Дефиниција: Природан број $p > 1$ је **прост** ако су му једини делиоци 1 и p.

Коментар: Сваки природан број $n \geq 2$ је или прост или производ простих.

Теорема: Постоји бесконачно много простих бројева.

Доказ: Нек, постоји коначно много простих бројева и нека су $p_1, p_2, \dots, p_n$ **сви** прости бројеви.

Посматрајмо $n = p_1 \cdot p_2 \cdot \dots \cdot p_n + 1$; и је или прост или производ простих.

1° $n > p_1 \cdot p_2 \cdot \dots \cdot p_n \geq p_i$ за $1 \leq i \leq n$.

па n није прост јер је веће од свих простих бројева $(p_1, \dots, p_n)$.

2° Дакле, n је производ простих и нека је p неки његов прост чинилац: $p \mid n$.

Како су $p_1, \dots, p_n$ сви прости бројеви, $p = p_i$ за неко $1 \leq i \leq n$: $p \mid p_1 \cdot p_2 \cdot \dots \cdot p_n$

Дакле, $p \mid n - p_1 p_2 \dots p_n = 1$, па $p = 1$ ↯ (1)

Теорема: Нека је p прост број.

(1) Ако $p \mid ab$, онда $p \mid a$ или $p \mid b$.

(2) Ако $p \mid a_1 \dots a_n$, онда $p \mid a_i$ за неко $1 \leq i \leq n$.

Доказ: (1) Нека је p прост и $p \mid ab$. Нека $p \nmid a$.

Тада $(p, a) = 1$: Делиоци од p су 1 и p, па заједнички делиоци од p и a су $\in \{1, p\}$

Како $p \nmid a$, то p није заједнички делилац, па 1 је једини заједнички делилац за p и a.

Дакле, $(p, a) = 1$.

Како $p \mid ab$ и $(p, a) = 1$, па $p \mid b$

(2) Нека $p \mid a_1 a_2 \cdot \ldots \cdot a_n$.

Према (1) ако $p \nmid a_1$, онда $p \mid a_2 a_3 \ldots a_n$.

-//- ако $p \nmid a_2$, онда $p \mid a_3 \cdot \ldots \cdot a_n$.

итд. ... ако $p \nmid a_{n-2}$, онда $p \mid a_{n-1} \cdot a_n$.

Према (1) $p \mid a_{n-1}$ или $p \mid a_n$. ∎

Теорема (Основна т. аритметике): Сваки природан број $n \geq 2$ записује се на јединствен (до на редослед чинилаца) начин као производ простих.

$36 = 2 \cdot 2 \cdot 3 \cdot 3 = 2 \cdot 3 \cdot 2 \cdot 3 = 2 \cdot 3 \cdot 3 \cdot 2 = \ldots$

У сваком производу фигуришу две 2 и две 3.

Доказ: Према претходној теореми сваки број $n \geq 2$ има (бар један) прост делилац.

Докажимо јединственост.

Нека $n = p_1^{\alpha_1} \cdot p_2^{\alpha_2} \cdot \ldots \cdot p_m^{\alpha_m} = q_1^{\beta_1} q_2^{\beta_2} \cdot \ldots \cdot q_k^{\beta_k}$ (*), где

- $p_1, p_2, \ldots, p_m, q_1, q_2, \ldots, q_k$ су прости
- $p_1 < p_2 < \ldots < p_m$ и $q_1 < q_2 < \ldots < q_k$.
- $\alpha_1, \ldots, \alpha_m, \beta_1, \ldots, \beta_k \geq 1$.

Нпр. доказујемо $\{p_1, p_2, \ldots, p_m\} = \{q_1, q_2, \ldots, q_k\}$:

⊆ фиксирајмо $1 \leq i \leq m$; треба: $p_i \in \{q_1, q_2, \ldots, q_k\}$.

Како p_i дели леву страну у (*), то p_i дели и десну страну, тј. $p_i \mid q_j$ за неко $1 \leq j \leq k$ према горњем. Међутим пошто p_i прост.

Како p_i и q_j прости, одавде следи $p_i = q_j$.

Дакле, $p_i \in \{q_1, q_2, \ldots, q_k\}$.

⊇ Симетрично.

Дакле, $m = k$, $p_1 = q_1$, $p_2 = q_2$, ..., $p_m = q_m$.

Добиваме (*): $n = p_1^{\alpha_1} \cdot p_2^{\alpha_2} \cdot \ldots \cdot p_m^{\alpha_m} = p_1^{\beta_1} \cdot p_2^{\beta_2} \cdot \ldots \cdot p_m^{\beta_m}$

$\alpha_1 = \beta_1$: Нека $\exists$ нпр. $\alpha_1 \le \beta_1$ (само $\beta_1 \le \alpha_1$ можемо да замениме леву и десну страну у (*))

Поделимо (*) са $p_1^{\alpha_1}$:

$$p_2^{\alpha_2} \cdot \ldots \cdot p_m^{\alpha_m} = p_1^{\beta_1 - \alpha_1} \cdot p_2^{\beta_2} \cdot \ldots \cdot p_m^{\beta_m}, \text{ где } \beta_1 - \alpha_1 \ge 0.$$

Ако $\beta_1 - \alpha_1 > 0$, онда p_1 дели десну страну, па дели и леву страну, тј. $p_1 \mid p_i$ за неко $2 \le i \le m$ према претх. тврђењу. Даље, $p_1 = p_i$ и $(p_1 < p_2 < \ldots)$

Даље, $\beta_1 - \alpha_1 = 0$, тј. $\beta_1 = \alpha_1$.

Слично, $\beta_2 = \alpha_2, \ldots, \beta_m = \alpha_m$. (!!)

Дефиниција: Нека је $m \ge 2$. На $\mathbb{Z}$ дефинишемо сада релацију $\equiv_m$: $a \equiv_m b$ ако $m \mid a - b$.

Напомена: Ако $a = mq_1 + r_1$, $0 \le r_1 < m$

$b = mq_2 + r_2$, $0 \le r_2 < m$

Тада $\boxed{-m < r_1 - r_2 < m.}$

Даље, $a \equiv_m b$ ако $m \mid a - b$ ако $m \mid m(q_1 - q_2) + (r_1 - r_2)$

ако $m \mid r_1 - r_2$ ако $r_1 - r_2 = 0$ ако $r_1 = r_2$.

Тврђење: Нека $a \equiv_m b$ и $a' \equiv_m b'$. Тада:

(1) $a + a' \equiv_m b + b'$ (2) $a \cdot a' \equiv_m b \cdot b'$

(3) $(\forall k \ge 0)\ a^k \equiv_m b^k$

(4) Ако је $P(x)$ полином са целобројним коеф, онда $P(a) \equiv_m P(b)$.

Доказ: (1) $(a + a') - (b + b') = \underbrace{(a - b)}_{m \mid} + \underbrace{(a' - b')}_{m \mid}$

$m \mid (a + a') - (b + b')$, тј. $a + a' \equiv_m b + b'$.

(2) $aa' - bb' = aa' - ab' + ab' - bb'$

$= a\underbrace{(a'-b')}_{m\mid} + \underbrace{(a-b)}_{m\mid}b'$

$m \mid aa'-bb'$, тј. $aa' \equiv_m bb'$.

(3) За $\boxed{n=0}$ $a^0 = 1 = b^0$, па $a^0 \equiv_m b^0$ здр (P).

Нек $a^k \equiv_m b^k$, тада

$a^{k+1} = a^k \cdot a \equiv_m b^k \cdot b = b^{k+1}$, па

индукцијом добијамо $(\forall k \geq 0)\ a^k \equiv_m b^k$.

(4) Нека $P(X) = c_n X^n + c_{n-1}X^{n-1} + \dots + c_1 X + c_0$, $c_0, \dots, c_n \in \mathbb{Z}$

$P(a) = c_n \cdot a^n + c_{n-1} \cdot a^{n-1} + \dots + c_1 \cdot a + c_0$

$\equiv_m c_n \cdot b^n + c_{n-1} \cdot b^{n-1} + \dots + c_1 \cdot b + c_0 = P(b)$ ■

Примене: (1) $3 \mid \overline{a_n a_{n-1} \dots a_1 a_0}$ акко $3 \mid a_n + a_{n-1} + \dots + a_1 + a_0$

$3 \mid \overline{a_n a_{n-1} \dots a_1 a_0}$ акко $3 \mid a_n \cdot 10^n + a_{n-1} \cdot 10^{n-1} + \dots + a_1 \cdot 10 + a_0$

$10 \equiv_3 1$ ⟶ акко $a_n \cdot 10^n + a_{n-1} \cdot 10^{n-1} + \dots + a_1 \cdot 10 + a_0 \equiv_3 0$

акко $a_n \cdot 1^n + a_{n-1} \cdot 1^{n-1} + \dots + a_1 \cdot 1 + a_0 \equiv_3 0$

акко $a_n + a_{n-1} + \dots + a_1 + a_0 \equiv_3 0$

акко $3 \mid a_n + a_{n-1} + \dots + a_1 + a_0$

(2) $11 \mid \overline{a_n a_{n-1} \dots a_1 a_0}$ акко $11 \mid a_0 - a_1 + a_2 - a_3 + \dots + (-1)^n a_n$

нпр. $11 \mid \overline{1\,4\,1\,9}$ јер $11 \mid 1 - 4 + 1 - 9 = -11$

$11 \mid \overline{a_n a_{n-1} \dots a_1 a_0}$ акко $a_n \cdot 10^n + a_{n-1} \cdot 10^{n-1} + \dots + a_1 \cdot 10 + a_0 \equiv_{11} 0$

$10 \equiv_{11} -1$ акко $a_n \cdot (-1)^n + a_{n-1} \cdot (-1)^{n-1} + \dots + a_1 \cdot (-1) + a_0 \equiv_{11} 0$

акко $11 \mid a_0 - a_1 + a_2 - a_3 + \dots + (-1)^n$

(3) Наћи остатак при дељењу 5^{2020} са 7.

$5 \equiv_7 5 \equiv_7 -2$, $5^2 \equiv_7 -3$, $5^3 \equiv_7 5 \cdot 5^2 \equiv_7 (-2)\cdot(-3) \equiv_7 6 \equiv_7 -1$

$5^6 \equiv_7 5^3 \cdot 5^3 \equiv_7 (-1)\cdot(-1) \equiv_7 1$

$2020 : 6 = 336$

18

22

18

40

36

4

$2020 = 6 \cdot 336 + 4$

$5^{2020} = 5^{6 \cdot 336 + 4} = (5^6)^{336} \cdot 5^4 = (5^6)^{336} \cdot 5^2 \cdot 5^2$

$\equiv_7 1^{336} \cdot (-2) \cdot (-2) \equiv_7 4$; остатък при делене с 4.

Твърдение: (1) Ако $ab \equiv_m ac$ и $(a, m) = 1$, тогава $b \equiv_m c$.

(2) Ако $aa' \equiv_m bb'$, $a \equiv_m b$ и $(a, m) = 1$, тогава $a' \equiv_m b'$.

Доказ: (1) $ab \equiv_m ac$ означава $m \mid a(b-c)$

тъй като $(m, a) = 1$, то $m \mid b - c$, т.е. $b \equiv_m c$.

(2) $aa' \equiv_m bb' \underset{a \equiv_m b}{\equiv_m} ab'$, от пункт (1) $a' \equiv_m b'$. ■

Пример: Да се намери общото р.ш. на $ax \equiv_m b$.

$ax \equiv_m b$ има решение ако $(\exists x) \quad m \mid ax - b$

ако $(\exists xy) \quad ax - b = m \cdot (-y)$

ако $(\exists xy) \quad ax + my = b$

ако Диоф. ур. $ax + my = b$ има реш.

ако $(a, m) \mid b$.

Нека $d := (a, m) \mid b$, т.е. $ax \equiv_m b$ има решение.

Х.т. решение $ax \equiv_m b$ ако (x, y) реш. $ax + my = b$

за някое y

Нека x_0 е някое решение т.ке $ax \equiv_m b$

нека y_0 т.ч. (x_0, y_0) реш. $ax + my = b$

Общо решение т.ке $ax + my = b$ е $\boxed{\begin{array}{l} x = x_0 + \frac{m}{d} t \\ y = y_0 - \frac{a}{d} t, \quad t \in \mathbb{Z} \end{array}}$

Общо решение $ax \equiv_m b$ е $\boxed{x = x_0 + \frac{m}{d} t, \quad t \in \mathbb{Z}}$

Ако $d=(m,a)=1$, онда $\boxed{x = x_0 + mt \;,\; t\in\mathbb{Z}}$

Задатак: Нека $(n-1)! \equiv_n -1$. Доказати да је n прост.

Тада $n \mid (n-1)!+1$, тј. $(n-1)!+1 = n\cdot k$

$(-1)\cdot(n-1)! + k\cdot n = 1$, па $x\cdot(n-1)! + y\cdot n = 1$ има реш.

па $((n-1)!, n) \mid 1$, тј. $((n-1)!, n) = 1$.

тј. $(1\cdot 2\cdot 3\cdot \ldots \cdot (n-1), n) = 1$.

Ако n није прост, нека је p неки прост делилац па $1 < p < n$, па $p \mid 1\cdot 2\cdot 3\cdot\ldots\cdot(n-1)$ и $p \mid n$.

Одавде $(1\cdot 2\cdot\ldots\cdot(n-1), n) \geq p > 1$ ↯.

Дакле, n је прост.

Теорема (Вилсонова т.): Број $p \geq 2$ је прост онда и само онда

$(p-1)! \equiv_p -1$.

Доказ: $\Leftarrow$ доказано у задатку

$\Rightarrow$ Нека је $p \geq 2$ прост број.

$\boxed{p=2}$ $(2-1)! = 1 \equiv_2 -1$

$\boxed{p=3}$ $(3-1)! = 2 \equiv_3 -1$

$\boxed{p \geq 5}$ Нека је $S = \{2, 3, \ldots, p-2\}$ ← Биће паран број тј. $p-3 = 2\cdot k$

Лема: За сваки $a \in S$, једн. $ax \equiv_p 1$ има јединствено решење у скупу S и то решење је различито од a.

Доказ леме: 1° Како $1 < a < p$ и p прост број, онда $(a,p) = 1$, па онда $(a,p) \mid 1$ тј. једн. $ax \equiv_p 1$ има решења. Штавише, ако је x_1 неко решење, сва решења су дата фор. ком.

$\boxed{x = x_1 + p\cdot t \;,\; t\in\mathbb{Z}}$ ←

2° Претпоставимо $x_1 = p\cdot q + x_0 \quad 0 \leq x_0 < p$.

онда $x_0 = x_1 + p\cdot(-q)$ је решење $ax \equiv_p 1$

Претпоставимо $x_0 \in S$. Како $0 \le x_0 < p$ треба да буде $x_0 \neq 0$, $x_0 \neq 1$ и $x_0 \neq p-1$.

$x_0 = 0$: $a x_0 \equiv_p 1$, тј. $a \cdot 0 \equiv_p 1$, тј. $0 \equiv_p 1$ ↯

$x_0 = 1$: $a x_0 \equiv_p 1$, тј. $a \cdot 1 \equiv_p 1$, тј. $p \mid a-1$

$2 \le a \le p-2 \quad / -1$

$1 \le a-1 \le p-3$ па $p \nmid a-1$, ↯

$x_0 = p-1$: $a(p-1) \equiv_p 1$, тј. $-a \equiv_p 1$, тј. $p \mid a+1$

$2 \le a \le p-2 \quad / +1$

$3 \le a+1 \le p-1$, па $p \nmid a+1$, ↯

Дакле, $x_0 \in S$.

3° Како је x_0 једно решење $a x \equiv_p 1$, онда су сва решења дата са $\boxed{x = x_0 + p \cdot t,\ t \in \mathbb{Z}}$

Сетимо се $0 \le x_0 < p$

за $t \ge 1$, онда $p \cdot t \ge p$

$p \le x_0 + pt$, тј. $x_0 + pt \notin S$

за $t \le -1$, онда $p \cdot t \le -p$

$x_0 + p \cdot t < p + (-p) = 0$, $x_0 + pt \notin S$

Дакле, једино за $t = 0$, $x_0 + 0 \cdot p = x_0 \in S$.

4° $a \neq x_0$: Ако $x_0 = a$, $a \cdot a \equiv_p 1$ тј. $p \mid a^2 - 1$

$p \mid (a-1)(a+1)$ па $p \mid a-1$ или $p \mid a+1$

$1 \le a-1 \le p-1$ и $3 \le a+1 \le p-1$, па $p \nmid a-1$ и $p \nmid a+1$ ↯

Дакле $x_0 \neq a$ ✓ лема

Означимо са a^* решење ј.не $a x \equiv_p 1$ у S, за $a \in S$.

тј. $a a^* \equiv_p 1$; $a \neq a^*$

Тада $(a^*)^* = a$ јер $a^* (a^*)^* \equiv_p 1$ и $a^* a \equiv_p 1$

и решење ј.не $a^* x \equiv_p 1$ је једнозначно у S

Дакле, $S = \{2, 3, \dots, p-2\} = \{a_1, a_1^*, a_2, a_2^*, a_3, a_3^*, \dots, a_n, a_n^*\}$

$(p-1)! = 1 \cdot 2 \cdot 3 \cdot \dots \cdot (p-2) \cdot (p-1) =$

$= 1 \cdot \underbrace{a_1 \cdot a_1^*} \cdot \underbrace{a_2 \cdot a_2^*} \cdot \dots \cdot \underbrace{a_n \cdot a_n^*} \cdot (p-1)$

$\equiv_p 1 \cdot 1 \cdot 1 \cdot \dots \cdot 1 \cdot (-1) \equiv_p \underline{-1}$ ☑

Теорема (Кинеска т. о остацима): Нека су $m_1, \dots, m_n$ по паровима узајамно прости природни бројеви, $(m_i, m_j) = 1$ за $1 \le i < j \le n$, и нека су $a_1, \dots, a_n$ произвољни цели бројеви. Систем:

$$\begin{cases} x \equiv_{m_1} a_1 \\ x \equiv_{m_2} a_2 \\ \vdots \\ x \equiv_{m_n} a_n \end{cases}$$

има решење. Решење x_0 где $0 \le x_0 < m_1 m_2 \dots m_n$ је јединствено и сва решења су дата ф-лом:

$$x = x_0 + m_1 m_2 \dots m_n t, \quad t \in \mathbb{Z}.$$

Доказ: Означимо $M = m_1 \cdot m_2 \cdot \dots \cdot m_n$

$$M_i = \frac{M}{m_i} = m_1 \cdot m_2 \cdot \dots \cdot m_{i-1} \cdot m_{i+1} \cdot \dots \cdot m_n, \quad 1 \le i \le n$$

1° $\underline{(m_i, M_i) = 1}$: Ако $(m_i, M_i) = d > 1$, нека је p прост делилац од d, тада $p \mid d \mid m_i, M_i$

Како $p \mid M_i = m_1 \dots m_{i-1} m_{i+1} \dots m_n$, то $p \mid m_j$ за неко $j \ne i$

Дакле, $p \mid m_i, m_j$, па $(m_i, m_j) \ne 1$ ↯

2° Једначина $1 = \alpha_i \cdot m_i + \beta_i \cdot M_i$ за $\alpha_i, \beta_i \in \mathbb{Z}$

$a_i = \alpha_i \cdot m_i \cdot a_i + \underline{\beta_i \cdot M_i \cdot a_i}$

Уочимо: $\beta_i M_i a_i \equiv_{m_j} 0$ за $j \ne i$ јер $m_j \mid M_i$

$\beta_i M_i a_i \equiv_{m_i} a_i - \alpha_i m_i a_i \equiv_{m_i} a_i - 0 \equiv_{m_i} a_i$

Нека је $x_1 = \beta_1 M_1 a_1 + \beta_2 M_2 a_2 + \dots + \beta_n M_n a_n$

Тада $x_1 = \underbrace{\beta_1 M_1 a_1}_{\equiv m_i\ 0} + \dots + \underbrace{\beta_i M_i a_i}_{a_i} + \dots + \underbrace{\beta_n M_n a_n}_{0}$

$\equiv m_i\ a_i$

тј. x_1 је решење система.

3° Записимо $x_1 = Mq + x_0$, $0 \le x_0 < M$

$x_0 = x_1 - Mq \equiv_{m_i} a_i - 0 \equiv_{m_i} a_i$

$\uparrow\ m_i \mid M$

па је x_0 такође решење система.

4° Како је x_0 решење $x \equiv_{m_1} a_1$, то су сва решења $x \equiv_{m_1} a_1$ $\underline{x = x_0 + m_1 t,\ t \in \mathbb{Z}}$.

Одредимо оно од њих које: $x_0 + m_1 t \equiv_{m_2} a_2$

$\uparrow\ m_2$

$a_2 + m_1 t$, па $m_1 t \equiv_{m_2} 0$

тј. $m_2 \mid m_1 \cdot t$, па $m_2 \mid t$ јер $(m_2, m_1) = 1$

$\underline{t = m_2 \cdot s}$

Заједничка решења за $x \equiv_{m_1} a_1$ и $x \equiv_{m_2} a_2$ су

$x = x_0 + m_1 m_2 \cdot s$, $s \in \mathbb{Z}$.

Одредимо од њих које: $x_0 + m_1 m_2 \cdot s \equiv_{m_3} a_3$

$\uparrow\ m_3$

$a_3 + m_1 m_2 s$, па $m_1 m_2 s \equiv_{m_3} 0$

тј. $m_3 \mid m_1 m_2 s$, па $m_3 \mid s$ јер $(m_3, m_1) = 1$, $(m_3, m_2) = 1$

$\underline{s = m_3 \cdot n}$

Заједничка решења за прва три услова су

$x = x_0 + m_1 m_2 m_3 \cdot n$, $n \in \mathbb{Z}$

Наставимо по стрелки. На крају имамо да су:

$$x = x_0 + \underbrace{m_1 m_2 m_3 \dots m_n}_{M} z, \quad z \in \mathbb{Z}$$

сва решења система.

једино решење које $0 \le x < M$ је за $z = 0$, тј. $x = x_0$ ☐

Пример: Решити:

$$x \equiv_3 1$$
$$x \equiv_4 2$$
$$x \equiv_5 4$$

$M = 60$

i	1	2	3
m_i	3	4	5
a_i	1	2	4
M_i	20	15	12
α_i	7	4	-7
β_i	-1	-1	3

$\alpha_i m_i + \beta_i M_i = 1$

$7 \cdot 3 + (-1) 20 = 1$

$4 \cdot 4 + (-1) 15 = 1$

$(-7) \cdot 5 + 3 \cdot 12 = 1$

$x_1 = \beta_1 \cdot M_1 \cdot a_1 + \beta_2 \cdot M_2 \cdot a_2 + \beta_3 \cdot M_3 \cdot a_3$

$= -20 - 30 + 144 = 94$

$x = 94 + 60 \cdot t, \quad t \in \mathbb{Z}$

$x_0 = 34$ за $t = -1$.

Општија теорема: Нека су $m_1, \dots, m_n \ge 2$, $a_1, \dots, a_n \in \mathbb{Z}$ и за $1 \le i < j \le n$ важи $(m_i, m_j) \mid a_i - a_j$.

Тада систем:

$$x \equiv_{m_1} a_1$$
$$x \equiv_{m_2} a_2$$
$$\vdots$$
$$x \equiv_{m_n} a_n$$

има решење.

Решење x_0 које $0 \le x_0 < [m_1, m_2, \dots, m_n]$ је једно и два решења су дата следећом ф-лом:

$$x = x_0 + [m_1, m_2, \dots, m_n] \cdot t, \quad t \in \mathbb{Z}.$$