші розв'язки. $b_1 = \dfrac{b}{\gcd(a,b)}, a_1 = \dfrac{a}{\gcd(a,b)}$.

Єдине питання полягає в тому, а як на практичному рівні знайти (x_0, y_0), щоб врешті-решт знайти інші розв'язки. Для цього треба використовувати алгоритм Евкліда.

Example 1.4.2 Розв'язати рівняння $392x + 693y = 14$.
За прикладом **Ex. 1.3.4**, $\gcd(392, 693) = 7 \mid 14$. Тобто рівняння розв'язок точно має. Але з прикладу **Ex. 1.3.5**, ми отримали розклад $\gcd(392, 693)$ на лінійну комбінацію таким чином:
$392 \cdot 23 + 693 \cdot (-13) = 7$.
Залишилось помножити на число 2 - отримаємо:

$392 \cdot 46 + 693 \cdot (-26) = 14$.
Таким чином, маємо $(x_0, y_0) = (46, -26)$. А тому загальний розв'язок такий:
$$\begin{cases} x = 46 + 99m \\ y = -26 - 56m \end{cases},$$
де числа $56, 99$ взялись після того, як кожне з чисел $392, 693$ поділили на їхній $\gcd(392, 693)$.

1.5 Найменше спільне кратне

Definition 1.5.1 Задані числа $a, b \in \mathbb{Z} \setminus \{0\}$.
Найменшим спільним кратним чисел a, b назвемо таке число:

$$\operatorname{lcm}(a, b) = \min\{c \in \mathbb{N} : a \mid c, b \mid c\}$$

Альтернативні позначення: $\text{НСК}(a, b)$ або $[a, b]$.

Remark 1.5.2 Можна визначити НСК для чисел $a_1, \ldots, a_n \in \mathbb{Z} \setminus \{0\}$ аналогічним чином:

$$\operatorname{lcm}(a_1, \ldots, a_n) = \min\{c \in \mathbb{Z} : a_i \mid c, i = \overline{1, n}\}$$

Theorem 1.5.3 Задані $a, b \in \mathbb{N}$. Тоді $\gcd(a, b) \cdot \operatorname{lcm}(a, b) = ab$.

Proof.
Позначимо $d = \gcd(a, b)$. Звідси $a = dr$ та $b = ds$ для деяких $r, s \in \mathbb{N}$.
Позначимо $m = \dfrac{ab}{d}$, ми хочемо показати, що $m = \operatorname{lcm}(a, b)$.
$$m = \frac{ab}{d} = \frac{drb}{d} = rb \implies b \mid m$$
$$m = \frac{ab}{d} = \frac{ads}{d} = sa \implies a \mid m.$$
Отже, m – спільне кратне чисел a, b. Покажемо, що найменше.
Нехай c – інше спільне кратне чисел a, b. Тобто $c = au, c = bv$ для деяких $u, v \in \mathbb{N}$. Ми знаємо, що $d = ax + by$ для деяких $x, y \in \mathbb{Z}$. Звідси випливає, що
$$\frac{c}{m} = \frac{cd}{ab} = \frac{c}{ab}(ax + by) = \frac{cx}{b} + \frac{cy}{a} = vx + uy.$$
$$\implies c = m(vx + uy) \implies m \mid c.$$
І так для кожного іншого спільного кратного. Тобто фактично ми довели, що $m = \operatorname{lcm}(a, b)$. Повертаючи все на місце, маємо
$$\operatorname{lcm}(a, b) = \frac{ab}{\gcd(a, b)}.$$ ■

Example 1.5.4 Зокрема, із **Ex. 1.3.4**, маємо, що
$\operatorname{lcm}(392, 693) = \dfrac{392 \cdot 693}{\gcd(392, 693)} = \dfrac{392 \cdot 693}{7} = 38808.$

Proposition 1.5.5 Задані числа $a, b \in \mathbb{Z} \setminus \{0\}$. Припустімо, що l – якесь спільне кратне чисел a, b. Тоді $\operatorname{lcm}(a, b) \mid k$.

Proof.
Маємо $k = q \operatorname{lcm}(a, b) + r$, де остача $0 \leq r < \operatorname{lcm}(a, b)$. Виразимо остачу: $r = k - q \operatorname{lcm}(a, b)$.
Із цієї рівності зауважимо, що $a \mid r$, $b \mid r$, тобто r – спільне кратне чисел a, b, а значить, $r \geq \operatorname{lcm}(a, b)$. Тому необхідно вимагати $r = 0$. Отримаємо $k = q \operatorname{lcm}(a, b) \implies \operatorname{lcm}(a, b) \mid k$. ■

1.6 Прості числа

Definition 1.6.1 Число $p > 1$ називається **простим**, якщо

лише $1, p$ – дільники числа p.

В інашкому випадку таке число називають **складеним**.

Example 1.6.2 Числа $2, 3, 5, 7$ - прості.
Число 8 – складене, бо окрім дільників $1, 8$ ще має дільник 2.

Proposition 1.6.3 Задано p – просте. Відомо, що $p \mid ab$. Тоді або $p \mid a$, або $p \mid b$.

Proof.
Якщо $p \mid a$, то автоматично закінчили доведення.
Якщо $p \nmid a$, тоді маємо $\gcd(a, p) = 1$, але ми знаємо, що $\gcd(a, p) = ax + py = 1$ для якихось $x, y \in \mathbb{Z}$. Помножимо на b – отримаємо
$abx + pby = b$.
Оскільки $p \mid ab$, то звідси $ab = kp$ при $k \in \mathbb{Z}$. Звідси
$kpx + pby = p(kx + py) = b \implies p \mid b$.
Отже, принаймні одне з чисел a, b зобов'язано ділитись націло на p. ■

Corollary 1.6.4 Задано p – просте. Відомо, що $p \mid a_1 \dots a_m$. Тоді $p \mid a_j$ для деякого $1 \leq j \leq m$.
Доведення можна провести за МІ за кількістю чисел a_i.

Theorem 1.6.5 Основна теорема арифметики
Будь-яке число $n > 1$ має єдиний розклад на добуток простих чисел з точністю до їхніх перестановок.

Proof.
Доведення проведемо за МІ за числом $n \in \mathbb{N}$.
База індукції (їх буде аж три для розуміння теореми):
$n = 2$ – нічого цікавого, розклад уже є.
$n = 3$ – нічого цікавого, розклад уже є.
$n = 6 = 3 \cdot 2 = 2 \cdot 3$ – інших пар нема (це можна ручками перебрати).
Припущення індукції: для чисел $1 < k < n$ ця теорема виконується.
Крок індукції: доведемо теорему для числа n. Спочатку покажемо, що взагалі-то можна розкласти.

I. *Існування.*
Випадок n – просте число – закінчили доведення.
Випадок n – складене число, тоді має знайтись інший дільник $1 < a < n$, для якого $n = ab$. За припущенням МІ, оскільки $1 < a < n, 1 < b < n$, ми можемо їх розкласти на добуток простих чисел. Тобто
$a = s_1 \dots s_m$
$b = t_1 \dots t_l$.
Тому $n = s_1 \dots s_m t_1 \dots t_l$ – всі ці числа прості.

II. *Єдиність.*
!Припустімо, що n розкладається двома різними способами:
$n = p_1 \dots p_r$;
$n = q_1 \dots q_s$.
Зауважимо, що $p_r \mid n \implies p_r \mid q_1 \dots q_s \implies \exists 1 \le j \le s : p_r \mid q_j$.
Оскільки вони обидва прості, то звідси $p_r = q_j$.
Розглянемо інше число $n' = p_1 \dots p_{r-1} = q_1 \dots q_{j-1} q_{j+1} \dots q_s$.
Маємо $n' < n$, а тому можна використати припущення МІ. А воно каже, що ці два вирази рівні з точністю до перестановки. Помножимо обидві частини на p_r, а справа $p_r = q_j$ (відмічено червоним) – тоді
$p_1 \dots p_{r-1} p_r = q_1 \dots q_j \dots q_s = n$
Отримали єдиний розклад з точністю до перестановок. Суперечність!
Висновок: фіксоване число n можна розкласти на добуток простих чисел, причому єдиним чином з точністю до перестановки.
МІ доведено. ■

Remark 1.6.6 Із цього випливає канонічний розклад числа n:
$n = p_1^{r_1} p_2^{r_2} \dots p_k^{r_k}$,
де $p_1, p_2, \dots, p_k$ – різні прості числа та $r_1, r_2, \dots, r_k > 0$.

Corollary 1.6.7 Припустімо, що два числа a, b розклалися на прості числа таким чином:
$a = p_1^{r_1} \dots p_k^{r_k}$
$b = p_1^{s_1} \dots p_k^{s_k}$

Тоді $\gcd(a,b) = p_1^{\min\{r_1,s_1\}} \dots p_k^{\min\{r_k,s_k\}}$.
Тоді $\operatorname{lcm}(a,b) = p_1^{\max\{r_1,s_1\}} \dots p_k^{\max\{r_k,s_k\}}$.

Example 1.6.8 Маємо два числа:
$3444 = 2^2 \cdot 3 \cdot 7 \cdot 41$
$244496 = 2^4 \cdot 7 \cdot 37 \cdot 59$.
Тоді $\gcd(3444, 244496) = 2^2 \cdot 7 = 28$.
Тоді $\operatorname{lcm}(3444, 244496) = 2^4 \cdot 3 \cdot 7 \cdot 37 \cdot 41 \cdot 59 = 30073008$.

Theorem 1.6.9 Задано число $n = p_1^{k_1} \dots p_k^{k_r}$. Тоді
$d \mid n \iff d = p_1^{a_1} \dots p_r^{a_r}$, причому $0 \le d_i \le k_i$.

Proof.
При $d = 1$ маємо $a_i = 0, i = \overline{1,r}$, а при $d = n$ маємо $a_i = k_i, i = \overline{1,r}$.
Тому розглянемо випадок $d > 1$, тож тоді $n = dd'$. За основною теоремою арифметики, $d = q_1 \dots q_s$, а також $d' = t_1 \dots t_u$. Всі ці числа прості.
Отже, $p_1^{k_1} \dots p_k^{k_r} = q_1 \dots q_s t_1 \dots t_u$.
Оскільки розклад єдиний, то тоді кожний q_j має один з p_i. А тому звідси ми й отримаємо, що
$d = p_1^{a_1} \dots p_r^{a_r}$.
І навпаки, якщо $d = p_1^{a_1} \dots p_r^{a_r}$, то тоді маємо:
$n = p_1^{k_1} \dots p_k^{k_r} = (p_1^{a_1} \dots p_r^{a_r}) p_1^{k_1 - a_1} \dots p_r^{k_r - a_r}$.
Отже, $d \mid n$. ■

1.7 Решето Ератосфена

Proposition 1.7.1 Задано $n \in \mathbb{N}$ - складене число. Тоді існує просте число $p \le \sqrt{n}$, для якого $p \mid n$.

Proof.
Оскільки n - складене, то тоді $n = bc$ при $1 < b < n$, $1 < c < n$. Не втрачаючи загальності, ми скажемо, що $b \le c$. Звідси отримаємо $b^2 \le bc = n$, а тому $b \le \sqrt{n}$.
Оскільки $b > 1$, то за основною теоремою арифметики, існує просте число $p \mid b$, де $p \le b \le \sqrt{n}$. Але водночас $b \mid n$, а тому звідси $p \mid n$. ■

Remark 1.7.2 Завдяки цього твердження, можна трохи ефективніше з'ясувати, чи буде якесь число простим.

Example 1.7.3 Розглянемо число $n = 509$. Зауважимо: $22 < \sqrt{n} < 23$, тож ми запишемо прості числа, що не більші за 22. Тобто
$p \in \{2, 3, 5, 7, 11, 13, 17, 19\}$. Можна пересвідчитись, що жодне з цих простих чисел $p \nmid n$. Таким чином, за твердженням вище, $n = 509$ - просте.

Решето Ератосфена

Маємо $n \in \mathbb{N}$ – деяке число. Мета: знайти всі прості числа від 1 до n.
Запишемо всі числа від 1 до n в природному порядку. Закреслимо 1, бо це явно не просте число.
Беремо число 2, а далі закреслюємо всі числа, що кратні 2.
Беремо число 3 (наступне просте число, бо не був закресленим на попередній ітерації). Далі закреслюємо всі числа, що кратні 3.
Беремо число 5. Далі закреслюємо всі числа, що кратні 5.
$\vdots$
Можна цей алгоритм продовжувати до кінця, але можна зупинити заздалегідь. Зауважимо, що коли $p > \sqrt{n}$, то нема що закреслювати.
Дійсно, маємо число $p > \sqrt{n}$. Зараз розглядатимемо числа формату $pa, a > 1$ – це ті самі числа, що кратні p. Зауважимо, що $n \neq pa$ для всіх $a > 1$, тобто або $pa < n$, або $pa > n$. Другий випадок ми ігноруємо, бо таких чисел просто нема в таблиці. У першому випадку я стверджую, що число pa вже було закреслено в решето.
Нехай a – просте, тоді зауважимо, що $a < \sqrt{n}$ (в силу нерівності $\sqrt{n}a < pa < n$). Число a уже брало участь вище, тобто ми вже закреслювали числа, що кратні a. Тому число pa уже закреслено в цьому випадку.
Нехай a – складене, то за твердженням вище, там знайдеться просте число $\tilde{p} < \sqrt{a} < \sqrt{pa} < \sqrt{n}$, для якого $\tilde{p} \mid a$. Тобто звідси $pa = \tilde{p} \cdot pq$. Оскільки $\tilde{p} < \sqrt{n}$, то за алгоритмом вище, ми вже закреслили всі числа, що кратні $\tilde{p}$.

Отже, всі числа, що не закреслилися, – прості.

Example 1.7.4 Знайдемо всі прості числа від 1 до 50.
Запишемо всі числа від 1 до 50. Число 1 можна закреслити.

~~1~~	2	3	4	5	6	7	8	9	10
11	12	13	14	15	16	17	18	19	20
21	22	23	24	25	26	27	28	29	30
31	32	33	34	35	36	37	38	39	40
41	42	43	44	45	46	47	48	49	50

Наступне незакреслене число – це 2, просте, його залишаємо. Закреслимо всі числа, що кратні 2.

~~1~~	2	3	~~4~~	5	~~6~~	7	~~8~~	9	~~10~~
11	~~12~~	13	~~14~~	15	~~16~~	17	~~18~~	19	~~20~~
21	~~22~~	23	~~24~~	25	~~26~~	27	~~28~~	29	~~30~~
31	~~32~~	33	~~34~~	35	~~36~~	37	~~38~~	39	~~40~~
41	~~42~~	43	~~44~~	45	~~46~~	47	~~48~~	49	~~50~~

Наступне незакреслене число – це 3, просте, його залишаємо. Закреслимо всі числа, що кратні 3.

~~1~~	2	3	~~4~~	5	~~6~~	7	~~8~~	~~9~~	~~10~~
11	~~12~~	13	~~14~~	~~15~~	~~16~~	17	~~18~~	19	~~20~~
~~21~~	~~22~~	23	~~24~~	25	~~26~~	~~27~~	~~28~~	29	~~30~~
31	~~32~~	~~33~~	~~34~~	35	~~36~~	37	~~38~~	~~39~~	~~40~~
41	~~42~~	43	~~44~~	~~45~~	~~46~~	47	~~48~~	49	~~50~~

Наступне незакреслене число – це 5, просте, його залишаємо. Закреслимо всі числа, що кратні 5.

~~1~~	2	3	~~4~~	5	~~6~~	7	~~8~~	~~9~~	~~10~~
11	~~12~~	13	~~14~~	~~15~~	~~16~~	17	~~18~~	19	~~20~~
~~21~~	~~22~~	23	~~24~~	~~25~~	~~26~~	~~27~~	~~28~~	29	~~30~~
31	~~32~~	~~33~~	~~34~~	~~35~~	~~36~~	37	~~38~~	~~39~~	~~40~~
41	~~42~~	43	~~44~~	~~45~~	~~46~~	47	~~48~~	49	~~50~~

Наступне незакреслене число – це 7, просте, його залишаємо. Закреслимо всі числа, що кратні 7.

~~1~~	2	3	~~4~~	5	~~6~~	7	~~8~~	~~9~~	~~10~~
11	~~12~~	13	~~14~~	~~15~~	~~16~~	17	~~18~~	19	~~20~~
~~21~~	~~22~~	23	~~24~~	~~25~~	~~26~~	~~27~~	~~28~~	29	~~30~~
31	~~32~~	~~33~~	~~34~~	~~35~~	~~36~~	37	~~38~~	~~39~~	~~40~~
41	~~42~~	43	~~44~~	~~45~~	~~46~~	47	~~48~~	~~49~~	~~50~~

Далі закінчуємо, бо наступне число $11 \not\leq \sqrt{n}$. Всі решта незакреслені числа будуть простими.

1.8 Твердження, пов'язані з простими числами

Theorem 1.8.1 Кількість простих чисел – нескінченна.

Proof.
!Припустімо, що всього k простих чисел, тобто маємо набір $p_1, p_2, \ldots, p_k$.

Побудуємо число $n = p_1 \dots p_k + 1$. Розглянемо два сценарії:
1) n – просте – автоматична суперечність нашому припущенню.
2) n – складене, тому $p_j \mid n$, бо ми можемо n розкласти як добуток простих чисел. Тоді звідси $p_j \mid n - (p_1 \dots p_k) = 1$. Тоді $p_j = 1$, але то вже непросте число. Суперечність! ■

Proposition 1.8.2 Для кожного $n \in \mathbb{N}$ можна знайти набір n послідовних складених чисел.

Proof.
Для фіксованого $n \in \mathbb{N}$ будуються такі числа:
$(n+1)! + 2$
$(n+1)! + 3$
$\vdots$
$(n+1)! + (n+1)$.
Всього n штук, послідовні та складені. ■

Proposition 1.8.3 Не існує неконстантного многочлена $f \in \mathbb{Z}[x]$, для якого $\forall n \in \mathbb{N} : f(n)$ - просте.

Proof.

!Припустимо, що такий многочлен $f \in \mathbb{Z}[x]$ існує. Маємо $f(x) = \sum_{k=1}^{N} a_k x^k$ - неконстантний многочлен.
$f(1) \overset{\text{позн.}}{=} p$ - просте.
Розглянемо ось таку різницю:

$$f(1+mp) - f(1) = \sum_{k=1}^{N} a_k (1+mp)^k - \sum_{k=1}^{N} a_k = \sum_{k=1}^{N} a_k \left[(1+mp)^k - 1\right] =$$

$$= \sum_{k=1}^{N} a_k \left[\sum_{l=1}^{k} C_k^l m^l p^l\right] = \sum_{k=1}^{N} \sum_{l=1}^{k} C_k^l a_k m^l p^l.$$

Винесемо з-під суми число p за дужки а суму позначимо за якесь число M. Тоді
$f(1+mp) - f(1) = pM \implies f(1+mp) = f(1) + pM = p + pM = p(M+1)$
Оскільки $f(1+mp)$ - просте число, то нам треба вимагати, щоб $M = 0$.
В результаті $\forall m \in \mathbb{N} : f(1+mp) = p$.
А далі розглянемо многочлен $g(x) = f(x) - p$, де $g \in \mathbb{Z}[x]$. Отримаємо, що $g(1+mp) = 0, \forall m \in \mathbb{N}$. Многочлен степені k може мати до k коренів рівняння, а тому єдиний можливий варіант - це $g(x) \equiv 0$, звідси $f(x) \equiv p$ - константний многочлен. Суперечність! ■

Theorem 1.8.4 Нехай число $2^n + 1$ – просте. Тоді або $n = 0$, або $n = 2^k$.
Можна сказати ще так: якщо $2^n + 1$ - просте, то єдиний простий множник числа n - це 2.

Remark 1.8.5 Число $F_k = 2^{2^k} + 1$ ще називають **числами Ферма**. Спочатку вважалось, що всі ці числа прості, але, виявилось, $F_5 = 2^{2^5} + 1$ ділиться націло на 641.

Proof.
Доведемо еквівалентну теорему: якщо n має не лише множник 2, то тоді $2^n + 1$ – складене.
Нехай $p \mid n$ та p - непарне просте (взяли з розкладу числа n). Тоді $n = mp$, а звідси $2^n + 1 = (2^m)^p + 1$. Для непарних степеней маємо формулу:
$x^p + 1 = (x + 1)(x^{p-1} - x^{p-2} + x^{p-3} - \cdots + 1)$
$\Longrightarrow (2^m)^p + 1 = (2^m + 1)(2^{m(p-1)} - 2^{m(p-2)} + \cdots + 1)$.
Таким чином, число $2^n + 1$ - складене. ■

Theorem 1.8.6 Нехай число $2^n - 1$ – просте. Тоді n – також просте.

Remark 1.8.7 Число $M_n = 2^n - 1$ ще називають **числами Мерсенна**.

Proof.
Припустимо, що n – складене, тобто $n = ab$. Тоді $2^n - 1 = (2^a)^b - 1$. Схожий крок доведення, але тут застосуємо формулу:
$x^n - 1 = (x - 1)(x^{n-1} + x^{n-2} + \cdots + 1)$
$\Longrightarrow 2^n - 1 = (2^a - 1)(2^{a(b-1)} + 2^{a(b-2)} + \cdots + 1)$.
Отже, звідси $2^n - 1$ – також складене. ■

Remark 1.8.8 Якщо n – просте, то не обов'язково $2^n - 1$ – просте число. Зокрема 11 - просте число, але $2^{11} - 1 = 2047 = 23 \cdot 89$ - тобто складене.

2 Модульна арифметика

2.1 Основи конгруенцій

Definition 2.1.1 Задані числа $a, b \in \mathbb{Z}$ та число $n \in \mathbb{N}$.
Числа a, b називаються **рівними за модулем** n, якщо

під час ділення a та b на n отримаємо однакові остачі.

Позначення: $a \equiv b \pmod{n}$ або часто в інших книгах $a \equiv b \ (n)$.
Часто ще кажуть **конгруентні за модулем** n.

Example 2.1.2 Зокрема $14 \equiv 5 \pmod{3}$, тому що
14 ділимо на 3 – дає остачу 2. 5 ділимо на 3 – дає остачу 2.

Proposition 2.1.3 $a \equiv b \pmod{n} \iff n \mid a - b$.

Proof.
$\boxed{\Rightarrow}$ Дано: $a \equiv b \pmod{n}$, тоді звідси $a = nq_1 + r$ та $b = nq_2 + r$. За означенням, у них однакові остачі. Отже,
$n \mid a - b = nq_1 + r - nq_2 - r = n(q_1 - q_2)$.

$\boxed{\Leftarrow}$ Дано: $n \mid a - b$. Припустимо, що $a = nq_1 + r_1$ та $b = nq_2 + r_2$, тобто в них дві різні остачі, тоді:
$a - b = n(q_1 - q_2) + (r_1 - r_2) \implies r_1 - r_2 = (a - b) - n(q_1 - q_2)$.
Із цієї рівності та умови $n \mid a - b$ випливає, що $r_1 - r_2 \mid n$, але оскільки $0 \le r_1 < n, 0 \le r_2 < n$, то звідси $-n < r_1 - r_2 < n$. Єдиний варіант, який нас влаштовує, – це $r_1 - r_2 = 0 \implies r_1 = r_2$.
Отримали, що a, b зобов'язані мати однакову остачу при діленні на n, а тому звідси $a \equiv b \pmod{n}$. ■

Corollary 2.1.4 Операція $\equiv \pmod{n}$ утворює відношення еквівалентності на множині $\mathbb{Z}$.
Вправа: довести.

Тоді ми можемо знайти неперетинні класи еквівалентності, а потім профакторизувати множину $\mathbb{Z}$.

Example 2.1.5 Розглянемо $n = 4$, як число, на яке будемо ділити. Отримаємо такі класи еквівалентності:
$\overline{0} = \{\dots, -8, -4, 0, 4, 8, \dots\}$
$\overline{1} = \{\dots, -7, -3, 1, 5, 9, \dots\}$
$\overline{2} = \{\dots, -6, -2, 2, 6, 10, \dots\}$
$\overline{3} = \{\dots, -5, -1, 3, 7, 11, \dots\}$.
Ну а оскільки вони неперетинні, то звідси $\overline{0} \cup \overline{1} \cup \overline{2} \cup \overline{3} = \mathbb{Z}$.

Definition 2.1.6 Множина $\{a_1, \ldots, a_n\}$ називається **повною системою лишків** (mod n), якщо

$$\overline{a_1} \cup \cdots \cup \overline{a_n} = \mathbb{Z}$$

Example 2.1.7 Зокрема з попереденього прикладу, $\{0, 1, 2, 3\}$ утворюють повну систему лишків за (mod 4). Але можна взяти інші: $\{4, 6, 7, 9\}$ або $\{-2, -1, 0, 1\}$.

Proposition 2.1.8 Задані $a \equiv b \pmod{n}$ та $c \equiv d \pmod{n}$. Тоді
$a + c \equiv b + d \pmod{n}$;
$ac \equiv bc \pmod{n}$.
Вправа: довести.

Proposition 2.1.9 Нехай $a \equiv b \pmod{n}$, а також $d \mid n$. Тоді
$a \equiv b \pmod{d}$.
Вправа: довести.

Example 2.1.10 Зокрема $3 \equiv 7 \pmod{4}$, але також $2 \mid 4$, а тому звідси $3 \equiv 7 \pmod{2}$.

Proposition 2.1.11 Нехай $a \equiv b \pmod{n}$, а також $c \in \mathbb{N}$. Тоді
$ac \equiv bc \pmod{nc}$.
Вправа: довести.

Corollary 2.1.12 Нехай $a \equiv b \pmod{n}$. Тоді $a^m \equiv b^m \pmod{n}, m \in \mathbb{N}$.

Corollary 2.1.13 Задано многочлен $f \in \mathbb{Z}[x]$, а також $a \equiv b \pmod{n}$. Тоді $f(a) \equiv f(b) \pmod{n}$.

Proposition 2.1.14 Нехай $ad \equiv bd \pmod{n}$ та $\gcd(d, n) = 1$. Тоді
$a \equiv b \pmod{n}$.

Proof.
Маємо $dx + ny = 1$, а також $n \mid d(a-b) \implies n \mid dx(a-b)$.
$n \mid (1 - ny)(a - b) = (a - b) - ny(a - b) \implies n \mid a - b \implies a \equiv b \pmod{n}$. ■

Remark 2.1.15 Для ділення обох частин умова $\gcd(d, n) = 1$ є важливою. Зокрема $2 \cdot 3 \equiv 2 \cdot 18 \pmod{10}$, але в жодному разі з цього НЕ випливає, що $3 \equiv 18 \pmod{10}$.

Proposition 2.1.16 Нехай $a \equiv b \pmod{c}$ та $a \equiv b \pmod{d}$. Тоді
$a \equiv b \pmod{\operatorname{lcm}(c, d)}$.
Зворотний бік також виконується. Вправа: довести.

Proof.
Із умови маємо $c \mid a-b$ та $d \mid a-b$, тобто маємо $a-b$ – спільне кратне чисел c, d. Тоді звідси $\operatorname{lcm}(c,d) \mid a-b$, тож $a \equiv b \pmod{\operatorname{lcm}(c,d)}$. ■

Example 2.1.17 Довести, що числа вигляду $11, 111, 1111, \ldots$ не можуть бути представлені як квадрат натурального числа.
Спочатку зауважимо, що рівняння $4k+3 = x^2$ не має цілих розв'язків. Тому що якби були розв'язки, то $x^2 \equiv 3 \pmod 4$. Достатньо перевірити рівність при $x \in \{0,1,2,3\}$. Перебравши всі, отримаємо, що жодний не задовольняє.
Тобто це означає, що жодне число виду $4k+3$ не можна представити як повний квадрат. Перефразувавши, якщо $a \equiv 3 \pmod 4$, то тоді a – не повний квадрат. Зокрема
$11 \equiv 3 \pmod 4$
$111 = 100 + 11 \equiv 0 + 3 = 3 \pmod 4$
$1111 = 1000 + 111 \equiv 0 + 3 = 3 \pmod 4$
$\vdots$

2.2 Правила ділення

Маємо деяке натуральне число $n = \overline{a_m \ldots a_1 a_0}$ у вигляді цифр $a_j \in \{0,1,\ldots,9\}$, тобто це число записується так: $n = a_0 + 10a_1 + \cdots + 10^m a_m$.

Theorem 2.2.1 Маємо правила ділення на $2, 5, 4, 25, 3, 9, 11, 37, 7, 13$.
$2 \mid n \iff a_0 \in \{0,2,4,6,8\}$
$5 \mid n \iff a_0 \in \{0,5\}$
$4 \mid n \iff 4 \mid \overline{a_1 a_0}$
$25 \mid n \iff \overline{a_1 a_0} \in \{0,25,50,75\}$
$3 \mid n \iff 3 \mid (a_0 + a_1 + \cdots + a_m)$
$9 \mid n \iff 9 \mid (a_0 + a_1 + \cdots + a_m)$
$11 \mid n \iff 11 \mid (a_0 - a_1 + \cdots + (-1)^m a_m)$
$37 \mid n \iff 37 \mid (\overline{a_2 a_1 a_0} + \overline{a_5 a_4 a_3} + \ldots)$
$7 \mid n \iff 7 \mid (\overline{a_2 a_1 a_0} - \overline{a_5 a_4 a_3} + \ldots)$
$13 \mid n \iff 13 \mid (\overline{a_2 a_1 a_0} - \overline{a_5 a_4 a_3} + \ldots)$

Proof.
Покажу доведення одного з правил. Решта можна самостійно.
$\boxed{\Rightarrow}$ Дано: $3 \mid n$, тобто $n \equiv 0 \pmod 3$. Зауважимо, що оскільки $10 \equiv 1 \pmod 3$, то звідси $10^k \equiv 1^k = 1 \pmod 3$ при $k \in \mathbb{N}$. Отже,
$n = a_0 + 10a_1 + \cdots + 10^m a_m \equiv a_0 + a_1 + \cdots + a_m \equiv 0 \pmod 3$
$\implies 3 \mid a_0 + a_1 + \cdots + a_m$.

$\boxed{\Leftarrow}$ Дано: $3 \mid (a_0 + a_1 + \cdots + a_m)$, звідси

$n = a_0 + 10a_1 + \cdots + 10^m a_m \overset{10^k \equiv 1 \pmod 3}{\equiv} a_0 + a_1 + \cdots + a_m \overset{\text{дано}}{\equiv} 0 \pmod 3$.
Звідси випливає, що $3 \mid n$. ■

Вказівка для правила ділення на 37 *націло:* $10^3 \equiv 1 \pmod{37}$.

Example 2.2.2 Розкласти число $n = 35256375$ на добуток простих.
У кінці n стоїть 75, тому стовпчиком ділимо на 25 – отримаємо:
$n = 5^2 \cdot 1410255$.
Остання цифра другого числа – 5, тому стовпчиком ділимо на 5:
$n = 5^3 \cdot 282051$.
Маємо $2 + 8 + 2 + 0 + 5 + 1 = 18 \vdots 9$, а тому $282051 \vdots 9$ – отримаємо
$n = 5^3 \cdot 3^2 \cdot 31339$.
Маємо $3 - 1 + 3 - 3 + 9 = 11 \vdots 11$, а тому $31339 \vdots 11$ – отримаємо:
$n = 5^3 \cdot 3^2 \cdot 11 \cdot 2849$.
Знову $2 - 8 + 4 - 9 = -11 \vdots 11$ – тож звідси
$n = 5^3 \cdot 3^2 \cdot 11^2 \cdot 259$.
Нарешті, отримаємо такий розклад: $n = 3^2 \cdot 5^3 \cdot 7 \cdot 11^2 \cdot 37$.

2.3 Лінійні конгруенції

Мета: знайти розв'язки цього рівняння:

$$ax \equiv b \pmod n$$

Нехай x_0 - розв'язок, тобто $ax_0 \equiv b \pmod n$, тоді $n \mid ax_0 - b$
$\implies ax_0 - kn = b$. Тоді звідси випливає, що $\gcd(a, n) \mid b$.

Нехай $d = \gcd(a, n) \mid b$ тоді рівняння $ax + ny = b$ має розв'язок відносно змінних $y_0, x_0 \in \mathbb{Z}$. І тому звідси $ax_0 = b + y_0 n \equiv b \pmod n$. Але це не єдиний такий розв'язок.

Із теорії діофантових рівнянь ми можемо отримати розв'язки вигляду:
$x = x_0 + m\frac{n}{d}, m \in \mathbb{Z}$
$k = y_0 - m\frac{n}{d}, m \in \mathbb{Z}$.
Зауважимо, що можна брати $0 \le m \le d - 1$.
Якщо $m \ge d$, то можна число записати як $m = d + r, r \ge 0$. Тоді $x = x_0 + (d + r)\frac{n}{d} = x_0 + n + r\frac{n}{d} \equiv x_0 + r\frac{n}{d}$.
Якщо $m \le 0$, то можна зробити заміну $m = -r, r \ge 0$. Тоді буде попередній сценарій, $0 \le -r \le d-1$. Але можна довести, що $x_0 + m\frac{n}{d} \equiv x_0 - r\frac{n}{d} \pmod n$.
Тепер треба переконатись, що ці розв'язки при решти $0 \le m \le d - 1$

різні за модулем. Припустімо, що $x_i \equiv x_j \pmod{n}$, тоді звідси $i\frac{n}{d} \equiv j\frac{n}{d} \pmod{n}$, тобто $(i-j)\frac{n}{d} = nl \implies d \nmid i-j \implies i \equiv j \pmod{d}$. Єдиний такий варіант - це бути $i = j$.

Підсумовуючи:

Theorem 2.3.1 $ax \equiv b \pmod{n}$ має розв'язок $\iff d = \gcd(a,n) \mid b$. Причому всього d різних за модулем розв'язків вигляду $x_p = x_0 + p \cdot \frac{n}{d}, 0 \le p \le d-1$, де x_0 – один з розв'язків.

Example 2.3.2 Розв'язати рівняння $12x \equiv 8 \pmod{20}$.
Оскільки $\gcd(12,20) = 4 \mid 8$, то розв'язок існує.
$12x_0 + 20y_0 = 4 \implies x_0 = 2$ та $y_0 = -1$ – неважко вгадати.
$12 \cdot 2 + 20 \cdot (-1) = 4$,
$12 \cdot 4 + 20 \cdot (-2) = 8$,
а тому звідси $x_0 = 4$ – перший розв'язок. Решта розв'язків генерується такою формулою:
$x_m = 4 + m\frac{20}{\gcd(12,20)} = 4 + 5m$.
Отже, маємо такі розв'язкі, що різні за модулем: $\{4, 9, 14, 19\}$.

2.4 Китайська теорема про остачі

Theorem 2.4.1 Задані числа $n_1, \ldots, n_k \in \mathbb{N}$ - попарно взаємно прості; числа $a_1, \ldots, a_k \in \mathbb{Z}$. Тоді система рівнянь

$$\begin{cases} x \equiv a_1 \pmod{n_1} \\ \vdots \\ x \equiv a_k \pmod{n_k} \end{cases}$$

має єдиний розв'язок, що рівний за $\pmod{N}$, де $N = n_1 \ldots n_k$.

Proof.
I. *Існування.*
Позначимо числа N_i - добуток чисел $n_1, \ldots, n_k$, але без n_i. Маємо $\gcd(N_i, n_i) = 1$, в силу попарно взаємної простоти. Тож $N_i x_i + n_i y_i = 1$ для деяких $x_i, y_i \in \mathbb{Z}$. Звідси $N_i x_i = 1 - n_i y_i \equiv 1 \pmod{n_i}$.
Помножимо обидві частини на a_i – отримаємо
$(N_i a_i) x_i \equiv a_i \pmod{n_i}$.
Встановимо $x = N_1 a_1 x_1 + \cdots + N_k a_k x_k$ – наш майбутній розв'язок. Зауважимо, що $N_i \equiv 0 \pmod{n_j}$ при $i \neq j$. Тоді для кожного j маємо
$x \equiv N_j a_j x_j \equiv a_j \pmod{n_j}$.

II. *Єдиність.*
!Припустимо, що маємо два різні розв'язки x, y за $\pmod N$. Тоді для кожного $j = \overline{1,k}$ маємо:
$x - y \equiv 0 \pmod{n_j} \implies n_j \mid x - y$.
Оскільки n_j попарно взаємно прості, то звідси $n_1 \dots n_k = N \mid x - y$, а тому $x \equiv y \pmod N$. Суперечність! ■

Кроки розв'язку таких систем описується на цьому прикладі:

Example 2.4.2 Розв'язати систему рівнянь $\begin{cases} x \equiv 2 \pmod 3 \\ x \equiv 3 \pmod 7 \\ x \equiv 9 \pmod{10} \end{cases}$.
Спочатку зауважимо (!), що числа $3, 7, 10$ – попарно взаємно прості між собою. Далі позначимо $N = 3 \cdot 7 \cdot 10 = 210$. Маємо такі числа:
$N_1 = 7 \cdot 10 = 70$
$N_2 = 3 \cdot 10 = 30$
$N_3 = 3 \cdot 7 = 21$.
Тепер нам треба знайти x_1, x_2, x_3 із таких рівнянь:
$70x_1 \equiv 1 \pmod 3$
$30x_2 \equiv 1 \pmod 7$
$21x_3 \equiv 1 \pmod{10}$
Розв'яжемо кожне окремо:
$70x_1 \equiv 1x_1 \equiv 1 \pmod 3 \iff x_1 = 1$.
$30x_2 \equiv 2x_2 \equiv 1 \pmod 7 \iff x_2 = 4$.
$21x_3 \equiv 1x_3 \equiv 1 \pmod{10} \iff x_3 = 1$.
Конструюємо розв'язок таким чином:
$x = 2N_1x_1 + 3N_2x_2 + 9N_3x_3 = 689$.
Можна залишити таку відповідь, але ми знаємо, що за модулем 210 розв'язок однаковий, тому краща відповідь: $x = 59$.

Example 2.4.3 Розв'язати систему рівнянь $\begin{cases} 2x \equiv 6 \pmod{14} \\ 3x \equiv 9 \pmod{15} \\ 5x \equiv 20 \pmod{60} \end{cases}$.
Ось тут не можна використовувати китайську теорему про остачі, оскільки маємо $\gcd(15, 60) \neq 1$. Тоді треба інший варіант.
Зауважимо, що $2x \equiv 6 \pmod{14} \iff \begin{cases} 2x \equiv 6 \pmod 2 \\ 2x \equiv 6 \pmod 7 \end{cases}$, просто тому що $\operatorname{lcm}(2, 7) = 14$. Перша рівність ніякої інформації не дає, бо завжди виконана.
Аналогічно $3x \equiv 9 \pmod{15} \iff \begin{cases} 3x \equiv 9 \pmod 5 \\ 3x \equiv 9 \pmod 3 \end{cases}$, а друга рівність

інформації не дає.

Аналогічно $5x \equiv 20 \pmod{60} \iff \begin{cases} 5x \equiv 20 \pmod{12} \\ 5x \equiv 20 \pmod{5} \end{cases}$, а друга рівність інформації не дає.

Отримаємо еквівалентну систему $\begin{cases} 2x \equiv 6 \pmod{7} \\ 3x \equiv 9 \pmod{5} \\ 5x \equiv 20 \pmod{12} \end{cases}$.

Тим не менш, ми досі не можемо використати китайську теорему. Нам необхідно розв'язати кожне лінійне конгруентне рівняння окремо. Я це розписувати не буду та запишу вже еквівалентну систему:

$\begin{cases} x \equiv 3 \pmod{7} \\ x \equiv 3 \pmod{5} \\ x \equiv 4 \pmod{12} \end{cases}$.

Тепер вже можна китайську теорему про остачі.

Позначимо $N = 7 \cdot 5 \cdot 12 = 420$, а також числа $N_1 = 5 \cdot 12 = 60$, $N_2 = 7 \cdot 12 = 84$, $N_3 = 7 \cdot 5 = 35$. Знайдемо x_1, x_2, x_3 із таких рівнянь:

$\begin{cases} 60x_1 \equiv 1 \pmod{7} \\ 84x_2 \equiv 1 \pmod{5} \\ 35x_3 \equiv 1 \pmod{12} \end{cases} \iff \begin{cases} x_1 = 2 \\ x_2 = 4 \\ x_3 = 11 \end{cases}$.

Маємо $x = 3N_1x_1 + 3N_2x_2 + 4N_3x_3 = 2908 \equiv 388 \pmod{420}$.

2.5 Теорема Вільсона

Lemma 2.5.1 Нехай p - просте число. Відомо, що $x^2 \equiv 1 \pmod{p}$. Тоді $x \equiv \pm 1 \pmod{p}$.

Proof.

Нехай $x^2 \equiv 1 \pmod{p}$. Тоді звідси $p \mid x^2 - 1 \implies p \mid (x-1)(x+1) \implies p \mid x-1$ або $p \mid x+1$.

Якщо $p \mid x-1$, то звідси $x \equiv 1 \pmod{p}$.

Якщо $p \mid x+1$, то звідси $x \equiv -1 \pmod{p}$. ■

Remark 2.5.2 Тут важливо, що p має бути простим.

Зокрема $5^2 \equiv 1 \pmod{12}$, але з цього не випливає, що $5 \equiv \pm 1 \pmod{12}$.

Theorem 2.5.3 Теорема Вільсона

p – просте число $\iff (p-1)! \equiv -1 \pmod{p}$.

Proof.

$\boxed{\Rightarrow}$ Дано: p – просте число.

Спочатку розглядається частинні випадки: $p = 2, p = 3$ – неважко.

Нехай $p \geq 5$ та просте. Розглянемо множину $\{2, 3, \ldots, p-2\}$. Зауважимо, що при $a \in \{2, 3, \ldots, p-2\}$ маємо $a^2 \not\equiv 1 \pmod{p}$, згідно з попередньої леми. Також зауважимо, що $\exists! b \in \{2, 3, \ldots, p-2\}$, для яких $ab \equiv 1 \pmod{p}$, в разі якщо $b \neq a$. Тому що підставте будь-яке число $a \neq b$ - і отримаєте лінійне рівняння, яке має єдиний розв'язок. І наостанок: $\{2, 3, \ldots, p-2\}$ має парну кількість елементів. Тому кожному числу завжди знайдеться єдине "обернене". Отже,
$(p-1)! = 1 \cdot 2 \cdot 3 \cdots (p-2) \cdot (p-1) = 1 \cdot (p-1) \cdot [2 \cdot 3 \cdots (p-2)] \equiv$
$\equiv 1 \cdot p - 1 \equiv -1 \pmod{p}$.

$\boxed{\Leftarrow}$ Дано: $(p-1)! \equiv -1 \pmod{p}$.
!Припустімо, що p - не просте число, тобто $n \mid p$, але $p \neq n$. Звідси випливає, що $n \in \{1, 2, 3, \ldots, p-1\}$. Але з цього випливає, що $n \mid (p-1)!$. Ми маємо $n \mid p$ та $p \mid ((p-1)! + 1)$ зверху, тобто $n \mid ((p-1)! + 1)$.
Отже, $n \mid ((p-1)! + 1 - (p-1)!) = 1$. Тобто $n = 1$. Суперечність! ■

Theorem 2.5.4 Задано p – непарне просте число.
$x^2 \equiv -1 \pmod{p}$ має розв'язок $\iff p \equiv 1 \pmod{4}$.

Proof.
$\boxed{\Rightarrow}$ Дано: $x^2 \equiv -1 \pmod{p}$ має розв'язок.
Припустімо, що $p \not\equiv 1 \pmod{4}$. Маючи той факт, що p – непарне просте, маємо $p \equiv 3 \pmod{4}$. Тоді $\dfrac{p-1}{2} = \dfrac{p-3}{2} + 1$ - непарне число.
За малою теоремою Ферма, $x^{p-1} \equiv 1 \pmod{p}$, неважко показати, що $p \nmid x$ в силу того, що $x^2 \equiv -1 \pmod{p}$. Таким чином,
$x^{p-1} = \left(x^2\right)^{\frac{p-1}{2}} \equiv (-1)^{\frac{p-1}{2}} \overset{\frac{p-1}{2}-\text{непарне}}{\equiv} -1 \pmod{p}$.
Отже, $-1 \equiv 1 \pmod{p} \implies p \mid 2$. Суперечність! Бо ми маємо справу з непарними простими числами.

$\boxed{\Leftarrow}$ Дано: $p \equiv 1 \pmod{4}$. Тоді звідси $4 \mid p-1$, а значить, число $\dfrac{p-1}{2}$ - парне число. Використовуючи теорему Вільсона, отримаємо:
$$-1 \equiv (p-1)! = \left(1 \cdot 2 \cdots \frac{p-1}{2}\right)\left(\left(\frac{p-1}{2} + 1\right) \cdots (p-2) \cdot (p-1)\right) \equiv$$
$$\equiv \left(1 \cdot 2 \cdots \frac{p-1}{2}\right)\left(-\frac{p-1}{2} \ldots (-2) \cdot (-1)\right) = \left(1 \cdot 2 \ldots \frac{p-1}{2}\right)^2.$$
Рівність вище $\pmod{p}$. Отже, $x = 1 \cdot 2 \cdots \dfrac{p-1}{2}$ задовольняє рівнянню $x^2 \equiv -1 \pmod{p}$. ■

Corollary 2.5.5 Існує нескінченна кількість простих чисел p, для яких $p \equiv 1 \pmod{4}$.

Proof.
!Припустімо, що лише скінченна кількість простих чисел задовольняє умові. Тобто $p_1, \ldots, p_k$ – такі прості, що $\equiv 1 \pmod 4$.
Побудуймо число $N = 4(p_1 \ldots p_n)^2 + 1$. Зауважимо, що $N \equiv 1 \pmod 4$. Якщо N – просте, то автоматом суперечність. Тому кажемо, що N – складене. Тобто $p \mid N \implies N \equiv 0 \pmod p \implies (2p_1 \ldots p_k)^2 \equiv -1 \pmod p$. А тому за попередньою теоремою, $p \equiv 1 \pmod 4 \implies p = p_i, i = \overline{1,k}$. Але $p_i \mid N, p_i \mid 4(p_1 \ldots p_k)^2 \implies p_i \mid N - 4(p_1 \ldots p_k)^2 = 1$. Суперечність! ■

2.6 Лема Гензеля

Theorem 2.6.1 Теорема Лагранжа
Задано функцію $f \in \mathbb{Z}[x]$ та p просте число, причому старший коефіцієнт не ділиться на p. Тоді $f(x) \equiv 0 \pmod p$ має до $\deg f(x)$ розв'язків.

Remark 2.6.2 Суттєво, щоб p був простим.
Зокрема $x^2 - 1 \equiv 0 \pmod{12}$ має аж $4 \neq \deg(x^2-1)$ розв'язки з точністю до конгруенції: $x \in \{1, 5, 7, 11\}$.

Proof.
Доведення за МІ за $\deg f(x) = n$.
База індукції: $n = 1$. Маємо многочлен $f(x) = ax + b$, де $p \nmid a$. Маємо рівняння $ax + b \equiv 0 \pmod p$, але таке ми навчились розв'язати. Маємо $\gcd(a, p) = 1 \mid b$, а тому мається розв'язок. Причому буде єдиний розв'язок.
Припущення індукції: твердження виконується для $\deg f(x) = k$.
Крок індукції: доведемо для $\deg f(x) = k + 1$.
Маємо f – многочлен, $\deg f(x) = k + 1$, старший коефіцієнт не ділиться на p. Якщо $\nexists a : f(a) \equiv 0 \pmod p$, то доведено. Тому нехай $\exists a : f(a) \equiv 0 \pmod p$. За теоремою Безу, $f(x) = (x - a)g(x) + f(a)$, причому $\deg g(x) = k$. Також важливо зауважити, що старший коефіцієнт при g не ділиться на p. Бо, припустивши зворотне, отримаємо, що старший коеф при f ділиится на p.
За припущенням МІ, $g(x) \equiv 0 \pmod p$ має до k розв'язків. Тоді $f(x) = (x - a)g(x) + f(a) \equiv (x - a)g(x) \equiv 0 \pmod p$ має до $k + 1$ розв'язків.
МІ доведено. ■

Lemma 2.6.3 Лема Гензеля
Задано функцію $f \in \mathbb{Z}[x]$, також p – просте число та $m \in \mathbb{N}$. Нехай є число $a \in \mathbb{Z}$, для якого виконуються умови:
$f(a) \equiv 0 \pmod{p^m}$;

$f'(a) \not\equiv 0 \pmod{p}$.
Тоді $\exists! t \in \{0, 1, \ldots, p-1\}$, для якого $f(a + tp^m) \equiv 0 \pmod{p^{m+1}}$.

Proof.
Позначимо $\deg f(x) = n$. В точці $x = a$ розкладемо за рядом Тейлора:
$f(x) = f(a) + \dfrac{f'(a)}{1!}(x-a) + \dfrac{f''(x)}{2!}(x-a)^2 + \cdots + \dfrac{f^{(n)}(a)}{n!}(x-a)^n.$
Підставимо сюди $x = a + tp^m$ - отримаємо:
$f(a + tp^m) = f(a) + \dfrac{f'(a)}{1!}tp^m + \cdots + \dfrac{f^{(n)}(a)}{n!}t^n p^{mn}.$
Покажемо, що $\dfrac{f^{(k)}(a)}{k!} \in \mathbb{Z}$.
Справді, якщо взяти якусь конкретну функцію $g(x) = x^r$, то для неї $\dfrac{g^{(k)}(a)}{k!} = C_r^k \in \mathbb{Z}$ (чому C_r^k ціле, буде зазначено в **Th. 3.4.6**). А довільна функція f - це лінійна комбінація x^r.
Отже, в силу $\dfrac{f^{(k)}(a)}{k!} \in \mathbb{Z}$, а значить, $f(a + tp^m) \equiv f(a) + f'(a)tp^m \pmod{p^{m+1}}$.
Тепер ми хочемо знайти таке t, щоб $f(a + tp^m) \equiv 0 \pmod{p^{m+1}}$.
Маємо $f(a) + f'(a)tp^m \equiv 0 \pmod{p^{m+1}}$. Оскільки $f(a) \equiv 0 \pmod{p^m}$, то звідси $p^m \mid f(a)$, а значить, $\dfrac{f(a)}{p^m} \in \mathbb{Z}$. Тож $\dfrac{f(a)}{p^m} + f'(a)t \equiv 0 \pmod{p}$.
Зауважимо, що це - лінійне конгруентне рівняння. Ще зауважимо, що $\gcd(f'(a), p) = 1$, оскільки $f'(a) \not\equiv 0 \pmod{p}$. Отже, дане рівняння має єдиний розв'язок t. Оскільки рівняння відносно $\pmod{p}$, то $t \in \{0, 1, \ldots, p-1\}$. ■

Proposition 2.6.4 Задано p – просте число та $m \in \mathbb{N}$. Тоді рівняння $x^{p-1} \equiv 1 \pmod{p^m}$ має рівно $p-1$ розв'язків.

Proof.
База індукції: $m = 1$, тоді маємо $x^{p-1} \equiv 1 \pmod{p}$. А це чисто мала теорема Ферма: там справді є $p-1$ розв'язків.
Припущення індкції: для деякого k твердження виконано.
Крок індукції: доведемо це для $k+1$.
Розглянемо функцію $f(x) = x^{p-1} - 1$. За МІ $f(x) \equiv 0 \pmod{p^k}$ існують рівно $p-1$ розв'язків, я їх назву $x_1, \ldots, x_{p-1}$. Отже, $f(x_i) \equiv 0 \pmod{p^k}$, а також $f'(x_i) = (p-1)x_i^{p-2} \not\equiv 0 \pmod{p^k}$ Зокрема $f'(x_i) \not\equiv 0 \pmod{p}$.
Отже, за лемою Гензеля, $\exists! t_i \in \{0, 1 \ldots, p-1\} : f(x_i + t_i p^k) \equiv 0 \pmod{p^{k+1}}$.
Звідси, в нас $p-1$ розв'язків типу $x_i + t_i p^k$ для рівняння $f(x) \equiv 0 \pmod{p^{k+1}}$.

Нехай y – ще один розв'язок, тобто
$f(y) \equiv 0 \pmod{p^{k+1}} \implies f(y) \equiv 0 \pmod{p^k}$.
За МІ, $y \equiv x_i \pmod{p^k}$. Повторюючи лему Гензеля, маємо $\exists! t : f(y + tp^k) \equiv 0 \pmod{p^{k+1}}$. Але $y + tp^k = x_i + tp^k$, а для числа x_i в нас існував єдиний t_i. Таким чином, $t = t_i$. І отримали: $y + tp^k = x_i + t_i p^k$ – розв'язок співпав з цими, що були вище.
МІ доведено. ■

Example 2.6.5 Розв'язати рівняння $x^2 + 15x + 31 \equiv 0 \pmod{125}$.
Позначимо $f(x) = x^2 + 15x + 31$. Звідси $f'(x) = 2x + 15$.

I. $\pmod 5$

$f(x) \equiv 0 \pmod 5 \iff x^2 + 1 \equiv 0 \pmod 5$. Маємо звідси $x \in \{2, 3\}$.
$f'(2) = 19 \not\equiv 0 \pmod 5$ та $f'(3) = 21 \not\equiv 0 \pmod 5$.
За лемою Гензеля, $\exists! t_1, t_2$:
$f(2 + 5t_1) \equiv 0 \pmod{25}$
$f(3 + 5t_2) \equiv 0 \pmod{25}$

Для $x = 2$ маємо $t_1 f'(2) \equiv -\dfrac{f(2)}{5} \pmod 5 \iff t_1 = 3$.

Для $x = 3$ маємо $t_2 f'(3) \equiv -\dfrac{f(3)}{5} \pmod 5 \iff t_2 = 3$.

II. $\pmod{25}$.

$f(x) \equiv 0 \pmod{25} \iff x^2 + 15x + 6 \equiv 0 \pmod{25}$. Маємо з минулого $x \in \{17, 18\}$. $f'(17) \not\equiv 0 \pmod 5$ та $f'(18) \not\equiv 0 \pmod 5$.
За лемою Гензеля, $\exists! t_1, t_2$:
$f(17 + 25t_1) \equiv 0 \pmod{125}$
$f(18 + 25t_2) \equiv 0 \pmod{125}$.

Для $x = 17$ маємо $t_1 f'(17) \equiv -\dfrac{f(17)}{25} \pmod 5 \iff t_1 = 3$.

Для $x = 18$ маємо $t_2 f'(18) \equiv -\dfrac{f(18)}{25} \pmod 5 \iff t_2 = 0$.

III. $\pmod{125}$.

$f(x) \equiv 0 \pmod{125}$ має розв'язки $x \in \{18, 92\}$.
Інших розв'язків нема, бо під час доведення леми Гензеля ми розв'язували лінійне конгруентне рівняння, що гарантувало єдиний розв'язок.

3 Арифметичні функції

Надалі ми будемо розглядати **арифметичні функції** $f\colon \mathbb{N} \to \mathbb{C}$ (хоча тут розглядатимуться частіше $\mathbb{N} \to \mathbb{N}$). Тобто це такі функції, область визначення яких – натуральні числа.

Definition 3.0.1 Арифметична функція $f\colon \mathbb{N} \to \mathbb{C}$ називається **мультиплікативною**, якщо

$$f(1) = 1$$
$$f(mn) = f(m)f(n) \text{ при } \gcd(m,n) = 1$$

Lemma 3.0.2 Задано число $n \in \mathbb{N}$, а також $f\colon \mathbb{N} \to \mathbb{N}$. Тоді
$\sum\limits_{d|n} f(d) = \sum\limits_{d|n} f\left(\frac{n}{d}\right)$.

Proof.
Маємо $d \mid n$, тоді звідси $\exists x \in \mathbb{Z} : n = xd$, а це означає, що $x \mid n$, але $x = \frac{n}{d}$. Якщо діяти навпаки, тобто $\frac{n}{d} \mid n$, то тоді миттєво $d \mid n$.
Тобто $d_1, \ldots, d_r$ – всі дільники числа $n \iff \frac{n}{d_1}, \ldots, \frac{n}{d_r}$ – всі дільники числа n.
Отже, $d_1 = \frac{n}{d_{j_1}}, \ldots, d_r = \frac{n}{d_{j_r}}$.

$$\sum_{d|n} f(d) = f(d_1) + \cdots + f(d_r) = f\left(\frac{n}{d_{j_1}}\right) + \cdots + f\left(\frac{n}{d_{j_r}}\right) \overset{\text{переставимо в природному порядку}}{=}$$
$$= f\left(\frac{n}{d_1}\right) + \cdots + f\left(\frac{n}{d_r}\right) = \sum_{d|n} f\left(\frac{n}{d}\right). \qquad \blacksquare$$

3.1 Функції τ, σ

Definition 3.1.1 Арифметична функція $\tau\colon \mathbb{N} \to \mathbb{N}$ визначає **кількість дільників** числа n, тобто інакше кажучи:

$$\tau(n) = \sum_{d|n} 1$$

Definition 3.1.2 Арифметична функція $\sigma\colon \mathbb{N} \to \mathbb{N}$ визначає **суму дільників** числа n, тобто інакше кажучи:

$$\tau(n) = \sum_{d|n} d$$

Example 3.1.3 Зокрема для числа 10 ми маємо дільники $1, 2, 5, 10$, а тому $\tau(10) = 4 \qquad \sigma(10) = 18$.

Theorem 3.1.4 Задано число $n = p_1^{k_1} \dots p_r^{r_k}$. Тоді
$\tau(n) = (k_1 + 1) \dots (k_r + 1)$
$\sigma(n) = \dfrac{p_1^{k+1} - 1}{p_1 - 1} \dots \dfrac{p_r^{k_r+1} - 1}{p_r - 1}$

Proof.
Маємо, що кожний дільник $d \mid n$ має форму $d = p_1^{a_1} \dots p_r^{a_r}$, причому $0 \le a_i \le k_i$. Із точки зору комбінаторики, у нас є $k_1 + 1$ варіантів обрати степінь a_1, …, у нас є $k_r + 1$ варіантів обрати степінь a_r. А тому всього $(k_1 + 1) \dots (k_r + 1)$ варіантів сконструювати число $p_1^{a_1} \dots p_r^{a_r}$, що є дільником. Отже, $\tau(n) = (k_1 + 1) \dots (k_r + 1)$.

А далі розглянемо ось такий вираз: $(1+p_1+\dots+p_1^{k_1}) \dots (1+p_r+\dots+p_r^{k_r})$. Якщо перемножити, то ми отримаємо суму всіх можливих дільників формату $p_1^{a_1} \dots p_r^{a_r}$, тобто суму всіх дільників числа n. Знаючи, що в кожній дужці - геометрична прогресія, отримаємо:
$\sigma(n) = (1 + p_1 + \dots + p_1^{k_1}) \dots (1 + p_r + \dots + p_r^{k_r}) =$
$= \dfrac{p_1^{k+1} - 1}{p_1 - 1} \dots \dfrac{p_r^{k_r+1} - 1}{p_r - 1}.$ ■

Remark 3.1.5 n – просте число $\iff \begin{cases} \tau(n) = 2 \\ \sigma(n) = n + 1 \end{cases}$.

Example 3.1.6 Число $180 = 2^2 \cdot 3^2 \cdot 5$, а тому звідси
$\tau(180) = (2 + 1)(2 + 1)(1 + 1) = 18$
$\sigma(180) = \dfrac{2^3 - 1}{2 - 1} \dfrac{3^3 - 1}{3 - 1} \dfrac{5^2 - 1}{5 - 1} = 546$

Theorem 3.1.7 $\displaystyle\prod_{d|n} d = n^{\frac{\tau(n)}{2}}$.

Proof.
$d \mid n \iff \dfrac{n}{d} = d' \mid n$, причому маємо $n = dd'$. Всього дільників d рівно $\tau(n)$ штук. Перемножимо ці $\tau(n)$ рівнянь:

$$n^{\tau(n)} = \prod_{d|n} d \prod_{d'|n} d' = \left(\prod_{d|n} d \right)^2.$$

Таким чином, $n^{\frac{\tau(n)}{2}} = \displaystyle\prod_{d|n} d$.

Єдине треба заспокоїтись та переконатись, що зліва завжди буде ціле число, навіть попри квадратного кореня. Маємо два випадки:
1) $\tau(n)$ – парне, тоді можна не перейматись.
2) $\tau(n)$ – непарне, тоді число n буде квадратом якогось числа. І дійсно, $\tau(n) = (k_1 + 1)\dots(k_r + 1)$ - цей вираз може бути парним тоді й тільки тоді, коли кожна дужка парна, тобто $k_i = 2s_i$. А тому $n = p_1^{k_1}\dots p_r^{r_k} = (p_1^{s_1}\dots p_1^{s_r})^2$. Отже, можна взяти квадратний корінь ліворуч. ■

Theorem 3.1.8 Функції τ, σ – мультиплікативні.

Proof.
Маємо $n = p_1^{k_1}\dots p_r^{k_r}$ та $m = q_1^{m_1}\dots q_s^{m_s}$, причому беремо так, щоб $\gcd(m,n) = 1$. Але в такому разі маємо $\gcd\left(p_i^{k_i}, q_j^{m_j}\right) = 1$. Отже, у нас буде $mn = q_1^{m_1}\dots q_s^{m_s}p_1^{k_1}\dots p_r^{k_r}$. І вони вже ніяк не перемножаться між собою. Разом отримаємо:
$\tau(mn) = (m_1 + 1)\dots(m_s + 1)(k_1 + 1)\dots(k_r + 1) = \tau(m)\tau(n)$
$$\sigma(mn) = \frac{q_1^{m_1+1} - 1}{q_1 - 1}\dots\frac{q_s^{m_s+1} - 1}{q_s - 1}\frac{p_1^{k+1} - 1}{p_1 - 1}\dots\frac{p_r^{k_r+1} - 1}{p_r - 1} = \sigma(m)\sigma(n)$$
Також ледве не забув $\tau(1) = 1$, $\sigma(1) = 1$ – тут з цим ясно. ■

Існує ще один варіант, як довести мультиплікативність цих двох функцій. Спочатку почну з леми.

Lemma 3.1.9 Задані числа m, n такі, що $\gcd(m,n) = 1$. Тоді множина дільників $d \mid mn$ складається з елементів формату d_1d_2, де $d_1 \mid m, d_2 \mid n$, $\gcd(d_1, d_2) = 1$, а також всі d_1d_2 – різні.

Proof.
Маємо $n = p_1^{k_1}\dots p_r^{k_r}$ та $m = q_1^{m_1}\dots q_s^{m_s}$, причому беремо так, щоб $\gcd(m,n) = 1$. Але в такому разі маємо $\gcd\left(p_i^{k_i}, q_j^{m_j}\right) = 1$. Отже, у нас буде $mn = q_1^{m_1}\dots q_s^{m_s}p_1^{k_1}\dots p_r^{k_r}$. І вони вже ніяк не перемножаться між собою. Знаю, що слово в слово повторюю, але хай буде.
$d \mid mn \iff d = (q_1^{a_1}\dots q_s^{a_s})\cdot(p_1^{b_1}\dots p_r^{b_r}) = d_1d_2$, де $\gcd(d_1,d_2) = 1$. ■

Theorem 3.1.10 Задано функцію f – мультиплікативна. Тоді функція $F(n) = \sum\limits_{d|n} f(n)$ – також мультиплікативна.

Proof.
$$F(mn) = \sum_{d|mn} f(d) \overset{\text{Lm. 3.1.9}}{=} \sum_{\substack{d_1|m\\ d_2|n}} f(d_1d_2) \overset{\gcd(d_1,d_2)=1}{=} \sum_{\substack{d_1|m\\ d_2|n}} f(d_1)f(d_2) =$$
$$= \sum_{d_1|m} f(d_1)\cdot\sum_{d_2|n} f(d_2) = F(m)F(n).$$ ■

Далі ми знаємо, що $f_1(n) = 1$, $f_2(n) = n$ – зрозумілим чином мультиплікативні. А тому за означенням τ, σ та отриманою теоремою, у нас будуть σ, τ мультиплікативні.

3.2 Функція φ (функція Ойлера)

Definition 3.2.1 Функцією Ойлера називають арифметичну функцію $\varphi\colon \mathbb{N} \to \mathbb{N}$, що задана таким чином:

$$\varphi(n) = \#\{m \mid 1 \leq m \leq n, \gcd(m, n) = 1\}$$

Часто ще позначають саме $\phi(n)$. Використовуватиму позначення вище.

Example 3.2.2 Наприклад, $\varphi(12) = 4$, бо взаємно прості числа з ним: $1, 5, 7, 11$ – всього 4 взаємно простих числа, що менші за 12.

Definition 3.2.3 Скороченою системою лишкків $(\mathrm{mod}\ n)$ називають множину

$$\{b_1, b_2, \ldots, b_{\varphi(n)}\} \subset \mathbb{Z},$$

для яких $\gcd(b_r, n) = 1$, а також вони всі різні $(\mathrm{mod}\ n)$. Причому їхня кількість обов'язково має бути $\varphi(n)$.

Example 3.2.4 Зокерма при $\varphi(12) = 4$ ми маємо такі скорочені системи лишків: $\{1, 5, 7, 11\}$, $\{1, -7, 7, -1\}$. Можна ще напридумати таких систем безліч.

Lemma 3.2.5 Задано $\{b_1, \ldots, b_{\varphi(n)}\}$ – скорочена система лишків. Оберемо число $a \in \mathbb{Z}$, для якого $\gcd(a, n) = 1$. Тоді $\{ab_1, \ldots, ab_{\varphi(n)}\}$ – також скорочена система лишків.

Proof.
Із того, що $\gcd(a, n) = 1, \gcd(b_i, n) = 1$ випливає $\gcd(ab_i, n) = 1$.
Зишилось показати, що $ab_i \not\equiv ab_j \ (\mathrm{mod}\ n)$ при $i \neq j$.
!Якщо припустити, що $ab_i \equiv ab_j \ (\mathrm{mod}\ n)$, то тоді оскільки $\gcd(a, n) = 1$, то звідси $b_i \equiv b_j \ (\mathrm{mod}\ n)$. Суперечність! ■

Theorem 3.2.6 Теорема Ойлера
Задані числа a, n так, що $\gcd(a, n) = 1$. Тоді $a^{\varphi(n)} \equiv 1 \ (\mathrm{mod}\ n)$.

Proof.
Нехай $\{b_1, \ldots, b_{\varphi(n)}\}$ – скорочена система лишків $(\mathrm{mod}\ n)$. За попередньою лемою, $\{ab_1, \ldots, ab_{\varphi(n)}\}$ – скорочена система лишків $(\mathrm{mod}\ n)$.

Звідси випливає таке рівняння:
$(ab_1)\dots(ab_{\varphi(n)}) \equiv b_1 \dots b_{\varphi(n)} \pmod n$.
$a^{\varphi(n)}x \equiv x \pmod n$, де число $x = b_1 \dots b_{\varphi(n)}$.
Із того, що $\gcd(b_i, n) = 1, i = \overline{1, \varphi(n)}$ випливає $\gcd(x, n) = 1$. Тому звідси $a^{\varphi(n)} \equiv 1 \pmod n$. ■

Corollary 3.2.7 мала теорема Ферма
Задано p – просте число та $a \in \mathbb{Z}$, причому $p \nmid a$. Тоді $a^{p-1} \equiv 1 \pmod p$.

Remark 3.2.8 Насправді, також існує метод доведення теореми Ойлера через інструменти з теорії груп. Можна подивитися в іншому пдфнику безпосередньо.

Example 3.2.9 Визначити останні 2 цифри числа 7^{950}. Еквівалетно кажучи, скоротити $7^{950} \pmod{100}$.
Досить трюковна задача, але зробимо ось що. Спочатку скоротимо це число двома шляхами: $\pmod 4$ та $\pmod{25}$.
Маємо $7^{950} = 7^{2\cdot 475} = 7^{\varphi(4)\cdot 475} = (7^{\varphi(4)})^{475} \overset{\text{бо } \gcd(7,4)=1}{\equiv} 1^{475} = 1 \pmod 4$.
Маємо $7^{950} = 7^{47\cdot 20+10} = 7^{10} \cdot (7^{\varphi(25)})^{47} \overset{\text{бо } \gcd(7,25)=1}{\equiv} 7^{10}1^{47} = 7^{10} = (7^2)^5 \equiv (-1)^5 = -1 \equiv 24 \pmod{25}$.
Тож ми маємо ось це:
$\begin{cases} 7^{950} \equiv 1 \pmod 4 \\ 7^{950} \equiv 24 \pmod{25} \end{cases}$. Тимчасово запишемо як $\begin{cases} x \equiv 1 \pmod 4 \\ x \equiv 24 \pmod{25} \end{cases}$ – отримали задачу на китайську теорему про остачі. Якщо її розв'язати, отримаємо $x \equiv 49 \pmod{100}$.
Отже, $7^{950} \equiv 49 \pmod{100}$. Тобто $4, 9$ – це останні 2 цифри.

Example 3.2.10 Задано p – просте число, причому $p \nmid a$. Нехай $1 \le m \le p-1$ - найменше число, для якого $a^m \equiv 1 \pmod p$. Довести, що $m \mid p-1$.
!Припустимо, що $p - 1 = mq + r$ та остача $r < m$. Тоді звідси
$1 \overset{\text{мала Ферма}}{\equiv} a^{p-1} = a^{mq+r} = (a^m)^q a^r \equiv 1^q a^r = a^r$.
Тобто $a^r \equiv 1 \pmod p$, але m – найменше таке число. Суперечність!

Theorem 3.2.11 Функція Ойлера φ – мультиплікативна.

Proof.
Ну ясно, що $\varphi(1) = 1$.
Нехай m, n – такі числа, що $\gcd(m, n) = 1$. Візьмемо якісь дві скорочені системи лишків $\pmod m$ та $\pmod n$:
$\{a_1, \dots, a_{\varphi(m)}\}$

$\{b_1, \ldots, b_{\varphi(n)}\}$
Доведемо, що $\{a_j n + b_k m \mid j = \overline{1, \varphi(m)}, k = \overline{1, \varphi(n)}\}$ – також буде скороченою системою лишків, але $\pmod{mn}$.
Зауважимо, що $\gcd(a_j n + b_k m, m) = \gcd(a_j n, m) = 1$. Остання рівність виконана, бо $\gcd(a_j, m) = 1, \gcd(n, m) = 1$.
Зауважимо, що $\gcd(a_j n + b_k m, n) = \gcd(b_k m, n) = 1$ – аналогічно.
Із двох рівностей маємо $\gcd(a_j n + b_k m, mn) = 1$ – одна умова є.
!Тепер припустимо, що маємо $a_j n + b_k m \equiv a_r n + b_s m \pmod{mn}$ при $(j, k) \neq (r, s)$. Тоді $(a_j - a_r)n \equiv (b_s - b_k)m \pmod{mn}$.
Звідси випливає, що $a_j - a_r \equiv 0 \pmod{m}$ та $b_s - b_k \equiv 0 \pmod{n}$ в силу $\gcd(m, n) = 1$. В обох випадках суперечність!
Отже, $a_j n + b_k m \not\equiv a_r n + b_s m \pmod{mn}$ - друга умова є. І тільки зараз можна казати, що кількість елементів в множині $\varphi(m)\varphi(n)$ штук.
Тобто принаймні для $\varphi(mn)$ ми вже маємо $\varphi(m)\varphi(n)$ елементів множини. А чи може бути більше? Хотілось б довести, що інших елементів даної множини не буде. Тобто припустивши, що є деяке число c, для якого $\gcd(c, mn) = 1$, ми хочемо показати, що $c \equiv a_j n + b_k m$.
За умовою, $mx + ny = 1$ для деяких $x, y \in \mathbb{Z}$. Із цієї рівності маємо $\gcd(m, y) = 1, \gcd(n, x) = 1$ (можна від супротивного показати).
А тепер доведемо, що $\gcd(cy, m) = 1, \gcd(cx, n) = 1$.
!Припустимо, що є просте число p, для якого $p \mid cy, p \mid m$. Тоді $p \mid c, p \mid m \implies p \mid c, p \mid mn$ (суперечність), або $p \mid y, p \mid m$ (суперечність)!
Аналогічним чином доводиться друге.
Із $\gcd(cy, m) = 1$ випливає $cy \equiv a_j \pmod{m}$ (дивись систему лишків).
Із $\gcd(cx, n) = 1$ випливає $cx \equiv b_k \pmod{n}$ (дивись систему лишків).
Тож $c = c(mx + ny) \equiv c(ny) \equiv a_j n \equiv a_j n + b_k m \pmod{m}$.
Аналогічно показується $c \equiv a_j n + b_k m \pmod{n}$.
Тоже $c \equiv a_j n + b_k m \pmod{mn}$. Тобто c співпав з одним серед $\varphi(m)\varphi(n)$ елементів систем лишків. Тобто кількість елементів $\varphi(m)\varphi(n) + 1$ штук бути не може.
Отже, $\varphi(nm) = \varphi(m)\varphi(n)$. ■

Lemma 3.2.12 Задано p – просте. Тоді $\varphi(p^r) = p^r - p^{r-1}$.

Proof.
$\varphi(p^r) = \#\{\{1, 2, 3, \ldots, p^r\} \setminus \{\text{всі числа кратні } p\}\} \boxed{=}$
$\{\text{всі числа кратні } p\} = \{p, 2p, 3p, \ldots, p^{r-1}p\}$.
$\boxed{=} p^r - p^{r-1}$. ■

Corollary 3.2.13 Маємо число $n = p_1^{r_1} \ldots p_k^{r_k}$. Тоді
$$\varphi(n) = n\left(1 - \frac{1}{p_1}\right)\ldots\left(1 - \frac{1}{p_k}\right).$$
Вправа: довести.

Example 3.2.14 Зокрема обчислимо $\varphi(100)$.
Маємо $100 = 5^2 \cdot 2$, тоді звідси $\varphi(100) = 100\left(1 - \frac{1}{2}\right)\left(1 - \frac{1}{5}\right) = 40$.

Example 3.2.15 Визначити всі числа $n \in \mathbb{N}$, для яких $\varphi(n) = 8$.
Маємо $\varphi(n) = n\left(1 - \frac{1}{p_1}\right)\ldots\left(1 - \frac{1}{p_k}\right)$, або запишемо так:
$p_1 \ldots p_k \varphi(n) = n(p_1 - 1)\ldots(p_k - 1)$.
Зауважимо, що права частина ділиться на $p_1 - 1$, але тоді ліва частина теж. $p_1, \ldots, p_k$ не можуть ділитись на $p_1 - 1$ (зауваж, що це вже парне число при $p_1 > 2$), тому що непарне не може ділитись на парне. Для рівності треба вимагати, щоб $\varphi(n)$ ділилось на $p_1 - 1$, тобто $p_1 - 1 \mid \varphi(n)$.
У нашому випадку, $p_1 - 1 \mid 8$. Це може бути при $p_1 \in \{2, 3, 5\}$.
Із рештою $p_j - 1$ міркування аналогічні. Звідси випливає, що $p_1, \ldots, p_k \in \{2, 3, 5\}$. Отже, число $n = 2^a 3^b 5^c$ при $a, b, c \geq 0$.
Тобто $\varphi(n) = 8 \implies n = 2^a 3^b 5^c$. В зворотному не завжди вірно. $\varphi(n) = \varphi(2^a)\varphi(3^b)\varphi(5^c)$. Думаю, тут неважко показати, що $\gcd(a^2 3^b, 5^c) = 1$, а згодом $\gcd(3^b, 5^c) = 1$.
Тобто маємо $8 = \varphi(2^a)\varphi(3^b)\varphi(5^c)$. І насправді, тут небагато варіантів:
$(0,1,1); (1,1,1); (2,0,1); (3,1,0); (4,0,0)$. І отримаємо:
$n \in \{15, 16, 20, 24, 30\}$.

Remark 3.2.16 На основі цього прикладу (точніше його розв'язку) можна довести, що $\varphi(n)$ приймає завжди парне значення при $n > 2$.

Proposition 3.2.17 $\sum_{d \mid n} \varphi(d) = n$.

Proof.
Спочатку зафіксуємо $d \mid n$.
Розглянемо множину $S_d = \{m \in \mathbb{Z} : 1 \leq m \leq n, \gcd(m, n) = d\}$. А також тимчасово розглянемо $S_{\frac{m}{d}} = \left\{x = \frac{m}{d} \in \mathbb{Z} : 1 \leq x \leq \frac{n}{d}, \gcd\left(\frac{m}{d}, \frac{n}{d}\right) = 1\right\}$.
Зауважимо, що $\#S_{\frac{m}{d}} = \varphi\left(\frac{n}{d}\right)$, а також $\#S_{\frac{m}{d}} = \#S_d$.
Також важливо показати, що $\{1, 2, \ldots, n\} = \bigsqcup_{d \mid n} S_d$. І дійсно,

$$m \in \{1, 2, \ldots, n\} \implies m \in S_{\gcd(m,n)} \overset{\gcd(m,n) \mid n}{\implies} m \in \bigsqcup_{d \mid n} S_d.$$

$$m \in \bigsqcup_{d \mid n} S_d \implies \exists d \mid n : m \in S_d \implies m \in \{1, 2, \ldots, n\}.$$

Ще $S_{d_1} \cap S_{d_2} = \emptyset$ при $d_1 \neq d_2$, тому що якби $x \in S_{d_1} \cap S_{d_2}$, було б $\gcd(x, n) = d_1 \neq d_2 = \gcd(x, n)$. Отже,

$$\#\{1,2,\ldots,n\} = n = \#\left(\bigsqcup_{d|n} S_d\right) = \sum_{d|n} \#S_d = \sum_{d|n} \varphi\left(\frac{d}{n}\right) = \sum_{d|n} \varphi(d).$$

Остаточно $\sum_{d|n} \varphi(d) = n$. ■

3.3 Функція μ (функція Мьобіуса)

Definition 3.3.1 Арифметична функція $\mu\colon \mathbb{N} \to \mathbb{N}$, яка визначається як

$$\mu(n) = \begin{cases} 1, & n = 1 \\ 0, & n \text{ не вільне від квадартів} \\ (-1)^l, & l = p_1 \ldots p_l, \text{ тут різні прості числа} \end{cases},$$

називається **функцією Мьобіуса**.
Останній випадок означає, що n – вільне від квадратів число та залежить від l – кількості різних простих чисел. Що таке число, що вільне від квадратів, дивись **Def. 6.1.8**.

Example 3.3.2 Зокрема $\mu(45) = 0$, бо не є вільним від квадратів. Також $\mu(42) = -1$, бо $42 = 2 \cdot 3 \cdot 7$ – вільне від квадратів та має 3 – непарну кількість - простих чисел.

Remark 3.3.3 Якщо p – просте, то $\mu(p) = -1$ та $\mu(p^k) = 0$ при $k > 1$.

Theorem 3.3.4 Функція μ – мультиплікативна.

Proof.
Маємо m, n такі, що $\gcd(m, n) = 1$. Розглянемо кілька випадків:
I. m або n – не вільне від квадратів. Тобто існує просте число p, для якого $p^2 \mid m$ або $p^2 \mid n$. В обох випадках отримаємо $p^2 \mid mn$, а тому також mn не буде вільним від квадратів. Отже, $\mu(mn) = 0 = \mu(m)\mu(n)$.
II. m та n - вільні від квадратів, нехай $m = p_1 \ldots p_r$ та $n = q_1 \ldots q_s$, причому p_i, q_j всі різні в силу $\gcd(m, n) = 1$. Отже, $mn = p_1 \ldots p_r q_1 \ldots q_s$, а тому $\mu(mn) = (-1)^{r+s} = (-1)^r(-1)^s = \mu(m)\mu(n)$. ■

Theorem 3.3.5 $\sum_{d|n} \mu(d) = 0$, якщо $n > 1$.

Remark 3.3.6 Якщо $n = 1$, то маємо лише дільник $d = 1$, тому буде лише $\mu(1) = 1$.

Proof.
Покладемо $F(n) = \sum_{d|n} \mu(d)$. Оскільки μ – мультиплікативна, то тоді F також. Відповідно при $n = p_1^{k_1} \dots p_r^{k_r}$ маємо $F(n) = F(p_1^{k_1}) \dots F(p_r^{k_r})$.
Далі треба з'ясувати, чому дорівнює $F(p^k)$. Маємо
$F(p^k) = \sum_{d|p^k} \mu(d) = \mu(1)+\mu(p)+\mu(p^2)+\dots+\mu(p^k) = 1-1+0+\dots+0 = 0.$
Разом отримали $F(n) = \sum_{d|n} \mu(d) = 0.$ ■

Theorem 3.3.7 Формула обернення Мьобіуса
Задані функції $F, f\colon \mathbb{N} \to \mathbb{N}$, що взаємно пов'язані такою формулою: $F(n) = \sum_{d|n} f(d)$.
Тоді $f(n) = \sum_{d|n} \mu(d) F\left(\frac{n}{d}\right) \overset{\text{або}}{=} \sum_{d|n} \mu\left(\frac{n}{d}\right) F(d).$

Proof.
$$\sum_{d|n} \mu(d) F\left(\frac{n}{d}\right) = \sum_{d|n} \left(\mu(d) \sum_{c|\frac{n}{d}} f(c) \right) = \sum_{d|n} \sum_{c|\frac{n}{d}} \mu(d) f(c) \boxed{=}$$
Можна показати, що $\begin{cases} d \mid n \\ c \mid \frac{n}{d} \end{cases} \iff \begin{cases} c \mid n \\ d \mid \frac{n}{c} \end{cases}$. Тоді буде трошки інший вираз в сумі.
$$\boxed{=} \sum_{c|n} \sum_{d|\frac{n}{c}} f(c)\mu(d) = \sum_{c|n} \left(f(c) \sum_{d|\frac{n}{c}} \mu(d) \right) \boxed{\boxed{=}}$$
Якщо $\frac{n}{c} = 1$ (а це буде можливо при $n = c$ в першій сумі), то тоді ця сума буде одиничкою. У всіх інших випадках онулюється.
$\boxed{\boxed{=}} \sum_{c=n} f(c) \cdot 1 = f(n).$ ■

Corollary 3.3.8 Для функцій τ, σ, на основі обернення Мьобіуса, маємо:
$1 = \sum_{d|n} \mu\left(\frac{n}{d}\right) \tau(d)$
$n = \sum_{d|n} \mu\left(\frac{n}{d}\right) \sigma(d)$

Theorem 3.3.9 Задано функцію F – мультиплікативна, $F(n) = \sum_{d|n} f(d)$.
Тоді функція f – мультиплікативна.

Proof.
Беремо m, n - такі числа, щоб $\gcd(m,n) = 1$. Тоді

$$f(mn) = \sum_{d|mn} \mu(d) F\left(\frac{mn}{d}\right) \overset{\text{Lm. 3.1.9}}{=} \sum_{\substack{d_1|m \\ d_2|n}} \mu(d_1 d_2) F\left(\frac{mn}{d_1 d_2}\right) =$$

$$= \sum_{\substack{d_1|m \\ d_2|n}} \mu(d_1)\mu(d_2) F\left(\frac{m}{d_1}\right) F\left(\frac{n}{d_2}\right) = \sum_{d_1|m} \mu(d_1) F\left(\frac{m}{d_1}\right) \cdot \sum_{d_2|n} \mu(d_2) F\left(\frac{n}{d_2}\right)$$

$$= f(m) f(n). \qquad \blacksquare$$

3.4 Ціла частина числа

Уже колись (можливо) використовувалось це, але хочеться показати деякі цікаві властивості. Залишу означення для нагадування.

Definition 3.4.1 Цілою частиною числа $x \in \mathbb{R}$ називають найбільше число t, для якого

$$x - 1 \leq t \leq x.$$

Позначення: $t = [x]$.

Зрозуміло, що виконується така рівність: $x = [x] + \theta$, де $\theta \in [0, 1)$.
Також цілком ясно, що $[a + b] \geq [a] + [b]$.

Theorem 3.4.2 Задано $n \in \mathbb{N}$ та p – просте число. Тоді найбільший степінь простого числа p, що ділить $n!$, дорівнює $\sum_{k=1}^{\infty} \left[\frac{n}{p^k}\right]$.

Remark 3.4.3 Даний вираз не є рядом, оскільки при $p^k > n$ маємо $\left[\frac{n}{p^k}\right] = 0$. Тобто в цій сумі завжди скінченна кількість доданків.

Proof.
Маємо n. Серед перших n чисел, що діляться на p, є $p, 2p, \ldots, tp$. Тут t – найбільше ціле число, для якого $tp \leq n$. Тобто $t \leq \frac{n}{p}$ та t – таке найбільше. Отже, $t = \left[\frac{n}{p}\right]$.
Тобто всього рівно $\left[\frac{n}{p}\right]$ чисел, що кратні p, що з'являються в $n!$, а саме: $p, 2p, \ldots, \left[\frac{n}{p}\right] p$ (1).

Проте серед цих чисел (1) можуть знайтися ті, що містять в розкладі більше, ніж одне просте число p. Тому ми серед перших n чисел оберемо ті, що діляться на p^2 - зокрема:
$p^2, 2p^2, \ldots, \left[\frac{n}{p^2}\right] p$ (2).
Але серед чисел (2) можуть знайтися ті, що містять окрім p^2 ще один p. Повторюємо все те саме.
Врешті-решт процес закінчиться, коли $p^{k_0} > n$ при деякому k_0. А тому щоб отримати кількість простих чисел p, що з'явиться в розкладі $n!$ (тобто найбільший степінь), треба просумувати:
$\left[\frac{n}{p}\right] + \left[\frac{n}{p^2}\right] + \cdots + \left[\frac{n}{p^{k_0-1}}\right]$. ■

Example 3.4.4 Для повного розуміння теореми, розглянемо 10!. З'ясуємо, скільки всього простих чисел $p = 3$ в розкладі.
Маємо $3, 6, 9$ - числа, що діляться на p. Маємо $3 = \left[\frac{10}{p}\right]$ простих чисел p в нашому розкладі. Але серед них є число, що має не одне p.
Маємо 9 - число, що ділиться на p^2. Маємо ще $1 = \left[\frac{10}{p^2}\right]$ просте число p в нашому розкладі.
Отже, всього $\left[\frac{10}{p}\right] + \left[\frac{10}{p^2}\right] = 3 + 1 = 4$ разів буде просте число $p = 3$.
Тобто 4 - найбільший степінь числа $p = 3$.

Corollary 3.4.5 Формула Лежандра
$$n! = \prod_{p \le n} p^{\sum_{k=1}^{\infty} \left[\frac{n}{p^k}\right]}$$

Theorem 3.4.6 $C_n^r \in \mathbb{N} \cup \{0\}$.
Насправді, з точки зору комбінаторики зрозуміло, що це буде невід'ємне ціле число. Проте для різноманіття можна провести інше доведення.

Proof.
Для кожного простого числа p в розкладі $r!(n-r)!$ маємо:
$$\left[\frac{n}{p^k}\right] = \left[\frac{r + (n-r)}{p^k}\right] \ge \left[\frac{r}{p^k}\right] + \left[\frac{n-r}{p^k}\right].$$
Просумувавши по k, отримаємо:
$$\sum_{k \ge 1} \left[\frac{n}{p^k}\right] \ge \sum_{k \ge 1} \left[\frac{r}{p^k}\right] + \sum_{k \ge 1} \left[\frac{n-r}{p^k}\right].$$
Ліва частина - це кількість простих чисел p, що з'явиться в $n!$. Права

частина – це кількість простих чисел p, що з'явиться в $r!(n-r)!$. Значить, в чисельнику кількість p або така сама, або більша за кількість в знаменнику. ■

Corollary 3.4.7 Добуток будь-яких послідовних $r \in \mathbb{N}$ натуральних чисел ділиться націло на $r!$.

Theorem 3.4.8 Задано f, F – арифметичні функції, де $F(n) = \sum_{d|n} f(d)$.

Тоді для кожного $N \in \mathbb{N}$ маємо $\sum_{n=1}^{N} F(n) = \sum_{k=1}^{N} f(k) \left[\frac{N}{k}\right]$.

Proof.

Маємо $\sum_{n=1}^{N} F(n) = \sum_{n=1}^{N} \sum_{d|n} f(d) = \sum_{d|1} f(d) + \cdots + \sum_{d|N} f(d)$.

Зафіксуємо деяке $1 \leq k \leq N$. У нашій сумі ми завжди зможемо знайти $f(k)$ хоча б один раз в k-ій сумі при $d = k$. Але наша мета – знайти загальну кількість $f(k)$.

$f(k)$ знаходиться в сумі $\sum_{d|n} f(d)$ тоді й тільки тоді, коли $k \mid n, n = \overline{1, N}$.

А тому серед чисел $1, 2, \ldots, N$ оберемо ті, що діляться на k – отримаємо такий список:

$k, 2k, \ldots, \left[\frac{N}{k}\right] k$.

Тобто всього $\left[\frac{N}{k}\right]$ дільників k, це теж саме, що $f(k)$ знаходиться в $\left[\frac{N}{k}\right]$ різних сумах формата $\sum_{d|n} f(d)$.

Отже, можемо переписати вираз

$\sum_{n=1}^{N} \sum_{d|n} f(d) = \sum_{k=1}^{N} f(k) \left[\frac{N}{k}\right]$. ■

Corollary 3.4.9 Для кожного $N \in \mathbb{N}$ маємо такі вирази:

$\sum_{n=1}^{N} \tau(n) = \sum_{n=1}^{N} \left[\frac{N}{n}\right]$;

$\sum_{n=1}^{N} \sigma(n) = \sum_{n=1}^{N} n \left[\frac{N}{n}\right]$.

4 Первісні корені

4.1 Порядок

Definition 4.1.1 Задано $n \in \mathbb{N}$ та $a \in \mathbb{Z}$ – взаємно прості.
Порядком $a \pmod n$ називають найменше число $m \in \mathbb{N}$, для якого

$$a^m \equiv 1 \pmod n$$

Позначення: $m = \mathrm{ord}_n(a)$.

Example 4.1.2 Зокрема $\mathrm{ord}_{12}(5) = 2$, оскільки маємо наступне:
$5 \not\equiv 1 \pmod{12}$;
$5^2 = 25 \equiv 1 \pmod{12}$.

Proposition 4.1.3 Задано $m = \mathrm{ord}_n(a)$. Тоді маємо:
$a^k \equiv 1 \pmod n \iff m \mid k$.

Proof.
$\boxed{\Rightarrow}$ Дано: $a^k \equiv 1 \pmod n$. Поділимо k на m – отримаємо $k = mq + r$. Вважаємо, що $0 < r < m$. Тоді
$a^r = 1 \cdot a^r \equiv a^m \cdot a^r \equiv (a^m)^q \cdot a^r = a^{mq+r} = a^k \equiv 1 \pmod n$.
Тож звідси $r \geq m$, що неможливо для нашого припущення. Тож вимагаємо $r = 0$. Отже, $m \mid k$.

$\boxed{\Leftarrow}$ Дано: $m \mid k$, тобто $k = mx, x \in \mathbb{Z}$. Звідси
$a^k = (a^m)^x \equiv 1^x = 1 \pmod n$. ■

Corollary 4.1.4 $\mathrm{ord}_n(a) \mid \varphi(n)$
Вказівка: **Th. 3.2.6**.

Proposition 4.1.5 $\mathrm{ord}_n(a^k) = \dfrac{\mathrm{ord}_n(a)}{\gcd(k, \mathrm{ord}_n(a))}$.
Нагадування, що коли n, a – взаємно прості, то тоді n, a^k – також взаємно прості, тож рівність має сенс.

Proof.
Позначимо $d = \gcd(k, \mathrm{ord}_n(a))$, тоді звідси $\dfrac{k}{d}, \dfrac{\mathrm{ord}_n a}{d} \in \mathbb{N}$. Таким чином,
$\left(a^k\right)^{\frac{\mathrm{ord}_n(a)}{d}} = \left(a^{\mathrm{ord}_n(a)}\right)^{\frac{k}{d}} \equiv 1^{\frac{k}{d}} = 1 \pmod n$.
Звідси маємо, що $\mathrm{ord}_n(a^k) \mid \dfrac{\mathrm{ord}_n(a)}{d}$ – це з одного боку.
Також $a^{k\,\mathrm{ord}_n(a^k)} = (a^k)^{\mathrm{ord}_n(a^k)} \equiv 1 \pmod n$.
Звідси маємо, що $\mathrm{ord}_n(a) \mid k\,\mathrm{ord}_n(a^k) \implies \dfrac{\mathrm{ord}_n(a)}{d} \mid \dfrac{k}{d}\mathrm{ord}_n(a^k)$. Але

оскільки $\frac{\mathrm{ord}_n(a)}{d}, \frac{k}{d}$ – взаємно прості, то тоді звідси $\frac{\mathrm{ord}_n(a)}{d} \mid \mathrm{ord}_n(a^k)$ – це з іншого боку.
Отже, $\frac{\mathrm{ord}_n(a)}{d} = \mathrm{ord}_n(a^k)$. ■

4.2 Первісні корені

Definition 4.2.1 Задано $n \in \mathbb{N}$ та $a \in \mathbb{Z}$ – взаємно прості.
Число a називається **первісним коренем** $(\mathrm{mod}\ n)$, якщо

$$\mathrm{ord}_n(a) = \varphi(n)$$

Example 4.2.2 Зокрема 3 - первісний корінь $(\mathrm{mod}\ 10)$. Дійсно,
$3^1 \equiv 3 \pmod{10}$
$3^2 \equiv 9 \pmod{10}$
$3^3 \equiv 7 \pmod{10}$
$3^4 \equiv 1 \pmod{10}$
Тобто $\mathrm{ord}_{10}(3) = 4$, але водночас $\varphi(10) = 4$.

Example 4.2.3 Покажемо, що жодне число не буде первісним коренем $(\mathrm{mod}\ 12)$.
По-перше, $\varphi(12) = 4$, а по-друге, $\gcd(a, 12) = 1 \iff a \in \{1, 5, 7, 11\}$. Тож достатньо подивитись лише на них. А решта чисел $a > 12$ розглядати не треба в силу конгруентності.
А ми вже знаємо з попереднього прикладу, що $a^2 \equiv 1 \pmod{12} \iff a \in \{1, 5, 7, 11\}$. Тобто ми отримали, що $\mathrm{ord}_{12}(a) = 2 \neq \varphi(12)$.

Theorem 4.2.4 Нехай p – просте число. Тоді існує примітивний корінь $(\mathrm{mod}\ p)$.

Але, насправді, ми доведемо більш строгу теорему:

Theorem 4.2.5 Якщо $d \mid p-1$, то тоді всього $\varphi(d)$ неконгруентних чисел порядка d за модулем p.

Proof.
Розглянемо множину $S_d = \{1 \leq m \leq p-1 \mid \mathrm{ord}_p(m) = d\}$. Зауважимо, що $\bigsqcup_{d|p-1} S_d = \{1, 2, \ldots, p-1\}$. В один напрямок – ясно, а в іншу треба зауважити, що $\mathrm{ord}_p(x) \mid p-1$, де $1 \leq x \leq p-1$. Диз'юнктивне об'єднання неважко показати.
Розглянемо функцію $f(d) = \#S_d$. В силу зауважень вище, ми маємо

$\sum_{d|p-1} f(d) = p-1$. Але ми знаємо, що $\sum_{d|p-1} \varphi(d) = p-1$, тобто маємо
$\sum_{d|p-1} f(d) = \sum_{d|p-1} \varphi(d)$.
Ми покажемо, що $f(d) \leq \varphi(d)$ для деякого дільника d, а це разом з рівнянням вище приведе потім до рівності.
Якщо $f(d) = 0$, то доведено. Інакше нехай $f(d) > 0$, тоді існує елемент a, для якого $\mathrm{ord}_p(a) = d$.
Розглянемо множину $\{a, a^2, \ldots, a^{d-1}, a^d\}$. Всі ці елементи - неконгруентні розв'язки $x^d - 1 \equiv 0 \pmod p$. !Якщо якась пара $a^i \equiv a^j \pmod p$, де $1 \leq j < i \leq d$, то тоді $a^{i-j} \equiv 1 \pmod p$, але число $0 \leq i-j < d-1$, та водночас $i - j \geq d$. Суперечність!
Більше розв'язків даного рівняння нема, оскільки за попередніми результатами, тут всього d розв'язків.
За попередньою формулою, $\mathrm{ord}_n(a^k) = \dfrac{d}{\gcd(k,d)}$. Зауважимо, що $\mathrm{ord}_n(a^k) = d$ лише тоді, коли $\gcd(k,d) = 1$. Отже, кількість розв'язків - рівно d, але лише $\varphi(d)$ з них будуть розв'язками порядку d.
Отже, звідси $f(d) = \varphi(d)$, але це для конкретного дільника d.
!Припустимо, що існує якийсь дільник d^*, для якого $f(d^*) < \varphi(d^*)$. Автоматично звідси $\sum_{d|p-1} f(d) < \sum_{d|p-1} \varphi(d)$. Суперечність!
Таким чином, $f(d) = \varphi(d), \forall d \mid p-1$. ■

А тепер якщо взяти $d = p-1$ з попередньої теореми, то тоді буде всього $\varphi(p-1)$ чисел порядка $p-1$ за модулем p. Отже, за модулем p знайдеться первісний корінь, як ми й хотіли з самого початку.

Theorem 4.2.6 Задано p – непарне просте число та r – первісний корінь $\pmod p$. (він існує за **Th. 4.2.4**). Тоді існує $m \in \mathbb{Z}$ такий, що $g = r + mp$ - первісний корінь $\pmod{p^k}$, для довільного $k \in \mathbb{N}$.

Proof.
Оскільки r – первісний корінь $\pmod p$, тоді $r^{p-1} \equiv 1 \pmod p$.
Тобто $r^{p-1} = 1 + px, x \in \mathbb{Z}$.
Побудуємо $g = r + mp$, де $m \in \mathbb{Z}$, яке скоро надам.
Хочемо довести, що $\mathrm{ord}_{p^k}(g) = \varphi(p^k)$. Я позначу $d = \mathrm{ord}_{p^k}(g)$.
Зауважимо, що $\varphi(p^k) = p^k - p^{k-1} = p^{k-1}(p-1)$. Відомо, що $d \mid p^{k-1}(p-1)$.
Водночас маємо $g \equiv r \pmod p$, а також $g^d \equiv 1 \pmod{p^k}$.
Тоді $g^d \equiv 1 \pmod p$, а отже,
$r^d \equiv g^d \equiv 1 \pmod p \implies \underset{=\mathrm{ord}_p(r)}{p-1} \mid d$.

$\begin{cases} d \mid p^{k-1}(p-1) \\ p-1 \mid d \end{cases} \implies d = (p-1)p^l$, де число $l \le k-1$.
Залишилось довести, що $l \ge k-1$.

$g = r + mp$

$$g^{p-1} = (r+mp)^{p-1} = r^{p-1} + \sum_{j=1}^{p-1} C_{p-1}^{j} m^j p^j r^{p-1-j} =$$

$$= 1 + px + p(p-1)mr^{p-2} + p^2 S.$$

Таку рівність я залишу на потім, а зараз запишу інакше:

$$\begin{aligned} g^{p-1} &= 1 + pz_0 \\ (g^{p-1})^p = (1+pz_0)^p &= 1 + p^2 z_1 \\ (g^{p-1})^{p^2} = (1+p^2 z_1)^p &= 1 + p^3 z_2 \\ &\vdots \\ (g^{p-1})^{p^l} = g^d &= 1 + p^{l+1} z_l \end{aligned}$$

Тоді, згадавши, що $d = \mathrm{ord}_{p^k}(g)$, ми маємо:
$1 + p^{l+1} z_l \equiv 1 \pmod{p^k} \implies p^{l+1} z_l \equiv 0 \pmod{p^k} \implies p^{l+1} \equiv 0 \pmod{p^k}$.
Таким чином, $p^k \mid p^{l+1}$, звідси $l + 1 \ge k \implies l \ge k-1$.
А це означає, що $l = k-1$, тоді $d = p-1)p^{k-1} = \varphi(p^k)$.
Тобто остаточно $\mathrm{ord}_{p^k}(g) = \varphi(p^k)$, майже завершили доведення.

Для перехода $\implies$ необхідно довести, що $\gcd(z_l, p^k) = 1$, але достатньо тут показати, що $\gcd(z_l, p) = 1$. Щоб довести дану рівність ми будемо робити ось такий ланцюг доведення:
$\gcd(z_0, p) = 1 \implies \gcd(z_1, p) = 1 \implies \cdots \implies \gcd(z_l, p) = 1$.
!Припустимо, що $\gcd(z_0, p) \ne 1$, тоді звідси $p \mid z_0$. Згадуємо, що $z_0 = x + (p-1)mr^{p-2} + pS$, звідси маємо $p \mid x + (p-1)mr^{p-2}$. Щоб була суперечність, нам треба підібрати m таким чином, щоб
$\gcd(p, x + (p-1)mr^{p-2}) = 1$. І ми оберемо $m \in \{0, 1\}$.
Якщо $\gcd(x, p) = 1$, то тоді беремо $m = 0$.
Якщо $\gcd(x, p) = p$, то тоді, взявши $m = 1$, матимемо
$\gcd(p, x + (p-1)r^{p-2}) = 1$. І рівність є правильною.
!Якби $\gcd(p, x + (p-1)r^{p-2}) = p$, то тоді звідси $p \mid r^{p-2} \implies r^{p-2} = pv \implies r^{p-1} = rpv = 1 + px \implies 0 \equiv 1 \pmod{p}$ Суперечність!
Резюмуючи, ми маємо m, щоб $\gcd(p, x+(p-1)mr^{p-2}) = 1$, завдяки якому ми прийшли до суперечності першого припущення! Тож $\gcd(z_0, p) = 1$.

!Припустимо, що $\gcd(z_1, p) = p$. У нашому випадку, якщо розписати, то $(g^{p-1})^p = 1 + p^2 z_0 + p^2 S_1$, тобто $z_0 + S_1 = z_1$.
Варто також зазначити, що $p \mid S_1$, це треба теж розписати, щоб побачити.
Отже, $p \mid z_0 = z_1 - S_1$. Суперечність! Отже, $\gcd(z_1, p) = 1$.

!Припустимо, що $\gcd(z_2, p) = p$. Абсолютно аналогічним чином прийдемо до суперечності! Отримаємо $\gcd(z_2, p) = 1$.
⋮
Ось такими кроками ми дійдемо до $\gcd(z_l, p) = 1$. ■

Example 4.2.7 Знайти первісні корені $\pmod 9$.
Ми знаємо, що за $\pmod 3$ існує первісний корінь 2. Тоді має існувати первісний корінь $\pmod 9$ за формулою $g = 2 + 3m$. Можливі варіанти: $g \in \{2, 5\}$.
Відомо, що $\varphi(9) = 6$, тож перевіримо:
$2^6 = 64 \equiv 1 \pmod 9$;
$5^6 = (25)^3 \equiv 7^3 = 7 \cdot 49 \equiv 7 \cdot 4 = 28 \equiv 1 \pmod 9$.

Lemma 4.2.8 Не існує первісного кореня $\pmod{2^m}$, де число $m \geq 3$.

Proof.
База індукції: $m = 3$. Нам треба розглянути числа $\{1, 3, 5, 7\}$.
Маємо $\mathrm{ord}_8(3) = 2, \mathrm{ord}_8(5) = 2, \mathrm{ord}_8(7) = 2$. Але $\varphi(8) = 4$, тому й не існує первісного кореня $\pmod 8$.
Припущення індукції: для $k \geq 3$ не існує первісних поренів $\pmod{2^k}$.
Крок індукції: доведемо для ситуації $\pmod{2^{k+1}}$. Для цього ми хочемо показати, що $\forall a \in \mathbb{Z} : \gcd(a, 2^{k+1}) = 1$ матимемо $a^{\varphi(2^k)} \equiv 1 \pmod{2^{k+1}}$.
Із припущення маємо, що $\forall a \in \mathbb{Z}, a$ - непарні : $a^{\frac{\varphi(2^k)}{2}} \equiv 1 \pmod{2^k}$.
Пояснення: за теоремою Ойлера, $a^{\varphi(2^k)} \equiv 1 \pmod{2^k}$, при a - непарне. Також a – не первісний, позначимо $d = \mathrm{ord}_{2^k}(a)$. Тоді $a^d \equiv 1 \pmod{2^k}$, а тому $d < \varphi(2^k)$ та $d \mid \varphi(2^k)$. Також $\varphi(2^k) = 2^{k-1}$, тому число $d = 2^l$, де $1 \leq l \leq 2^{k-2} = \dfrac{\varphi(2^{k-1})}{2}$. Звідси випливає, що $d \mid \dfrac{\varphi(2^{k-1})}{2}$, а тому й отримується бажана рівність.
Коротше, ми маємо $a^{2^{k-2}} \equiv 1 \pmod{2^k}$, а тому
$a^{2^{k-2}} = 1 + x \cdot 2^k$ для деякого $x \in \mathbb{Z}$.
Взведемо обидві частини в квадрат:
$a^{2^{k-1}} = 1 + x \cdot 2^{k+1} + x^2 \cdot 2^{2k} \equiv 1 \pmod{2^{k+1}}$.
У нас виникла степінь менша за $\varphi(2^{k+1})$, для якого виконується конгруенція 1 для будь-якого непарного числа. А тому первісних коренів $\pmod{2^{k+1}}$ не має.
МІ доведено. ■

Lemma 4.2.9 Не існує первісного кореня $\pmod{m_1 m_2}$, де $m_1, m_2 > 2$ та $\gcd(m_1, m_2) = 1$.

Proof.
Позначимо $n = m_1 m_2$. Справедлива така рівність:

$\frac{1}{2}\varphi(n) = \left(\frac{\varphi(m_1)}{2}\right)\varphi(m_2) = \varphi(m_1)\left(\frac{\varphi(m_2)}{2}\right)$.
Тоді звідси маємо дві конгруенції за Ойлером:
$a^{\frac{1}{2}\varphi(n)} = \left(a^{\frac{\varphi(m_2)}{2}}\right)^{\varphi(m_1)} \equiv 1 \pmod{m_1}$.
$a^{\frac{1}{2}\varphi(n)} = \left(a^{\frac{\varphi(m_1)}{2}}\right)^{\varphi(m_2)} \equiv 1 \pmod{m_2}$.
Тоді оскільки $\gcd(m_1, m_2) = 1$, маємо $a^{\frac{\varphi(n)}{2}} \equiv 1 \pmod{n}$. І знову отримали степінь меншу за $\varphi(n)$, де конгруенція один. ■

Theorem 4.2.10 Задано p – непарне просте число. Тоді існує первісний корінь $\pmod{2p^k}$, для довільного $k \in \mathbb{N}$.

Proof.
Припустимо, що r – первісний корінь $\pmod{p^k}$. Він існує в силу того, що існує первісний корінь $\pmod{p}$, а згодом й $\pmod{p^k}$.
Побудуємо $g = \begin{cases} r & r \text{ – непарне} \\ r + p^k & r \text{ – парне} \end{cases}$.
Це розгалуження робиться для того, щоб $\gcd(g, 2p^k) = 1$.
Позначимо $d = \operatorname{ord}_{2p^k}(g)$, хочемо показати, що $d = \varphi(2p^k)$.
$g^d \equiv 1 \pmod{2p^k} \implies g^d \equiv r^d \equiv 1 \pmod{p^k}$.
Звідси випливає, що $\underset{=\operatorname{ord}_{p^k}(r)}{\varphi(p^k)} \mid d$. Але також відомо, що $d \mid \varphi(2p^k)$.
Але важливо зауважити, що $\varphi(p^k) = \varphi(2p^k)$, бо p – непарне. Тож остаточно $d = \varphi(2p^k)$. ■

Theorem 4.2.11 Існує первісний корінь $\pmod{n} \iff$
$\iff n \in \{1, 2, 4, p^k, 2p^k\}$, де p – непарні прості числа.

Proof.
$\boxed{\Rightarrow}$ Дано: існує первісний $\pmod{n}$. Ми доведемо ось це:
ми візьмемо $n \notin \{1, 2, 4, p^k, 2p^k\}$ та покажемо, що вони не дають первісні корені. Але якщо $n \notin \{1, 2, 4, p^k, 2p^k\}$, то тоді спрацьовує одна з двох лем вище. Тож первісних коренів дійсно не буде.

$\boxed{\Leftarrow}$ Дано: $n \in \{1, 2, 4, p^k, 2p^k\}$, де p – непарні прості числа. Для $1, 2, 4$ перевірити існування первісного кореня неважко. Ми вже знаємо, що для p існує первісний корінь, а тому за попередніми теоремами, знайдуться якісь первісні корні за модулем p^k та за модулем $2p^k$. ■

Example 4.2.12 З'ясувати, хто має первісний корінь за такими модулями: $\{4, 8, 9, 10, 12, 16, 22, 27, 28, 31, 33\}$.
Ми знаємо, що число, яке потрапляє в $\{1, 2, 4, p^k, 2p^k \mid p > 2, k \geq 1\}$,

буде мати первісний. Тоді числа
$4 \qquad 9 = 3^2$
$10 = 2 \cdot 5 \quad 22 = 2 \cdot 11$
$27 = 3^3 \qquad 31$
будуть мати первісні. Решта – не матимуть в силу неспівпадіння з бажаним розкладом.

Theorem 4.2.13 Тест на первісний корінь $(\mathrm{mod}\ p)$
r – первісний корінь $(\mathrm{mod}\ p) \iff \forall q - \text{просте} : q \mid p-1 : r^{\frac{p-1}{q}} \not\equiv 1 \ (\mathrm{mod}\ p)$.

Proof.
$\boxed{\Rightarrow}$ Дано: r – первісний корінь $(\mathrm{mod}\ p)$. Тобто $\mathrm{ord}_p(r) = p-1$, але числа $\dfrac{p-1}{q}$ ясна річ менші за $p-1$, тобто конгруенція одиниці неможлива.

$\boxed{\Leftarrow}$ Дано: $\forall q : q \mid p-1 : r^{\frac{p-1}{q}} \not\equiv 1 \ (\mathrm{mod}\ p)$.
Ми доведемо, що якщо r – не первісний корінь, то тоді $\exists q \mid p-1 :$
$r^{\frac{p-1}{q}} \equiv 1 \ (\mathrm{mod}\ p)$.
$r^d \equiv 1 \ (\mathrm{mod}\ p)$ для деякого $d \mid p-1$ (тому як наслідок, $d < p-1$).
Маємо $p-1 = dk, k \neq 1$. Оскільки $k > 1$, то запишемо $k = qx$ для деякого $x \in \mathbb{Z}$, де число q – просте.
Тоді $\dfrac{p-1}{q} = dx$, але $r^{\frac{p-1}{q}} = (r^d)^x \equiv 1 \ (\mathrm{mod}\ p)$. ■

Example 4.2.14 Знайти первісний корінь $(\mathrm{mod}\ 29)$.
Ми використаємо для цього отриманий тест. Для числа $29-1 = 28$ будуть два простих дільника: $2, 7$. Маємо:
$2^{\frac{28}{7}} = 2^4 = 16 \not\equiv 1 \ (\mathrm{mod}\ 29)$.
$2^{\frac{28}{2}} = 2^7 \equiv 12 \not\equiv 1 \ (\mathrm{mod}\ 29)$.
Отже, 2 – первісний корінь $(\mathrm{mod}\ 29)$.
Також можна перевірити, що всі ці корені будуть первісними $(\mathrm{mod}\ 29)$, як-от: $\{2, 3, 8, 10, 11, 14, 15, 18, 19, 21, 26, 27\}$. Більше за 29 перевіряти не треба, достатньо від 1 до 29.

Proposition 4.2.15 Задано r – первісний корінь $(\mathrm{mod}\ n)$.
r^m – первісний корінь $(\mathrm{mod}\ n) \iff \gcd(m, \varphi(n)) = 1$.

Proof.
$\boxed{\Rightarrow}$ Нехай $\gcd(m, \varphi(n)) = d > 1$. Тоді ми знаємо, що
$$\mathrm{ord}_n(r^m) = \frac{\mathrm{ord}_n(r)}{\gcd(m, \mathrm{ord}_n(r))} = \frac{\varphi(n)}{\gcd(m, \varphi(n))} < \varphi(n).$$
Отже, r^m не може бути первісним коренем.

$\boxed{\Leftarrow}$ Дано: $\gcd(m, \varphi(n)) = 1$.
Тоді $\operatorname{ord}_n(r^m) = \dfrac{\operatorname{ord}_n(r)}{\gcd(m, \operatorname{ord}_n(r))} = \dfrac{\varphi(n)}{\gcd(m, \varphi(n))} = \varphi(n)$.
Отже, r^m - первісний корінь $\pmod n$. ■

Corollary 4.2.16 Якщо за $\pmod n$ існує первісний корінь, то всього їх $\varphi(\varphi(n))$ неконгруентних первісних коренів.

Proposition 4.2.17 Задано a, причому $\operatorname{ord}_n(a) = k$.
$a^i \equiv a^j \pmod n \iff i \equiv j \pmod k$.

Proof.
$\boxed{\Rightarrow}$ Дано: $a^i \equiv a^j \pmod n$. Нехай $i \geq j$, не втрачаючи загальності. Оскільки $\gcd(a, n) = 1$, то тоді $\gcd(a^j, n) = 1$, а тому
$a^{i-j} \equiv 1 \pmod n \implies k \mid i - j \implies i \equiv j \pmod k$.

$\boxed{\Leftarrow}$ Дано: $i \equiv j \pmod k$. Тоді $i = j + kq$ при $q \in \mathbb{Z}$. Тоді
$a^i = a^{j+kq} = a^j \cdot (a^k)^q \equiv a^j \pmod n$. ■

Corollary 4.2.18 Задано r - первісний корінь $\pmod n$.
$r^a \equiv r^b \pmod n \iff a \equiv b \pmod{\varphi(n)}$.

Example 4.2.19 Розв'язати $x^3 \equiv 5 \pmod{17}$.
Неважко показати, що 3 - буде первісним $\pmod{17}$.
Встановимо $x = 3^y$ для деякого $y \in \mathbb{N}$. Тоді також зауважимо, що $5 \equiv 3^5 \pmod{17}$, тож
$3^{3y} \equiv 3^5 \pmod{17} \iff 3y \equiv 5 \pmod{\varphi(17)} \iff 3y \equiv 5 \pmod{16}$.
Розв'язавши, отримаємо $y \equiv 7 \pmod{16}$, тобто $x = 3^7 \equiv 11 \pmod{17}$.
Перевірка:
$11^3 = 121 \cdot 11 \equiv 2 \cdot 11 = 22 \equiv 5 \pmod{17}$.

ФУУУУУУУУУХ... нарешті...

4.3 Дискретний логарифм

Definition 4.3.1 Задано a, n – взаємно прості та r – первісний корінь.
Індексом числа a відносно числа r називають найменше невід'ємне число $k \in \mathbb{Z}$, для якого

$$r^k \equiv a \pmod n$$

Позначення: $\operatorname{ind}_r(a) = k$.

Remark 4.3.2 Зауважимо, що $\operatorname{ind}_r(a) \in \{0, 1, \ldots, \varphi(n) - 1\}$.
Фактично тому що після $\varphi(n)$ буде лише $r^k \equiv 1 \pmod n$.

Example 4.3.3 Відомо, що 2 – первісний корінь $\pmod{11}$. Запишемо таку табличку:

m	0	1	2	3	4	5	6	7	8	9
2^m	1	2	4	8	5	10	9	7	3	6

Зауважимо, що $\operatorname{ind}_2 5 = 4$, просто тому що $2^4 \equiv 5 \pmod{11}$.

Corollary 4.3.4 $r^{\operatorname{ind}_r(a)} \equiv a \pmod{n}$.

Proposition 4.3.5 Властивості індекса
Задано r – первісний корінь $\pmod{n}$. Також a, b – такі числа, що $\gcd(a, n) = 1, \gcd(b, n) = 1$. Тоді:
1) $\operatorname{ind}_r(ab) \equiv \operatorname{ind}_r(a) + \operatorname{ind}_r(b) \pmod{\varphi(n)}$;
2) $\operatorname{ind}_r(1) \equiv 0 \pmod{\varphi(n)}$;
3) $\operatorname{ind}_r(r) \equiv 1 \pmod{\varphi(n)}$;
4) $\operatorname{ind}_r(a^m) \equiv m \operatorname{ind}(a) \pmod{\varphi(n)}$;
5) $\operatorname{ind}_r(-1) = \dfrac{\varphi(n)}{2}$.

Remark 4.3.6 Саме завдяки означенню та наданим властивостям, індексом ще називають **дискретним логарифмом**.

Proof.
Доведемо (майже) всі властивості: Маємо $a \equiv r^k \pmod{n}$ та $b \equiv r^l \pmod{n}$. Запишемо інакше:
$r^{\operatorname{ind}_r(a)} \equiv r^k \pmod{n}$ та $r^{\operatorname{ind}_r(b)} \equiv r^l \pmod{n}$. Тоді звідси випливає, що $\operatorname{ind}_r(a) \equiv k \pmod{\varphi(n)}$ та $\operatorname{ind}_r(b) \equiv l \pmod{\varphi(n)}$.

1) Водночас маємо $ab \equiv r^{\operatorname{ind}_r(ab)} \equiv r^k r^l = r^{k+l} \pmod{n}$, а тому $\operatorname{ind}_r(ab) \equiv k + l \pmod{\varphi(n)}$. Отже,
$\operatorname{ind}_r(a) + \operatorname{ind}_r(b) \equiv k + l \equiv \operatorname{ind}_r(ab) \pmod{\varphi(n)}$.

2) *Вправа: довести.*

3) *Вправа: довести.*

4) Водночас маємо $a^m \equiv r^{\operatorname{ind}_r(a^m)} \equiv (r^k)^m = r^{km} \pmod{n}$, а тому $\operatorname{ind}_r(a^m) \equiv km \equiv m \operatorname{ind}_r(a) \pmod{\varphi(n)}$.

5) Позначимо $u = \operatorname{ind}_r(-1)$. Це означає, що
$r^u \equiv -1 \pmod{n}$ та u – найменше таке число. Тоді
$r^{2u} \equiv 1 \pmod{n} \implies 2u \equiv 0 \pmod{\varphi(n)}$.
Тобто $2u \in \{\varphi(n), 2\varphi(n), \dots\}$. Нема від'ємних чисел, бо індекс – невід'ємний. Також $2u \neq 0$, бо в інакшому випадку $(-1)^0 = -1$, що очевидно суперечить. Водночас ми знаємо, що $u \in \{0, 1, 2, \dots, \varphi(n) - 1\}$.
Із цих двох випливає, що єдина можливість - це $k = \dfrac{\varphi(n)}{2}$.

Всі (майже) властивості доведені. ■

Theorem 4.3.7 Множина $\{\pm 5, \pm 5^2, \ldots, \pm 5^{2^{n-2}}\}$ буде скороченою системою лишків $(\mathrm{mod}\ 2^n)$ при $n \geq 3$.

Proof.
Зауважимо, що $\varphi(2^n) = 2^n - 2^{n-1} = 2^{n-1} = 2 \cdot 2^{n-2}$, тож кількість елементів на множині вище збігається з $\varphi(2^n)$.
Доведемо, що всі вони – неконгруентні між собою $(\mathrm{mod}\ 2^n)$.
Розглянемо $5, 5^2, \ldots, 5^{2^{n-2}}$ та покажемо, що вони між собою не конгруентні. Яким чином? А ми доведемо, що $\mathrm{ord}_{2^n}(5) = 2^{n-2}$. І це якраз допоможе доведенню бажаного.
!Якщо за такими умовами припустити, що $5^i \equiv 5^j \pmod{2^n}$*, то буде звідси випливати, що число* $i - j < 2^{n-2}$ *буде порядком, що суперечить!*
Довести $\mathrm{ord}_{2^n}(5) = 2^{n-2}$ – це теж саме, що довести, що $2^n \mid 5^{2^{n-2}} - 1$, але водночас $2^{n+1} \nmid 5^{2^{n-2}} - 1$, причому $\forall n \geq 3$. Доведення за індукцією.
База індукції: $n = 3$, тобто $5^2 - 1 = 24$, тож $2^3 \mid 5^2 - 1$, але вже $2^4 \nmid 5^2 - 1$.
Припущення індукції: маємо $2^k \mid 5^{2^{k-2}} - 1$, але водночас $2^{k+1} \nmid 5^{2^{k-2}} - 1$ для деякого k.
Крок індукції: покажемо це для $k + 1$.
$5^{2^{k-1}} - 1 = (5^{2^{k-2}})^2 - 1 = \left(5^{2^{k-2}} - 1\right)\left(5^{2^{k-2}} + 1\right)$.
За МІ, $5^{2^{k-2}} = 2^k \cdot a$, де число a – непарне, тому що $2^{n+1} \nmid 5^{2^{n-2}} - 1$.
Також $5^{2^{k-2}} + 1 \equiv 2 \pmod 4$, в принципі легко зауважити. Тоді число $5^{2^{k-2}} + 1 = 2 \cdot b$, де число b – непарне, бо тоді конгруенція не виконається.
Разом $5^{2^{k-1}} - 1 = 2^{k+1} \cdot ab$, причому число ab залишається непарним, а тому $2^{k+1} \mid 5^{2^{k-1}} - 1$, але $2^{k+2} \nmid 5^{2^{k-1}} - 1$.
МІ доведено. А це в свою чергу означає, що $\mathrm{ord}_{2^n}(5) = 2^{n-2}$.

Висновок: $\{5, 5^2, \ldots, 5^{2^{n-2}}\}$ між собою неконгруентні. Неважко додумати, що $\{-5, -5^2, \ldots, -5^{2^{n-2}}\}$ – теж неконгруентні між собою. Лишилось тепер показати, що $5^x, -5^y$ не будуть конгруентні між собою.
!Припустимо $5^x \equiv -5^y \pmod{2^n}$. Тоді $5^x + 5^y \equiv 0 \pmod{2^n}$, але оскільки $n \geq 3$, то тоді $5^x + 5^y \equiv 0 \pmod 4$.
Із іншого боку, $5^x + 5^y \equiv 1^x + 1^y = 2 \pmod 4$. Тобто $0 \equiv 2 \pmod 4$. Суперечність!
Висновок: $\{\pm 5, \pm 5^2, \ldots, \pm 5^{2^{n-2}}\}$ має $\varphi(2^n)$ елементів, всі взаємно прості з 2^n, а також неконгруентні між собою. Тож це – скорочена система лишків. ■

Example 4.3.8 Розв'язати $7x^3 \equiv 3 \pmod{11}$.
Якщо тимчасово замінити $x^3 = t$, то отримаємо лінійне конгруентне

рівняння, яке розв'язується дуже просто. В результаті отримаємо еквівалентне рівняння:
$x^3 \equiv 2 \pmod{11}$.
Важливо зауважити, що 2 – первісний корінь $\pmod{11}$, тому
$x^3 \equiv 2 \pmod{11} \iff 2^{\mathrm{ind}_2(x^3)} \equiv 2^1 \pmod{11} \iff$
$\mathrm{ind}_2(x^3) \equiv 1 \pmod{\varphi(11)}$.
$3\,\mathrm{ind}_2(x) \equiv 1 \pmod{10}$.
Знову маємо лінійне конгруентне рівняння, маємо еквівалентне
$\mathrm{ind}_2(x) \equiv 7 \pmod{10} \iff x \equiv 2^7 \equiv 7 \pmod{10}$.

Example 4.3.9 Знайти остачу при діленні 3^{3^3} на 17.
Математично кажучи, $3^{3^3} \equiv r \pmod{17}$, де r – остача, яку шукаємо. Можна перевірити, що 3 - первісний корінь $\pmod{17}$, а тому запишемо еквівалетне рівняння:
$3^3 \equiv \mathrm{ind}_3(r) \pmod{16}$.
$11 \equiv \mathrm{ind}_3(r) \pmod{16} \iff r \equiv 3^{11} \equiv 7 \pmod{17}$.
Отже, остача від ділення 3^{3^3} на 17 буде число 7.

Theorem 4.3.10 Задано n – число, де існує первісний корінь, та таке a, що $\gcd(a, n) = 1$.
$x^k \equiv a \pmod{n}$ має розв'язок $\iff a^{\frac{\varphi(n)}{\gcd(k,\varphi(n))}} \equiv 1 \pmod{n}$.

Corollary 4.3.11 Якщо $x^k \equiv a \pmod{n}$ має розв'язок, то їх всього $\gcd(k, \varphi(n))$ штук.

Proof.
Нехай r - первісний корінь $\pmod{n}$, тоді
$$a^{\frac{\varphi(n)}{\gcd(k,\varphi(n))}} \equiv 1 \pmod{n} \iff \frac{\varphi(n)}{\gcd(k,\varphi(n))}\,\mathrm{ind}_r(a) \equiv 0 \pmod{\varphi(n)}$$
$$\iff \varphi(n) \mid \frac{\varphi(n)}{\gcd(k,\varphi(n))}\,\mathrm{ind}_r(a) \iff \gcd(k,\varphi(n)) \mid \mathrm{ind}_r(a) \iff$$
рівняння $kt \equiv \mathrm{ind}_r(a) \pmod{\varphi(n)}$ має розв'язок $t_0 \iff$
$\iff x^k \equiv a \pmod{n}$ має розв'язок $x_0 = r^{t_0}$. ■

Example 4.3.12 Розв'язати рівняння $3x^4 \equiv 8 \pmod{11}$.
Перепишемо еквівалетно ось так:
$x^4 \equiv 10 \pmod{11}$.
А далі зауважимо, що
$10^{\frac{\varphi(11)}{\gcd(4,\varphi(11))}} = 10^{\frac{10}{\gcd(4,10)}} = 10^5 = (10^2)^2 \cdot 10 \equiv 10 \not\equiv 1 \pmod{11}$.
Отже, розв'язків нема.

5 Квадратичний закон взаємності

5.1 Квадратичні лишки

Definition 5.1.1 Число $a \neq 0$ називається **квадратичним лишком** $(\mathrm{mod}\ n)$, якщо існує розв'язок рівняння

$$x^2 \equiv a \pmod{n}$$

Якщо ні, то тоді називають **квадратичним нелишком**.
По суті, тут описується щось на кшталт квадратного кореня з a.

Remark 5.1.2 Напевно, для зручності ми вимагаємо $a \neq 0$. Поки точної відповіді дати не можу, але цим буду користуватися. Хоча само число $a = 0$ є квадратичним лишком.

Example 5.1.3 Нехай $n = 7$. Маємо таку табличку:

k	k^2
1	1
2	4
3	2
4	2
5	4
6	1

Із цієї таблички видно, що:
$1, 2, 4$ – квадратичні лишки $(\mathrm{mod}\ 7)$
$3, 5, 6$ – квадратичні нелишки $(\mathrm{mod}\ 7)$.

Remark 5.1.4 Деякі автори вимагають додаткову умову $\gcd(a, n) = 1$ під час означення квадратичного лишка.

Example 5.1.5 Більш цікава задача
Знайти всі $m, n \in \mathbb{N}$, для яких виконується рівність: $1!+2!+\cdots+n! = m^2$.
Запишемо ліву частину за модулем 5 - отримаємо при $n \geq 4$:
$(1! + 2! + 3! + 4! + 5! + \cdots + n!) \equiv 1! + 2! + 3! + 4! \equiv 3 \pmod{5}$.
Фактично ми маємо рівність $m^2 \equiv 3 \pmod{5}$. Але якщо перебрати всі m, то ми отримаємо або 1, або 4 за заданим модулем. Тому рівність неможлива.
Отже, при $n \geq 4$ нема розв'язків. Тому розглянемо $n \in \{1, 2, 3\}$.
$n = 1$ маємо $1! = m^2 \implies m = 1$.
$n = 2$ маємо $3 = m^2$, але розв'язків в натуральних не має.
$n = 3$ маємо $9 = m^2 \implies m = 3$.
Отже, $(m, n) \in \{(1, 1), (3, 3)\}$ - єдина пара розв'язків.

Theorem 5.1.6 Задано p – непарне просте число. Тоді в кожній скороченій системі лишків всього $\frac{p-1}{2}$ квадратичних лишків $\pmod p$ та $\frac{p-1}{2}$ квадратичних нелишків $\pmod p$.

Remark 5.1.7 При $p = 2$ ми взагалі маємо лише 1 квадратичний лишок та 0 квадратичних нелишків $\pmod 2$.

Proof.
Візьмемо скорочену систему лишків $\pmod p$ ось таку:
$\left\{-\frac{p-1}{2}, -\frac{p-1}{2}+1, \ldots, -1, 1, 2, \ldots, \frac{p-1}{2}\right\}$.
Якщо взяти в квадрат кожне число, то буде така множина:
$\left\{1^2, 2^2, \ldots, \left(\frac{p-1}{2}\right)^2\right\}$.
Спочатку покажемо, що всі ці квадрати неконгруентні $\pmod p$.
!Припустимо, що $a^2 \equiv b^2 \pmod p$, якщо $1 \le a < b \le \frac{p-1}{2}$.
Але тоді $p \mid a^2 - b^2 = (a-b)(a+b)$, звідси $p \mid a-b$ або $p \mid a+b$.
$p \mid a-b \implies a \equiv b \pmod p$
$p \mid a+b \implies a \equiv -b \pmod p$.
У обох випадках суперечність! Це в силу того, як ми обирали a, b.
Отже, $\left\{1^2, 2^2, \ldots, \left(\frac{p-1}{2}\right)^2\right\}$ - всі неконгруентні $\pmod p$, а також ці числа належать (не скороченій, але все одно) системі лишків $\pmod p$. А це означає, що для кожного квадрата можна знайти число a з першої скороченої системи лишків, щоб $x^2 \equiv a \pmod p$. Тож це – система всіх квадратичних лишків.
Тож дійсно всього $\frac{p-1}{2}$ квадратичних лишків, а решта $\frac{p-1}{2}$ – квадратичні нелишки. ■

5.2 Символ Лежандра

Definition 5.2.1 Задано p – непарне просте число.
Символом Лежандра називають такий вираз:

$$\left(\frac{a}{p}\right) = \begin{cases} 1, & a \text{ – квадратичний лишок} \pmod p \\ -1, & a \text{ – квадратичний нелишок} \pmod p \\ 0, & p \mid a \end{cases}$$

Власне, символ Лежандра просто дає відповідь, чи буде число a квадратичним лишком $\pmod p$.

Example 5.2.2 Кілька прикладів:
$\left(\frac{2}{7}\right) = 1$, бо 2 – квадратичний лишок $\pmod 7$.
$\left(\frac{3}{7}\right) = -1$, бо 3 – квадратичний нелишок $\pmod 7$.
$\left(\frac{35}{7}\right) = 0$, просто тому що $35 \equiv 0 \pmod 7$.

Theorem 5.2.3 Критерій Ойлера
$\left(\frac{a}{p}\right) \equiv a^{\frac{p-1}{2}} \pmod p$.

Proof.
I. Випадок $a \equiv 0 \pmod p$.
Тоді ясно, що $a^{\frac{p-1}{2}} \equiv 0 \pmod p$, а також $\left(\frac{a}{p}\right) = 0$. Отже, конгруентна рівність виконана.

II. Випадок a – квадратичний лишок $\pmod p$.
Тоді існує число b, для якого $a \equiv b^2 \pmod p$. Але тоді
$a^{\frac{p-1}{2}} \equiv b^{p-1} \overset{\text{мала Th. Ферма}}{\equiv} 1 \pmod p$, а також відомо $\left(\frac{a}{p}\right) = 1$.
Малу теорему Ферма можна застосовувати, бо $\gcd(b, p) = 1$. Отже, конгруентна рівність виконана.

III. Випадок a – квадратичний нелишок $\pmod p$.
Розглянемо число $k_1 \in \{1, 2, \ldots, p-1\}$. Ми можемо знайти $l_1 \neq k_1$ (причому єдине), для якого $k_1 l_1 \equiv a \pmod p$ як розв'язок лінійного конгруентного рівняння. Вимагаємо $l_1 \neq k_1$, бо тоді буде суперечність факту, що a - квадратичний нелишок.
Розглянемо число $k_2 \in \{1, 2, \ldots, p-1\} \setminus \{k_1, l_1\}$. Аналогічно існує $l_2 \neq k_2$, для якого $k_2 l_2 \equiv a \pmod p$. Важливо зауважити, що $l_2 \notin \{k_1, l_1\}$, бо інакше порушиться єдиність розв'язку двох конгруентних рівнянь.
$\vdots$
У результаті рано чи пізно закінчимо процес, і тоді буде така картина:
$\{1, 2, \ldots, p-1\} = \{k_1, l_1\} \sqcup \{k_2, l_2\} \sqcup \cdots \sqcup \{k_{\frac{p-1}{2}}, l_{\frac{p-1}{2}}\}$. Тоді
$a^{\frac{p-1}{2}} = a \cdot a \cdots a \equiv (k_1 l_1) \cdot (k_2 l_2) \ldots (k_{\frac{p-1}{2}} l_{\frac{p-1}{2}}) = (p-1)! \overset{\text{Th. Вільсона}}{\equiv} -1 \pmod p$.

Водночас ми маємо $\left(\frac{a}{p}\right) = -1$. Отже, конгруентна рівність виконана.
Всі випадки розглянуті. ■

Remark 5.2.4 Спрведливе питання: чому ця теорема називається критерієм? Фактично кажучи, ця теорема каже про це:
a – квадратичний лишок $\pmod p \iff a^{\frac{p-1}{2}} \equiv 1 \pmod p$.
Якщо $n > 2$ – таке число, що $\gcd(a, n) = 1$, то тоді
a – квадратичний лишок $\pmod n \implies a^{\frac{\varphi(n)}{2}} \equiv 1 \pmod n$.
Проте в зворотний бік не працює. Для контрприкладу розгляньте $n = 8$ та $a = 3$ та переконайтеся, що a – не квадратичний лишок $\pmod n$.

Corollary 5.2.5 Задано a – квадратичний лишок $\pmod p$, де p – непарне просте. Тоді a – не первісний корінь $\pmod p$.

Corollary 5.2.6 Властивості
Задано p - непарне просте. Тоді:
1) Якщо $a \equiv b \pmod p$, то тоді $\left(\frac{a}{p}\right) = \left(\frac{b}{p}\right)$;
2) $\left(\frac{a}{p}\right)\left(\frac{b}{p}\right) = \left(\frac{ab}{p}\right)$;
3) $\left(\frac{a^2}{p}\right) = 1$;
4) $\left(\frac{1}{p}\right) = 1$;
5) $\left(\frac{-1}{p}\right) = \begin{cases} 1, & p \equiv 1 \pmod 4 \\ -1, & p \equiv 3 \pmod 4 \end{cases}$.
В принципі, довести неважко.

Example 5.2.7 З'ясувати, чи має розв'язок $x^2 \equiv 12 \pmod{23}$.
За критерієм Ойлера, ми маємо:
$\left(\frac{12}{23}\right) = \left(\frac{4}{23}\right)\left(\frac{3}{23}\right)$ $\boxed{=}$
Легко зауважити, що $4 \equiv 2^2 \pmod{23}$, тобто 4 - квадратичний лишок.
$\boxed{=}\left(\frac{3}{23}\right) = 3^{11} = 3^2(3^3)^3 \equiv 9 \cdot 4^3 = 9 \cdot 64 \equiv 9 \cdot 18 = 162 \equiv 1 \pmod{23}$.
Отже, $\left(\frac{12}{23}\right) = 1$, тобто 12 – квадратичний лишок, а тому рівняння $x^2 \equiv 12 \pmod{23}$ має розв'язок.

Example 5.2.8 Якщо a – квадратичний лишок $\pmod p$, де p – непарне просте, довести:

$p-a$ – квадратичний лишок $\pmod p \iff p \equiv 1 \pmod 4$.
Дійсно, $\left(\frac{p-a}{p}\right) \overset{p-a\equiv -a}{=} \left(\frac{-a}{p}\right) = \left(\frac{-1}{p}\right)\left(\frac{a}{p}\right) \overset{a- \text{ лишок}}{=} \left(\frac{-1}{p}\right)$.
Тоді $\left(\frac{p-a}{p}\right) = 1 \iff p \equiv 1 \pmod 4$.

Theorem 5.2.9 Задано p – непарне просте число. Тоді $\sum_{a=1}^{p-1} \left(\frac{a}{p}\right) = 0$.

Випливає з того факту, що кількість квадратичних лишків та нелишків однакова.

5.3 Квадратичний закон взаємності

Lemma 5.3.1 Лема Гауса
Задано p – непарне просте число та таке a, що $p \nmid a$. Позначимо n – кількість чисел зі списка $a, 2a, \ldots, \frac{p-1}{2}a$, чиї остачі при діленні на p більші за $\frac{p}{2}$. Тоді $\left(\frac{a}{p}\right) = (-1)^n$.

Proof.
Коли будемо брати остачі серед цих чисел, то ми отримаємо таку множину $\{r_1, \ldots, r_n, s_1, \ldots, s_m\}$. Тут я позначив $r_1, \ldots, r_n$ – остачі, що більші за $\frac{p}{2}$, а також $s_1, \ldots, s_m$ - остачі, що менші за $\frac{p}{2}$. Оскільки p – непарне, то це означає, що жодне число не може дати остачу рівно $\frac{p}{2}$.
Ясно, що $n + m = \frac{p-1}{2}$. Числа $p - r_1, \ldots, p - r_n, s_1, \ldots, s_m$ - такі, що менші за $\frac{p}{2}$. Покажемо, що вони всі різні.
Достатньо лише показати, що $s_j \neq p - r_i$. Бо той факт, що $s_j \neq s_i$ та $p - r_j \neq p - r_i$, цілком ясний.
!Припустимо, що $s_j = p - r_i$. Значить, $s_j + r_i \equiv 0 \pmod p$. Але ці остачі ми отримували в результаті ділення $k_1 a, k_2 a$ на число p. Тож звідси $s_j + r_i \equiv k_1 a + k_2 a \equiv 0 \pmod p$. Але за умовою, $\gcd(a, p) = 1$, а тому $k_1 + k_2 \equiv 0 \pmod p$. Суперечність! А все тому, що $1 \leq k_1, k_2 \leq \frac{p-1}{2}$, а тому звідси $2 \leq k_1 + k_2 \leq p - 1$, а конгруентних чисел $\pmod p$ нема звідти.
Отже, насправді, ці $\frac{p-1}{2}$ числа зі списку $p - r_1, \ldots, p - r_n, s_1, \ldots, s_m$ можна відсортувати та отримати список остач $1, 2, \ldots, \frac{p-1}{2}$. Перемножуючи ці числа, отримаємо:

$1 \cdot 2 \cdots \dfrac{p-1}{2} = (p-r_1)\ldots(p-r_n)s_1\ldots s_m \equiv (-1)^n r_1\ldots r_n s_1\ldots s_m \equiv$
$\equiv (-1)^n a \cdot 2a \cdots \dfrac{p-1}{2}a \pmod p.$
Але всі числа $1, 2, \ldots, \dfrac{p-1}{2}$ взаємно прості з p, а тому можна скоротити – отримаємо:
$1 \equiv (-1)^n a^{\frac{p-1}{2}} \pmod p \implies a^{\frac{p-1}{2}} \equiv (-1)^n \pmod p.$
За критерієм Ойлера, $\left(\dfrac{a}{p}\right) \equiv a^{\frac{p-1}{2}} \equiv (-1)^n \pmod p.$ ■

Lemma 5.3.2 Задано p – непарне просте та таке a, що $\gcd(a, 2p) = 1$. Тоді $\left(\dfrac{a}{p}\right) = (-1)^t$, де $t = \displaystyle\sum_{j=1}^{\frac{p-1}{2}} \left[\frac{ja}{p}\right]$.

Proof.
Ви використаємо ті самі позначення r_i, s_k, що з леми Гауса.
Маємо $ja = q_j p + t_j$, тоді $\dfrac{ja}{p} = q_j - \dfrac{t_j}{p}$. Звідси випливає, що $q_j = \left[\dfrac{ja}{p}\right]$.
Отже, $ja = \left[\dfrac{ja}{p}\right] + t_j$, де t_j - один з остач $r_1, \ldots, r_n$ або $s_1, \ldots, s_m$.
Ці числа ja ми просумуємо до $\dfrac{p-1}{2}$ - отримаємо:
$$\sum_{j=1}^{\frac{p-1}{2}} ja = p\sum_{j=1}^{\frac{p-1}{2}} \left[\frac{ja}{p}\right] + \sum_{j=1}^{\frac{p-1}{2}} t_j = p\sum_{j=1}^{\frac{p-1}{2}} \left[\frac{ja}{p}\right] + \sum_{i=1}^{n} r_i + \sum_{k=1}^{m} s_k.$$
Із леми Гауса ми пам'ятаємо, що остачі $p-r_1, \ldots, p-r_n, s_1, \ldots, s_m$ - це просто пересортовані числа $1, 2, \ldots, \dfrac{p-1}{2}$. А тому
$$\sum_{j=1}^{\frac{p-1}{2}} j = \sum_{i=1}^{n}(p-r_i) + \sum_{k=1}^{m} s_k = pn + \sum_{k=1}^{m} s_k - \sum_{i=1}^{n} r_i.$$
Перше рівняння віднімемо від другого – матимемо:
$$(a-1)\sum_{j=1}^{\frac{p-1}{2}} j = p\left(\sum_{j=1}^{\frac{p-1}{2}} \left[\frac{ja}{p}\right] - n\right) + 2\sum_{i=1}^{n} r_i = p(t-n) + 2\sum_{i=1}^{n} r_i.$$
При p – непарному простому числу сказати, що $\gcd(a, 2p) = 1$ – це теж саме, що a – непарне з умовою $\gcd(a, p) = 1$. А тому $a \equiv p \equiv 1 \pmod 2$.
Отже,
$0 \equiv t - n \pmod 2 \implies t \equiv n \pmod 2 \implies (-1)^t = (-1)^n.$
За попередньою лемою, $\left(\dfrac{a}{p}\right) = (-1)^n = (-1)^t.$ ■

Corollary 5.3.3 $\left(\frac{2}{p}\right) = (-1)^{\frac{p^2-1}{8}} = \begin{cases} 1, & p \equiv \pm 1 \pmod 8 \\ -1, & p \equiv \pm 3 \pmod 8 \end{cases}$

Remark 5.3.4 Число $\frac{p^2-1}{8} \in \mathbb{N}$, оскільки p – непарне просте.
Дійсно, p - непарне, а тому воно приймає один з виглядів $\{8k+1, 8k+3, 8k+5, 8k+7\}$. Якщо для кожного варіанта обчислити p^2-1, а потім пошукати конгруенцію $\pmod 8$, то отримаємо, що $p^2 - 1 \equiv 0 \pmod 8$.

Proof.
Скористаємось рівністю з попередньої леми, а саме:

$$(a-1)\sum_{j=1}^{\frac{p-1}{2}} j = p(t-n) + 2\sum_{i=1}^{n} r_i.$$

Зауважимо, що $\sum_{j=1}^{\frac{p-1}{2}} j = \frac{p^2-1}{8}$. Також підставимо сюди $a = 2$. Звідси випливає, що $t = \sum_{j=1}^{\frac{p-1}{2}} \left[\frac{2j}{p}\right] = 0$. Разом ми отримаємо:

$$\frac{p^2-1}{8} = (-p)n + 2\sum_{i=1}^{n} r_i \equiv n \pmod 2.$$

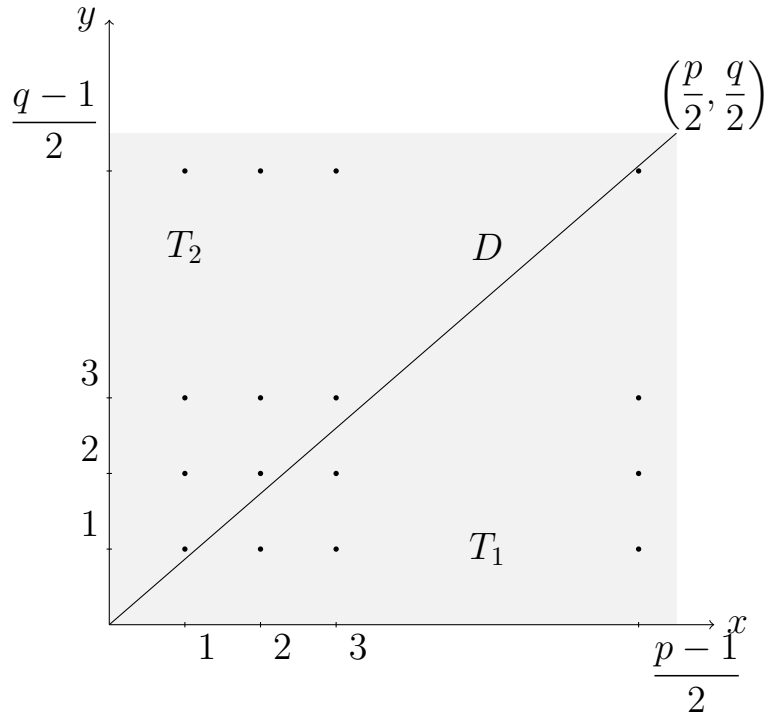
$$n \equiv \frac{p^2-1}{8} \pmod 2.$$

За лемою Гауса, $\left(\frac{2}{p}\right) = (-1)^n = (-1)^{\frac{p^2-1}{8}}$. ■

Theorem 5.3.5 Закон квадратичної взаємності
Задані p, q – різні непарні прості числа. Тоді $\left(\frac{p}{q}\right)\left(\frac{q}{p}\right) = (-1)^{\frac{p-1}{2}\frac{q-1}{2}}$.

Proof.
Ми розглянемо на площині OXY прямокутник з координатами $(0,0)$, $\left(\frac{p}{2}, 0\right)$, $\left(0, \frac{q}{2}\right)$, $\left(\frac{p}{2}, \frac{q}{2}\right)$. Позначимо R – регіон прямокутника, не включаючи її границі.
Оскільки p, q – непарні, то решітка регіона R складається з точок (m, n), де $1 \le n \le \frac{p-1}{2}$ та $1 \le m \le \frac{q-1}{2}$. Решітка – це точки з цілими коефами. Кількість таких точок $\frac{p-1}{2}\frac{q-1}{2}$.
Діагональ D даного прямокутника має рівняння $y = \frac{q}{p}x \iff py = qx$.

Але оскільки p, q - різні, тобто $\gcd(p, q) = 1$, то жодна точка з решітки не потрапить в діагональ D.
!Бо якби була така точка (x_0, y_0), що $py_0 = qx_0$, то тоді $p \mid qx_0$, але в силу того, що $\gcd(p, q) = 1$, маємо $p \mid x_0$. Проте $1 \leq x_0 \leq \dfrac{p-1}{2}$, а тому суперечність!
Зробимо ще кілька позначень:
T_1 – частина R, що лежить під діагоналлю D;
T_2 – частина R, що лежить над діагоналлю D.
Порахуємо кількість решіток в T_1 та T_2.



Оберемо $1 \leq k \leq \dfrac{p-1}{2}$. Кількість цілих чисел з інтервала $0 < y < \dfrac{kq}{p}$ всього $\left[\dfrac{kq}{p}\right]$ штук. Тобто інакше кажучи, всього $\left[\dfrac{kq}{p}\right]$ точок решітки T_1, що знаходяться над $(k, 0)$ та під діагоналлю D. Тоді загальна кількість точок решітки T_1 становить $\displaystyle\sum_{k=1}^{\frac{p-1}{2}} \left[\frac{kq}{p}\right] \overset{\text{позн.}}{=} t_1$.
Аналогічними міркуваннями можна сказати, що загальна кількість точок решітки T_2 становить $\displaystyle\sum_{j=1}^{\frac{q-1}{2}} \left[\frac{jp}{q}\right] \overset{\text{позн.}}{=} t_2$.
Власне звідси отримаємо:

$$\frac{p-1}{2}\frac{q-1}{2} = \sum_{k=1}^{\frac{p-1}{2}} \left[\frac{kq}{p}\right] + \sum_{j=1}^{\frac{q-1}{2}} \left[\frac{jq}{p}\right] = t_1 + t_2.$$

Застосувавши лему Гауса, а також всі інші наслідки, отримаємо:

$$\left(\frac{p}{q}\right)\left(\frac{q}{p}\right) = (-1)^{t_1}(-1)^{t_2} = (-1)^{t_1+t_2} = (-1)^{\frac{p-1}{2}\frac{q-1}{2}}.$$ ■

Corollary 5.3.6 Задано p, q – різні непарні прості числа. Тоді

$$\left(\frac{p}{q}\right)\left(\frac{q}{p}\right) = \begin{cases} 1, & p \equiv 1 \pmod 4 \text{ або } q \equiv 1 \pmod 4 \\ -1, & p \equiv 3 \pmod 4 \text{ та } q \equiv 3 \pmod 4 \end{cases}$$

Example 5.3.7 Обчислити $\left(\frac{-79}{101}\right)$.

Зауважимо, що $-79 \equiv 22 \pmod{101}$, тож

$$\left(\frac{-79}{101}\right) = \left(\frac{22}{101}\right) = \left(\frac{2}{101}\right)\left(\frac{11}{101}\right) \boxed{=}$$

Далі треба побачити, що $101 \equiv -3 \pmod 8$, а тому $\left(\frac{2}{101}\right) = -1$

$$\boxed{=} - \left(\frac{11}{101}\right) \boxed{=}$$

Я ще заздалегідь зауважу, що $11 \equiv 3 \pmod 4$, але $101 \equiv 3 \pmod 1$. Значить, $\left(\frac{11}{101}\right)\left(\frac{101}{11}\right) = 1$. Це суттєво спростить обчислення ось так:

$$\boxed{=} - \left(\frac{11}{101}\right) \cdot \left(\frac{11}{101}\right)\left(\frac{101}{11}\right) = - \left(\frac{101}{11}\right) = - \left(\frac{2}{11}\right) = -(-1) = 1.$$

Example 5.3.8 З'ясувати, при яких простих числах $p > 3$ число 3 буде квадратичним лишком $\pmod p$.

Перефразую питання: при яких p вираз $\left(\frac{3}{p}\right) = 1$?

Застосувавши наслідок закона квадратичної взаємності, отримаємо

$$\left(\frac{3}{p}\right) = \begin{cases} +\left(\frac{p}{3}\right), & p \equiv 1 \pmod 4 \\ -\left(\frac{p}{3}\right), & p \equiv 3 \pmod 4 \end{cases}.$$

Далі окремо $\left(\frac{p}{3}\right) = \begin{cases} 1, & p \equiv 1 \pmod 3 \\ -1, & p \equiv 2 \pmod 3 \end{cases}$ – легко перевірити окремо, коли p буде квадратичним лишком $\pmod 3$.

Тепер ми хочемо $\left(\frac{3}{p}\right) = 1$, а для цього є два сценарії:

1. $\left(\frac{3}{p}\right) = +\left(\frac{p}{3}\right) = +(+1) = 1$, це працює при $\begin{cases} p \equiv 1 \pmod 4 \\ p \equiv 1 \pmod 3 \end{cases}$.

Інакше кажучи, $p \equiv 1 \pmod{12}$, можна переконатись через китайську теорему про остачі.

2. $\left(\frac{3}{p}\right) = -\left(\frac{p}{3}\right) = -(-1) = 1$, це працює при $\begin{cases} p \equiv 3 \pmod 4 \\ p \equiv 1 \pmod 3 \end{cases}$.

Інакше кажучи, $p \equiv 11 \pmod{12}$.

Резюмуючи, $\left(\frac{3}{p}\right) = 1$ при $p \equiv \pm 1 \pmod{12}$.

Example 5.3.9 Довести, що 397 – просте число.

Нехай $p \mid 397$ – якийсь простий множник. Тоді маємо $397 \equiv 0 \pmod p$. Зауважимо, що $397 = 20^2 - 3$, а тому звідси $20^2 \equiv 3 \pmod p$, тобто $\left(\frac{3}{p}\right) = 1$. Але ця рівність можлива лише при $p \equiv 1, 11 \pmod{12}$.

Тоді звідси $p \in \{1, 11, 13\}$. Нам достатньо саме такі числа, більше не треба. Серед всіх простих чисел $11, 13$ явні кандидати. Але якщо перевірити, то $11 \nmid 397, 13 \nmid 397$, тож єдиний можливий варіант – це $p = 1$. Тобто простих дільників числа 397 ми не маємо. Отже, 397 – просте.

Remark 5.3.10 $\left(\frac{-2}{p}\right) = \begin{cases} 1, & p \equiv 1, 3 \pmod 8 \\ -1, & p \equiv 5, 7 \pmod 8 \end{cases}$.

Показати неважко, але мені це знадобиться зараз.

Theorem 5.3.11 Кількість простих чисел вигляду $8k + 3$ - нескінченна.

Proof.

!Припустимо, що $p_1, \ldots, p_n$ – лише вони прості формату $8k + 3$. Позначу $x = p_1 \ldots p_n$. Причому варто зауважити, що $x \equiv 1, 3 \pmod 8$.

Побудуємо число $N = x^2 + 2$. Маємо $N \equiv 3 \pmod 8$, ще знадобиться.

Нехай $p \mid N$, тоді $N \equiv 0 \pmod p \implies x^2 \equiv -2 \pmod p$. Тобто -2 – квадратичний лишок $\pmod p$, а тому звідси $\left(\frac{-2}{p}\right) = 1$. Проте це виконується при $p \equiv 1, 3 \pmod 8$.

Отже, якщо $p \mid N$, то обов'язково $p \equiv 1, 3 \pmod 8$. Серед цих простих чисел існує просте q, для якого якраз $q \equiv 3 \pmod 8$. Бо якби абсолютно всі прості числа були $\equiv 1 \pmod 8$, то тоді число $N \equiv 1 \pmod 8$, якщо N розкласти в добуток простих чисел, що суперечить нашій умові.

Отже, принаймні якийсь $q \equiv 3 \pmod 8$, але тоді $q = p_j$. Отже, $p_j \mid N, p_j \mid (p_1 \ldots p_n)^2 \implies p_j \mid 2 \implies p_j = 2$. Суперечність! ■

5.4 Квадратні конгруенції

Розглянемо таке конгруентне рівняння:

$$ax^2 + bx + c \equiv 0 \pmod p,$$

де p – непарне просте число та $p \nmid a$. Мета: розв'язати його.
За умовою, $\gcd(a,p)=1 \implies \gcd(4a,p)=1$, тоді маємо еквівалентне рівняння:
$4a(ax^2+bx+c) \equiv 0 \pmod{p}$
$(2ax+b)^2 \equiv b^2-4ac \pmod{p}$
Зробимо тимчасові заміни $2ax+b=y$, а також $b^2-4ac=D$ – отримаємо ось таку еквівалетну задачу:
$y^2 \equiv D \pmod{p}$

Нехай x_0 – розв'язок початкового рівняння, тоді
$(2ax_0+b)^2 \equiv b^2-4ac \pmod{p}$
$y_0^2 \equiv D \pmod{p}$
Тобто D – квадратичний лишок $\pmod{p}$.

Нехай $y^2 \equiv D \pmod{p}$ та D – квадратичний лишок. Тобто y_0 – розв'язок даного рівняння, а також $p-y_0$ буде розв'язком, причому вони неконгруентні. Неважко це показати. Тоді $2ax+b \equiv y_0 \pmod{p}$ або $2ax+b \equiv p-y_0 \pmod{p}$. У двох рівняннях розв'язок існувати буде, оскільки $\gcd(a,p)=1 \implies \gcd(2a,p)=1$.
Висновок:

Theorem 5.4.1 Задано p – непарне просте число та $p \nmid a$.
$ax^2+bx+c \equiv 0 \pmod{p}$ має розв'язок $\iff D=b^2-4ac$ – квадратичний лишок $\pmod{p}$ або $D=0$.

Example 5.4.2 Розв'язати рівняння $x^2+7x+10 \equiv 0 \pmod{11}$.
Маємо 11 – непарне просте число та $\gcd(1,11)=1$, тож спрацьовує алгоритм розв'язку вище, отримаємо еквівалентне рівняння:
$(2x+7)^2 \equiv 9 \pmod{11}$.
Заміна: $2x+7=y$, тоді отримаємо
$y^2 \equiv 9 \pmod{11}$.
Зауважимо, що $y \equiv 3 \pmod{11}$ та $y \equiv 8 \pmod{11}$ будуть розв'язками.
Тоді $\begin{bmatrix} 2x+7 \equiv 3 \pmod{11} \\ 2x+7 \equiv 8 \pmod{11} \end{bmatrix} \iff \begin{bmatrix} x \equiv 9 \pmod{11} \\ x \equiv 6 \pmod{11} \end{bmatrix}$

6 Репрезентація чисел як сума квадратів

6.1 Сума двох квадратів

Наразі порушується питання, коли можна число $n \in \mathbb{N}$ записати як суму квадратів, тобто $n = a^2 + b^2$.

Lemma 6.1.1 Задано n, m – числа, які записуються як сума двох квадратів. Тоді mn теж записується як сума двох квадратів.

Proof.
Маємо ось такі репрезентації:
$n = a^2 + b^2$
$m = c^2 + d^2$
Тоді, використавши алгебраїчні перетворення, отримаємо:
$mn = (a^2 + b^2)(c^2 + d^2) = a^2c^2 + a^2d^2 + b^2c^2 + b^2d^2 =$
$= (ac)^2 + 2acbd + (bd)^2 + (ad)^2 - 2adbc + (bc)^2 = (ac + bd)^2 + (ad - bc)^2$. ■

Lemma 6.1.2 Задано p – таке просте число, що $p \equiv 3 \pmod 4$. Відомо, що $p \mid x^2 + y^2$. Тоді $p \mid x$ та $p \mid y$.

Proof.
Маємо $p \mid x^2 + y^2$, тобто $x^2 + y^2 \equiv 0 \pmod p$, або $x^2 \equiv -y^2 \pmod p$.
!Припустимо, що умова $p \mid x$ та $p \mid y$ не виконується. Є три випадки:
I. $p \mid x$, але $p \nmid y$. Тоді ми отримаємо $0 \equiv -y^2 \pmod p$ – неможливо.
II. $p \nmid x$, але $p \mid y$ – аналогічно.
III. $p \nmid x$ та $p \nmid y$. Тоді за малою теоремою Ферма,
$1 \equiv x^{p-1} = \left(x^2\right)^{\frac{p-1}{2}} \equiv \left(-y^2\right)^{\frac{p-1}{2}} = (-1)^{\frac{p-1}{2}} y^{p-1} \equiv (-1)^{\frac{p-1}{2}} \pmod p$.
Причому оскільки $p \equiv 3 \pmod 4$, то тоді маємо $1 \equiv -1 \pmod p$, що можливо при $p = 2$, хоча $2 \not\equiv 3 \pmod 4$.
У всіх трьох випадках ми отримали суперечність! ■

Proposition 6.1.3 Задано p – таке просте число, що $p \equiv 3 \pmod 4$. Тоді p не розписується як сума двох квадратів.

Proof.
!Припустимо, що $p = a^2 + b^2$, але тут же отримаємо, що $p \mid a^2 + b^2 \implies p \mid a, p \mid b$. Тобто звідси $a = k_1 p, b = k_2 p$. Отже,
$p = p^2(k_1^2 + k_2^2) \implies 1 = p(k_1^2 + k_2^2)$.
Ясно, що така рівність неможлива, а тому суперечність! ■

Lemma 6.1.4 Лема Туе
Задано p – просте число та таке a, щоб $p \nmid a$. Тоді $ax \equiv y \pmod p$ має цілий розв'язок (x_0, y_0), причому $0 < |x_0| < \sqrt{p}$ та $0 < |y_0| < \sqrt{p}$.

Proof.
Розглянемо множину $S = \left\{ ax - y \;\middle|\; \begin{array}{l} 0 \le x \le \left[\sqrt{p}\right] \\ 0 \le y \le \left[\sqrt{p}\right] \end{array} \right\}$.
Зауважимо, що $\#S = (1 + \left[\sqrt{p}\right])^2$, причому
$\#S = (1 + \left[\sqrt{p}\right])^2 + 1 + 2\left[\sqrt{p}\right] + \left[\sqrt{p}\right]^2 > 1 + 2(\sqrt{p} - 1) + (\sqrt{p} - 1)^2 = p.$
Але за $(\mathrm{mod}\ p)$ різних чисел може бути лише p штук. Тоді за принципом Діріхле, на множині S знайдуться принаймні два елементи $ax_1 - y_1$ або $ax_2 - y_2$, що рівні за $(\mathrm{mod}\ p)$. Причому важливо, що не може виконуватися одночасно $x_1 = x_2, y_1 = y_2$.
Отже, $a(x_1 - y_1) \equiv y_1 - y_2 \pmod{p}$.
Позначимо $x_0 = x_1 - x_2$ та $y_0 = y_1 - y_2$, тоді звідси $ax_0 \equiv y_0 \pmod{p}$ – розв'язок знайшли. Причому $|x_0| < [\sqrt{p}], |y_0| < [\sqrt{p}]$, тобто
$|x_0|, |y_0| < \sqrt{p}$. Переконаємось, що неможливо мати $x_0 = 0$ або $y_0 = 0$.
!Припустимо, що $x_0 = 0$, тобто $x_1 = x_2$. Тоді $y_0 \equiv 0 \pmod{p}$, тож звідси $y_0 = 0$ – і це єдиний варіант, бо $|y_0| < \sqrt{p}$. Але тоді $y_1 = y_2$, що неможливо. Суперечність!
Аналогічно, припустивши, що $y_0 = 0$, прийдемо до суперечності, але тут ще в силу вступає умова $p \nmid a \implies \gcd(a, p) = 1$. ■

Theorem 6.1.5 Задано p – непарне просте число.
p розписується як сума двох квадратів $\iff p \equiv 1 \pmod{4}$.

Proof.
$\boxed{\Rightarrow}$ Випливає з **Prp. 6.1.3**.

$\boxed{\Leftarrow}$ Дано: $p \equiv 1 \pmod{4}$. Тобто це означає, що $\left(\dfrac{-1}{p}\right) = 1$, тобто рівняння $a^2 \equiv -1 \pmod{p}$ має розв'язок, причому $\gcd(a, p) = 1$. За лемою Туе, $ax \equiv y \pmod{p}$ має розв'язок (x_0, y_0), а тому звідси
$-x_0^2 \equiv a^2 x_0^2 = (ax_0)^2 \equiv y_0^2 \pmod{p} \implies x_0^2 + y_0^2 \equiv 0 \pmod{p}$.
Отже, $x_0^2 + y_0^2 = kp$ при $k \ge 1$. Але ми знаємо ще за Лемою Туе, що $0 < x_0^2 + y_0^2 < 2p$, а значить, $k = 1$ – єдиний варіант.
Отже, $p = x_0^2 + y_0^2$, тобто розписали як суму двох квадратів. ■

Corollary 6.1.6 Кожне просте число $p \equiv 1 \pmod{4}$ розписується як сума двох квадратів єдиним чином з точністю до перестановки доданків. Ще припускається, що $a^2 = (-a)^2$ - це один випадок.

Proof.
Залишилось, власне, довести єдиність.
!Припустимо, що є дві можливості записати число p:
$p = a^2 + b^2$
$p = c^2 + d^2$.

Тоді зауважимо, що $a^2d^2 - c^2b^2 = p(d^2 - b^2) \equiv 0 \pmod{p}$.
Тобто $(ad - cb)(ad + cb) \equiv 0 \pmod{p}$, а тому оскільки p – просте число, то звідси $\begin{bmatrix} ad \equiv cb \pmod{p} \\ ad \equiv -cb \pmod{p} \end{bmatrix}$. Але із попередньої теореми, ми знаємо, що $a, b, c, d < \sqrt{p}$, тож звідси ми маємо $\begin{bmatrix} ad - cb = 0 \\ ad + cb = p \end{bmatrix}$.
Нехай $ad = cb$, тоді $a \mid cb$, а оскільки $\gcd(a, b) = 1$, то звідси маємо $a \mid c$, тобто $c = ka$. Після цього отримаємо $d = bk$. Але тоді
$p = c^2 + d^2 = k^2(a^2 + b^2)$, а щоб була рівність, треба $k = 1$. Разом отримаємо $c = a, b = d$.
Окремо поясню, чому $\gcd(a, b) = 1$. Припустимо, що $q \mid a, q \mid b$, де q – деяке просте число. Тоді звідси $q \mid a^2 + b^2 = p$, тож або $q = 1$, або $q = p$. При $q = p$ маємо $p \mid a, p \mid b$, що не є можливим в силу того, що $p = a^2+b^2$. Тобто випадок $\gcd(a, b) > 1$ неможливий.
Нехай виконується $ad + cb = p$, тоді звідси
$p^2 = (a^2+b^2)(c^2+d^2) = (ad+bc)^2+(ac-bd)^2 = p^2+(ac-bd)^2 \implies ac = bd$.
Випадок $ac = bd$ аналогічний попередньому випадку. Теж отримаємо врешті-решт $a = c, b = d$.
У двох випадках отримали суперечність! ■

Example 6.1.7 Зокрема $p = 13$, має форму $13 = 3^2 + 2^2$.

Definition 6.1.8 Число $m \in \mathbb{Z}$ називається **вільним від квадратів** (або **безквадратним**), якщо

$$\forall n^2 : n^2 \nmid m$$

Тобто жодний квадрат числа не ділить на m.

Remark 6.1.9 Інтуїтивно кажучи, число m називається вільним від квадратів, коли під час розкладу числа m жодне число не виноситься за квадратний корінь.

Example 6.1.10 Зокрема маємо такі приклади:
10 – вільний від квадратів. Можна перевірити ручками.
8 – не вільний від квадратів, тому що, інтуїтивно кажучи, $\sqrt{8} = \sqrt{2 \cdot 4} = 2\sqrt{2}$. Тобто ми знайшли число, що можна було винести за корінь.

Remark 6.1.11 Число $m > 2$, що вільний від квадратів, зобов'язаний мати хоча б один непарний простий множник в розкладі.
Бо якщо $m = 2^k, k \geq 2$, тобто в розкладі нема непарного простого числа, то це вже не буде вільним від квадратів число, оскільки $2^2 \mid 2^k$.

Theorem 6.1.12 Задано n – таке число, що $n = N^2 m$, де m – вільне від квадратів число.
n розписується як сума двох квадратів $\iff$ m не містить простих множників $p \equiv 3 \pmod 4$.

Proof.
$\boxed{\Rightarrow}$ Дано: $n = a^2 + b^2 = N^2 m$. Розглянемо випадок $m > 2$.
Нехай $p \mid m$ – деяке непарне просте число. Якщо $\gcd(a, b) = d$, то тоді $a = dr, b = ds$, тобто звідси $d^2(r^2 + s^2) = N^2 m$, причому $\gcd(r, s) = 1$.
Оскільки m – вільне від квадратів, то $d^2 \nmid m$, а тому вимагається $d^2 \mid N^2$.
Власне, звідси
$$r^2 + s^2 = \frac{N^2}{d^2} m = tp \equiv 0 \pmod p.$$
Але оскільки $\gcd(r, s) = 1$, то тоді звідси $\begin{bmatrix} \gcd(r, p) = 1 \\ \gcd(s, p) = 1 \end{bmatrix}$. Бо в інакшому випадку ми отримаємо $\gcd(r, s) > 1$. Ми розглянемо $\gcd(r, p) = 1$, інший аналогічно.
Тоді має існувати число r', для якого $rr' \equiv 1 \pmod p$, як розв'язок лінійного рівняння. А тому
$(rr')^2 + (sr')^2 \equiv 1 + (sr')^2 \equiv 0 \pmod p \implies (sr')^2 \equiv -1 \pmod p \implies \left(\frac{-1}{p}\right) = 1$, а цей випадок можливий лише при $p \equiv 1 \pmod 4$.
Отже, $p \mid m \implies p \not\equiv 3 \pmod 4$.

$\boxed{\Leftarrow}$ Дано: при $m > 1$ маємо $m = p_1 \dots p_r$, де кожне просте $p_i = 2$ або $p_i \equiv 1 \pmod 4$. Відомо, що в кожному варіанті p_i допускає розклад на суму двох квадратів, а тому добуток $p_1 \dots p_r$ також допускає розклад на суму двох квадратів. Звідси $m = x^2 + y^2$ при деяких x, y.
Отже, $n = N^2 m = (Nx)^2 + (Ny)^2$ розклали на суму двох квадратів.
Випадок $m = 1$: маємо $n = N^2 = N^2 + 0^2$ – розклали. ■

Corollary 6.1.13 Число $n \in \mathbb{N}$ розписується як сума двох квадратів $\iff$ кожний простий множник $p \equiv 3 \pmod 4$ має парний степінь.

Example 6.1.14 Зокрема маємо:
459 не розписується як сума двох квадратів, бо $459 = 3^3 \cdot 17$, і тут число 3 має непарний степінь.
$153 = 3^2 \cdot 17$, тут 3 має парний степінь, а тому допускає розклад на суму двох квадратів. Зокрема $153 = 3^2(4^2 + 1^2) = 12^2 + 3^2$.

Remark 6.1.15 Довільне число (але не просте число $p \equiv 1 \pmod 4$), що допускає розклад, не розкладається єдиним чином.
Зокрема $25 = 3^2 + 4^2 = 5^2 + 0^2$. Або ще $745 = 27^2 + 4^2 = 24^2 + 13^2$.

Останній приклад був побудований на основі факту, що коли $a \equiv b \pmod 2$, то маємо $ab = \left(\frac{a+b}{2}\right)^2 - \left(\frac{a-b}{2}\right)^2$. Тож за бажанням можна ще погенерувати.

Theorem 6.1.16 Задано $n \in \mathbb{N}$.
n розписується як різниця двох квадратів $\iff n \not\equiv 2 \pmod 4$.

Proof.
$\boxed{\Rightarrow}$ Дано: $n = a^2 - b^2$.
Зауважимо, що $a^2 \equiv 0, 1 \pmod 4$, для всіх цілих чисел a, тоді звідси $a^2 - b^2 \equiv 0, 1, 3 \pmod 4$. Тобто не існує таких a, b, для яких $a^2 - b^2 = n \equiv 2 \pmod 4$.

$\boxed{\Leftarrow}$ Дано: $n \not\equiv 2 \pmod 4$.
Якщо $n \equiv 1, 3 \pmod 4$, то тоді $n+1, n-1$ – обидва парні числа, а значить, n розпишемо так:
$n = \left(\frac{n+1}{2}\right)^2 - \left(\frac{n-1}{2}\right)^2$.
Якщо $n \equiv 0 \pmod 4$, то тоді n розпишемо так:
$n = \left(\frac{n}{4}+1\right)^2 - \left(\frac{n}{4}-1\right)^2$. ■

Corollary 6.1.17 Непарне просте число розписується як різниця двох послідовних квадратів єдиним чином.

Proof.
Маємо $p = a^2 - b^2 = (a-b)(a+b)$. За попередньою теоремою, $a - b = 1$, а оскільки p просте, то звідси $a + b = p$. Отже, $a = \frac{p+1}{2}, b = \frac{p-1}{2}$, власне
$p = \left(\frac{p+1}{2}\right)^2 - \left(\frac{p-1}{2}\right)^2$.
Тобто задається різниця квадратів однозначно числом p. ■

Remark 6.1.18 Для інших чисел не завжди єдиним чином відбувається розклад в різницю двох квадратів. Зокрема $24 = 7^5 - 5^2 = 5^2 - 1^2$.
У загальному випадку це можна записати ось так:
$n = dd' = \left(\frac{d+d'}{2}\right)^2 - \left(\frac{d-d'}{2}\right)^2$. Тут $d \mid n$, а також $d' = \frac{n}{d}$; припускається, що вони мають однакову парність.

Example 6.1.19 Довести, що якщо n – це сума двох трикутних чисел, то тоді $4n+1$ розписується як сума двох квадартів.

Дійсно, маємо $n = \frac{m(m+1)}{2} + \frac{k(k+1)}{2}$, тоді
$4n+1 = 2m^2 + 2m + 2k^2 + 2k + 1 =$
$= m^2 + k^2 + 2km + 2m + 2k + 1 + m^2 - 2km + k^2 =$
$= (m+k+1)^2 + (m-k)^2.$

6.2 Сума більше двох квадратів

Theorem 6.2.1 Теорема Лежандра
Число k розписується як сума 3-х квадратів $\iff$ $k \neq 4^n(8m+7)$, де $m, n \geq 0$.

Proof.
$\boxed{\Rightarrow}$ Дано: k – число формата $4^n(8m+7)$. Доведемо, що k не розпишеться як сума трьох квадратів.
Спочатку доведемо, що $8m+7$ не записується як сума трьох квадратів. Дійсно, для довільного числа a маємо $a^2 \equiv 0, 1, 4 \pmod 8$, а значить, $a^2 + b^2 + c^2 \equiv 0, 1, 2, 3, 4, 5, 6 \pmod 8$, а водночас $8m + 7 \equiv 7 \pmod 8$, а тому рівність $8m + 7 = a^2 + b^2 + c^2$ при всіх a, b, c неможлива.
!Повернімось до $4^n(8m+7)$ та припустимо, що $4^n(8m+7) = a^2 + b^2 + c^2$ для деяких a, b, c. Тоді a, b, c – всі зобов'язані бути парними в силу того, що ліва частина ділиться на 4. Тобто $a = 2a_1, b = 2b_1, c = 2c_1$.
$4^{n-1}(8m+7) = a_1^2 + b_1^2 + c_1^2$.
Якщо $n - 1 \geq 1$, то повторити крок. А там ми дістанемось до рівності $8m + 7 = a_l^2 + b_l^2 + c_l^2$. Суперечність!

$\boxed{\Leftarrow}$ *в іншу сторону дуже важко, тому просто залишу це як факт.* ■

Тобто, в принципі, ми вже знаємо, коли ми можемо записати число $n = a^2 + b^2 + c^2$. Підемо далі.

Lemma 6.2.2 Лема Ейлера
Задано n, m – числа, які записуються як сума чотирьох квадратів. Тоді mn теж записується як сума чотирьох квадратів.

Proof.
Доведення не дуже чесне. Можна подивитися в пдфнику абстрактної алгебри: буде чесне доведення з використанням кватерніонів. Маємо
$n = a_1^2 + a_2^2 + a_3^2 + a_4^2$
$m = b_1^2 + b_2^2 + b_3^2 + b_4^2$.
Тоді, скориставшись не дуже очевидними алгебраїнчними перетвореннями, ми отримаємо такий величезний вираз:
$mn = (a_1b_1 + a_2b_2 + a_3b_3 + a_4b_4)^2 + (a_1b_2 - a_2b_1 + a_3b_4 - a_4b_3)^2 +$
$+ (a_1b_3 - a_2b_4 - a_3b_1 + a_4b_2)^2 + (a_1b_4 + a_2b_3 - a_3b_2 - a_4b_1)^2.$ ■

Lemma 6.2.3 Задано p – непарне просте. Тоді $x^2 + y^2 + 1 \equiv 0 \pmod{p}$ має розв'язок (x_0, y_0), причому $0 \leq x_0 \leq \frac{p-1}{2}$ та $0 \leq y_0 \leq \frac{p-1}{2}$.

Proof.
Розглянемо множину

$$S = \left\{ 1 + 0^2, 1 + 1^2, \ldots, 1 + \left(\frac{p-1}{2}\right)^2, -0^2, -1^2, \ldots, -\left(\frac{p-1}{2}\right)^2 \right\}.$$

Зауважимо, що $\#S = 2 \cdot \left(\frac{p-1}{2} + 1\right) = p + 1 > p$. Але всього p різних чисел за $\pmod{p}$. А тому за принципом Діріхлє, мають існувати різні елементи $u, v \in S$, де $u \equiv v \pmod{p}$. Є три сценарії:
1) $u = x^2$ та $v = y^2$. У нас вже $x^2 \equiv y^2 \pmod{p}$, але звідси або $x \equiv y \pmod{p}$, або $x \equiv -y \pmod{p}$ – жодний з двох варіантів неможливий, бо $0 \leq x \leq \frac{p-1}{2}$, $0 \leq y \leq \frac{p-1}{2}$
2) $u = -1 - x^2$ та $v = -1 - y^2$ – аналогічно неможливо за 1)
3) $u = x^2$ та $v = -1 - y^2$ (або навпаки). Тоді звідси $x^2 + y^2 + 1 \equiv 0$ при обмеженнях x, y. ■

Corollary 6.2.4 Задано p – непарне просте число. Тоді існує таке число $k < p$, що kp розписується як сума чотирьох квадратів.

Proof.
Дійсно, за попередньою лемою, $x^2 + y^2 + 1 \equiv 0 \pmod{p}$ має розв'язок. Тобто $x_0^2 + y_0^2 + 1^2 + 0^2 = kp$ при деякому k. Але, знаючи обмеження на x_0, y_0, отримаємо:
$kp = x_0^2 + y_0^2 + 1 < \frac{p^2}{4} + \frac{p^2}{4} + 1 < p^2$.
Отже, якщо існує k, то обов'язково $k < p$. ■

Theorem 6.2.5 Будь-яке просте число p розписується як сума чотирьох квадратів.

Proof.
Для $p = 2$ маємо $2 = 1^2 + 1^2 + 0^2 + 0^2$.
Далі розглядаємо непарні прості числа. Тоді за наслідком,
$kp = x^2 + y^2 + z^2 + w^2$, ми оберемо $k < p$, щоб k було найменшим додатним числом. Ми хочемо показати, що $k = 1$.
!Припустимо, що k – парне число, тоді w, x, y, z зобов'язані бути: або всі парні, або всі непарні, або два парних та два непарних. У такому випадку $x \equiv y \pmod{2}$ та $z \equiv w \pmod{2}$.
Отже, $\frac{1}{2}(x-y), \frac{1}{2}(x+y), \frac{1}{2}(z-w), \frac{1}{2}(z+w)$ будуть цілими числами, тоді

$$\frac{1}{2}kp = \left(\frac{x-y}{2}\right)^2 + \left(\frac{x+y}{2}\right)^2 + \left(\frac{z-w}{2}\right)^2 + \left(\frac{z+w}{2}\right)^2.$$

Тобто $\frac{k}{2}p$ є сумою чотирьох квадратів. Але k – найменше число, де kp є сумою чотирьох квадратів, а отримали $\frac{k}{2}$. Суперечність!

!Припустимо далі, що k – непарне, але $k \geq 3$. Звідси ми можемо обрати числа a, b, c, d, щоб

$a \equiv x \pmod{k}, b \equiv y \pmod{k}, c \equiv z \pmod{k}, d \equiv w \pmod{k}$

$|a| < \frac{k}{2}, |b| < \frac{k}{2}, |c| < \frac{k}{2}, |d| < \frac{k}{2}$.

На прикладі як знайшли a. Маємо $x = qk + r$. Якщо $r < \frac{k}{2}$, тоді покладемо $a = r$. Якщо $r > \frac{k}{2}$, тоді покладемо $a = r - k$. Ну й ясно, що $a \equiv x \pmod{k}$.

Із цього випливає, що

$a^2 + b^2 + c^2 + d^2 \equiv x^2 + y^2 + z^2 + w^2 \equiv 0 \pmod{k}$, тобто

$a^2 + b^2 + c^2 + d^2 = nk$ для деякого $n \geq 0$.

У силу обмежень a, b, c, d, ми отримаємо

$$0 \leq nk = a^2 + b^2 + c^2 + d^2 < 4\left(\frac{k}{2}\right)^2 = k^2 \implies 0 \leq nk < k^2.$$

Якщо $n = 0$, то тоді звідси $a = b = c = d = 0$. Як наслідок, $k \mid x, k \mid y, k \mid z, k \mid w$, тоді $k^2 \mid kp \implies k \mid p$, що неможливо, бо $1 < k < p$.

Отже, ми маємо $0 < n < k$. Зауважимо тепер, що

$k^2np = (kp)(kn) = r^2 + s^2 + t^2 + u^2$.

За першою лемою, kp, kn – суми чотирьох квадратів, а тому k^2np - також сума чотирьох квадратів. Причому

$r = xa + yb + zc + wd$

$s = xb - ya + zd - wc$

$t = xc - yd - za + wb$

$u = xd + yc - zb - wa$.

Також треба зауважити, що $k \mid r, k \mid s, k \mid t, k \mid u$. На прикладі r пояснення.

$r = xa + yb + zc + wd \equiv a^2 + b^2 + c^2 + d^2 \equiv 0 \pmod{k}$.

Таким чином, маємо

$$np = \left(\frac{r}{k}\right)^2 + \left(\frac{s}{k}\right)^2 + \left(\frac{t}{k}\right)^2 + \left(\frac{u}{k}\right)^2.$$

Кожний дріб – ціле число, але при цьому оскільки $0 < n < k$, то ми прийшли до суперечності! Знову ж таки, k - найменше число, де kp - сума чотирьох квадратів.

Із всіх варіантів лишається тільки $k = 1$. ■

Theorem 6.2.6 Теорема Лагранжа
Будь-яке натуральне число представляється як сума чотирьох квадратів. Деякі можуть бути нулями.
Зрозуміло, як доводиться.

Example 6.2.7 Розписати 459 як суму чотирьох квадратів.
Тут активно застосовується лема Ейлера.
$459 = 3^3 \cdot 17 = 3^2(1^2+1^2+1^2+0^2)(4^2+1^2+0^2+0^2) =$
$= 3^2[(4+1+0+0)^2+(1-4+0-0)^2+(0-0-4+0)^2+(0+0-1-0)^2] =$
$= 3^2(5^2+3^2+4^2+1^2) = 15^2+9^2+12^2+3^2.$

7 Досконалі числа

7.1 Вступ

Definition 7.1.1 Число n називається **досконалим**, якщо n дорівнює сумі всіх його дільників, не включаючи n.

Example 7.1.2 Зокрема 28 має дільники $1, 2, 4, 7, 14$, не включаючи самого себе. Водночас $28 = 1 + 2 + 4 + 7 + 14$.
Отже, 28 - досконале число.

Proposition 7.1.3 Число n досконале $\iff \sigma(n) = 2n$.
Вказівка: n *- досконале* $\overset{\text{def.}}{\iff} n = \sigma(n) - n$

Theorem 7.1.4 Нехай число $2^k - 1, k > 1$ - просте. Тоді $n = 2^{k-1}(2^k - 1)$ буде досконалим числом. Кожне парне досконале число має форму числа n.

Proof.
Маємо $2^k - 1 = p$ - якесь парне, а також число $n = 2^{k-1}p$. Оскільки $\gcd(2^{k-1}, p) = 1$, то звідси
$\sigma(n) = \sigma(2^{k-1})\sigma(p) = (2^k - 1)(p + 1) = (2^k - 1)2^k = 2n$.
Отже, n - досконале число.

Нехай n - парне досконале число. Тоді запишемо його як $n = 2^{k-1}m, k > 1$, де m - непарне число. В силу того, що $\gcd(2^{k-1}, m) = 1$, маємо
$\sigma(n) = \sigma(2^{k-1})\sigma(m) = (2^k - 1)\sigma(m)$.
Оскіьки за умовою $\sigma(n) = 2n$, то звідси
$2^k m = (2^k - 1)\sigma(m)$.
Із цього рівняння вимагається $2^k - 1 \mid m \implies m = (2^k - 1)M$. Отже,
$\sigma(m) = 2^k M$.
Оскільки m, M - обидва дільники числа m, маємо
$2^k M = \sigma(m) \geq m + M = 2^k M$.
Тобто $2^k M = \sigma(m) = m + M$.
Отже, m має всього лише два дільника: m, M. Значить, m зобов'язане бути простим, а число $M = 1$. Звідси $m = (2^k - 1)M = 2^k - 1$ - просте число. Остаточно, $n = (2^k - 1)2^k$. ■

Таким чином, знаходження парних досконалих чисел зводиться до знаходження простих чисел формата $2^k - 1$.

Lemma 7.1.5 Задано $a^k - 1$ - парне число, $a > 1, k > 1$.
Тоді $a = 2$, а також k - парне число.
Таке твердження вже було, але тут вона більш загальне.

Proof.
Маємо $a^k - 1 = (a-1)(a^{k-1} + \cdots + a + 1)$.
Множник $a^{k-1}+\cdots+a+1 \geq a+1 > 1$ та множник $a-1 \geq 1$. Але оскільки $a^k - 1$ - парне число, то звідси один з двох множників зобов'язаний бути рівним одиниці. Лише можливий $a - 1 = 1 \implies a = 2$.
!Припустімо, що k - складене число, тобто $k = rs$, причому беремо $r > 1, s > 1$. Тому
$a^k - 1 = (a^r)^s - 1 = (a^r - 1)(a^{r(s-1)} + \cdots + a^r + 1)$.
Кожний з множників явно більше одиниці, тобто $a^k - 1$ стане складеним числом. Суперечність! ■

Theorem 7.1.6 Задано n - парне досконале число.
Тоді n закінчується цифрою 6 або 8.

Proof.
Маємо $n = 2^{k-1}(2^k - 1)$, згідно з попередньою теоремою, де $2^k - 1$ - просте. А значить, k також просте.
При $k = 2$ маємо $n = 6$ - виконана теорема.
При $k \equiv 1 \pmod 4$ маємо
$n = 2^{4m}(2^{4m+1} - 1) = 2^{8m+1} - 2^{4m} = 2 \cdot 16^{2m} - 16^m$.
Індуктивно можна довести, що $16^t \equiv 6 \pmod{10}, t \in \mathbb{N}$. Значить,
$n \equiv 2 \cdot 6 - 6 = 6 \pmod{10}$.
При $k \equiv 3 \pmod 4$ маємо
$n = 2^{2m+2}(2^{4m+3} - 1) = 2^{8m+5} - 2^{4m+2} = 2 \cdot 16^{2m+1} - 4 \cdot 16^m$.
$n \equiv 2 \cdot 6 - 4 \cdot 6 = 8 \pmod{10}$. ■

Remark 7.1.7 Насправді, можна більш строгу теорему дати. Власне, кожне парне досконале число закінчується цифрами 6 або 28.

7.2 Трошки про числа Мерсенна

Theorem 7.2.1 Нехай p та $q = 2p + 1$ - прості числа.
Тоді або $q \mid M_p$, або виключно $q \mid M_p + 2$. Тут M_p - число Мерсенна.

Proof.
За малою теоремою Ферма, $2^{q-1} \equiv 1 \pmod q$ або
$(2^{\frac{q-1}{2}} - 1)(2^{\frac{q-1}{2}} + 1) = (2^p - 1)(2^p + 1) \equiv 0 \pmod q$.
$M_p(M_p + 2) \equiv 0 \pmod q$.
Отже, $q \mid M_p(M_p+2)$, тоді в силу простоти q, маємо $q \mid M_p$ або $q \mid M_p+2$.
Одночасно не можуть, бо тоді буде $q \mid 2$, що суперечить умові. ■

Example 7.2.2 Приклад застосування теореми полягає в наступному. Нехай $p = 23$ та $q = 2p + 1 = 47$ - вони обидва прості. Тоді або $47 \mid M_{23}$,

або $47 \mid M_{23} + 2$ - лише один варіант з двох.
Можна показати, що справді $2^{23} \equiv 1 \pmod{47}$, а тому $47 \mid M_{23}$.
А це означає, що $M_{23} = 2^{23} - 1$ - складене число.

Theorem 7.2.3 Нехай $q = 2n + 1$ - просте число. Тоді
$q \mid M_n \iff q \equiv 1$ або $7 \pmod 8$
$q \mid M_n + 2 \iff q \equiv 3$ або $5 \pmod 8$

Proof.
Доведу лише перший випадок, бо другий аналогічний.
$q \mid M_n \iff 2^n = 2^{\frac{q-1}{2}} \equiv 1 \pmod q \iff 2^{q-1} \equiv 1 \pmod q \iff$
$\iff \left(\frac{2}{q}\right) = 1 \iff q \equiv 1, 7 \pmod 8$. ■

Corollary 7.2.4 Нехай $p \equiv 3 \pmod 4$ та $q = 2p + 1$ - прості числа.
Тоді $q \mid M_p$.

Таким чином, для чисел $p \in \{11, 23, 83, 131, 179, 181, 239, 251\}$ число $q = 2p + 1$ буде також простим, а тому число M_p стане складеним.

Theorem 7.2.5 Задано p - непарне просте число.
Тоді будь-який дільник M_p є числом формата $2kp + 1$.

Proof.
Нехай q - просте число та $q \mid M_p$, тобто $2^p \equiv 1 \pmod q$.
Якщо позначити $\mathrm{ord}_q(2) = k$, то тоді $k \mid p$. Причому $k \neq 1$, бо в інакшому випадку було б $q \mid 1$.
$k \mid p$ та $k > 1$, а оскільки p - просте, то тоді $k = p$.
Також маємо $k \mid q - 1$, тобто $p \mid q - 1 \implies q = 1 + pt$.
Число t зобов'язане бути парним, бо в інакшому випадку стало б число q парним, а це вже порушує умову простоти числа q.
Таким чином, $q = 2kp + 1$. ■

Theorem 7.2.6 Задано p - непарне просте число.
Тоді будь-який простий дільник q числа M_p буде $\equiv \pm 1 \pmod 8$.

Proof.
Нехай $q = 2n + 1$ - простий дільник M_p. Позначимо число $a = 2^{\frac{p+1}{2}}$, тоді отримаємо:
$a^2 - 2 = 2^{p+1} - 2 = 2M_p \equiv 0 \pmod q$.
Піднесемо до n-ій степені - отримаємо:
$a^{2n} = a^{q-1} \equiv 2^n \pmod q$.
Оскільки q - непарне число, то тоді $\gcd(a, q) = 1$, а тому $a^{q-1} \equiv 1 \pmod q$ за Ферма. Тобто звідси $2^n \equiv 1 \pmod q \implies q \mid M_n \implies q \equiv \pm 1 \pmod 8$. ■

Theorem 7.2.7 Теорема Ейлера
Задано n - непарне доскональе число.
Тоді $n = p_1^{k_1} p_2^{2j_2} \dots p_r^{2j_r}$, де p_i - різні непарні прості числа, а також $p_1 \equiv k_1 \equiv 1 \pmod 4$.

Proof.
Маємо $n = p_1^{k_1} \dots p_r^{k_r}$ - досконале число. Тоді
$2n = \sigma(n) = \sigma(p_1^{k_1}) \dots \sigma(p_r^{k_r})$.
Раз n - непарне, то тоді $n \equiv 1, 3 \pmod 4 \implies 2n \equiv 2 \pmod 4$.
Значить, $2 \mid \sigma(n)$, але $4 \nmid \sigma(n)$.
Це означає, що (не втрачаючи загальності) $\sigma(p_1^{k_1})$ має бути парним (але не ділитись на 4), а всі решта - непарні.
Всі p_i - непарні прості в силу непарності n.
Випадок $p_i \equiv 3 \equiv -1 \pmod 4$.
$\sigma(p_i^{k_i}) = 1 + p_i + \dots + p_i^{k_i} \equiv 1 + (-1) + \dots + (-1)^{k_i} \equiv$
$$\equiv \begin{cases} 0 \pmod 4, & k_i \text{ непарне} \\ 1 \pmod 4, & k_i \text{ парне} \end{cases}.$$
Оскільки $\sigma(p_1^{k_1}) \equiv 2 \pmod 4$, то тоді звідси $p_1 \equiv 1 \pmod 4$. Бо в інакшому випадку було б $\sigma(p_1^{k_1}) \equiv 0$ або $1 \pmod 4$, що неможливо.
Коли $\sigma(p_i^{k_i}) \equiv 0 \pmod 4$ при $i = 2, \dots, r$, то отримаємо: $\sigma(p_i^{k_i})$ - парне, що неможливо. Тому обов'язково $\sigma(p_i^{k_i}) \equiv 1 \pmod 4$, а значить, k_i - парні.

Випадок $p_i \equiv 1 \pmod 4$.
$\sigma(p_i^{k_i}) = 1 + p_i + \dots + p_i^{k_i} \equiv k_i + 1 \pmod 4$.
Оскільки $\sigma(p_1^{k_1}) \equiv 2 \pmod 4$, то звідси вимагається $k_1 \equiv 1 \pmod 4$.
Для інших $\sigma(p_i^{k_i}) \equiv 1, 3 \pmod 4$, а тому $\sigma(p_i^{k_i}) \equiv 0, 2 \pmod 4$, тобто k_i все одно будуть парними. ■

Corollary 7.2.8 Задано n - непарне досконале число.
Тоді $n = p^k m^2$, де $p \nmid m, p \equiv k \equiv 1 \pmod 4$ - просте число. Також $n \equiv 1 \pmod 4$.

Proof.
Дійсно, $n = p_1^{k_1}(p_2^{j_2} \dots p_r^{j_r})^2 = p^k m^2$.
Оскільки $p \equiv 1 \pmod 4$, маємо $p^k \equiv 1 \pmod 4$. Зауважимо, що m - непарне число, тобто $m \equiv 1, 3 \pmod 4$, а значить, $m^2 \equiv 1 \pmod 4$.
Отже, $n = p^k m^2 \equiv 1 \cdot 1 = 1 \pmod 4$. ■

7.3 Трошки про числа Ферма

Theorem 7.3.1 $641 \mid F_5$. Тут F_n - число Ферма.

Proof.
Позначимо $a = 2^7$ та $b = 5$, таким чином
$1 + ab = 641$.
Можна зауважити, що
$1 + ab - b^4 = 1 + (a - b^3)b + 1 = 1 + 3b = 2^4$.
Тоді звідси випливає, що
$F_5 = 2^{2^5} + 1 = 2^{32} + 1 = 2^4a^4 + 1 = (a + ab - b^4)a^4 + 1 =$
$= (a + ab)a^4 + (1 - a^4b^4) = (1 + ab)[a^4 + (1 - ab)(1 + a^4b^2)] = 641 \cdot n.$
Отже, $641 \mid F_5$. ■

Theorem 7.3.2 $\gcd(F_m, F_n) = 1$, де $m > n \geq 0$.

Proof.
Позначимо $d = \gcd(F_m, F_n)$. Всі числа Ферма непарні, а тому d також є непарним. Позначимо $x = 2^{2^n}$ та $k = 2^{m-n}$. Тоді
$$\frac{F_m - 2}{F_n} = \frac{(2^{2^n})^{2^{m-n}} - 1}{2^{2^n} + 1} = \frac{x^k - 1}{x + 1} = x^{k-1} - x^{k-2} + \cdots - 1.$$
Таким чином, $F_n \mid F_m - 2$. Оскільки $d \mid F_n$, то тоді $d \mid F_m - 2$. Також $d \mid F_m$, а тому звідси $d \mid 2$. В силу непарності $d = 1$ - єдиний можливий варіант. ■

8 Ланцюгові дроби

8.1 Числа Фібоначчі та властивості

Відомо, що числа Фібоначчі задаються такою послідовністю:
$0, 1, 1, 2, 3, 5, 8, 13, \ldots$
Тобто $u_0 = 0, u_1 = 1, u_n = u_{n-1} + u_{n-2}, n \geq 2$.

Theorem 8.1.1 $\gcd(u_n, u_{n+1}) = 1$, причому для кожного $n \geq 1$.

Proof.
!Припустимо, що $d \mid u_n, d \mid u_{n+1}$, але при цьому $d > 1$. Тоді $d \mid u_{n+1} - u_n = u_{n-1}$. Далі $d \mid u_n - u_{n-1} = u_{n-2}$...
Продовжуючи, отримаємо $d \mid u_1 = 1$, а тому $d = 1$. Суперечність! ■

Remark 8.1.2 Можна зауважити, що $u_3 = 2, u_5 = 5, u_7 = 13, u_{11} = 89$.
Тобто коли в нас простий індекс, то число Фібоначчі також просте.
Але $u_{19} = 4181 = 37 \cdot 113$ - цей патерн не спрацьовує.

Lemma 8.1.3 $u_{m+n} = u_{m-1}u_n + u_m u_{n+1}$

Proof.
Число m зафіксуємо, доводимо за індукцією по n.
База: $n = 1$, матимемо $u_{m+1} = u_{m-1}u_1 + u_m u_2 = u_m + u_{m-1}$.
Крок: нехай для чисел до k даний вираз виконаний. Доведемо для $k+1$.
$u_{m+k} = u_{m-1}u_k + u_m u_{k+1}$
$u_{m+(k-1)} = u_{m-1}u_{k-1} + u_m u_k$
Додамо ці дві рівності:
$u_{m+k} + u_{m+(k-1)} = u_{m-1}(u_k + u_{k-1}) + u_m(u_{k+1} + u_k)$.
$u_{m+(k+1)} = u_{m-1}u_{k+1} + u_m u_{k+2}$.
МІ доведено. ■

Theorem 8.1.4 $u_m \mid u_{mn}$, причому виконано для кожного $m, n \geq 1$.

Proof.
Знову за МІ по n, а число m фіксуємо.
База: $n = 1$. Тоді $u_m \mid u_m$ - ну тут ясно.
Крок: нехай для чисел до k дана теорема виконана. Доведемо для $k+1$.
Маємо $u_{m(k+1)} = u_{mk+m} = u_{mk-1}u_m + u_{mk}u_{m+1}$.
За МІ, $u_m \mid u_{mk}$, а тому автоматично $u_m \mid u_{m(k+1)}$.
МІ доведено. ■

Lemma 8.1.5 Задано $m = qn + r$. Тоді $\gcd(u_m, u_n) = \gcd(u_r, u_n)$.

Proof.
$\gcd(u_m, u_n) = \gcd(u_{qn+r}, u_n) = \gcd(u_{qn-1}u_r + u_{qn}u_{r+1}, u_n) \boxed{=}$.
Скористаємось фактом, що $\gcd(a + c, b) = \gcd(a, b)$ при $b \mid c$.
У нашому випадку $u_n \mid u_{qn}$.
$\boxed{=} \gcd(u_{qn-1}u_r, u_n)$.
Покажемо тепер, що $\gcd(u_{qn-1}, u_n) = 1$. Позначимо тимчасово $\gcd(u_{qn-1}, u_n) = d$. Зараз маємо $d \mid u_n$, а також $u_n \mid u_{qn}$. Миттєво звідси $d \mid u_{qn}$. Але також $d \mid u_{qn-1}$. Але оскільки u_{qn-1}, u_{qn} є сусідніми членами, то звідси $\gcd(u_{qn-1}, u_{qn}) = d = 1$.
Отже, $\gcd(u_{qn-1}u_r, u_n) = \gcd(u_r, u_n)$ в силу того, що $\gcd(u_{qn-1}, u_n) = 1$.
■

Theorem 8.1.6 $\gcd(u_m, u_n) = u_d$, причому $d = \gcd(m, n)$.

Proof.
Припустимо, що $m \geq n$. Застосуємо алгоритм Евкліда:
$m = q_1 n + r_1$
$n = q_2 r_1 + r_2$
$r_1 = q_3 r_2 + r_3$
$\vdots$
$r_{n-2} = q_n r_{n-1} + r_n$
$r_{n-1} = q_{n+1} r_n$.
Причому $0 < r_n < r_{n-1} < \cdots < r_3 < r_2 < r_1 < n$. Тоді за лемою,
$\gcd(u_m, u_n) = \gcd(u_{r_1}, u_n) = \gcd(u_{r_1}, u_{r_2}) = \cdots = \gcd(u_{r_{n-1}}, u_{r_n})$.
Але оскільки $r_n \mid r_{n-1}$, то за попередньою теоремою, $u_{r_n} \mid u_{r_{n-1}}$, а тому $\gcd(u_{r_{n-1}}, u_{r_n}) = u_{r_n}$. Але водночас r_n - остання ненульова остача, тому $\gcd(m, n) = r_n$.
Разом $\gcd(u_m, u_n) = u_{\gcd(m,n)}$. ■

Corollary 8.1.7 Якщо $u_m \mid u_n$, то тоді $m \mid n$.

Corollary 8.1.8 $u_m \mid u_n \iff m \mid n$ при $m \geq 2$.

Example 8.1.9 Обчислити $\gcd(u_{16}, u_{12}) = \gcd(987, 144)$.
Застосувавши алгоритм Евкліда, отримаємо $\gcd(897, 144) = 3$, а тому звідси
$\gcd(u_{16}, u_{12}) = 3 = u_4 = u_{\gcd(16,12)}$.

Proposition 8.1.10 $u_1 + \cdots + u_n = u_{n+2} - 1$.
Вказівка: розписати від 1 *до* n *рівняння* $u_n = u_{n+2} - u_{n+1}$.

Proposition 8.1.11 $u_n^2 = u_{n+1}u_{n-1} + (-1)^{n-1}$ для чисел $n \geq 2$.

Proof.
Маємо
$u_n^2 - u_{n+1}u_{n-1} = u_n(u_{n-1} + u_{n-2}) - u_{n+1}u_{n-1} =$
$= (u_n - u_{n+1})u_{n-1} + u_n u_{n-2}$.
Знаємо, що $u_{n+1} = u_n + u_{n-1}$, а тому отримаємо
$u_n^2 - u_{n+1}u_{n-1} = (-1)(u_{n-1}^2 - u_n u_{n-2})$.
Отримали таке рекурентне співвідношення, що можна опустити до
$u_n^2 - u_{n+1}u_{n-1} = (-1)(u_{n-1}^2 - u_n u_{n-2}) = (-1)^2(u_{n-2}^2 - u_{n-1}u_{n-3}) = \dots$
$= (-1)^{n-2}(u_2^2 - u_3 u_1) = (-1)^{n-1}$. ■

Theorem 8.1.12 Будь-яке натуральне число можна записати як скінченну суму різних чисел Фібоначчі.

Proof.
Достатньо показати за МІ по $n > 2$, що кожне число $1, 2, 3, \dots, u_n - 1$ є сумою чисел із множини $\{u_1, u_2, \dots, u_{n-2}\}$ без повторень.
База: $n = 3$. Маємо лише число 1 зі списку, але $1 = u_2$.
Крок: нехай це твердження виконано для $n = k$. Тобто нехай числа $1, 2, \dots, u_k - 1$ розписані як сума різних чисел зі $\{u_1, \dots, u_{k-2}\}$.
Оберемо таке число N, щоб $u_k - 1 < N < u_{k+1}$. Це буде тіпа наступне число.
Оскільки $N - u_{k-1} < u_{k+1} - u_{k-1} = u_k$, то за індукцією, $N - u_{k-1}$ розписується як сума різних чисел зі $\{u_1, \dots, u_{k-2}\}$. Тоді число N, а як наслідок, і кожне число $1, 2, 3, \dots, u_{k+1} - 1$ розписується як сума різних чисел зі $\{u_1, \dots, u_{k-1}\}$.
МІ доведено. ■

8.2 Скінченні ланцюгові дроби

Definition 8.2.1 Скінченним лацнюговим дробом назвемо дріб такого вигляду

$$a_0 + \cfrac{1}{a_1 + \cfrac{1}{a_2 + \cfrac{1}{\ddots \cfrac{1}{a_{n-1} + \cfrac{1}{a_n}}}}},$$

де $a_0 \in \mathbb{Z}$ та $a_1, \dots, a_n \in \mathbb{N}$.
Позначення: $[a_0; a_1, a_2, \dots, a_{n-1}, a_n]$.

Remark 8.2.2 Хоча дозволяється a_i бути дійсним, навіть комплексним числом. Це зауваження буде суттєвим лише для майбутньої **Th. 8.2.11**.

Example 8.2.3 $[3;4,1,4,2] = 3 + \cfrac{1}{4 + \cfrac{1}{1 + \cfrac{1}{4 + \cfrac{1}{2}}}} = \frac{170}{53}.$

Remark 8.2.4 Будь-який скінченний ланцюговий дріб буде раціональним числом.
Вказівка: довести за MI за кількістю a_i.

Theorem 8.2.5 Будь-яке раціональне число можна записати як скінченний ланцюговий дріб.

Proof.
Маємо $\frac{a}{b} \in \mathbb{Q}$, $b > 0$. За алгоритмом Евкліда, маємо:
$a = ba_0 + r_1$
$b = r_1a_1 + r_2$
$r_1 = r_2a_2 + r_3$
$\vdots$
$r_{n-2} = r_{n-1}a_{n-1} + r_n$
$r_{n-1} = r_na_n,$
причому $0 < r_n < r_{n-1} < \cdots < r_3 < r_2 < r_1 < b$.
Зауважимо, що $a_1, \ldots, a_n$ є додатними числами, оскільки кожна остача r_k додатна. Перепишемо ці рівняння ось так:
$$\frac{a}{b} = a_0 + \frac{r_1}{b} = a_0 + \cfrac{1}{\cfrac{b}{r_1}}$$
$$\frac{b}{r_1} = a_1 + \frac{r_2}{r_1} = a_1 + \cfrac{1}{\cfrac{r_1}{r_2}}$$
$$\frac{r_1}{r_2} = a_2 + \frac{r_3}{r_2} = a_2 + \cfrac{1}{\cfrac{r_2}{r_3}}$$
$\vdots$
$$\frac{r_{n-1}}{r_n} = a_n.$$
Підставимо в перше рівняння другу рівність, а потім третю рівність тощо. В результаті отримаємо ланцюговий дріб $\frac{a}{b} = [a_0; a_1, \ldots, a_n]$. ■

Example 8.2.6 Представимо $\frac{19}{51}$ як ланцюговий дріб. Застосовуючи алгоритм Евкліда кілька разів, отримаємо:

$$\frac{19}{51} = \frac{1}{\frac{51}{19}} = \frac{1}{2+\frac{13}{19}} = \frac{1}{2+\frac{1}{\frac{19}{13}}} =$$

$$= \frac{1}{2+\frac{1}{1+\frac{6}{13}}} = \frac{1}{2+\frac{1}{1+\frac{1}{\frac{13}{6}}}} = \frac{1}{2+\frac{1}{1+\frac{1}{2+\frac{1}{6}}}}.$$

Отже, $\frac{19}{51} = [0; 2, 1, 2, 6]$.

Remark 8.2.7 Репрезентація раціонального числа на ланцюговий дріб не єдина.

Для $a_n > 1$ маємо $a_n = (a_n - 1) + 1 = (a_n - 1) + \frac{1}{1}$

Отже, $[a_0; a_1, \ldots, a_n] = [a_0; a_1, \ldots, a_n - 1, 1]$.

Для $a_n = 1$ маємо $a_{n-1} + \frac{1}{a_n} = a_{n-1} + 1$.

Отже, $[a_0; a_1, \ldots, a_{n-1}, a_n] = [a_0; a_1, \ldots, a_{n-1}, a_{n-1} + 1]$.

Таким чином, кожне раціональне число має дві репрезентації: одна з парною кількістю, друга з непарною кількістю (причому інших вже нема).

Example 8.2.8 Зокрема $\frac{19}{51} = [0; 2, 1, 2, 6] \overset{\text{або}}{=} [0; 2, 1, 2, 5, 1]$.

Example 8.2.9 Більш важливий

Запишемо $\frac{u_{n+1}}{u_n}$ як ланцюговий дріб (тут числа Фібоначчі). Нам уже відомо, що $\gcd(u_{n+1}, u_n) = 1$ завжди, а тому буде $n-1$ рівнянь в алгоритмі Евкліда

$u_{n+1} = 1 \cdot u_n + u_{n-1}$

$u_n = 1 \cdot u_{n-1} + u_{n-2}$

$\vdots$

$u_4 = 1 \cdot u_3 + u_2$

$u_3 = 2u_2$.

Таким чином, $\frac{u_{n+1}}{u_n} = [1; 1, 1, \ldots, 1, 2]$, але згідно з зауваженням про розклад, ми можемо це записати інакше:

$\frac{u_{n+1}}{u_n} = [1; 1, 1, \ldots, 1, 1, 1]$, причому тут $n + 1$ одиничок.

Нехай задано $[a_0; a_1, \ldots, a_n]$. Зробимо певні позначення:

$C_k = [a_0; a_1, \ldots, a_k], 0 \leq k \leq n$ - ланцюговий дріб, який отримали, відрізаючи розклад після a_k.

Число C_k хтось називає **k-им раціональним вкороченням** або **k-им підхідним дробом**. Англійською це називають **k-th convergent**.

Example 8.2.10 Зокрема маємо $\frac{19}{51} = [0; 2, 1, 2, 6]$, тож звідси
$C_0 = [0] = 0$
$C_1 = [0; 2] = \frac{1}{2}$
$C_2 = [0; 2, 1] = \frac{1}{3}$
$C_3 = [0; 2, 1, 2] = \frac{3}{8}$
$C_4 = [0; 2, 1, 2, 6] = \frac{19}{51}$.

Theorem 8.2.11 Задано $[a_0; a_2, \ldots, a_n]$ - ланцюговий дріб. Тоді $C_k = \frac{p_k}{q_k}$, де числа p_k, q_k задаються так:

$p_0 = a_0$	$q_0 = 1$
$p_1 = a_1 a_0 + 1$	$q_1 = a_1$
$p_k = a_k p_{k-1} + p_{k-2}$	$q_k = a_k q_{k-1} + q_{k-2}$.

Proof.
База індукції при C_0, C_1 буде неважко.
Крок індукції: нехай для $2 \leq m < n$ виконується
$C_m = [a_0; a_1, \ldots, a_{m-1}, a_m] = \frac{p_m}{q_m} = \frac{a_m p_{m-1} + p_{m-2}}{a_m q_{m-1} + q_{m-2}}$. Доведемо це твердження для C_{m+1}.
Зазначимо, що $p_{m-1}, q_{m-1}, p_{m-2}, q_{m-2}$ напряму залежать від $a_1, \ldots, a_{m-1}$, але жодним чином не залежать від a_m. Отже, в рівнянні вище ми a_m замінимо на $a_m + \frac{1}{a_{m+1}}$ - отримаємо:

$$\left[a_0; a_1, \ldots, a_{m-1}, a_m + \frac{1}{a_{m+1}}\right] = \frac{\left(a_m + \frac{1}{a_{m+1}}\right) p_{m-1} + p_{m-2}}{\left(a_m + \frac{1}{a_{m+1}}\right) q_{m-1} + q_{m-2}}.$$

$$\left[a_0; a_1, \ldots, a_{m-1}, a_m + \frac{1}{a_{m+1}}\right] = [a_0; a_1, \ldots, a_{m-1}, a_m, a_{m+1}] = C_{m+1}.$$

$$C_{m+1} = \frac{\left(a_m + \frac{1}{a_{m+1}}\right) p_{m-1} + p_{m-2}}{\left(a_m + \frac{1}{a_{m+1}}\right) q_{m-1} + q_{m-2}} = \frac{a_{m+1}(a_m p_{m-1} + p_{m-2}) + p_{m-1}}{a_{m+1}(a_m q_{m-1} + q_{m-2}) + q_{m-1}} =$$
$$= \frac{a_{m+1} p_m + p_{m-1}}{a_{m+1} q_m + q_{m-1}}.$$
MI доведено. ■

Theorem 8.2.12 Задано $[a_0; a_1, \ldots, a_n]$ - ланцюговий дріб та C_k. Тоді $p_k q_{k-1} - q_k p_{k-1} = (-1)^{k-1}$ при $1 \leq k \leq n$.

Proof.
База індукції: при $k = 1$ теж зрозуміла.
Крок індукції: нехай ця формула виконана для $1 \leq m < n$, тоді
$p_{m+1}q_m - q_{m+1}p_m = (a_{m+1}p_m + p_{m-1})q_m - (a_{m+1}q_m + q_{m-1})p_m =$
$= -(p_m q_{m-1} - q_m p_{m-1}) \overset{\text{МІ}}{=} -(-1)^{m-1} = (-1)^m$.
МІ доведено. ■

Corollary 8.2.13 $\gcd(p_k, q_k) = 1$ при $1 \leq k \leq n$.

Example 8.2.14 Розв'яжемо рівняння $172x + 20y = 1000$.
Оскільки $\gcd(172, 20) = 4$, то розв'язок є, а також $43x + 5y = 250$.
Але ми розв'яжемо таке рівняння:
$43x + 5y = 1$ (дане рівняння схоже на рівняння з **Th. 8.2.12**).
Запишемо число $\frac{43}{5}$ як ланцюговий дріб. Це буде $\frac{43}{5} = [8; 1, 1, 2]$, тоді звідси $C_0 = \frac{8}{1}, C_1 = \frac{9}{1}, C_2 = \frac{17}{2}, C_3 = \frac{43}{5}$, а тому отримаємо $p_2 = 17, q_2 = 2, p_3 = 43, q_3 = 5$. За попередньою теоремою,
$p_3 q_2 - q_3 p_2 = (-1)^{3-1}$
$43 \cdot 2 - 5 \cdot 17 = 1$
$43 \cdot 500 + 5(-4250) = 250$.
Знайшли розв'язок $x_0 = 500, y_0 = -4250$, ну а далі легко записати загальний розв'язок. Мені вже лінь.

Lemma 8.2.15 Задано $[a_0; a_1, \ldots, a_n]$ - ланцюговий дріб. Нехай q_k - знаменник C_k. Тоді $q_{k-1} \leq q_k$, причому нерівність строга при $k > 1$.

Proof.
База індукції: $k = 1$, маємо $q_0 = 1 \leq a_1 = q_1$.
Крок індукції: нехай для деякого $1 \leq m < n$ нерівність виконана. Тоді
$q_{m+1} = a_{m+1}q_m + q_{m-1} > a_{m+1}q_m \geq 1 \cdot q_m = q_m$.
МІ доведено. ■

Theorem 8.2.16 Послідовність $\{C_{2k}, k \geq 0\}$ - строго зростає. Послідовність $\{C_{2k+1}, k \geq 0\}$ - строго спадає.

Proof.
$$C_{n+2} - C_n = (C_{n+2} - C_{n+1}) + (C_{n+1} - C_n) = \left(\frac{p_{n+2}}{q_{n+2}} - \frac{p_{n+1}}{q_{n+1}}\right) + \left(\frac{p_{n+1}}{q_{n+1}} - \frac{p_n}{q_n}\right)$$
$$= \frac{(-1)^{n+1}}{q_{n+2}q_{n+1}} + \frac{(-1)^n}{q_{n+1}q_n} = \frac{(-1)^n(q_{n+2} - q_n)}{q_n q_{n+1} q_{n+2}}.$$

За щойно доведеною лемою, $q_{n+2} > q_{n+1} \geq q_n \implies q_{n+2} - q_n > 0$.
Якщо $n = 2k$, то отримаємо $C_{2k+2} - C_{2k} > 0$.
Якщо $n = 2k+1$, то отримаємо $C_{2k+3} - C_{2k} < 0$. ■

Theorem 8.2.17 $C_{2k+1} \geq C_{2m}$, для кожного $k, m \geq 0$.
Простіше кажучи, кожне непарне C_i більше за кожне парне C_j.

Proof.
$C_n - C_{n-1} = \dfrac{p_n}{q_n} - \dfrac{p_{n-1}}{q_{n-1}} = \dfrac{(-1)^{n-1}}{q_n q_{n-1}}$.
Підставивши $n = 2j$, отримаємо $C_{2j} < C_{2j-1}$. Скориставшись попередньою теоремою та щойно одержаною оцінкою, отримаємо, що
$C_{2m} < C_{2m+2k+2} < C_{2m+2k+1} < C_{2k+1}$. ■

8.3 Нескінченні ланцюгові дроби

Definition 8.3.1 Нескінченним лацнюговим дробом назвемо дріб такого вигляду

$$a_0 + \cfrac{1}{a_1 + \cfrac{1}{a_2 + \cfrac{1}{\ddots}}},$$

де $a_0 \in \mathbb{Z}$ та $a_1, a_2, \cdots \in \mathbb{N}$.
Позначення: $[a_0; a_1, a_2, \dots]$
Значення ланцюгового дробу дорівнює

$$[a_0; a_1, a_2, \dots] = \lim_{n\to\infty} C_n,$$

де $C_n = [a_0; a_1, a_2, \dots, a_n]$.

Remark 8.3.2 Аналогічно див. **Rm. 8.2.2**

Proposition 8.3.3 Коректність означення
Якщо визначені $C_n = [a_0; a_1, a_2, \dots, a_n]$, то $\lim\limits_{n\to\infty} C_n$ існує.

Proof.
Із попереднього підрозділу, маємо такі ланцюги нерівностей
$C_0 < C_2 < C_4 < \cdots < C_{2n} < C_{2n+1} < \cdots < C_5 < C_3 < C_1$.
Таким чином, послідовність $\{C_{2n}, n \geq 1\}$ не лише монотонно зростає, а ще й обмежена сверху числом C_1; послідовність $\{C_{2n+1}, n \geq 1\}$ не лише монотонно спадає, а ще й обмежена знизу числом C_0. У такому разі обидва мають границю за Вейєрштрассом.

Позначимо $\alpha = \lim\limits_{n\to\infty} C_{2n}$ та $\alpha' = \lim\limits_{n\to\infty} C_{2n+1}$. Зауважимо, що $\alpha' \le C_{2n+1}$ та $\alpha \ge C_{2n}$. Отже, маємо

$$\alpha' - \alpha \le C_{2n+1} - C_{2n} = \frac{p_{2n+1}}{q_{2n+1}} - \frac{p_{2n}}{q_{2n}} = \frac{1}{q_{2n}q_{2n+1}}.$$

А тому звідси випливає, що

$$0 \le |\alpha' - \alpha| \le \frac{1}{q_{2n}q_{2n+1}} < \frac{1}{q_{2n}^2}.$$

Зрозуміло, що q_k строго зростає, а тому й q_{2n}. Таким чином, $\forall \varepsilon > 0 : \exists N : 0 \le |\alpha' - \alpha| < \frac{1}{q_{2N}^2} < \varepsilon$. Таким чином, маємо $\alpha = \alpha'$. Звідси абсолютно всі часткові границі послідовності $\{C_n, n \ge 0\}$ дорівнюють α, а тому звідси $\lim\limits_{n\to\infty} C_n = \alpha$. ■

Example 8.3.4 Зокрема уже доводили, що $C_n = \frac{u_{n+1}}{u_n} = [1; \underbrace{1, \dots, 1}_{n \text{ разів}}]$.

Позначимо $x = \lim\limits_{n\to\infty} C_n$, тоді звідси отримаємо

$$x = \lim_{n\to\infty} \frac{u_{n+1}}{u_n} = \lim_{n\to\infty} \frac{u_n + u_{n-1}}{u_n} = 1 + \frac{1}{\lim\limits_{n\to\infty} \frac{u_n}{u_{n-1}}} = 1 + \frac{1}{x}.$$

Розв'язавши рівняння $x = 1 + \frac{1}{x}$, отримаємо додатний корінь $x = \frac{1+\sqrt{5}}{2}$.

Отже, $[1; 1, 1, 1, \dots] = \frac{1+\sqrt{5}}{2}$.

Definition 8.3.5 Періодичним нескінченним ланцюговим дробом назвемо ось це:

$$[a_0; a_1, \dots, a_m, b_1, \dots, b_n, b_1, \dots, b_n, b_1, \dots, b_n, \dots]$$

Позначення: $[a_0; a_1, \dots, a_m, \overline{b_1, \dots, b_n}]$.

$b_1, \dots, b_n$ називають тут **періодом**, а число n називають **довжиною** даного періода.

Theorem 8.3.6 $[a_0; a_1, \dots] \notin \mathbb{Q}$.

Proof.

Позначимо $x = [a_0; a_1, \dots]$.

!Припустимо, що $x \in \mathbb{Q}$, тобто $x = \frac{a}{b}$. Із попереднього твердження, $C_n \le x \le C_{n+1}$, а тому

$$0 < |x - C_n| < |C_{n+1} - C_n| = \left|\frac{p_{n+1}}{q_{n+1}} - \frac{p_n}{q_n}\right| = \frac{1}{q_n q_{n+1}}.$$

$$0 < \left|\frac{a}{b} - \frac{p_n}{q_n}\right| < \frac{1}{q_n q_{n+1}}$$

$$0 < |aq_n - bp_n| < \frac{b}{q_{n+1}}.$$

Оскільки q_k строго зростає, то знайдеться номер N, щоб $\frac{b}{q_{N+1}} < 1$, а тому $0 < |aq_n - bp_n| < 1$. Проте при $a, b, q_n, p_n \in \mathbb{Z}$ отримали суперечність! Бо в середині модуля ціле число, яке не може мати таку оцінку. ■

Theorem 8.3.7 Задані $[a_0; a_1, \dots] = [b_0; b_1, \dots]$ - два нескінченні ланцюгові дроби. Тоді $a_n = b_n, n \geq 0$.

Remark 8.3.8 Перед цим слід зазначити, що виконується рівність:
$[a_0; a_1, a_2, \dots] = a_0 + \frac{1}{[a_1; a_2, a_3, \dots]}$.

Proof.
Маємо $[a_0; a_1, a_2, \dots] = x = [b_0; b_1, b_2, \dots]$, або згідно з зауваженням,
$a_0 + \frac{1}{[a_1; a_2, \dots]} = x = b_0 + \frac{1}{[b_1; b_2, \dots]}$.
Відомо, що $C_0(a) < x < C_1(a)$, тобто $a_0 < x < a_0 + \frac{1}{a_1}$. Зважаючи, що $a_1 \geq 1$, маємо $a_0 < x < a_0 + 1$, тобто звідси $[x] = a_0$. Аналогічно при $C_0(b) < x < C_1(b)$ отримаємо $[x] = b_0$.
Таким чином, $a_0 = [x] = b_0$, а також звідси $[a_1; a_2, \dots] = [b_1; b_2, \dots]$.
А далі повторюються буквально ті самі кроки, що приводить до рівності $a_n = b_n, n \geq 0$. ■

Example 8.3.9 Знайдемо число, що є репрезентацією $x = [3; 6, \overline{1, 4}]$.
Позначимо $x = [3; 6, y]$, де $y = [\overline{1, 4}] = [\overline{1, 4}, y]$. Тоді
$y = 1 + \frac{1}{4 + \frac{1}{y}} = \frac{5y + 1}{4y + 1}$.
Отримаємо квадратне рівняння $4y^2 - 4y - 1 = 0$, що має лише корінь $y = \frac{1 + \sqrt{2}}{2}$ в силу того, що $y > 0$. Звідси маємо
$x = 3 + \frac{1}{6 + \frac{1}{y}} = \dots = \frac{14 - \sqrt{2}}{4}$.

Theorem 8.3.10 Будь-яке ірраціональне число можна розписати як нескінченний ланцюговий дріб єдиним чином.

Proof.
Маємо число $x_0 \notin \mathbb{Q}$. Ми хочемо, щоб $x_0 = [a_0; a_1, a_2, \dots]$.
Визначимо числа $a_0, a_1, \dots$ таким чином:

$a_k = [x_k]$, де $x_{k+1} = \dfrac{1}{x_k - a_k}$.
За МІ можна довести, що кожний $x_k \notin \mathbb{Q}$. А отже,
$0 < x_k - a_k = x_k - [x_k] < 1$.
Тобто $x_{k+1} = \dfrac{1}{x_k - a_k} > 1$, а звідси $a_{k+1} = [x_{k+1}] \geq 1$.
Тобто $a_0, a_1, a_2, \ldots$ - всі додатні, окрім, можливо, a_0.
Із рівності $x_{k+1} = \dfrac{1}{x_k - a_k}$ випливає, що $x_k = a_k + \dfrac{1}{x_{k+1}}$, а тому

$$x_0 = a_0 + \frac{1}{x_1} = a_0 + \frac{1}{a_1 + \dfrac{1}{x_2}} = a_0 + \frac{1}{a_1 + \dfrac{1}{a_2 + \dfrac{1}{x_3}}} = \cdots =$$

$$= [a_0; a_1, a_2, \ldots, a_n, x_{n+1}]$$

Це виконано $\forall n \geq 1$.
Зафіксуємо n. Перші $n+1$ числа C_k із ланцюгового дробу $[a_0; a_1, a_2, \ldots]$ такі самі за значенням як з дробу $[a_0; a_1, a_2, \ldots, a_n, x_{n+1}] \overset{\text{позн.}}{=} C'_{n+1}$.

$$x_0 = C'_{n+1} = [a_0; a_1, a_2, \ldots, a_n, x_{n+1}] = \frac{x_{n+1}p_n + p_{n-1}}{x_{n+1}q_n + q_{n-1}}.$$

Таким чином, отримаємо

$$x_0 - C_n = \frac{x_{n+1}p_n + p_{n-1}}{x_{n+1}q_n + q_{n-1}} - \frac{p_n}{q_n} = \frac{(-1)(p_nq_{n-1} - q_np_{n-1})}{(x_{n+1}q_n + q_{n-1})q_n} =$$

$$= \frac{(-1)^n}{(x_{n+1}q_n + q_{n-1})q_n}.$$

Враховуючи нерівність $x_{n+1} > a_{n+1}$, отримаємо:

$$|x_0 - C_n| = \frac{1}{(x_{n+1}q_n + q_{n-1})q_n} < \frac{1}{(a_{n+1}q_n + q_{n-1})q_n} = \frac{1}{q_{n+1}q_n}.$$

Знову q_n строго зростає, а тому існує $\lim\limits_{n\to\infty} C_n = [a_0; a_1, a_2, \ldots] = x_0$. ■

Corollary 8.3.11 $|x_0 - C_n| < \dfrac{1}{q_{n+1}q_n} < \dfrac{1}{q_n^2}$.

Example 8.3.12 Розпишемо число $x = \sqrt{23}$ як нескінченний ланцюговий дріб за алгоритмом вище.

$$x_0 = \sqrt{23} = 4 + (\sqrt{23} - 4) \qquad a_0 = 4$$

$$x_1 = \frac{1}{x_0 - [x_0]} = \frac{1}{\sqrt{23} - 4} = 1 + \frac{\sqrt{23} - 3}{7} \qquad a_1 = 1$$

$$x_2 = \frac{1}{x_1 - [x_1]} = \frac{7}{\sqrt{23} - 3} = 3 + \frac{\sqrt{23} - 3}{2} \qquad a_2 = 3$$

$$x_3 = \frac{1}{x_2 - [x_2]} = \frac{2}{\sqrt{23} - 3} = 1 + \frac{\sqrt{23} - 4}{7} \qquad a_3 = 1$$

$$x_4 = \frac{1}{x_3 - [x_3]} = \frac{7}{\sqrt{23} - 4} = 8 + (\sqrt{23} - 4) \qquad a_4 = 8$$

А далі зазначимо, що $x_5 = x_1$, $x_6 = x_2$ тощо, тобто ланцюговий дріб буде періодичним, а тому
$\sqrt{23} = [4; \overline{1, 3, 1, 8}]$.

Remark 8.3.13 Можна показати, що
$x \notin \mathbb{Q}$ має періодичний ланцюговий дріб $\iff$ x має формат числа $r + s\sqrt{d}$, де $r, s \in \mathbb{Q}$ та $s \neq 0$, а також d - не квадрат числа.

Example 8.3.14 Ще кілька прикладів:
$\pi = [3; 7, 15, 1, 292, \dots]$ - тут взагалі певного патерну нема;
$e = [2; 1, 2, 1, 1, 4, 1, 1, 6, 1, 1, 8, \dots]$ - нециклічний, але є патерн.

Lemma 8.3.15 Задано $C_n = \dfrac{p_n}{q_n}$, що взято від розкладу в ланцюговий дріб числа $x \notin \mathbb{Q}$. Задані також $a, b \in \mathbb{Z}$, де $1 \leq b < q_{n+1}$. Тоді
$|q_n x - p_n| \leq |bx - a|$.

Proof.
Розглянемо таку систему рівнянь:
$$\begin{cases} p_n\alpha + p_{n+1}\beta = a \\ q_n\alpha + q_{n+1}\beta = b \end{cases}.$$
Зауважимо, що $\Delta = p_n q_{n+1} - q_n p_{n+1} = (-1)^{n+1}$ - визначник коефіцієнтів. Тоді за методом Крамера, отримаємо цілий розв'язок
$\alpha = (-1)^{n+1}(aq_{n+1} - bp_{n+1}) \quad \beta = (-1)^{n+1}(bp_n - aq_n)$.
Зауважимо, що $\alpha \neq 0$. Інакше було б $aq_{n+1} = bp_{n+1}$, але оскільки $\gcd(p_{n+1}, q_{n+1}) = 1$, то звідси $q_{n+1} \mid b \implies b \geq q_{n+1}$, що суперечить.
При $\beta = 0$ нерівність в лемі виконується. Дійсно, маємо із системи рівнянь $a = p_n\alpha, b = q_n\alpha$, тоді
$|bx - a| = |\alpha||q_n x - p_n| \geq |q_n x - p_n|$.

Далі припускаємо, що $\beta \neq 0$. Покажемо, що α, β мають різні знаки.
При $\beta < 0$ рівняння $q_n\alpha = b - q_{n+1}\beta$ показує, що $q_n\alpha > 0 \implies \alpha > 0$.
При $\beta > 0$ маємо $b < q_{n+1} < \beta q_{n+1} \implies q_n\alpha = b - q_{n+1}\beta < 0 \implies \alpha < 0$.
Звідси випливає, що $q_n x - p_n$ та $q_{n+1}x - p_{n+1}$ матимуть протилежні знаки. Тому що число x зажато між C_n та C_{n+1}. Раз так, то тоді числа $\alpha(q_n x - p_n)$ та $\beta(q_{n+1}x - p_{n+1})$ матимуть один знак. Це буде суттєво в рівності $\overset{(*)}{=}$ Отже,
$|bx - a| = |(q_n\alpha + q_{n+1}\beta)x - (p_n\alpha + p_{n+1}\beta)| =$
$= |\alpha(q_n x - p_n) + \beta(q_{n+1}x - p_{n+1})| \overset{(*)}{=} |\alpha||q_n x - p_n| + |\beta||q_{n+1}x - p_{n+1}| >$
$> |\alpha||q_n x - p_n| \geq |q_n x - p_n|$. ■

Theorem 8.3.16 Нехай $1 \leq b \leq q_n$, де $b \in \mathbb{N}$. Тоді для $\dfrac{a}{b} \in \mathbb{Q}$ маємо
$$\left|x - \frac{p_n}{q_n}\right| \leq \left|x - \frac{a}{b}\right|.$$

Proof.
!Припустимо, що $\left|x - \frac{p_n}{q_n}\right| > \left|x - \frac{a}{b}\right|$. Тоді
$|q_n x - p_n| = q_n\left|x - \frac{p_n}{q_n}\right| > b\left|x - \frac{a}{b}\right| = |bx - a|$.
Але ця нерівність виконується навпаки за лемою. Суперечність! ■

По суті кажучи, дана теорема дозволяє апроксимувати ірраціональне число x до деякої точності числами C_n. При цьому кожне інше раціональне число таким же чи меншим знаменником від C_n має меншу точність.

Example 8.3.17 Зокрема зауважимо, що $\left|\pi - \frac{22}{7}\right| \approx 0.0012645$, де дріб $\frac{22}{7}$ - це число C_1 для числа π. Саме тому число π раніше заміняли часто на $\frac{22}{7}$, просто тому що будь-яке інше раціональне число з меншим або тим самим знаменником дає меншу точність.

Theorem 8.3.18 Задано $x \notin \mathbb{Q}$ та нескоротимий дріб $\frac{a}{b} \in \mathbb{Q}$ такий, що задовольняє $\left|x - \frac{a}{b}\right| < \frac{1}{2b^2}$, тоді звідси $\frac{a}{b} = C_n$ для деякого $n \geq 0$.

Proof.
!Припустимо, що $\frac{a}{b} \neq C_n$ взагалі. Знаючи, що $\{q_k, k \geq 1\}$ зростає, існує єдиний $n \in \mathbb{N}$, для якого $q_n \leq b < q_{n+1}$. Тоді за лемою,
$|q_n x - p_n| \leq |bx - a| = b\left|x - \frac{a}{b}\right| < \frac{1}{2b} \implies \left|x - \frac{p_n}{q_n}\right| < \frac{1}{2bq_n}$.
За припущенням, $bp_n - aq_n \neq 0$, тобто $1 \leq |bp_n - aq_n|$. Звідси випливає, що
$\frac{1}{bq_n} \leq \left|\frac{bp_n - aq_n}{bq_n}\right| = \left|\frac{p_n}{q_n} - \frac{a}{b}\right| \leq \left|\frac{p_n}{q_n} - x\right| + \left|x - \frac{a}{b}\right| < \frac{1}{2bq_n} + \frac{1}{2b^2}$.
Тобто звідси маємо $b < q_n$, суперечність! ■

8.4 Рівняння Пелля

Розглянемо рівняння такого вигляду:

$$x^2 - dy^2 = 1,$$

де $x, y \in \mathbb{Z}$ - невідомі; d - додатне число, що не є точним квадратом. Мета: знайти розв'язок в цілих числах.

Обґрунтую для початку обмеження на d. Але спочатку, який б ми $d \in \mathbb{Z}$

не обрали, завжди існує розв'язок $(1,0),(-1,0)$.
При $d<-1$ маємо $x^2-dy^2\geq 1$, окрім випадку $(0,0)$. Інших нема.
При $d=-1$ маємо рівняння $x^2+y^2=1$, звідти будуть розв'язки $(0,1),(0,-1)$.
При $d=n^2$ для деякого $n\in\mathbb{N}$ буде рівняння $x^2-n^2y^2=1 \implies (x-ny)(x+ny)=1$. Рівність можлива тоді й тільки тоді, коли $x+ny=x-ny=\pm 1$. Звідси випливає, що $x=\dfrac{(x+ny)+(x-ny)}{2}=\pm 1$. Тобто інших нових розв'язків не буде.
Залишається випадок $d\neq n^2$ для кожного $n\in\mathbb{N}$.

Зауважимо, що якщо знайшли розв'язок (x,y) при $x>0,y>0$, то тоді розв'язками також будуть $(\pm x,\pm y)$. Тож надалі шукаємо лише додатні розв'язки.

Theorem 8.4.1 Нехай p,q є додатними розв'язками $x^2-dy^2=1$. Тоді $\dfrac{p}{q}=C_n$, де C_n - частина нескінченного ланцюгового дробу, який має розклад числа $\sqrt{d}$.

Proof.
Ми маємо $p^2-dq^2=1$, звідси випливає, що $p>q\sqrt{d}$. Також із першого рівняння отримаємо
$$(p-q\sqrt{d})(p+q\sqrt{d})=1 \implies \frac{p}{q}-\sqrt{d}=\frac{1}{q(p+q\sqrt{d})}.$$
Значить,
$$0<\frac{p}{q}-\sqrt{d}=\frac{1}{q(p+q\sqrt{d})}<\frac{\sqrt{d}}{q(q\sqrt{d}+q\sqrt{d}}=\frac{\sqrt{d}}{2q^2\sqrt{d}}=\frac{1}{2q^2}.$$
Отже, за **Th. 8.3.18**, отримаємо, що $\dfrac{p}{q}=C_n$ для деякого $n\in\mathbb{N}$. ■

Remark 8.4.2 Зворотне твердження загалом невірне. Тобто не всі C_n від $\sqrt{d}$ дають розв'язок рівняння Пелля.

Theorem 8.4.3 Нехай $\dfrac{p}{q}=C_n$, де C_n - частина нескінченного ланцюгового дробу, який має розклад числа $\sqrt{d}$. Тоді $x=p,y=q$ будуть розв'язками $x^2-dy^2=k$, де $|k|<1+2\sqrt{d}$.

Proof.
Оскільки $\dfrac{p}{q}=C_n$ для числа $\sqrt{d}$, то звідси, за **Crl. 8.3.11**, $\left|\sqrt{d}-\dfrac{p}{q}\right|<\dfrac{1}{q^2}$, тобто $|p-q\sqrt{d}|<\dfrac{1}{q}$. Також

$$\left|p+q\sqrt{d}\right| = \left|(p-q\sqrt{d})+2q\sqrt{d}\right| < \frac{1}{q}+2q\sqrt{d} < \left(1+2\sqrt{d}\right)q.$$
Маючи це, отримаємо:
$$|k| = |p^2-dq^2| = \left|p-q\sqrt{d}\right|\left|p+q\sqrt{d}\right| < \frac{1}{q}\left(1+2\sqrt{d}\right)q = 1+2\sqrt{d}. \quad \blacksquare$$

Example 8.4.4 Випадок $d=7$. Можемо розкласти $\sqrt{7}=[2;\overline{1,1,1,4}]$, також маємо $C_0=\frac{2}{1}, C_1=\frac{3}{1}, C_2=\frac{5}{2}, C_3=\frac{8}{3},\ldots$.
Обчислюючи $p_n^2-7q_n^2$, проходячи по C_n, отримаємо, що при C_3 маємо $8^2-7\cdot 3^2=1$. Тобто $x=8, y=3$ дає додатний розв'ящок рівняння Пелля $x^2=7y^2=1$.

Theorem 8.4.5 Якщо d не є квадратом, то $\sqrt{d}=[a_0;\overline{a_1,a_2,\ldots,a_n}]$, причому $a_0=\left[\sqrt{d}\right]$ та $a_n=2a_0$.
Без доведення.

Example 8.4.6 Зокрема $\sqrt{94}=[9;\overline{1,2,3,1,1,5,1,8,1,5,1,1,3,2,1,18}]$. Цей корінь має найдовший період серед чисел $\sqrt{d}$ при $d<100$.

Період розкладу $\sqrt{d}$ надає інформацію, яка потрібна для того, щоб знайти розв'язок $x^2-dy^2=1$. Насправді, кількість розв'язків нескінченна, всі вони здобуваються через C_n для $\sqrt{d}$.

Lemma 8.4.7 Нехай $\frac{p_k}{q_k}=C_k$ від числа $\sqrt{d}$. Якщо n - це довжина періоду розкладу $\sqrt{d}$, тоді $p_{kn-1}^2-dq_{kn-1}^2=(-1)^{kn}, k\in\mathbb{N}$.

Proof.
Ланцюговий дріб $\sqrt{d}$ можна записати в вигляді
$\sqrt{d}=[a_0;a_1,a_2,\ldots,a_{kn-1},x_{kn}]$, де $x_{kn}=[2a_0;\overline{a_1,\ldots,a_{n-1},2a_0}]=a_0+\sqrt{d}$.
Можна отримати, як було в доведенні **Th. 8.2.11** (?) що
$$\sqrt{d}=\frac{x_{kn}p_{kn-1}+p_{kn-2}}{x_{kn}q_{kn-1}+q_{kn-2}}.$$
Підставимо x_{kn} та спростимо вираз - отримаємо:
$\sqrt{d}(a_0q_{kn-1}+q_{kn-2}-p_{kn-1})=a_0p_{kn-1}+p_{kn-2}-dq_{kn-1}$.
Права частина раціональне, а ліва ірраціональна, тоді для рівності вимагаємо $a_0q_{kn-1}+q_{kn-2}=p_{kn-1}$ та $a_0p_{kn-1}+p_{kn-2}=dq_{kn-1}$.
Перше рівняння помножимо на p_{kn-1} та друге на $-q_{kn-1}$, а потім їх додамо - отримаємо:
$$p_{kn-1}^2-dq_{kn-1}^2=p_{kn-1}q_{kn-2}-q_{kn-1}p_{kn-2}\overset{\textbf{Th. 8.2.12}}{=}(-1)^{kn-2}=(-1)^{kn}. \quad \blacksquare$$

Theorem 8.4.8 Нехай $\frac{p_k}{c_k}=C_k$ від числа $\sqrt{d}$ та n - довжина періоду розкладу $\sqrt{d}$.

1. Якщо n парне, тоді всі додатні розв'язки рівняння $x^2 - dy^2 = 1$ записуються як $x = p_{kn-1}, y = q_{kn-1}$.

2. Якщо n непарне, тоді всі додатні розв'язки рівняння $x^2 - dy^2 = 1$ записуються як $x = p_{2kn-1}, y = q_{2kn-1}$.

Всюди $k \in \mathbb{N}$.

Proof.
Отже, якщо (x_0, y_0) розв'язок $x^2 - dy^2 = 1$, тоді $x_0 = p_k, y_0 = q_k$ для деякого C_k. Маючи при собі лему, $x = p_{kn-1}, y = q_{kn-1}$ буде розв'язком $\iff (-1)^{kn} = 1$. ■

Example 8.4.9 Уже розв'язували рівняння $x^2 - 7y^2 = 1$, але тепер можна знайти кілька розв'язків. У силу того, що $\sqrt{7} = [2; \overline{1, 1, 1, 4}]$, маємо перші 12 шматочків ланцюгового дробу C_k, як-от:
$\frac{2}{1}, \frac{3}{1}, \frac{5}{2}, \frac{8}{3}, \frac{37}{14}, \frac{45}{17}, \frac{82}{31}, \frac{127}{48}, \frac{590}{223}, \frac{717}{271}, \frac{1307}{494}, \frac{2024}{765}$.
Число $\sqrt{7}$ має період довжини 4, тоді p_{4k-1}, q_{4k-1} мають формувати розв'язок рівняння Пелля. Наприклад, $\frac{p_3}{q_3} = \frac{8}{3}, \frac{p_7}{q_7} = \frac{127}{48}, \frac{p_{11}}{q_{11}} = \frac{2024}{765}$, а тому звідти отримаємо розв'язки $(8, 3), (127, 48), (2024, 765)$. Тощо.

Definition 8.4.10 Фундаментальним розв'язком рівняння Пелля $x^2 - dy^2 = 1$ називають найменший додатний розв'язок (x_0, y_0).

Remark 8.4.11 За доведеною теоремою, отримаємо фундаментальні розв'язки:
$x = p_{n-1}, y = q_{n-1}$ при n парне;
$x = p_{2n-1}, y = q_{2n-1}$ при n непарне.
Значить, рівняння $x^2 - dy^2 = 1$ можна розв'язати за n або $2n$ кроків.

Remark 8.4.12 Шукати фундаментальні розв'язки не завжди легко. Зокрема рівняння $x^2 - 991y^2 = 1$ має відносно мале число $d = 991$, але фундаментальний розв'язок такий:
$x = 379\,516\,400\,906\,811\,930\,638\,014\,896\,080$
$y = 12\,055\,735\,790\,331\,359\,447\,442\,538\,767$.

Remark 8.4.13 Може навіть таке статися, що, змінивши d на чуток, фундаментальний розв'язок може бути божевільним.
$x^2 - 60y^2 = 1$ адекватне, $x = 31, y = 4$.
$x^2 - 61y^2 = 1$ неадекватне, $x = 17\,663\,319\,049, y = 226\,153\,980$.
$x^2 - 62y^2 = 1$ адекватне, $x = 63, y = 8$.
Хоча у числа $\sqrt{d}$, де $d \in \{60, 61, 62\}$, період не дуже великий, але таке теж буває.

Theorem 8.4.14 Нехай (x_1, y_1) - фундаментальний розв'язок $x^2 - dy^2 = 1$. Якщо $(x_n.y_n)$ задається за умовою $x_n + y_n\sqrt{d} = \left(x_1 + y_1\sqrt{d}\right)^n$, то тоді (x_n, y_n) також додатний розв'язок.

Proof.
Зауважимо, що $x_n - y_n\sqrt{d} = \left(x_1 - y_1\sqrt{d}\right)^n$. Тоді
$x_n^2 - dy_n^2 = \left(x_n + y_n\sqrt{d}\right)\left(x_n - y_n\sqrt{d}\right) = \left(x_1 + y_1\sqrt{d}\right)^n \left(x_1 - y_1\sqrt{d}\right)^n = (x_1^2 - dy_1^2)^n = 1$.
Отже, (x_n, y_n) - розв'язок. Чому додатний, тут ясно. ■

Theorem 8.4.15 Нехай (x_1, y_1) - фундаментальний розв'язок $x^2 - dy^2 = 1$. Якщо $(x_n.y_n)$ додатний розв'язок, то вони визначаються за умовою $x_n + y_n\sqrt{d} = \left(x_1 + y_1\sqrt{d}\right)^n$.

Proof.
!Припустимо, що (u, v) додатний розв'язок, що не задовольняє формулі. Оскільки $x_1 + y_1\sqrt{d} > 1$, тоді $\left(x_1 + y_1\sqrt{d}\right)^n$ зростає постійно, тобто це означає (також в силу припущення), що
$\left(x_1 + y_1\sqrt{d}\right)^n < u + v\sqrt{d} < \left(x_1 + y_1\sqrt{d}\right)^{n+1}$.
$x_n + y_n\sqrt{d} < u + v\sqrt{d} < \left(x_n + y_n\sqrt{d}\right)\left(x_1 + y_1\sqrt{d}\right)$.
Помножимо на $x_n - y_n\sqrt{d}$, що є додатним.
$1 < \left(x_n - y_n\sqrt{d}\right)\left(u + v\sqrt{d}\right) < x_1 + y_1\sqrt{d}$.
Визначимо числа r, s через рівняння $r + s\sqrt{d} = \left(x_n - y_n\sqrt{d}\right)\left(u + v\sqrt{d}\right)$.
Тобто це означає, що $r = x_n u - y_n v d$ та $s = x_n v - y_n u$. Як наслідок,
$r^2 - ds^2 = (x_n^2 - dy_n^2)(u^2 - dv^2) = 1$.
Отже, (r, s) - розв'язок $x^2 - dy^2 = 1$, причому $1 < r + s\sqrt{d} < x_1 + y_1\sqrt{d}$.
Оскільки $1 < r + s\sqrt{d}$, тоді $0 < r - s\sqrt{d} < 1$, тому
$2r = \left(r + s\sqrt{d}\right) + \left(r - s\sqrt{d}\right) > 1 + 0 > 0$
$s\sqrt{d} = \left(r + s\sqrt{d}\right) - \left(r - s\sqrt{d}\right) > 1 - 1 = 0$.
Тобто (r, s) - додатний розв'язок. Але оскільки (x_1, y_1) фундаментальний розв'язок, то тоді $x_1 < r, y_1 < s \implies x_1 + y_1\sqrt{d} < r + s\sqrt{d}$. Суперечність!
■

Відкриті задачі теорії чисел

Станом на 2 квітня 2024 р.маємо такі відкриті задачі:

1. **Гіпотеза Гольдбаха.** Будь-яке парне число $n \geq 4$ записується як сума двох простих чисел.

2. Уже відомо, що якщо $\sigma(n) = 2n + 1$, то тоді n непарне та є квадратом деякого числа. Але невідомо, яке конкретне число n можна підібрати (бо рапотом їх нема).

3. Кількість чисел-близнюків нескінченна. Числа-близнюки - пара простих чисел $(p, p + 2)$.

4. Існує арифметична прогресія простих чисел довільної довжини.

5. Чи кількість досконалих чисел нескінченна?

6. Чи кількість простих чисел Ферма нескінченна?