ELEMENTARNA TEORIJA BROJEVA

1.1. DJELJIVOST

$\mathbb{N} = \{1, 2, 3, \dots\}$ – operacije zbrajanja i množenja $(+, \cdot)$

komutativnost, asocijativnost, distributivnost

$\mathbb{N}_0 = \{0\} \cup \mathbb{N}$

$\mathbb{Z} = \{\dots, -2, -1, 0, 1, 2, \dots\}$ – skup cijelih brojeva

$\mathbb{Q} = \{ \frac{a}{b} : a \in \mathbb{Z}, b \in \mathbb{N} \}$ – skup racionalnih brojeva

$S \subseteq \mathbb{N}$ $(\min S) \in S$ → minimalni element

↳ neprazan podskup od $\mathbb{N}$

→ princip matematičke indukcije

$S \subseteq \mathbb{N}$

$1 \in S$ BAZA INDUKCIJE

Pretp. $n \in S \Rightarrow n+1 \in S$

↳ KORAK INDUKCIJE

Zaključak: $S = \mathbb{N}$

DEF. 1.1. $a \neq 0$ $a, b \in \mathbb{Z}$

a DIJELI b $a \mid b$ „a djelitelj od b", „b višekratnik od a"

↳ ako $\exists k \in \mathbb{Z}$ $b = k \cdot a$

ako b nije djeljiv sa a → $a \nmid b$

$n \in \mathbb{N}$ $a^n \parallel b$

↳ najveća potencija koji dijeli b

↳ $a^n \mid b$ ali $a^{n+1} \nmid b$

RELACIJA PARCIJALNOG UREĐAJA na skupu $\mathbb{N}$ relacije „biti djeljiv"

(1) $n \mid n$ refleksivnost

(2) $n \mid m$ i $m \mid n \Rightarrow m = n$ antisimetričnost

$(\mathbb{Z}: n = \pm m)$

(3) $n \mid m$ $m \mid k$ $\Rightarrow n \mid k$ tranzitivnost

TM 1. Teorem o dijeljenju s ostatkom

$a \in \mathbb{N}$, $b \in \mathbb{Z}$ $\Rightarrow$ $\exists!\ g$ i $r \in \mathbb{Z}$

takvi da je $b = ag + r$, $0 \leq r < a$

<u>DOKAZ</u>: $S = \{b - am : m \in \mathbb{Z}\}$

r - najmanji nenegativni član tog skupa

$r = \min(S \cap \mathbb{N}_0)$

po definiciji $0 \leq r < a$ i $\exists g \in \mathbb{Z}$ takav da je $b - ga = r$

dokazivanje jedinstvenosti od g i r → pretp. suprotno → postoji g_1 i r_1

$$\left.\begin{aligned} b &= ag_1 + r_1 \\ b &= ag + r \end{aligned}\right\} -$$

$$\underset{\text{pretp.}}{0 <} r_1 - r = a(g - g_1) < a$$

s jedne strane $0 < r_1 - r < a$

s druge strane $r_1 - r = a(g - g_1) \geq a$

$r = r_1$, pa je stoga $g_1 = g$

DEF. 1.2. Najveći zajednički djelitelj

$b, c \in \mathbb{Z}$ $a | b$ i $a | c$ → a je djelitelj od b i c

$nzd(b, c)$ najveći zajednički djelitelj

$nzd(b, c) = 1$ b i c su relativno prosti

$nzd(b_1, b_2, \ldots, b_k) = 1$ $b_1, b_2, \ldots, b_k$ su relativno prosti

$nzd(b_i, b_j) = 1$ $1 \leq i < j \leq k$

↳ u parovima relativno prosti

TM. 2. $nzd(b,c) = \min(\underbrace{\{bx+cy : x,y \in \mathbb{Z}\}}_{S} \cap \mathbb{N})$ II

cjelobrojna linearna kombinacija brojeva b i c

DOKAZ: $g = nzd(b,c)$

l - najmanji pozitivni član skupa S

$l = \min S$

$\exists\, x_0, y_0 \in \mathbb{Z} \quad l = bx_0 + cy_0$

I $\quad l \mid b \quad l \mid c$

pretp. $l \nmid b$

po teoremu 1. $\exists\, q$ i r takvi da je $b = lq + r \quad 0 < r < l$

$r = b - lq$

$= b - (bx_0 + cy_0) \cdot q$

$= b(1 - qx_0) + c \cdot q\, y_0$

u suprotnosti s minimalnošću od l

$l \mid b$ i $l \mid c$ - l je djelitelj

$l \leq nzd(b,c) = g$

$l \leq g$

II $\quad g = nzd(b,c)$

$\exists\, \beta, \gamma \in \mathbb{Z}$ takvi da je $b = g \cdot \beta$

$c = g \cdot \gamma$

$l = bx_0 + cy_0 = g(\beta x_0 + \gamma y_0) \Rightarrow g \leq l$

Dokazali smo da je $g = l$

PROPOZICIJA 1.

$\left.\begin{array}{l} nzd(a,m) = 1 \\ nzd(b,m) = 1 \end{array}\right\} \; nzd(ab,m) = 1$

DOKAZ prema teoremu 2. $\exists\, x_0, y_0, x_1, y_1 \in \mathbb{Z}$: $\left.\begin{array}{l} ax_0 + my_0 = 1 \\ bx_1 + my_1 = 1 \end{array}\right\} * \Rightarrow 1 = ab\underbrace{\{\}}_{\mathbb{Z}} + m\underbrace{\{\}}_{\mathbb{Z}}$

$nzd(ab,m) = 1$

PROPOZICIJA 2

$nzd(a,b) = nzd(a, b+ax)$

DOKAZ

$nzd(a,b) = d \quad nzd(a, b+ax) = g$

po TM. 2 $\exists x_0, y_0 \in \mathbb{Z}$ takvi da je $d = ax_0 + by_0$

$d = a(x_0 - xy_0) + (b+ax)y_0 \Rightarrow g | d$

$d|a \quad d|b \rightarrow d|(b+ax)$

$\hookrightarrow$ d je zajednički djelitelj od a i b+ax

$\hookrightarrow$ po TM 2. $- d|g$

$d = g$

TM. 3. Euklidov algoritam

$b, c \in \mathbb{Z}, \quad c > 0$

uzastopna primjena TM 1.

$b = cg_1 + r_1, \quad 0 < r_1 < c$

$c = r_1 \cdot g_2 + r_2, \quad 0 < r_2 < r_1$

$r_1 = r_2 \cdot g_3 + r_3, \quad 0 < r_3 < r_2$

$\vdots$

$r_{j-2} = r_{j-1} \cdot g_j + r_j \quad 0 < r_j < r_{j-1}$

$r_{j-1} = r_j \cdot g_{j+1}$ $\rightarrow$ najveći zajednički djelitelj

Tvrdnja: $r_j = nzd(b,c)$

$r_j = bx_0 + cy_0$ $\quad x_0, y_0$ se dobivaju na algoritam

DOKAZ: po PROP. 2

$$nzd(b,c) = nzd(b - cg_1, c) = nzd(r_1, c) = nzd(r_1, c - r_1 g_2) = nzd(r_1, r_2)$$
$$= nzd(r_1 - r_2 g_3, r_2) = nzd(r_3, r_2)$$

$nzd(b,c) = nzd(r_{j-1}, r_j) = nzd(r_j, 0) = r_j$

$r_1 = b - cg_1$ je linearna komb. od b i c

i r_2 ; prtp. da vrijedi i za r_{i-1}, r_{i-2}

$r_i \rightarrow$ lin komb. r_{i-1} i r_{i-2} $\rightarrow$ lin komb. od b i c

EUKLIDOV ALGORITAM

$b > c \geq 0$

```
while (c>0
    (b,c) = (c, b mod c))
return b
```

Pr. 1.1. $d = nzd(252, 198)$

$d = ?$

$252 = 198 \cdot 1 + 54$

$198 = 54 \cdot 3 + 36$

$54 = 36 \cdot 1 + \boxed{18}$ $\qquad d = 18$

$36 = 18 \cdot 2$

i	-1	0	1	2	3
q_i			1	3	1
x_i	1	0	1	-3	4
y_i	0	1	-1	4	-5

$18 = 54 - 36 \cdot 1 = 54 - (198 - 54 \cdot 3) = 4 \cdot 54 - 1 \cdot 198 = 4 \cdot (252 - 198 \cdot 1) - 1 \cdot 198$

$= 4 \cdot 252 - 5 \cdot 198$

$bx + cy = nzd(b, c)$

$r_{-1} = b \qquad r_0 = c \qquad r_i = r_{i-2} - q_i r_{i-1}$

$x_{-1} = 1 \qquad x_0 = 0 \qquad x_i = x_{i-2} - q_i x_{i-1}$

$y_{-1} = 0 \qquad y_0 = 1 \qquad y_i = y_{i-2} - q_i y_{i-1}$

$bx_i + cy_i = r_i \quad , \quad za \quad i = -1, 0, 1, \ldots, j+1$

Pr. 1.2 $g = nzd(3587, 1819)$

$3587x + 1819y = g$

$3587 = 1819 \cdot 1 + 1768 \quad \to q_i$

$1819 = 1768 \cdot 1 + 51$

$1768 = 51 \cdot 34 + 34$

$51 = 34 \cdot 1 + \boxed{17}$

$34 = 17 \cdot 2$

$g = 17$

$3587 \cdot \underset{x}{(-36)} + 1819 \cdot \underset{y}{71} = 17$

i	-1	0	1	2	3	4
q_i			1	1	34	1
x_i	1	0	1	-1	35	-36
y_i	0	1	-1	2	-69	71

$x_1 = 1 - 1 \cdot 0 = 1$

$y_1 = 0 - 1 \cdot 1 = -1$

$x_2 = 0 - 1 \cdot 1 = -1$

$y_2 = 1 - 1 \cdot (-1) = 2$

$x_3 = 1 - 34 \cdot (-1) = 35$

$y_3 = -1 - 34 \cdot 2 = -69$

$x_4 = -1 - 1 \cdot 35 = -36$

$y_4 = 2 - 1 \cdot (-69) = 71$

- za tablicu vrijedi:

$$x_{i-1}y_i - x_iy_{i-1} = (-1)^i$$ ← kad se pomnože unakrsno u tablici

$\Rightarrow nzd(x_i, y_i) = 1, \ \forall i$

→ Broj koraka u Euklidovom algoritmu

$$j < 2\log_2 c$$

TM. 4. Svaki prirodan broj $n>1$ je produkt prostih (s jednim ili više faktora)

DOKAZ: Matematička indukcija

$n=2$ prost

pretp. $n>2$ prost / složen

te da tvrdnja teorema vrijedi za sve m: $2 \leq m < n$

$n = n_1 \cdot n_2$

$1 < n_1 < n$, $1 < n_2 < n$

dokazujemo da je i n prost

po pretpostavci n_1 i n_2 su produkti prostih brojeva

TM. 5. (OSNOVNI TEOREM ARITMETIKE) Svaki prirodan broj $n>1$ se može jedinstveno prikazati kao produkt prostih do na poredak prostih faktora

DOKAZ: Za dokaz nam treba

PROP. $p|ab$, p-prost $\Rightarrow p|a$ ili $p|b$

$p|a_1 \cdots a_n$, p-prost $\Rightarrow p|a_1$ ili ... $p|a_n$

pretp. suprotno $p_1 \cdot p_2 \cdots p_k = q_1 \cdot q_2 \cdots q_s$ $\quad p_i \neq q_j \ \forall i,j$

prop $\Rightarrow p_1 | q_1 q_2 \cdots q_s$

$p_1 | q_j$, q_j-prost $\Rightarrow p_i = q_j$

↳ kontradikcija

$p_1 < p_2 < \ldots$ prosti brojevi (različiti)

$n = p_1^{\alpha_1} p_2^{\alpha_2} \cdots p_k^{\alpha_k}$ $\quad p_1 < p_2 < \ldots < p_k$ prosti, $\alpha_1, \ldots, \alpha_k \in \mathbb{N}$ $\Big\}$ KANONSKI RASTAV na proste faktore

$n = \prod_p p^{\alpha(p)}$ $\quad \alpha(p) \in \mathbb{N}_0$

$p \mid n \quad \alpha(p) \geq 1 \qquad p \nmid n \quad \alpha(p) = 0$

TM. 6. Skup prostih je beskonačan

DOKAZ: pretp. da je $S = \{p_1, p_2, \ldots, p_k\}$ skup prostih brojeva.

$n = 1 + p_1 p_2 \cdots p_k \qquad p_i \nmid n$ za $\forall\, i = 1, \ldots, k$

po TM. 4. $\Rightarrow \exists\, q$-prost $\quad q \mid n \quad q \neq p_i \quad i = 1, \ldots, k \quad q \in S$ KONTRADIKCIJA

PROPOZICIJA Svaki složen $n > 2$ ima prostog djelitelja $\leq \sqrt{n}$

DOKAZ: p - najmanji koji dijeli n

$n = p \cdot m \geq p^2 \quad m \in \mathbb{N} \quad m \geq p$

$p \leq \sqrt{n}$

→ Najmanji zajednički višekratnik od a i b

$a \mid m$ i $b \mid m$

najmanji prirodan m : nzv(a,b) $\qquad$ (lcm(a,b))

$a = \prod_p p^{\alpha(p)}, \quad b = \prod_p p^{\beta(p)}$

$ab = \prod_p p^{\alpha(p) + \beta(p)}$

DJELITELJ - presjek

VIŠEKRATNIK - UNIJA

$\text{nzd}(a,b) = \prod p^{\min(\alpha(p), \beta(p))}$

$\text{nzv}(a,b) = \prod p^{\max(\alpha(p), \beta(p))}$

$\min(\alpha(p), \beta(p)) + \max(\alpha(p), \beta(p)) = \alpha(p) + \beta(p)$

$|ab| = \text{nzd}(a,b) \cdot \text{nzv}(a,b)$

2. PREDAVANJE

prirodan broj a

$\mathbb{N} \to \quad a = \prod_p p^{\alpha(p)} \qquad \alpha(p) \geq 0$ akko $p \mid a$

$\alpha(p) = 0$ akko $p \nmid a$

↳ za skoro sve proste brojeve

$\boxed{|ab| = nzd(a,b) \cdot nzv(a,b)}$

$a = \square \iff \alpha(p) = 0$ ili $\alpha(p)$ parne

$\square \nmid a \iff \alpha(p) \in \{0,1\}$

$p^k \| a \iff \alpha(p) = k$

ERATOSTENOVO SITO

~~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

PAROVI BLIZANCI

precrtajmo svaki drugi počevši od 2, pa 3^2 (pa svaki treći), 5^2, 7^2...

{DETALJNIJE knjiga str. 10}

Pr. 1. Za svaki n postoji n uzastopnih složenih brojeva

Rj. $\underbrace{(n+1)!+2}_{2|}, \ \underbrace{(n+1)!+3}_{3|}, \ \ldots, \ \underbrace{(n+1)!+n+1}_{n+1|}$

$\Rightarrow$ postoje 2 uzastopna prosta p_k, p_{k+1}, $d(p_k, p_{k+1}) \geq n$

$x \in \mathbb{R}$

$\pi(x)$ – broj prostih brojeva koji su $\leq x$

Teorem o prostim brojevima

↳ $\pi(x) \sim \dfrac{x}{\ln x}$

{NE TREBA ZNAT DOKAZ}

SPECIJALNI OBLICI PROSTIH BROJEVA

I $f_n = 2^{2^n} + 1$ FERMATOV BROJ

$f_0 = 3,\ f_1 = 5,\ f_2 = 17,\ f_3 = 257,\ f_4 = 65537$

$f_5 = 2^{32} + 1 \to$ složen (Euler $641 | f_5$)

HIPOTEZA : Postoji samo konačno mnogo prostih Fermatovih brojeva

II $M_p = 2^p - 1$, p - prost broj MERSENNOV BROJ

$M_7 = 127$ - prost

$M_{11} = 28 \cdot 39$ - složen

HIPOTEZA : Postoji beskonačno mnogo prostih Mers. brojeva

$\to$ Internet (GIMPS projekt)

III $n! \pm 1$ FAKT. BROJ

IV $\underbrace{n\#}_{2 \cdot 3 \cdot 5 \cdot 7 \cdot 11 \cdot \ldots} \pm 1$ PRIMORIJELNI

$\hookrightarrow$ produkt prostih brojeva

V $2p + 1$ Sophie G.

$\to$ VEZANO UZ FERMATOVE BROJEVE

Tvrdnja : $2^k + 1$ prost $\to$ $k = 0$ ili $k = 2^n$ $n \geq 0$

Rj : Pretp. da je p - prost i da $p | k$ i neka je $p > 2$

$k = p \cdot m,\ m \in \mathbb{N}$

$$2^k + 1 = (2^m)^p + 1^p = (2^m + 1)(2^{m(p-1)} - 2^{m(p-2)} + \ldots + 1)$$

$\hookrightarrow$ djeljiv sa $(2^m + 1)$

$\hookrightarrow$ složen

$p = 2$

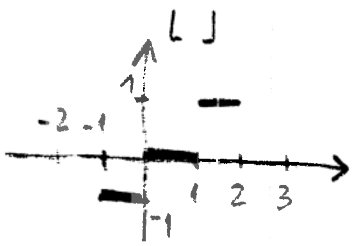
PROPOZICIJA : Potencija s kojom prosti broj p ulazi u rastav broja $n!$ na proste faktore jednaka je

$$\left\lfloor \frac{n}{p} \right\rfloor + \left\lfloor \frac{n}{p^2} \right\rfloor + \left\lfloor \frac{n}{p^3} \right\rfloor + \dots$$

konačna suma brojeva $\neq 0$

$(p^k > n) \to \left\lfloor \frac{n}{p^k} \right\rfloor = 0$

↳ tu stajemo, beskonačno mnogo 0



DOKAZ : $\left\lfloor \frac{n}{p} \right\rfloor$ = viš. od p u nizu $1, 2, \dots, n$

$1\ 2\ \underline{3}\ 4\ 5\ \underline{6}\ 7\ 8\ \underline{\underline{9}}\ 10$

$p = 3$

$\left\lfloor \frac{n}{p^2} \right\rfloor$ = viš. od p^2

$10! = 2^{\alpha(2)} \cdot 3^{\alpha(3)}$

$\vdots$

$\left\lfloor \frac{n}{p^k} \right\rfloor$ = viš. od p^k

Pr. 2. S kojom potencijom ulaze 2 i 3 u kanonski rastav od 20!

$$n! = 20! = 1 \cdot \underline{\overset{1}{2}} \cdot 3 \cdot \underline{\overset{2}{4}} \cdot 5 \cdot \underline{\overset{1}{6}} \cdot 7 \cdot \underline{\overset{3}{8}} \cdot 9 \cdot \underline{\overset{1}{10}} \cdot 11 \cdot \underline{\overset{2}{12}} \cdot 13 \cdot \underline{\overset{1}{14}} \cdot 15 \cdot \underline{\overset{4}{16}} \cdot 17 \cdot \underline{\overset{1}{18}} \cdot 19 \cdot \underline{\overset{2}{20}}$$

$\prod_p p^{\alpha(p)}$

$$\alpha(2) = \left\lfloor \frac{20}{2} \right\rfloor + \left\lfloor \frac{20}{4} \right\rfloor + \left\lfloor \frac{20}{8} \right\rfloor + \left\lfloor \frac{20}{16} \right\rfloor = 18$$

$$\alpha(3) = \left\lfloor \frac{20}{3} \right\rfloor + \left\lfloor \frac{20}{9} \right\rfloor + \cancelto{0}{\left\lfloor \frac{20}{27} \right\rfloor} = 6 + 2 = 8$$

$$20! = 2^{18} \cdot 3^{8} \cdot \ldots$$

$$\left.\begin{array}{l} p < q \\ \alpha(p) \geq \alpha(q) \end{array}\right\} \text{rastav od } n!$$

Pr. 3. Odredite s koliko nula završava broj 562! [Pr. 1.7]

Rj: naći najveću potenciju broja 10 koja dijeli 562!

$10 = 2 \cdot 5$ → DOVOLJNO NAĆI NAJVEĆU POTENCIJU PROSTOG BROJA 5

$$n! = 2^{\alpha(2)} \cdots 5^{\alpha(5)} \cdots = 10^{\min(\alpha(2), \alpha(5))}$$

$\downarrow$ $\alpha(5)$

$2 < 5$

$\alpha(2) > \alpha(5)$

$$\alpha(5) = \left\lfloor \frac{562}{5} \right\rfloor + \left\lfloor \frac{562}{25} \right\rfloor + \left\lfloor \frac{562}{125} \right\rfloor + 0$$

$$= 112 + 22 + 4 = 138$$

Pr. 4. Odredite broj nula s kojim završava br. $\binom{2010}{1000}$

Rj:
$$\binom{n}{k} = \frac{\overset{a!}{n!}}{\underset{b!}{k!}\,\underset{c!}{(n-k)!}} = \frac{2^{\alpha(2)} \cdots 5^{\alpha(5)} \cdots}{2^{\beta(2)} \cdot 5^{\beta(5)} \cdots 2^{\gamma(2)} \cdots 5^{\gamma(5)}} = 2^{\alpha(2)-\beta(2)-\gamma(2)} \cdots 5^{\alpha(5)-\beta(5)-\gamma(5)} \cdots$$

$a! \to \prod p^{\alpha(p)}$

$b! \to \prod p^{\beta(p)}$

$c! \to \prod p^{\gamma(p)}$

$$a = 2010 \to \alpha(5) = \left\lfloor \frac{2010}{5} \right\rfloor + \left\lfloor \frac{2010}{25} \right\rfloor + \left\lfloor \frac{2010}{125} \right\rfloor + \left\lfloor \frac{2010}{625} \right\rfloor + 0 = 501$$

$$b = 1000 \to \beta(5) = \left\lfloor \frac{1000}{5} \right\rfloor + \left\lfloor \frac{1000}{25} \right\rfloor + \left\lfloor \frac{1000}{125} \right\rfloor + \left\lfloor \frac{1000}{625} \right\rfloor = 249$$

$$c = 1010 \to \gamma(5) = \left\lfloor \frac{1010}{5} \right\rfloor + \left\lfloor \frac{1010}{25} \right\rfloor + \left\lfloor \frac{1010}{125} \right\rfloor + \left\lfloor \frac{1010}{625} \right\rfloor = 251$$

$$5^{\alpha(5)-\beta(5)-\gamma(5)} \Rightarrow 501 - 249 - 251 = \underline{\underline{1}}$$

1.2. KONGRUENCIJE

$a, b, m \in \mathbb{Z}, \; m \neq 0$

$m \mid a-b \overset{def}{\Longleftrightarrow} a \equiv b \pmod{m}$

„a kongruentan b modulo m"

$\exists k \in \mathbb{Z} \quad a-b = m \cdot k$

$a = b + mk$

$m \mid a-b \Leftrightarrow -m \mid a-b$

Dogovor: $m \in \mathbb{N}$

PROPOZICIJA 1: „Biti kongruentan modulo m" je relacija ekvivalencije na skupu $\mathbb{Z}$

DOKAZ:

$a \equiv a \pmod{m} \Leftrightarrow m \mid a-a = 0$
$m \mid 0$ — REFLEKSIVNOST

SIMETRIČNOST

$a \equiv b \pmod{m}$ & $b \equiv a \pmod{m}$

$\exists k \in \mathbb{Z}$ takav da je $a-b = m \cdot k$

$b-a = m \cdot (-k) \Rightarrow b \equiv a \pmod{m}$

$a \equiv b \pmod{m} \quad b \equiv c \pmod{m} \quad a \equiv c \pmod{m}$

$m \mid a-b$ & $m \mid b-c \Rightarrow m \mid a-b+b-c$

$m \mid a-c$

dijeli i njihov zbroj

TRANZITIVNOST

→ Svojstva kongruencije

PROPOZICIJA 2:

1) $a \equiv b \pmod m$, $c \equiv d \pmod m$ $\Rightarrow$ $a \pm c \equiv b \pm d \pmod m$; $ac \equiv bd \pmod m$

2) $a \equiv b \pmod m$, $d \mid m$ $\Rightarrow$ $a \equiv b \pmod d$

3) $a \equiv b \pmod m$ $\Rightarrow$ $ac \equiv bc \pmod{mc}$; $ac \equiv bc \pmod m$

4) $a \equiv b \pmod m$
$f \in \mathbb{Z}[x] \Rightarrow f(a) \equiv f(b) \pmod m$
↳ pol. su cjelobrojni koef.

5) $ax \equiv ay \pmod m \Leftrightarrow x \equiv y \left(\bmod \dfrac{m}{nzd(a,m)}\right)$

5') $ax \equiv ay \pmod m$, $nzd(a,m) = 1 \Rightarrow x \equiv y \pmod m$

specijalni slučaj

DOKAZ: (1) $a = b + mk$
$c = d + ml$

a) $(a+c) - (b+d) = m(k+l)$
$(a-c) - (b-d) = m(k-l)$

$a+c \equiv b+d \pmod m$
$a-c \equiv b-d \pmod m$

b) $ac - bd = a(c-d) + d(a-b)$
$= m(al + dk)$

(2) $a - b = m \cdot k$ $\quad m = d \cdot e$
$a - b = \underbrace{d \cdot (e \cdot k)}_{m}$ $\Rightarrow d \mid a-b$

(3) $a - b = mk$
$ac - bc = (mc) \cdot k$

(4) $f(x) = a_n x^n + a_{n-1} x^{n-1} + \ldots + a_0$ $\quad a_i \in \mathbb{Z}$

↪

(4) nastavak

$$a \equiv b \pmod m$$

$$a^2 \equiv b^2 \pmod m \quad \longrightarrow \text{koristimo pod } (1)$$

$$a^3 \equiv b^3 \pmod m$$

$$\vdots$$

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

$$\Downarrow$$

$$c_i a^i \equiv c_i b^i \pmod m$$

$$c_n a^n + c_{n-1} a^{n-1} + \dots + c_0 \equiv c_n b^n + c_{n-1} b^{n-1} + \dots + c_0 \pmod m$$

(5) $\Rightarrow ax - ay = m \cdot z \quad / : nzd(a,m) \qquad z \in \mathbb{Z}$

$$\frac{a(x-y)}{nzd(a,m)} = \frac{m}{nzd(a,m)} \cdot z$$

$$\frac{m}{nzd(a,m)} \Big|$$

$\frac{a}{nzd(a,m)}$ i $\frac{m}{nzd(a,m)}$ su relativno prosti

tj. $\frac{m}{nzd(a,m)}$ dijeli $x-y$

$$\Leftarrow \quad x - y = \frac{m}{nzd(a,m)} \cdot z \quad / \cdot a$$

$$ax - ay = \frac{a \cdot m}{nzd(a,m)} \cdot z \quad \Rightarrow \quad m \mid ax - ay$$

DEFINICIJA Potpun sustav ostataka modulo m

$S = \{x_1, x_2, \dots, x_m\}$

$\forall y \in \mathbb{Z} \quad \exists! \; x_j \in S$ takav da je $y \equiv x_j \pmod m$

$m = 6$ $\{0, 1, 2, 3, 4, 5\}$ → sustav najmanjih nenegativnih ost.

$\{-2, -1, 0, 1, 2, 3\}$ → sustav apsolutno najmanjih ost.

$m = 5$ $\{-2, -1, 0, 1, 2\}$

TEOREM $\{x_1, x_2, \dots, x_m\}$ P. S. O. modulo m

$a \in \mathbb{Z}$, $nzd(a, m) = 1$

tada je $\{a x_1, a x_2, \dots, a x_m\}$ također P. S. O.

<u>DOKAZ:</u> pretp. $a x_i \equiv a x_j \pmod m \underset{(5')}{\Longrightarrow} x_i \equiv x_j \pmod m$

Broj rješenja **kongruencije** je broj međusobno nekongruentnih rješenja

$\Longleftrightarrow$ broj rješenja u P. S. O.

$5x \equiv 2 \pmod 7$ $x = \cancel{0}, \cancel{1}, \cancel{2}, \cancel{3}, \cancel{4}, \cancel{5}, 6$

uvrštavamo redom brojeve

$x_0 = 6$ ima jedinstveno rješenje

Sva rješenja : $x \equiv 6 \pmod 7$

$ax \equiv b \pmod m$, $a, m \in \mathbb{N}$, $b \in \mathbb{Z}$

?

<u>Linearna kongruencija</u>

$x_0 \in \mathbb{Z}$, $a x_0 \equiv b \pmod m \Rightarrow a(x_0 + mk) \equiv b \pmod m$, $\forall k$

TEOREM $\quad a, m \in \mathbb{N}, \; b \in \mathbb{Z}$

(1) $ax \equiv b \pmod{m}$ ima rješenja akko $\underbrace{nzd(a,m)}_{d} \mid b$

(2) ako ima rješenja ima ih točno d

DOKAZ: (1) $\Rightarrow$ $\quad \exists x_0 : dx_0 \equiv b \pmod{m}$

$$ax_0 - nk = b \Rightarrow d \mid b$$

(1) $\Leftarrow$, (2) $\quad a' = \frac{a}{d}, \quad b' = \frac{b}{d}, \quad m' = \frac{m}{d}$

a' i m' su relativno prosti

$nzd(a', m') = 1$

$a'x = b' \pmod{m'}$

P.S.O. $\{x_1, \dots, x_{m'}\}$ $\quad nzd(a', m') = 1$

po TM.1. $\{a'x_1, \dots, a'x_{m'}\}$ P.S.O.

$\Rightarrow \exists x_k : a'x_k \equiv b' \pmod{m'}$

$x_0 = x_k$ je jedno rješenje kongruencije $ax \equiv b \pmod{m}$

$x_n = x_0 + n \cdot m', \quad n = 0, 1, \dots, d-1$ $\qquad$ SVA RJEŠENJA U P.S.O.

→ PROCEDURA RJEŠAVANJA $\quad ax \equiv b \pmod{m}$

(1) $d = nzd(a, m)$ pomoću E.A.

(2) $a'x \equiv b' \pmod{m'}$ $\qquad [a' = \frac{a}{d}, \dots]$

$nzd(a', m') = 1 \quad \exists u, v \in \mathbb{Z}$

$a'u + m'v = 1 \quad / \cdot b'$

$a'(ub') + m'(vb') = b'$

$a'(ub') \equiv b' \pmod{m'}$ $\qquad x \equiv ub' \pmod{m'}$

(3) $x_0 \neq um'$

$n = 0, 1, \dots, d-1$

PRIMJER

$$\underset{a}{589}x \equiv \underset{b}{209} \pmod{\underset{m}{817}}$$

$\left.\begin{matrix} (a<m \\ b<m) \end{matrix}\right\}$ mijek se svodi na ovo

(1)

$$817 = 589 \cdot \overset{q_i}{1} + 228$$
$$589 = 228 \cdot 2 + 133$$
$$228 = 113 \cdot 1 + 95$$
$$113 = 95 \cdot 1 + 38$$
$$95 = 38 \cdot 2 + \boxed{19} \Rightarrow d = 19$$
$$38 = 19 \cdot 2$$

$a' = \frac{a}{d}$

$a' = 31$

$b' = 11$

$m' = 43$

(2) $a'x \equiv b' \pmod{m'}$

$$31x = 11 \pmod{43}$$

$$a'u + m'v = 1$$
$$31u + 43v = 1$$

$$31u \equiv 1 \pmod{43}$$

q_i			1	2	1	1	2
y_i	0	1	-1	-3	-4	-7	-18

$$31 \cdot (-18) \equiv 1 \pmod{43} \quad /\cdot 11$$

$$31(-18 \cdot 11) = 11 \pmod{43} \Rightarrow x \equiv -198 \pmod{43}$$

$-198 + 43 + 43 + 43 \ldots 17$

198 → x

$x \equiv 17 \pmod{43}$ ← sva rješenja ili: $x \equiv 17 + n \cdot 43 \pmod{817}$, $n = 0, \ldots, 18$

17 = P.S.O. najmanjih nenegat. ost.

SVA RJEŠENJA: 17, 17 + 43 = 60, 60 + 43 = 103, ..., 791

x_0, x_1, x_2, x_{18}

$\boxed{\text{Pr. 13.}}$

$$\left.\begin{aligned} x &\equiv 3 \pmod{10} \\ x &\equiv 8 \pmod{15} \\ x &\equiv 5 \pmod{84} \end{aligned}\right\}$$ nisu u parovima relativno prosti - ne možemo direktno primjeniti kineski teorem

$x \equiv 3 \pmod 2$ $\quad$ $x \equiv 3 \pmod 5$ $\rightarrow x \equiv 3 \bmod (5)$

$x \equiv 8 \pmod 3$ $\quad$ $x \equiv 8 \pmod 5$

$x \equiv 5 \pmod 4$ $\quad$ $x \equiv 5 \pmod 3$ $\quad$ $x \equiv 5 \pmod 7$

$x \equiv 3 \pmod 2$ $\quad$ $x \equiv 5 \pmod 4 \rightarrow x \equiv 1 \pmod 4$

$x \equiv 8 \pmod 3$ $\quad$ $x = 5 \pmod 3 \rightarrow x \equiv 2 \pmod 3$

$$\left.\begin{aligned} x &\equiv 1 \pmod 4 \\ x &\equiv 2 \pmod 3 \\ x &\equiv 3 \pmod 5 \\ x &\equiv 5 \pmod 7 \end{aligned}\right\}$$

KINESKI TEOREM:

$m = 4 \cdot 3 \cdot 5 \cdot 7 = 420$

$n_1 = \frac{420}{4} = 105$

$n_2 = \frac{420}{3} = 140$

$n_3 = \frac{420}{5} = 84$

$n_4 = \frac{420}{7} = 60$

$105 x_1 \equiv 1 \pmod 4 \rightarrow x_1 = 1 \pmod 4 \rightarrow x_1 = 1$

$140 x_2 = 2 \pmod 3 \rightarrow 2x_2 = 2 \pmod 3 \rightarrow x_2 = 1$

$84 x_3 \equiv 3 \pmod 5 \rightarrow 4x_3 = 3 \pmod 5 \rightarrow x_3 = 2$

$60 x_4 \equiv 5 \pmod 7 \rightarrow 4x_4 = 5 \pmod 7 \rightarrow x_4 = 3$

$$x \equiv 105 \cdot 1 + 140 \cdot 1 + 84 \cdot 2 + 60 \cdot 3 = 593 \equiv 173 \pmod{420}$$

$\boxed{\text{Pr.}}$ Odredite najmanji prirodni broj djeljiv sa 7 koji pri dijeljenju s 2, 3, 4, 5, 6 daje ostatak 1

$x \equiv 0 \pmod 7$ - djeljiv sa 7

$x \equiv 1 \pmod 2$

$x \equiv 1 \pmod 3$ $\quad\quad x \equiv 1 \pmod 4$

$x \equiv 1 \pmod 4$

$x \equiv 1 \pmod 5$

$x \equiv 1 \pmod 6 \longrightarrow$ $x \equiv 1 \pmod 2$, $x \equiv 1 \pmod 3$

$$x \equiv 0 \pmod 7$$
$$x \equiv 1 \pmod 5$$
$$x \equiv 1 \pmod 3$$
$$x \equiv 1 \pmod 4$$

$$m = 7 \cdot 5 \cdot 3 \cdot 4 = 420$$

$$n_1 = \frac{420}{4} = 105$$

$$n_2 = \frac{420}{3} = 140$$

$$n_3 = \frac{420}{5} = 84$$

$$n_4 = \frac{420}{7} = 60$$

$$105 x_1 \equiv 1 \pmod 4 \Rightarrow x_1 \equiv 1 \pmod 4 \Rightarrow x_1 = 1$$

$$140 x_2 \equiv 1 \pmod 3 \Rightarrow 2x_2 \equiv 1 \pmod 3 \Rightarrow x_2 = 2$$

$$84 x_3 \equiv 1 \pmod 5 \Rightarrow 4x_3 \equiv 1 \pmod 5 \Rightarrow x_3 = 4$$

$$60 x_4 \equiv 0 \pmod 7 \Rightarrow x_4 = 0$$

$$x \equiv 105 \cdot 1 + 140 \cdot 2 + 84 \cdot 4 = 721 \equiv 301 \pmod{420}$$

najmanji!

Napomena! $\left.\begin{array}{l} x \equiv 1 \pmod{3} \\ x \equiv 2 \pmod{3} \end{array}\right\}$ sustav NEMA rješenja

$x \equiv a_1 \pmod{m_1}$

$x \equiv a_2 \pmod{m_2}$

$(m_1, m_2) = 1$

Euklid $\rightarrow$ $\left.\begin{array}{l} u m_1 + v m_2 = 1 \\ x = u m_1 a_2 + v m_2 a_1 \pmod{m_1 m_2} \end{array}\right\}$ bitno za KRIPTOGRAFIJU

DEFINICIJA 1.8. REDUCIRANI SUSTAV OSTATAKA MODULO m

$r_i \in \mathbb{Z}$ $\quad nzd(r_i, m) = 1$

$r_i \not\equiv r_j \pmod{m}$ za $i \neq j$

$\forall x \in \mathbb{Z}$ $\quad nzd(x, m) = 1$ $\quad \exists\, r_i$ takav da je $x \equiv r_i \pmod{m}$

skup svih brojeva $a \in \{1, 2, \ldots, m\}$ koji su relativno prosti sa m

$\varphi(m)$ - Eulerova funkcija

$\varphi(1) = 1$

$\varphi(2) = 1$

$\varphi(3) = 2$

$\varphi(4) = 2$

$\varphi(5) = 4$

$\varphi(6) = 2$

$\varphi(7) = 6$

TEOREM 1.21. Neka je $\{r_1, r_2, \ldots, r_{\varphi(m)}\}$ reducirani sustav ostataka modulo m

$nzd(a, m) = 1$

$\{a r_1, \ldots, a r_{\varphi(m)}\}$ reducirani sustav ostataka modulo m

TEOREM 1.22. (EULEROV)

$$nzd(a,m)=1 \Rightarrow a^{\varphi(m)} \equiv 1 \pmod{m}$$

DOKAZ:
$$\prod_{i=1}^{\varphi(m)} r_i \equiv \prod_{j=1}^{\varphi(m)} a\cdot r_j \pmod{m}$$

$$a^{\varphi(m)} \cdot \prod_{j=1}^{\varphi(m)} r_j \equiv \prod_{i=1}^{\varphi(m)} r_i \pmod{m}$$

$$nzd(r_i,m)=1$$

$$1 \equiv a^{\varphi(m)} \bmod (m)$$

TEOREM 1.23. p-prost broj

$$p \nmid a \Rightarrow a^{p-1} \equiv 1 \pmod{p}$$

Mali Fermatov teorem.

$$a^{p-1} \equiv 1 \pmod{p} \quad /\cdot a$$

$\forall$ cijeli broj $a \Rightarrow a^p \equiv a \pmod{p}$

(ako $p \mid a \longrightarrow \emptyset \quad \emptyset$)

$\boxed{\text{Pr. 1.14.}}$ 3^{400} - odrediti zadnje dvije znamenke (:100 ↳ 25·4)

Rj: $\varphi(25)=20$

$$3^{\varphi(25)} \equiv 1 \pmod{25}$$

$$\left.\begin{aligned} 3^{20} &\equiv 1 \pmod{25} \\ &\vdots \\ 3^{20} &\equiv 1 \pmod{25} \end{aligned}\right\} \text{pomnožimo 20 istih kongruencija} \Rightarrow 3^{400} \equiv 1 \pmod{25}$$

$3^1 \equiv 3 \pmod{4}$

$3^2 \equiv 9 \equiv 1 \pmod{4}$

$3^3 \equiv 3^2\cdot 3 \equiv 1\cdot 3 \equiv 3 \pmod{4}$

$3^4 \equiv 3\cdot 3^3 \equiv 3\cdot 3 \equiv 3^2 \equiv 1 \pmod{4}$

$3^5 \equiv 3 \pmod{4}$

$$\Rightarrow 3^{400} \equiv 1 \pmod{4}$$
$$\Downarrow$$
$$3^{400} \equiv 1 \pmod{100}$$

zadnje znamenke 01

DEFINICIJA 1.11. MULTIPLIKATIVNA FUNKCIJA

$$\vartheta : \mathbb{N} \to \mathbb{C}$$

1) $\vartheta(1) = 1$

2) $\vartheta(mn) = \vartheta(m) \cdot \vartheta(n) \quad \forall m, n$ takve da je $(m, n) = 1$

TEOREM 1.25. Eulerova funkcija φ je multiplikativna

$\forall\ n > 1 \quad n \in \mathbb{N}$ vrijedi:

$$\varphi(n) = n \cdot \prod_{p \mid n} \left(1 - \frac{1}{p}\right)$$

p - prost

$$n = p_1^{\alpha_1} p_2^{\alpha_2} \cdots p_k^{\alpha_k}$$

$$\varphi(n) = \varphi\left(p_1^{\alpha_1} p_2^{\alpha_2} \cdots p_k^{\alpha_k}\right) \overset{\text{MULT}}{=} \varphi(p_1^{\alpha_1})\, \varphi(p_2^{\alpha_2}) \cdots \varphi(p_k^{\alpha_k})$$

$$\varphi(p^{\alpha}) = p^{\alpha} - p^{\alpha - 1}$$

$$= \left(p_1^{\alpha_1} - p_1^{\alpha_1 - 1}\right)\left(p_2^{\alpha_2} - p_2^{\alpha_2 - 1}\right) \cdots \left(p_k^{\alpha_k} - p_k^{\alpha_k - 1}\right)$$

$$= p_1^{\alpha_1} p_2^{\alpha_2} p_3^{\alpha_3} \cdots p_k^{\alpha_k} \left(1 - \frac{1}{p_1}\right)\left(1 - \frac{1}{p_2}\right) \cdots \left(1 - \frac{1}{p_k}\right)$$

$\boxed{\text{npr}}$ $\varphi(100) = 100 \cdot \left(1 - \frac{1}{5}\right)\left(1 - \frac{1}{2}\right) \qquad 100 = 5^2 \cdot 2^2$

$$= 100 \cdot \frac{4}{5} \cdot \frac{1}{2} = 40$$

$\boxed{\text{Pr. 1.16.}}$ $\varphi(n)=12$

odrediti sve prirodne brojeve n

$n = p_1^{\alpha_1} p_2^{\alpha_2} \cdots p_k^{\alpha_k}$

$\varphi(n) = p_1^{\alpha_1-1} p_2^{\alpha_2-1} \cdots p_k^{\alpha_k-1} (p_1-1)(p_2-1)\ldots(p_k-1) = 12$

$p_i - 1 \mid 12$

$p_i - 1 \in \{1, 2, 3, 4, 6, 12\}$

$p_i \in \{2, 3, 4, 5, 7, 13\}$

1°) $n = 13 \cdot k$

$12 = \varphi(n) = \varphi(13k) \overset{M}{=} \varphi(13) \cdot \varphi(k)$

$\varphi(13) = 12$

$= 12 \cdot \varphi(k) \rightarrow \varphi(k) = 1$

$\downarrow$

$k = 1, k = 2 \implies n = 13$ ili $n = 26$

2°) $n = 7 \cdot k$

$12 = \varphi(n) = \varphi(7k) = \varphi(7) \cdot \varphi(k) = 12$

$\varphi(7) = 6$

$= 6 \cdot \varphi(k) = 12 \implies \varphi(k) = 2$ — $k = 2^\alpha 3^\beta$, $k = 2^\alpha$, $k = 3^\beta$

$\varphi(2^\alpha) = 2^{\alpha-1}(2-1) = 2$ $\hookrightarrow \alpha = 2$ $\implies k = 4 \rightarrow n = 28$

$\varphi(3^\beta) = 3^{\beta-1}(3-1) = 2$ $\hookrightarrow \beta = 1$ $\implies k = 3 \rightarrow n = 21$

$\varphi(2^\alpha 3^\beta) = 2^{\alpha-1} 3^{\beta-1} (2-1)(3-1) = 2$ $\hookrightarrow \alpha = 1$ $\hookrightarrow \beta = 1$ $\implies k = 6 \rightarrow n = 42$

3°) $n = 5 \cdot k$

$$\varphi(n) = \varphi(5 \cdot k) = \varphi(5) \cdot \varphi(k)$$
$$= 4 \cdot \varphi(k) = 12$$
$$\varphi(k) = 3$$

$\hookrightarrow$ neparno pa se ne gleda

4°)

$$\left.\begin{array}{l} \varphi(2^{\alpha}) = 2^{\alpha-1}(2-1) = 12 \\ \varphi(3^{\beta}) = 3^{\beta-1}(3-1) = 12 \end{array}\right\} \text{nema rješenja}$$

za $n = k$

$$\varphi(\underbrace{2^{\alpha}3^{\beta}}_{n}) = 2^{\alpha-1}3^{\beta-1}(2-1)(3-1) = 12$$

$$\alpha = 2, \beta = 2$$

$$n = 2^{\alpha}3^{\beta} = \underline{\underline{36}}$$

<u>f - multiplikativna</u>

$$g(n) = \sum_{d|n} f(d)$$

$$g(m,n) = \sum_{d|m}\sum_{d'|n} f(d,d') = \sum_{d|m}\sum_{d'|n} f(d) \cdot f(d')$$

$$= \left(\sum_{d|m} f(d)\right) \cdot \left(\sum_{d'|n} f(d')\right)$$

$$= g(m) \cdot g(n)$$

g je multiplikativna

DEFINICIJA 1.12. $n \in \mathbb{N}$

$\tau(n)$ - broj pozitivnih djelitelja broja n

$\sigma(n)$ - suma svih -||- -||-

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

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

$$\tau(p^j) = j+1$$

$$\sigma(p^j) = 1 + p + p^2 + \dots + p^j = \frac{p^{j+1}-1}{p-1}$$

$$\tau(p_1^{\alpha_1} \cdots p_k^{\alpha_k}) = (\alpha_1+1)(\alpha_2+1) \cdot \ldots \cdot (\alpha_k+1)$$

$$\sigma(p_1^{\alpha_1} \cdots p_k^{\alpha_k}) = \frac{p_1^{\alpha_1+1}-1}{p_1-1} \cdot \ldots \cdot \frac{p_k^{\alpha_k+1}-1}{p_k-1}$$

TEOREM 1.26. $\sum_{d|n} \varphi(d) = n$

DOKAZ: $g(n) = \sum_{d|n} \varphi(d)$ - multiplikativna

dovoljno provjeriti $g(p^\alpha) = p^\alpha$

jer: $g(n) = g(p_1^{\alpha_1} \cdots p_k^{\alpha_k}) = g(p_1^{\alpha_1}) \cdots g(p_k^{\alpha_k}) = p_1^{\alpha_1} \cdots p_k^{\alpha_k} = n$

$$g(p^\alpha) = \varphi(1) + \varphi(p) + \varphi(p^2) + \dots + \varphi(p^\alpha)$$

$$= 1 + (p-1) + (p^2-p) + \dots + (p^\alpha - p^{\alpha-1}) = p^\alpha$$

TEOREM 1.27. (WILSON)

p - prost

$(p-1)! \equiv -1 \pmod p$

$p = 2, 3$ - kongruencija je zadovoljena

$p \geq 5$ $\quad \{2, 3, \ldots, p-2\}$ parovi (i, j)

$i \cdot j \equiv 1 \pmod p \qquad i \neq j$

$2 \cdot 3 \cdots (p-2) \equiv 1 \pmod p$

$(p-1)! \equiv 1 \cdot 1 \cdot (p-1) \equiv -1 \pmod p$

TEOREM 1.28. p - prost

$x^2 \equiv -1 \pmod p$ ima rješenja akko $p = 2$ ili $p \equiv 1 \pmod 4$

DOKAZ: $p = 2 \Rightarrow x = 1$

$p \equiv 1 \pmod 4$

Wilson: $\left[1 \cdot 2 \cdot 3 \cdot \ldots \cdot \frac{p-1}{2}\right] (p-1)(p-2) \cdots \left(p - \frac{p-1}{2}\right) \equiv \left[\left(\frac{p-1}{2}\right)!\right]^2 \equiv -1 \pmod p$

$x = \left(\frac{p-1}{2}\right)!$ jedno rješenje

$p \equiv 3 \pmod 4 \qquad x^2 \equiv -1 \pmod p$

$x^{p-1} \equiv (-1)^{\frac{p-1}{2}} \equiv -1 \pmod p$

$\hookrightarrow$ kontradikcija s malim Fermatovim teoremom

Pr. 1.17. rješavao prof pa reko da to ne trebamo znat (pogledati ipak za svaki slučaj)

$\boxed{\text{Zad.}}$ Odredite sve $n \in \mathbb{N}$

$\varphi(n) = 30$

$n = p_1^{\alpha_1} p_2^{\alpha_2} \cdots p_k^{\alpha_k}$

$\varphi(n) = p_1^{\alpha_1 - 1} p_2^{\alpha_2 - 1} \cdots p_k^{\alpha_k - 1} (p_1 - 1)(p_2 - 1) \cdots (p_k - 1) = 30$

$p_i - 1 \mid 30$

$p_i - 1 \in \{1, 2, 3, 5, 6, 10, 15, 30\}$

$p_i \in \{2, 3, \cancel{4}, \cancel{6}, 7, 11, \cancel{16}, 31\}$

$\hookrightarrow$ prost broj

1°) $31 \mid n$ $\qquad (31, k) = 1$

$n = 31k$

$\varphi(n) = \varphi(31k) = \underbrace{\varphi(31)}_{30} \cdot \varphi(k) = 30$

$= 30 \cdot \varphi(k) = 30 \implies \varphi(k) = 1 \quad \begin{matrix} \nearrow k = 1 \\ \searrow k = 2 \end{matrix}$

$n = 31k \to n = 31, 62$

2° $11 \mid n$ $\qquad (11, k) = 1$

$\varphi(n) = \varphi(11k) = \underbrace{\varphi(11)}_{10} \cdot \varphi(k) = 30$

$= 10 \cdot \varphi(k) = 30 \implies \underline{\varphi(k) = 3}$

nema rješenja

3° $7 \mid n$

$n = 7k$

$\varphi(n) = \varphi(7k) = \underbrace{\varphi(7)}_{6} \cdot \varphi(k) = 30$

$= 6 \cdot \varphi(k) = 30 \implies \underline{\varphi(k) = 5}$

nema rješenja

$4^\circ)$ $2^\alpha,\ 3^\beta,\ 2^\alpha \cdot 3^\beta$

$2^{\alpha-1}(2-1) = 30 \Rightarrow$ nema rješenja

$3^{\beta-1}(3-1) = 30 \Rightarrow$ nema rješenja

$2^{\alpha-1}3^{\beta-1}(3-1)(2-1) = 30 \Rightarrow$ nema rješenja

$\boxed{\text{Zadatak}}$ Odredimo zadnje dvije znam. broja 2^{2012}

$$2^{2012} \equiv a \pmod{100}$$

$$\Updownarrow$$

$$2^{2012} \pmod 4$$
$$2^{2012} \pmod{25}$$

$2^{2012} \equiv 0 \pmod 4$

$2^{2012} \equiv ? \pmod{25}$

$(2,25) = 1$

$2^{\varphi(25)} \equiv 1 \pmod{25}$

$\varphi(25) = 25\left(1-\frac{1}{5}\right) = 20$

$2^{20} \equiv 1 \pmod{25}$

$(2^{20})^{100} \equiv 1^{100} \pmod{25}$

$2^{2000} \equiv 1 \pmod{25}$

$2^{2012} = \underbrace{2^{2000}}_{1} \cdot 2^{12}$

$\equiv 2^{12} \pmod{25}$

$2^5 = 32 \equiv 7 \pmod{25}$

$32 - 25$

$2^{12} = 2^{10} \cdot 2^2 = \underbrace{(2^5)^2} \cdot 2^2$

$\equiv 49 \cdot 2^2 \pmod{25}$

$\equiv -1 \cdot 4 \pmod{25}$

$\equiv -4 \pmod{25}$

$\equiv 21 \pmod{25}$

$\left.\begin{aligned} x &\equiv 0 \pmod 4 \\ x &\equiv 21 \pmod{25} \end{aligned}\right\}$ KIN. TEOREM

$x = 25x_1 + 4x_2 \pmod{100}$

zadnje dvije znam. su 96

$25x_1 \equiv 0 \pmod 4 \rightarrow x_1 = 0$

$4x_2 \equiv \underset{-4}{\underset{\sim}{21}} \pmod{25} \rightarrow x_2 = 24$

$x = 4 \cdot 24 = 96 \pmod{100}$

DEFINICIJA 1.13. $(a,n)=1$

najmanji $d \in \mathbb{N}$ takav da je $a^d \equiv 1 \pmod n$

zove se red od a modulo n

PROPOZICIJA 1.30. Neka je d red od a modulo n

$$a^k \equiv 1 \pmod n \iff d \mid k$$

specijalno vrijedi $\rightarrow$ $d \mid \varphi(n)$

DOKAZ: $d \mid k \rightarrow k = l \cdot d$

$$a^k \equiv (a^d)^l \equiv 1^l \equiv 1 \pmod n$$

drugi smjer $\rightarrow$ $a^k \equiv 1 \pmod n$

$$k = g \cdot d + r, \quad 0 \le r < d$$

$$a^k \equiv a^{gd+r} \equiv \underbrace{(a^d)}_{1}{}^{g} a^r \pmod n \equiv a^r \equiv 1 \pmod n$$

$$\Downarrow$$

$$r = 0$$

$$\Downarrow$$

$$d \mid k$$

$\boxed{\text{Pr. 1.18.}}$ Svaki prosti djelitelj od $2^{2^n}+1$ za $n>1$

ima oblik $p = k \cdot 2^{n+1} + 1$, $k \in \mathbb{Z}$

$$p \mid 2^{2^n}+1$$

$$2^{2^n}+1 \equiv 0 \pmod p$$

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

$$2^{2^n} \cdot 2^{2^n} \equiv (-1)^2 \pmod p$$

$$2^{2^{n+1}} \equiv 1 \pmod p$$

$$2^{n+1} \mid \varphi(p)$$

$$2^{n+1} \mid p-1$$

$$p-1 = k \cdot 2^{n+1}$$

$$p = k \cdot 2^{n+1} + 1$$

DEFINICIJA 1.14. Ako je red od a modulo n jednak $\varphi(n)$, ...

onda se a zove primitivni korijen modulo n

TEOREM 1.31. p-prost broj

postoji točno $\varphi(p-1)$ primitivnih korijena mod p

DOKAZ ne treba jer je divlji

TEOREM 1.32. Za prirodan broj n postoji primitivni

korijen mod n

akko $n = 2, 4, p^i$ ili $2p^i$

p - neparan prost broj

dokaz je također divljaštvo

Kako se nalazi primitivni korijen?

$g = 2$, $g = 3$.

ne treba testirati . g_0^k ako g_0 nije prim. korijen

g je prim. korijen mod p akko za svaki prosti

faktor q od p-1 vrijedi :

$$g^{(p-1)/q} \not\equiv 1 \pmod{p}$$

$\boxed{\text{Pr. 1.19}}$ Nađite najmanji prim korijen

a) mod 5 b) mod 11 c) mod 23

a) $2^{\frac{5-1}{2}} = 2^2 = 4$ [počinjemo od 2, pa 3, ...]

$4 \not\equiv 1 \pmod 5$

2 je najmanji prim korijen mod 5

b) $11 - 1 = 10$ $10 = 5 \cdot 2$

$2^{\frac{10}{2}} = 2^5 = 32$

$32 \not\equiv 1 \pmod{11}$

$2^{\frac{10}{5}} = 2^2 = 4$

$4 \not\equiv 1 \pmod{11}$

2 je najm. prim korijen mod 11

c) $23 - 1 = 22$
$22 = 2 \cdot 11$

$2^{\frac{22}{11}} = 2^2 = 4$

$4 \not\equiv 1 \pmod{23}$

$2^{\frac{22}{2}} = 2^{11} = 32 \cdot 64 \equiv 9 \cdot (-5) \equiv 1 \pmod{23}$

2 nije prim. korijen mod 23

---

ispitujemo dalje za 3:

$3^2 = 9 \not\equiv 1 \pmod{23}$

$3^{11} = (\underbrace{3^3}_{27})^3 \cdot 3^2 \equiv (4)^3 \cdot 9 \equiv 64 \cdot 9 \equiv -5 \cdot 9 = -45 \equiv 1 \pmod{23}$

3 nije prim. korijen

za 4 ne treba provjeravati jer 2 nije

za 5:

$5^2 = 25 \equiv 2 \not\equiv 1 \pmod{23}$

$5^{11} = (\underbrace{5^2}_{25})^5 \cdot 5 \equiv (2)^5 \cdot 5 = 32 \cdot 5 \equiv 9 \cdot 5 = 45 \equiv -1 \not\equiv 1 \pmod{23}$

5 je najmanji prim. korijen mod 23

$\boxed{\text{Pr.}}$ Koliko ima prim korijena mod 23?

$p = 23$

$\varphi(23-1) = \varphi(22) = \varphi(2) \cdot \varphi(11)$

$= 22\left(1-\frac{1}{2}\right)\left(1-\frac{1}{11}\right) = 10$

10 prim. korijena mod 23.

DEFINICIJA 1.15. g - prim korijen modulo n

$1, g, g^2, \dots, g^{\varphi(n)-1}$ → reducirani sustav ostataka modulo n

$a \in \mathbb{Z} \quad (a,n) = 1 \quad \exists!\, l \quad g^l \equiv a \pmod{n}$

l – indeks od a (u odnosu na g)

oznake → $\operatorname{ind}_g a$ ili $\operatorname{ind} a$

TEOREM 1.34.

(1) $\operatorname{ind} a + \operatorname{ind} b \equiv \operatorname{ind}(ab) \pmod{\varphi(n)}$

(2) $\operatorname{ind} 1 = 0, \quad \operatorname{ind} g = 1$

(3) $\operatorname{ind}(a^m) \equiv m \operatorname{ind} a \pmod{\varphi(n)} \quad m \in \mathbb{N}$

(4) $\operatorname{ind}(-1) = \frac{1}{2}\varphi(n) \quad n \geq 3$

PROPOZICIJA 1.35. $(n, p-1) = 1 \Rightarrow x^n \equiv a \pmod p$

ima jedinstveno rješenje

DOKAZ: $x^n \equiv a \pmod p$

$$\Downarrow$$

$$\operatorname{ind}(x^n) \equiv \operatorname{ind} a \pmod{\varphi(p)}$$

$$n \cdot \operatorname{ind} x \equiv \operatorname{ind} a \pmod{p-1}$$

$(n, p-1) = 1 \Rightarrow$ jed. rješenje

$\boxed{\text{Pr. 1.20}}$ $x^5 \equiv 2 \pmod 7$

$7 - 1 = 6 \rightarrow \frac{6}{2}, \frac{6}{3}$

$2^2 = 4 \not\equiv 1 \pmod 7$

$2^3 = 8 \equiv 1 \pmod 7$ $\rightarrow$ 2 nije prim. korijen mod 7

$3^2 = 9 \not\equiv 1 \pmod 7$

$3^3 = 27 \equiv 6 \not\equiv 1 \pmod 7$ $\rightarrow$ 3 je prim. korijen mod 7

$\operatorname{ind}_g a \rightarrow$ gdje je g prim. korijen

$\operatorname{ind}_3 (x^5) \equiv \operatorname{ind}_3 2 \pmod 6$ $\rightarrow \varphi(7)$

$5 \cdot \operatorname{ind}_3 x \equiv \underbrace{\operatorname{ind}_3 2}_{2} \pmod 6$

$5 \cdot \operatorname{ind}_3 x \equiv 2 \pmod 6$

$(5,6) = 1$

$5 \operatorname{ind}_3 x \equiv 20 \pmod 6 \quad /:5$

$\operatorname{ind}_3 x = 4$

$x \equiv \underbrace{3^4}_{81} \pmod 7$

$x \equiv 4 \pmod 7$

$\operatorname{ind}_3 2$ pogađamo 2

$3^1 \equiv 3 \pmod 7$

$3^{2} \equiv 2 \pmod 7$

$\uparrow$

$\operatorname{ind}_3 2 = 2$

Naći sve prim. korijene mod 7

$\varphi(7-1) = \varphi(6) = 2 \longrightarrow$ postoje 2 prim. korijena mod 7

$\cancel{2}, 3, \cancel{4}, \underbrace{5, 6}$

provjeriti još 5 i 6

$5^2 = 25 \not\equiv 1 \pmod 7$
$5^3 = 125 \not\equiv 1 \pmod 7$ } 5 je prim. korijen mod 7

6 nije (postoje samo 2 prim. korijena)

$\boxed{\text{Pr. 1.21.}}$ $5x^4 \equiv 3 \pmod{11}$

$\hookrightarrow$ 2 je najmanji prim. korijen mod 11

$\mathrm{ind}_2(5x^4) \equiv \mathrm{ind}_2 3 \pmod{10}$ $\to p-1$

$\underbrace{\mathrm{ind}_2 5}_{4} + 4\,\mathrm{ind}_2 x \equiv \underbrace{\mathrm{ind}_2 3}_{8} \pmod{10}$

$2^4 \equiv 5 \pmod{11}$
$2^8 \equiv 3 \pmod{11}$

$4 + 4\,\mathrm{ind}_2 x \equiv 8 \mod (10)$

$4\,\mathrm{ind}_2 x = 4 \mod (10) \longrightarrow (4,10) = 2 \longrightarrow$ 2 rješenja

$4\,\mathrm{ind}_2 x \equiv 4 \pmod{10} \ / :2$ $\left[\left(\mathrm{mod}\ \underbrace{\frac{10}{\gcd(4,10)}}_{5} \right) \right]$

$2\,\mathrm{ind}_2 x \equiv 2 \pmod 5 \ / :2$ $(2,5) = 1$

$\mathrm{ind}_2 x \equiv 1 \pmod 5$

$\mathrm{ind}_2 x \equiv 1 \pmod{10}$ $\mathrm{ind}_2 x \equiv 6 \pmod{10}$

$x = 2^1 \pmod{11}$ $x = \underbrace{2^6}_{64} \pmod{11}$

$x = 2 \pmod{11}$ $x = 9 \pmod{11}$

$\boxed{\text{Pr. 1.22.}}$ $3^x \equiv 2 \pmod{23}$

$\hookrightarrow$ 5 je prim. korijen

$$ind_5(3^x) \equiv ind_5 2 \pmod{22}$$

$$x \underbrace{ind_5 3}_{16} \equiv \underbrace{ind_5 2}_{2} \pmod{22}$$

$5^{16} \equiv 3 \pmod{23}$
$5^{2} \equiv 2 \pmod{23}$

$16x \equiv 2 \pmod{22} \rightarrow (16, 22) = 2$

$\hookrightarrow$ 2 rješenja

$16x \equiv 2 \pmod{22} \; / :2$

$8x \equiv 1 \pmod{11}$ $(8, 11) = 1$

$8x \equiv 56 \pmod{11} \; / :8$

$x \equiv 7 \pmod{11}$

$x \equiv 7 \pmod{22}$ $x \equiv 18 \pmod{22}$

1.3. KVADRATNI OSTATCI

DEFINICIJA 1.16. $(a,m)=1$

Ako $x^2 \equiv a \pmod m$ ima rješenja $\Rightarrow$ a je KVADRATNI OSTATAK modulo m

u protivnom $\rightarrow$ a je kvadratni NEOSTATAK modulo m

$\boxed{\text{Pr.}}$ modulo 5

$x^2 \equiv a \pmod 5$ $\rightarrow$ 1 i 4 kvadratni ostatci

$\rightarrow$ 2 i 3 neostatci

$1^2 \equiv 1 \pmod 5$

$2^2 \equiv 4 \pmod 5$

$3^2 \equiv 4 \pmod 5$

$4^2 \equiv 1 \pmod 5$

TEOREM 1.36. p - neparan prost broj

reducirani sustav ostataka mod p

sastoji se od $\frac{p-1}{2}$ kvadratnih ostataka

i $\frac{p-1}{2}$ kvadratnih neostataka

DOKAZ: $-\frac{p-1}{2}, -\frac{p-3}{2}, \ldots, -1, 1, \ldots, \frac{p-1}{2}$

$1^2, 2^2, \ldots, \left(\frac{p-1}{2}\right)^2$

tj. $p \mid k-l$

ili

$p \mid k+l$

k, l $\qquad k^2 \equiv l^2 \pmod p$

$k^2 - l^2 \equiv 0 \pmod p$

$0 < k-l < k+l < 2 \cdot \frac{p-1}{2} < p-1 < p$

$(k-l)(k+l) \equiv 0 \pmod p$

DEFINICIJA 1.17. p-neparan prost broj

$$\left(\frac{a}{p}\right) = \begin{cases} 1, & a \text{ kvadratni ost. mod } p \\ -1, & a \text{ kvadratni neost. mod } p \\ 0, & p \mid a \end{cases}$$

Broj rješenja jedn. $x^2 \equiv a \pmod p$:

$$1 + \left(\frac{a}{p}\right)$$

TEOREM 1.37. (EULEROV KRITERIJ)

$$\left(\frac{a}{p}\right) \equiv a^{\frac{p+1}{2}} \pmod p$$

PROPOZICIJA 1.38.

(1) $a \equiv b \pmod p \Rightarrow \left(\frac{a}{p}\right) = \left(\frac{b}{p}\right)$

(2) $\left(\frac{a}{p}\right)\left(\frac{b}{p}\right) = \left(\frac{ab}{p}\right)$

(3) $(a,p) = 1$ $\qquad \left(\frac{a^2}{p}\right) = 1$

(4) $\frac{1}{p} = 1$ $\qquad \left(\frac{-1}{p}\right) = (-1)^{\frac{p-1}{2}}$

DOKAZ:

(2) $\left(\frac{a}{p}\right)\left(\frac{b}{p}\right) \equiv a^{\frac{p-1}{2}} b^{\frac{p-1}{2}} \equiv (ab)^{\frac{p-1}{2}} \equiv \left(\frac{ab}{p}\right) \pmod p$

Gaussov kvadratni zakon reciprociteta

p, q → različiti prosti brojevi

$$\left(\frac{p}{q}\right)\left(\frac{q}{p}\right) = (-1)^{\frac{(p-1)(q-1)}{4}}$$

$p < q$

DEFINICIJA 1.18. m - neparan prirodan broj

$$m = \prod p_i^{\alpha_i}$$

Jacobijev simbol : $\left(\frac{a}{m}\right) = \prod \left(\frac{a}{p_i}\right)^{\alpha_i}$

Očito $(a,m) > 1 \rightarrow \left(\frac{a}{m}\right) = 0$

a - kvadratni ostatak mod m

a - kvadratni ostatak mod p_i

$\Rightarrow \left(\frac{a}{m}\right) = 1$

obrat ne vrijedi tj.

$\left(\frac{a}{m}\right) = 1 \not\Rightarrow$ a kvadr. ostatak mod m

PRAVILA

(1) $a \equiv b \pmod m \Rightarrow \left(\frac{a}{m}\right) = \left(\frac{b}{m}\right)$

(2) $\left(\frac{ab}{m}\right) = \left(\frac{a}{m}\right)\left(\frac{b}{m}\right)$ $\left(\frac{a}{mn}\right) = \left(\frac{a}{m}\right)\left(\frac{a}{n}\right)$

(3) $\left(\frac{-1}{m}\right) = (-1)^{\frac{m-1}{2}} = \begin{cases} 1, & m \equiv 1 \pmod 4 \\ -1, & m \equiv 3 \pmod 4 \end{cases}$

(4) $\left(\frac{2}{m}\right) = (-1)^{\frac{m^2-1}{8}} = \begin{cases} 1, & m \equiv 1,7 \pmod 8 \\ -1, & m \equiv 3,5 \pmod 8 \end{cases}$

(5) $\left(\frac{m}{n}\right)\left(\frac{n}{m}\right) = (-1)^{\frac{(m-1)(n-1)}{4}}$ $(m,n) = 1$

Pr. 1.24. $\left(\frac{105}{317}\right)$

$$\left(\frac{105}{317}\right)\left(\frac{317}{105}\right) = (-1)^{\frac{104\cdot 316}{4}}$$

$$= 1$$

$$\left(\frac{105}{317}\right) = \left(\frac{317}{105}\right) = \left(\frac{2}{105}\right) = 1$$

Pr. 1.25 $\left(\frac{-23}{83}\right)$

$$= \left(\frac{-1\cdot 23}{83}\right) = \underbrace{\left(\frac{-1}{83}\right)}_{-1}\left(\frac{28}{83}\right)$$

$$= -\left(\frac{23}{83}\right)$$

$$\left(\frac{23}{83}\right)\cdot\left(\frac{83}{23}\right) = (-1)^{\frac{22\cdot 82}{4}} = -1$$

$$= -\left(-\left(\frac{83}{23}\right)\right) = \frac{83}{23} = \left(\frac{14}{23}\right)$$

$$= \underbrace{\left(\frac{2}{23}\right)}_{1}\left(\frac{7}{23}\right) = \left(\frac{7}{23}\right)$$

$$\left(\frac{7}{23}\right)\left(\frac{23}{7}\right) = (-1)^{\frac{6\cdot 22}{4}} = (-1)$$

$$-\left(\frac{23}{7}\right) = -\left(\frac{2}{7}\right) = \underline{\underline{-1}}$$