[illegible] definicije

TEORIJA BROJEVA 2012 Vježbe UM

5. VJEŽBE

①

$\mathbb{N} := \{1, 2, 3, 4, \dots\}$ osnovne računske operacije: $+, \cdot$

$\mathbb{Z} := \{\dots, -2, -1, 0, 1, 2, \dots\}$ osnovne računske operacije: $+, -, \cdot$

Teorem (dijeljenje s ostatkom) Neka su $a \in \mathbb{Z}$, $b \in \mathbb{N}$. Tada postoje jedinstveni q i (q ← KVOCIJENT) koji zadovoljavaju

$$\begin{cases} a = b \cdot q + r \\ 0 \le r < l \end{cases}$$

OS

~~$q = k$ DIV l~~ ~~$r = k$ MOD l~~

Definicija Za $a, b \in \mathbb{Z}$ kažemo da a dijeli b, i pišemo ako postoji $k \in \mathbb{Z}$ takav da je $b = a \cdot k$.

Primjer

$2 \mid 4$ jer je $4 = 2 \cdot 2$

$-2 \mid 4$ jer je $4 = (-2) \cdot (-2)$

$2 \mid -4$ jer je $-4 = 2 \cdot (-2)$

$5 \mid -5$ jer je $-5 = 5 \cdot (-1)$

$7 \mid 0$ jer je $0 = 7 \cdot 0$

$0 \mid 0$ jer je $0 = 0 \cdot 31$ ☺

Kako dokazati $l \nmid k$? Ako je $l = 0$, jednostavno metodom kontradikcije:

$0 \nmid 7$, jer bi inače bilo $7 = 0 \cdot m = 0$ ↯

Ako je $l > 0$, po teoremu: ako nađemo $r \neq 0$ koji zadovoljava uvjete, znamo da je jedinstven.

$3 \nmid 8$ jer je $8 \text{ MOD } 3 = 2 \neq 0$ (jer je $8 = 3 \cdot 2 + 2$ i $0 \le 2 < 3$)

$5 \nmid -17$ jer je $(-17) \text{ MOD } 5 = 3 \neq 0$ (jer je $-17 = 5 \cdot (-4) + 3$ i $0 \le 3 < 5$)

Ako je $l < 0$, znamo da je $l \mid k$ ekvivalentno s $-l \mid k$ $(k = l \cdot m = (-l) \cdot (-m))$

$-5 \nmid 16$ jer $5 \nmid 16$ (jer $16 = 5 \cdot 3 + 1$ i $0 < 1 < 5$)

ako je $r = k \text{ MOD } l \neq 0$, tada je $(-k) \text{ MOD } l = l - r$ KORISNO

Zadatak Ispitajte svojstva relacije $\mid$ na ⓐ $\mathbb{Z}$, ⓑ $\mathbb{N}$.

ⓐ & ⓑ: refl ✓ jer za svaki k, $k \mid k$ (jer $k = k \cdot 1$)

tranz ✓ jer $a \mid b \mid c$ povlači $b = a \cdot k$ i $c = b \cdot l$, a tada je $c = b \cdot l = (a \cdot k) \cdot l = a \cdot (\underbrace{k \cdot l}_{\in \mathbb{Z}})$, pa $a \mid c$.

sim ✗ jer $2 \mid 6$, ali $6 \nmid 2$
$(6 = 2 \cdot 3)$ $(2 \text{ MOD } 6 = 2 \neq 0)$

irefl ✗ jer $3 \mid 3$ $(3 = 3 \cdot 1)$

ⓐ antisim ✗ jer $5 \mid -5$ i $-5 \mid 5$, ali $5 \neq -5$
$(-5 = 5 \cdot (-1))$ $(5 = (-5) \cdot (-1))$

VAŽNO!

ⓑ antisim ✓ jer $a \mid b \mid a$ povlači $a = b \cdot k$ i $b = a \cdot l$, pa je $a = a \cdot l \cdot k$ $/ : a\ (> 0)$, odnosno $l \cdot k = 1$

Iz $a, b > 0$ dobijemo $l, k > 0$ $\Rightarrow$

Zadatak ⓐ Ako $a \mid b$ i $a \mid c$, tada $a \mid b + c$ i $a \mid b - c$.

DZ ⓑ Ako $a \mid b$ ili $a \mid c$, tada $a \mid b \cdot c$.

~~Obrati ovih tvrdnji~~ NE VRIJEDE! ~~ⓐ $2 \mid 3 - 1$ i $2 \mid 3 + 1$~~ ~~ⓑ $6 \mid 2 \cdot 3$, ali $6 \nmid 2$~~

Dokaz:

$a \mid b \Leftrightarrow \exists k \in \mathbb{Z},\ b = ak$
$a \mid c \Leftrightarrow \exists l \in \mathbb{Z},\ c = al$ $\Rightarrow$

$\Rightarrow \exists k, l \in \mathbb{Z}$
$b + c = a(k + l)$ $\Rightarrow a \mid b + c$

Zadatak Dokažite: $3 \mid n^3 - n$ (za svaki cijeli broj n)

$n^3 - n = n(n^2-1) = n(n-1)(n+1) = (n-1)n(n+1)$ → PRODUKT 3 UZASTOPNA BROJA

Od 3 uzastopna broja, jedan je sigurno djeljiv s 3 (zašto? jer ostaci pri dijeljenju s 3 su im ~~točno~~ 0, 1, 2, pa je jedan od njih 0), pa je produkt djeljiv s 3.

uo ? po
cajevima:

~~Ili 1°) n MOD 3 = 0 : $n = 3k$ za neki k~~

~~$n^3 - n = (3k)^3 - 3k = 27k^3 - 3k = 3\cdot\overbrace{(9k^3 - k)}^{\in\mathbb{Z}}$~~

~~2°) n MOD 3 = 1 : $n = 3k+1$ za neki k~~

~~$n^3 - n = (3k+1)^3 - (3k+1) = 27k^3 + 27k^2 + 9k + 1 - 3k - 1 = 3\cdot\overbrace{(9k^3 + 9k^2 + 2k)}^{\in\mathbb{Z}}$~~

~~3°) n MOD 3 = 2 : $n = 3k+2$ za neki k~~

~~$n^3 - n = (3k+2)^3 - (3k+2) = 27k^3 + 54k^2 + 36k + 8 - 3k - 2 = 3\cdot\overbrace{(9k^3 + 18k^2 + 11k + 2)}^{\in\mathbb{Z}}$~~

Zadatak Dokažite: $5 \mid n^5 - n$.

$n^5 - n = n(n^4-1) = n(n^2-1)(n^2+1) = n(n-1)(n+1)(n^2+1)$

1° $n = 5k$ za neki $k\in\mathbb{Z}$: OK 2° $n = 5\ell+1$ za neki $\ell\in\mathbb{Z}$ ⇒ $(n-1) = 5\ell$ OK

~~1°) n MOD 5 ∈ {0, 1, 4} n, n−1 ili n+1 je djeljiv s 5, pa je i produkt~~

3°) ~~n MOD 5 = 2~~ : $n = 5k+2$ za neki $k\in\mathbb{Z}$; $n^2+1 = (5k+2)^2+1 = 25k^2 + 20k + 4 + 1 = 5\overbrace{(5k^2+4k+1)}^{\in\mathbb{Z}}$ ✓

4°) ~~n MOD 5 = 3~~ : kao gore ↗, ~~ili (−n) MOD 5 = 5 − 3 = 2, a (−n)² + 1 = n² + 1, pa je djeljivo s 5~~

$n = 5\ell+3$ za neki $\ell\in\mathbb{Z}$ $(n^2+1) = ((5\ell+3)^2+1) = (25\ell^2 + 20\ell + 9 + 1) = 5\underbrace{(5\ell^2 + 4k + 2)}_{\in\mathbb{Z}}$

DZ $7 \mid n^7 - n$ 5°) $n = 5\ell+4$ za neki $k\in\mathbb{Z}$ ⇒ $n+1 = 5\ell+5 = 5(\ell+1)$ OK

~~Definicija Za $n \geq 2$ kažemo da je prim-broj ako $k \mid n$ povlači $k \in \{1, n, -1, -n\}$. Primijetimo da obrat uvijek vrijedi: $1 \mid n$, $-1 \mid n$, $n \mid n$, $-n \mid n$. Dakle, prim-brojevi su oni koji imaju točno 4 djelitelja (složeni više od 4, 1 i −1 imaju 2, a 0 ima beskonačno mnogo~~

Def Kažemo da je prirodan broj prost ili prim-broj ako vrijedi $p > 1$ & $(\forall n\in\mathbb{N})(n \mid p \Rightarrow n \in \{1, p$

VAŽNE ČINJENICE:

- Euklidov teorem: prostih brojeva ima beskonačno mnogo.
- Osnovni teorem aritmetike: svaki prirodan broj se može na jedinstven način zapisati kao produkt prim-brojeva, zanemarujući poredak

5 = 3 · 5 · 7
4 = 2 · 2 · 2 · 3
99 = 29 · 31
7 = 7 ← produkt 1 prim-broja
1 ← produkt 0 prim-brojeva

Zadatak Neka je m produkt prvih 100 prim-brojeva.

ⓐ Odredite zadnju znamenku od m.

$m = 2\cdot 3\cdot 5\cdot 7 \cdots p_{100} = 10\cdot\overbrace{3\cdot 7\cdots}^{\in\mathbb{Z}}$

Dakle, $10 \mid m$, pa je zadnja znamenka od m jednaka 0.

ⓑ Odredite ~~m MOD 4~~ ostatak pri dijeljenju m

$m = 2\cdot\underbrace{p_2\, p_3 \cdots p_{100}} = 2\cdot(2k+1) = 4k + \underline{\underline{2}}$: 0:

svi su neparni, pa im je produkt nepar

Dakle, ~~m MOD 4 = 2~~, ostatak je 2.

Zadatak Može li zbroj 4 uzastopna cijela broja biti prim-broj?

Pretpostavimo: $n + (n+1) + (n+2) + (n+3) = 4n + 6 = \underbrace{2(2n+3)}_{\text{paran}}$ je prim-broj $\Big\}$ $2(2n+3) = \overset{\text{JEDINI PARAN P}}{\downarrow}2 \;/:2$

$2n + 3 = 1$
$\underline{n = -1}$

Dakle, jedini takav slučaj je $(-1) + 0 + 1 + 2 = 2$

~~Zadatak P = {n ≥ 2 : n prim-broj} = {2, 3, 5, 7, 11, 13, 17, 19, 23, 29, 31, 37}~~

Zadatak Ako je n neparan, odredite ~~[illegible]~~ ostatak pri dijeljenju n^2 s 8. ⑧ XX

$$n^2 = (2k+1)^2 = 4k^2+4k+1 = 4\underbrace{k(k+1)}_{\text{UMNOŽAK 2 UZASTOPNA BROJA} \to \text{PARAN}}+1 = 4\cdot 2l+1 = 8l+1 \;;\; 0 \le 1 < 8$$

↳ ostatak je 1

Zadatak Možda ne

Ako su $n_1=\overline{abc}$ i $n_2=\overline{def}$ dva troznamenkasta prirodna broja čiji je zbr dijeljiv s 37, tada je i $n=\overline{abcdef}$ djeljiv s 37.

Pretpostavimo: $37 \mid n_1+n_2$, dakle $n_1+n_2 = 37k$ za neki $k\in\mathbb{Z}$. ~~Tada~~

$$n = \overline{abcdef} = \overline{abc000}+\overline{def} = 1000\cdot n_1+n_2 = 1000n_1+37k-n_1 = 999n_1+37k = 37(k+$$

Definicija Neka su $a,b\in\mathbb{Z}\setminus\{0\}$ ~~[illegible]~~. Za d ~~[illegible]~~ prirodan broj kažemo da je najveća zajednička mjera od a i b, i pišemo $d = NZM(a,b)$, ako ima sljedeća svojstva:

- $d\mid a$ i $d\mid b$
- ako $c\in\mathbb{N}$ zadovoljava $c\mid a$ i $c\mid b$, ~~povlači~~ onda $c\mid d$

ako su d i d' dvije NZM, tada $d'\mid d$ i $d\mid d'$, pa $d'=d$ jer su prirodni brojevi, a | je antisimetrična na $\mathbb{N}$

Teorem $NZM(a,b)$ je najmanji prirodan broj oblika ~~[illegible]~~ $ax+by$, $x,y\in\mathbb{Z}$.

- ~~Postoji prirodan broj tog oblika (npr. $a\cdot a+b\cdot b=a^2+b^2>0$ jer a i b nisu oba 0), pa postoji i najmanji takav (zbog principa indukcije, korolar.)~~

Označimo: $d := NZM(a,b)\in\mathbb{N}$; $c := \min(\mathbb{N}\cap\{ax+by : x,y\in\mathbb{Z}\})\in\mathbb{N}$

$\boxed{d\mid c}$ $c = ax_0+by_0$, a $d\mid a$ i $d\mid b$, dakle $d\mid ax_0$ i $d\mid by_0$, pa $d\mid c$ ✓

$\boxed{c\mid d}$ ~~Dovoljno je dokazati $c\mid a$. Tada analogno $c\mid b$, pa $c\mid d$. Pretpostavimo suprotno, …~~ ~~Označimo … mod … tada $0<r<a$ (r je prirodan broj manji od c) … Kontradikcija …~~

Podijelimo s ostatkom:

$d = c\cdot q+r$, $0\le r<c$

$\Rightarrow r = ax_0+by_0-q(ax_1+by_1) = a(x_0-qx_1)+b(y_0-qy_1)$ ← broj tog oblika ≥ 0, a manji od c. Slijedi $r=0$. Dakle, $c\mid d$.

Zadatak Dokažite $\underbrace{NZM(a,b)}_{d:=} = \underbrace{NZM(a,a+b)}_{e:=}$

Oboje $d,e\in\mathbb{N}$. Dakle $e\mid d$ i $d\mid e$ povlači $e=d$.

$\boxed{d\mid e}$ Imamo: $d\mid a$, $d\mid b \Rightarrow d\mid a+b$ $\Big\}$ $d\mid e$

$\boxed{e\mid d}$ Imamo: $e\mid a$, $e\mid a+b \Rightarrow e\mid b$ $\Big\}$ $e\mid d$ ✓

Zadatak DZ Dokažite $NZM(a,b) = NZM(b,a-b) = NZM(b, a \bmod b)$

~~Npr. $NZM(420,195) = NZM(195, 420 \bmod 195) = NZM(195,30) = NZM(30,15) = NZM(15,0) = 15$~~ ~~$195\cdot 2+30$~~ ~~$=30\cdot 6+15$~~ ~~$=15\cdot 2+0$~~

~~Koliko je $NZM(a,0)$? Djelitelji 0 su svi cijeli brojevi. Zajednički djelitelji 0 i a su dakle djelitelji od a. Najveći od njih je upravo $|a|$.~~

~~$NZM(a,0)=|a|$~~

Euklidov algoritam: dijelimo veći broj manjim, i zamijenimo veći broj ostatkom.

$NZM(a,b)=?$ $a>b$ To radimo dok ostatak ne postane 0 — tada je |manji broj| NZM.

$a = b\cdot q_1+r_1$ (~~Često~~ zanemarujemo predznake, jer $NZM(a,b) = NZM(|a|,|b|)$.)

$b = r_1 q_2 + r_2$

$999 : 37 = 27$ $\overline{\underline{XXIII}}$

) n neparan, $n^2 \bmod 8$

$$n^2 = (2k+1)^2 = 4k^2 + 4k + 1 = 4\underbrace{\overset{\text{par}}{\overbrace{k(k+1)}}} + 1 = 8k + 1$$

Zad Ako su $n_1 = \overline{abc}$ i $n_2 = \overline{def}$ dva troznam. pr. broja čiji je zbroj djeljiv s 37, onda je i $n = \overline{abcdef}$

$$n = \overline{abcdef} = \overline{abc000} + \overline{def} = 1000 \cdot n_1 + n_2 = 999 n_1 + (n_1 + n_2) =$$

$$= 999 n_1 + 37k = 37(27 n_1 + k)$$

Def NZD: Neka su $a, b \in \mathbb{Z}$. Za $d \in \boxed{\mathbb{N}}$ kažemo da je NZD ako:

1) $d \mid a$ i $d \mid b$
2) $c \mid a$ i $c \mid b \Rightarrow c \mid d$

jedinstvenost
$d \mid d'$ i $d' \mid d$

Tm. $NZD(a,b)$ je najmanji prirodni broj oblika $k \cdot a + l \cdot b$ za neke $k, l \in \mathbb{Z}$

Dokaz Neka je $d = NZD(a,b)$, $c = \min\left(\{k \cdot a + l \cdot b \mid k, l \in \mathbb{Z}\} \cap \mathbb{N}\right)$

$\boxed{d \mid c}$ $c = k_0 \cdot a + l_0 \cdot b$ i $d \mid a$ i $d \mid b \Rightarrow d \mid k_0 a$, $d \mid l_0 \cdot b \Rightarrow$ ~~d~~ $d \mid c$

$\boxed{c \mid d}$ dovoljno: $c \mid a$. Pretp. $c \nmid a$. Tada je $a = q \cdot c + r$, $0 < r < c$

$$\Rightarrow r = a - q \cdot c = a - q(k_0 \cdot a + l_0 \cdot b) =$$

$$= a - q \cdot k_0 \cdot a - q \cdot l_0 \cdot b = \underbrace{(1 - q k_0)}_{\in \mathbb{Z}} a + \underbrace{(-q l_0)}_{\in \mathbb{Z}} \cdot b$$

$$\Rightarrow r \in \{k \cdot a + l \cdot b \mid k, l \in \mathbb{Z}\} \cap \mathbb{N} \text{ i } r < c \quad \boxed{\Rightarrow\Leftarrow}$$

ZAD $NZD(a,b) = NZD(b, a-b) = NZD(b, a \bmod b)$

$$\underset{d}{\Downarrow}$$

~~$d \mid a-b \Rightarrow$~~

$d = k_0 \cdot a + l_0 \cdot b = (k_0 + l_0)a - l_0 a + l_0 b = (k_0 + l_0)a + (-l_0)(a-b)$

$c \mid b \ , \ c \mid a-b \Rightarrow c \mid a \Rightarrow c \mid d$

$d \mid a \bmod b \Rightarrow d \mid a$ $\qquad a = b \cdot q + r$

$d \mid q \qquad a = b \cdot d \cdot \cancel{x} + r$

$a = d^2 x y + r$

$c \mid a \ , \ c \mid b$

$a = b \cdot q + \boxed{r}$

$r = a - bq$

$d = NZD(a,b) = (NZD(a, a+b)) = e$

$\left.\begin{array}{l} d \mid a \ , \ d \mid b \Rightarrow d \mid a+b \Rightarrow d \mid e \\ e \mid a, \ e \mid a+b \overset{\text{slično}}{\Rightarrow} e \mid b \Rightarrow e \mid d \end{array}\right\} \Rightarrow d = e$

Zadatak Odredite NZM(3094, 19950) Euklidovim algoritmom.

a	b	a MOD b
	a DIV b	

→ ④ XXIV

19950 3094 1386 322 98 28 $\boxed{14}$ 0
6 2 4 3 3 2 ← NZM

Iz Euklidovog algoritma možemo dobiti i zapis NZM$(a,b) = \underline{k_0}\cdot a + \underline{l_0}\cdot b$, ovako:

$\text{NZM}(3094, 19950) = 14 = 98 \text{ MOD } 28 = \underline{98 - 3\cdot 28} = 98 - 3\cdot(322 \text{ MOD } 98) = 98 - 3\cdot(322 - 3\cdot 98)$

$= 98 - 3\cdot 322 + 3\cdot 3\cdot 98 = \underline{(1+3\cdot 3)}\cdot 98 - 3\cdot 322 = \underline{10\cdot 98 - 3\cdot 322} = 10\cdot(1386 \text{ MOD } 322) - 3\cdot 322$

$= 10\cdot(1386 - 4\cdot 322) - 3\cdot 322 = 10\cdot 1386 - \underline{(10\cdot 4 + 3)}\cdot 322 = \underline{10\cdot 1386 - 43\cdot 322} = [\text{1386 MOD}$

$= 10\cdot 1386 - 43\cdot(3094 - 2\cdot 1386) = \underline{(10 + 43\cdot 2)}\cdot 1386 - 43\cdot 3094 = \underline{96}\cdot(\underbrace{19950 - 6\cdot 3094}_{=1386}) -$

$\underline{-43\cdot 3094} = \underline{96\cdot 19950 + (-619)\cdot 3094}$

$14 = \boxed{1}\cdot 14 + 0\cdot\boxed{28} =$
$= \boxed{1}\,\boxed{98} - 3\cdot\boxed{28} =$
$= \boxed{10}\,\boxed{98} - 3\cdot\boxed{322} =$
$= \boxed{10}\cdot\boxed{1386} - \boxed{43}\,\boxed{322} =$
$= \boxed{96}\cdot 1386 - 43\,\boxed{3094} =$
$= \boxed{96}\cdot 19950 - 619\cdot 3094$

Bolji zapis

$14 = 0\cdot 28 + \boxed{1}\cdot 14 =$
$= \boxed{1}\cdot 98 + (-3)\cdot 28 =$
$= (-3)\cdot 322 + \boxed{10}\cdot 98 =$
$= \boxed{10}\cdot 1386 + \boxed{(-43)}\cdot 322 =$
$= \boxed{(-43)}\cdot 3094 + 96\cdot 1386 =$
$= 96\cdot 19950 + (-619)\cdot 3094$

$= 1 - 3\cdot(-3)$

$= -3 - 4\cdot\boxed{10}$

19950 : 3094 = 6
1386
3094 : 1386 = 2
322
1386 : 322 = 4
98
322 : 98 = 3
28
98 : 28 = 3
$\boxed{14}$ ← MJE
28 : 14 = 2
0

	6	2	4	3	3	2
−619	96	−43	10	−3	1	0

	x	
y−q·x	x	y

Sve skupa: $\boxed{19950 \quad 3094}$ 1386 322 98 28 $\boxed{14}$ 0
6 2 4 3 3 2
$\boxed{-619 \quad 96}$ −43 10 −3 $\boxed{1 \quad 0}$

Kako doći zapis $ax_0 + l$
$14 = ⓽⓼ - 3\cdot(28) = (98) - 3\cdot((322)$
$= 10\cdot(98) - 3\cdot(322) = 10\cdot((1386)$
$- 3\cdot(322) = 10\cdot(1386) - 43\cdot(322)$
$= 10\cdot(1386) - 43\cdot(\boxed{3094} - 2(13$
$= -43\cdot\boxed{3094} + 96\cdot(1386) =$
$= -43\cdot\boxed{3094} + 96\cdot(\boxed{19950} - 6\cdot$
$= 96\cdot\boxed{19950} - 619\cdot\boxed{30$

Zadatak Odredite NZM(483327, 226304) i prikažite je kao linearnu kombinaciju argumenata.

483327 226304 30719 11271 8177 3094 1989 1105 884 $\boxed{221}$ 0
2 7 2 1 2 1 1 1 4
$\boxed{472 \quad -221}$ 30 −11 8 −3 2 −1 1 0

$\text{NZM} = 221 = 472\cdot 226304 - 221\cdot 483327$

D.Z. $\text{NZM}(3050, 2107) = k_0\cdot 3050 + l_0\cdot 2107$. Odredite k_0 i l_0.

Definicija Za brojeve a i b kažemo da su relativno prosti ako je NZM(a, b) = 1.

Zadatak Dokažite da se razlomak $\frac{7n+1}{21n+4}$ ne može skratiti ni za koji n.

Dokazujemo da su $7n+1$ i $21n+4$ relativno prosti, za svaki n.

$\text{NZM}(7n+1, 21n+4) = \text{NZM}(7n+1, 21n+4-(7n+1)) = \text{NZM}(7n+1, 14n+3) = \text{NZM}(7n+1, 7n+$
$= \text{NZM}(7n+1, 1) =: d$ Znamo: $d \mid 1$, $d \in \mathbb{N} \Rightarrow$ dakle, $\boxed{d=1}$ ✓ Općenito, $\boxed{\text{NZM}(a,1) =}$

Relativno prosti brojevi imaju svojstvo da je neka njihova linearna kombinacija jednaka 1 (i obrnuto, ako takva postoji, očito je 1 najmanji takav, pa je NZM=1). To je vrlo korisno.

6 VJEŽBE

(8) X

KARAKTERIZACIJA NZM-a od M(a,b)

Lema Ako $a \mid b \cdot c$ i $NZM(a,b)=1$, tada $a \mid c$.

~~Dokaz: Pretpostavimo $b \cdot c = a \cdot m_0$ i $a \cdot k + b \cdot l = 1$ za neke $k, l, m_0 \in \mathbb{Z}$~~

~~$c = c \cdot 1 = c \cdot (a \cdot k + b \cdot l) = c \cdot a \cdot k + \boxed{b \cdot c} \cdot l = a \cdot (c \cdot k + m_0 \cdot l)$, dakle $a \mid c$.~~

$M(a,b) = 1 \Rightarrow$
$1 = ax + by$ za ne(ke) $x, y \in \mathbb{Z}$
Pomnožimo s c: $\Rightarrow$
$c = cax + cby$ djeljivo

~~**Propozicija** Ako $a \mid c$, $b \mid c$ i $NZM(a,b)=1$, tada $a \cdot b \mid c$.~~

~~Dokaz: Pretpostavimo $a \mid c$, $b \mid c$ i $NZM(a,b)=1$~~

~~$c = a \cdot m$ za neki m~~

~~Dakle $b \mid a \cdot m$ i $NZM(b,a)=1$ [illegible] $b \mid m$ [illegible]~~

~~[illegible] $c = a \cdot m = a \cdot (b \cdot n) = (a \cdot b) \cdot n$, dakle $a \cdot b \mid c$~~

Korolar Ako je p ~~[illegible]~~ prost i $p \mid a \cdot b$, tada $p \mid a$ ili $p \mid b$.

Dokaz: Pretpostavimo p ~~[illegible]~~ prost, $p \mid a \cdot b$, i $p \nmid a$. (Trebamo: $p \mid b$)

Što je $NZM(p,a)$? ~~[illegible]~~

Jedini prirodni djelitelji od p su 1 i p.

p nije zajednički djelitelj od a i p jer $p \nmid a$.

Dakle, jedini (pa i najveći) zajednički djelitelj je 1.

prost broj je relativno prost s nekim drugim brojem ako i samo ako ga ne dijeli

Dakle, $p \mid a \cdot b$ i $NZM(p,a)=1$. Po Lemi, $p \mid b$ ✓

Napomena Bez uvjeta o (relativnoj) prostosti gornje tvrdnje ne vrijede!

~~[illegible]~~ $6 \mid 8 \cdot 9 = 72$, ali $6 \nmid 8$ i $6 \nmid 9$

do tud

Definicija Za $a, b \in \mathbb{Z}$ i $n \in \mathbb{N}$, kažemo da su a i b kongruentni modulo n i pišemo $a \equiv b \pmod n$, ako $n \mid a-b$. ← a i b imaju isti ostatak pri dijeljenju s n.

Osnovna svojstva relacije $\equiv \pmod n$ (za fiksni n)

Samo zapisat da se prisjetimo def. relacije ekvivalencije i klase

refl ✓ $a - a = 0$, $n \mid 0$ za svaki n, dakle $a \equiv a \pmod n$ ✓

sim ✓ Ako $n \mid a-b$, tada $b - a = (-1) \cdot (a-b)$, dakle $a-b \mid b-a$, pa $n \mid b-a$ ✓

tranz ✓ Ako $n \mid a-b$ i $n \mid b-c$, tada $n \mid (a-b)+(b-c) = a-c$, pa je $a \equiv c \pmod n$ ✓

antiref ✗ jer $5 \equiv 5 \pmod n$ (jer $n \mid 5-5=0$)

antisim ✗ jer $0 \equiv n \pmod n$ (jer $n \mid 0-n = -n = n \cdot (-1)$) i $n \equiv 0 \pmod n$ (zbog simetričnosti) ali $n \neq 0$ jer $n \in \mathbb{N}$.

Dakle, $\equiv \pmod n$ je relacija ekvivalencije. Kako izgledaju klase ekvivalencije?

$[0]_n = \{x : x \equiv 0 \pmod n\} = \{x : n \mid x - 0 = x\} = \{\dots, -2n, -n, 0, n, 2n, \dots\} = n\mathbb{Z}$

$[1]_n = \{x : x \equiv 1 \pmod n\} = \{x : n \mid \underbrace{x-1}_{=k \cdot n}\} = \{kn+1 : k \in \mathbb{Z}\} = \{\dots, 1-2n, 1-n, 1, n+1, 2n+1, \dots\}$

$[2]_n = \{kn+2 : k \in \mathbb{Z}\}$

$[n-1]_n = \{kn+n-1 : k \in \mathbb{Z}\} = \{\boxed{(k+1)}n + (-1) : \boxed{k+1} \in \mathbb{Z}\} = [-1]_n$

$[n]_n = [0]_n$ a tako dalje ciklički. Dakle, imamo točno n klasa.

Što je jednako u svakoj klasi? Ostatak pri dijeljenju s n!

n klasa ostataka $[0] = \{nk \mid k \in \mathbb{Z}\}$ $[1] = \{nk+1 \mid k \in \mathbb{Z}\}$ ... $[n-1] = \{nk$

čunanje s klasama (modularna aritmetika)

Propozicija: Ako je $a \equiv c \pmod{n}$ i $b \equiv d \pmod{n}$, tada je

ⓐ $a+b \equiv c+d \pmod{n}$

$\boxed{D2}$ ⓑ $a-b \equiv c-d \pmod{n}$

ⓒ $a \cdot b \equiv c \cdot d \pmod{n}$

ⓓ $a^k \equiv c^k \pmod{n}$, za svaki $k \in \mathbb{N}$

Kongruencije se mogu međusobno zbrajati, oduzimati i množiti, te potencirati prirodnim brojem (baš kao i cijeli brojevi) $\boxed{+,-,\cdot}$

kaz: Pretpostavimo ~~$a-c = n \cdot l$ i $d-b = n \cdot m$~~ za neke l i m. Tada: $a = c+nl$, $b = d+nm$

~~$(a+b)-(c+d) = c+nl+d+nm-c-d = nl+nm = n(l+m)$ ← djeljivo s n~~

~~$(a-b)-(c-d) = c+nl-(d+nm)-(c-d) =$ [illegible] $= n(l-m)$ ← djeljivo s n~~

~~$a \cdot b - c \cdot d = (c+nl)(d+nm) - cd = cd + ndl + cnm + n^2lm - cd = n(dl+cm+nlm)$~~

~~$a^k - c^k = (a-c)(a^{k-1} + a^{k-2}c + \dots + ac^{k-2} + c^{k-1})$ ← djeljivo s n, dakle $a^k \equiv c^k$~~

&vc

$(a-c)+(b-d)$

$(a-b)-(c-d)$

$\equiv cd$ (mod n)

ⓒ $n \mid a-c \Rightarrow n \mid ab-cb$
$n \mid b-d \Rightarrow n \mid cb-cd$ $\Big\} \Rightarrow n \mid ab-cb+cb-cd$
$\Rightarrow n \mid ab-cd$

ⓓ ku

12 ⓒ

ecijalno, kongruencije se mogu množiti cijelim brojem:

$12 \equiv 27 \pmod{5}$ / $\cdot 3$ (zapravo množimo kongruencijom $3 \equiv 3 \pmod{5}$)

$36 \equiv 81 \pmod{5}$ ✓

Mogu li se kratiti (s brojem $\neq 0$)? Ne uvijek! ‖ $12 \equiv 42 \pmod{10}$ /:6 $2 \equiv 7 \pmod{10}$? ali $2 \not\equiv 7 \pmod{10}$!

MOŽEMO KRATITI SAMO S NEČIM ŠTO JE REL PRO S MODULOM!

mogu se kratiti nečim što je relativno prosto s modulom.

ropozicija: Ako je $m \cdot a \equiv m \cdot b \pmod{n}$ i $NZM(m,n) = 1$, tada je $a \equiv b \pmod{n}$.

Dokaz: Pretpostavimo $n \mid m \cdot a - m \cdot b = m \cdot (a-b)$. Po Lem → , tada $n \mid a-b$. ✓

~~[illegible] $\equiv r \pmod{n}$ [illegible]~~

~~[illegible] $a = q \cdot n + r$, $0 \le r < n$ [illegible] $0 \le r < n$ [illegible]~~

Zadatak: Odredite ostatak pri dijeljenju $325 \cdot 837 - 258 \cdot 392$ brojem 9.

$325 \equiv 325 - \underbrace{270}_{9 \mid} = 55 \equiv 55 - \underbrace{54}_{9 \mid} = 1 \pmod{9}$

$837 \equiv 837 - 810 = 27 \equiv 0 \pmod{9}$

$258 \equiv 258 - 270 = -12 \equiv -12 + 18 = 6 \pmod{9}$

$392 \equiv 392 - 360 = 32 \equiv 32 - 27 = 5 \pmod{9}$

ILI:

$325 : 9 = 36$ i ost. 1
55
1

$837 : 9 = 93$ i ost. 0
27

$392 : 9 = 43$ i ost.
32

$258 : 9 = 28$ i ost. 6
78
6

$x := 325 \cdot 837 - 258 \cdot 392 \equiv 1 \cdot 0 - 6 \cdot 5 = -30 \equiv -30 + 36 = 6 \pmod{9}$ i $0 \le 6 < 9$

Dakle, ostatak je ~~[illegible]~~ 6.

Zadatak: Odredite zadnju znamenku broja $43567 \cdot 23408 \cdot 32147 - 2543$

Ⓓ2 $x := 43567 \cdot 23408 \cdot 32147 - 2543 \equiv 7 \cdot 8 \cdot 7 - 3 = 56 \cdot 7 - 3 \equiv 6 \cdot 7 - 3 = 42 - 3 \equiv 2 - 3 = -1 \equiv \pmod{10}$

ili: $\equiv (-3) \cdot (-2) \cdot (-3) - 3 = -18 - 3 = -21 \equiv 9 \pmod{10}$ & $0 \le 9 < 10 \Rightarrow$ ~~[illegible]~~ ostatak je 9.

Očito je $x > 0$, pa je zadnja znamenka od x jednaka 9.

Zadatak Odredite ostatak pri dijeljenju 3^{71} s 41.

Tražimo neku potenciju od 3 koja ima lijep ostatak pri dijeljenju s 41.

$(3^0=1,)\ 3^1=3,\ 3^2=9,\ 3^3=27,\ 3^4=81\equiv 40\equiv \underline{-1} \pmod{41}$ ← −1 je lako potencirati!

$3^{71}=3^{4\cdot 17+3}=(3^4)^{17}\cdot 3^3\equiv(-1)^{17}\cdot 27=-27\equiv -27+41=14$ & $0\leq 14<41$

Dakle, ostatak je 14.

Zadatak Odredite ostatak pri dijeljenju $225^{52}\cdot 113^{23}\cdot 557^{29}+240^{157}\cdot 518^{258}$ brojem 37

$37\cdot 3=111$

$225\equiv 225-222\equiv 3 \pmod{37}$

$113\equiv 113-111=2 \pmod{37}$

$557\equiv 557-555=2 \pmod{37}$

$240\equiv 240-222=18 \pmod{37}$

$518\equiv 518-555=-37\equiv 0$

$225^{52}\cdot 113^{23}\cdot 557^{29}+240^{157}\cdot 518^{258}\equiv 3^{52}\cdot\underbrace{2^{23}\cdot 2^{29}}+18^{157}\cdot 0^{258}=$

$=3^{52}\cdot 2^{52}+\cancel{18^{157}\cdot 0}=6^{52}=6^{2\cdot 26}=(6^2)^{26}=36^{26}\equiv(-1)^{26}=1 \pmod{37}$ & $0\leq 1<37$

Dakle, ~~$225^{52}\cdot 113^{23}\cdot 557^{29}+240^{157}\cdot 518^{258}$~~ ostatak je 1.

Zadatak Odredite zadnje 2 znamenke broja 205^{205}.

$205^{205}\equiv \underline{5^{205}}=5^{202}\cdot 5^3=5^{202}\cdot 125\equiv 5^{202}\cdot 25=5^{202}\cdot 5^2=\underline{5^{204}}\equiv 5^{203}\equiv 5^{202}\equiv\ldots\equiv 5^3\equiv 5^2=$

$\pmod{100}$ & $0\leq 25<100$ ⟹ zadnje dvije znamenke od 205^{205} su 25.

DZ Odredite 2^{100} MOD ⓐ 11 ⓑ 25 ⓒ 62)

LINEARNE KONGRUENCIJE

TO NE RADIMO.

~~Za a, b, n zadane $(n>0)$ tražimo sve x takve da je $ax\equiv b \pmod{n}$~~

~~Preciznije, za zadane klase $[a]_n$ i $[b]_n$, tražimo klasu (ili više njih) $[x]_n$ t.d. $[a]_n[x]_n$~~

~~Kao kod linearnih jednadžbi: $5x=7\ /\cdot 5^{-1}$, dakle stvar se svodi na nalaženje inverz~~

~~$x=7\cdot 5^{-1}$~~

~~Inverz od $[a]_n$ je klasa $[k]_n$ t.d. $[a]_n[k]_n=[1]_n$, odnosno $ak\equiv 1 \pmod{n}$.~~

~~Raspišimo: $n\mid ak-1$, dakle $ak-1=n\cdot l$, odnosno $ak+n\cdot(-l)=1$.~~

~~Takav k znamo da postoji ako i samo ako su a i n relativno prosti,~~

~~i znamo ga naći Euklidovim algoritmom.~~

~~**Primjer** $\underline{7}x\equiv 2 \pmod{\underline{104}}\ /\cdot 15$~~

~~$\underbrace{7\cdot 15}_{\equiv 1}x\equiv 2\cdot 15 \pmod{104}$~~

~~$\boxed{x\equiv 30 \pmod{104}}$ → Kongruencija ima jedinstveno rješenje (klasu $[30]_{104}$)~~

~~primijetimo da u toj klasi ima beskonačno mnogo brojeva: 30, 134, 550~~

~~104 7 6 $\boxed{1}$ 0~~

~~14 1 6~~

~~$\boxed{15}$ −1 1 0 0~~

~~znamo $7\cdot 15+104\cdot(-1)=1$~~

~~$7\cdot 15-1=104$~~

~~$104\mid 7\cdot 15-1$~~

~~$7\cdot 15\equiv 1 \pmod{104}$~~

~~Što kada a i n nisu relativno prosti?~~

~~6 4 $\boxed{2}$ 0~~

~~1 2~~

~~−1 1 0~~

~~Ne postoji k takav da je $4k\equiv 1 \pmod{6}$~~

~~**Ali:** $4\cdot(-1)\equiv 2 \pmod{6}$~~

~~$4\cdot(-1)+6\cdot 1=2$~~

~~$2\cdot(-1)+3\cdot 1=1$~~

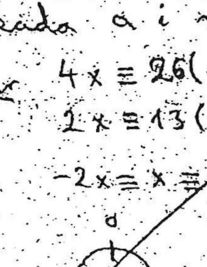
~~**Primjer** $4x\equiv 26 \pmod{6}\ /:2$~~

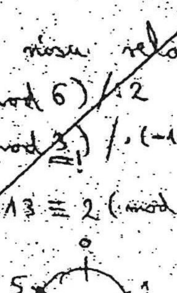
~~$2x\equiv 13 \pmod{\underset{!}{3}}\ /\cdot(-1)$~~

~~$-2x\equiv x\equiv -13\equiv 2 \pmod{3}$ Dakle, $x\equiv 2 \pmod{3}$. Koje su to klase mod 6? $[2]_6,\ [2+3]_6$~~

~~+3~~

~~(Kao sat: 7 (mod 12) znači 7 ili 19 (mod 24))~~





$10-14=-4$, $4|-4$

$10\equiv -2 \pmod 4$ $10-(-2)=10+2=12$ ✓

Def Za $a,b\in\mathbb{Z}$ kažemo da su **kongruentni modulo** $n\in\mathbb{N}$ i pišemo

$$a\equiv b \pmod n$$

ako $n|a-b$. „a i b se razlikuju za višekratnik od n"

Nap: $a=q_1n+r_1$, $r_1\in\{0,1,\dots n-1\}$

$b=q_2n+r_2$, $r_2\in\{0,1,\dots n-1\}$

$$\Rightarrow a-b=(q_1-q_2)n+(r_1-r_2)$$

$$n|a-b \Leftrightarrow n|\underbrace{r_1-r_2}_{\cap} \Leftrightarrow r_1-r_2=0 \Leftrightarrow r_1=r_2$$

$$r_1-r_2\in\{-(n-1),\dots -1,0,1,\dots n-1\}$$

Dakle, $a\equiv b \pmod n$ akko a i b daju isti ost. pri dijeljenju s n.

Kongruencija modulo n je relacija ekvivalencije:

$$(\forall a\in\mathbb{Z})(a\equiv a \pmod n)$$

$$(\forall a,b\in\mathbb{Z})(a\equiv b \pmod n \Rightarrow b\equiv a \pmod n)$$

$$(\forall a,b,c\in\mathbb{Z})(a\equiv b \pmod n \land b\equiv c \pmod n \Rightarrow a\equiv c \pmod n)$$

Prop: Ako je $a\equiv b \pmod n$ i $c\equiv d \pmod n$, onda je

a) $a+c\equiv b+d \pmod n$

b) $a-c\equiv b-d \pmod n$

c) $a\cdot c\equiv b\cdot d \pmod n$

d) $a^k\equiv b^k \pmod n$, $\forall k\in\mathbb{N}$

Kongruencije se mogu međusobno zbrajati, oduzimati i množiti, te potencirati prirodnim brojevima

DOKAZ: Pretp. $a \equiv b \pmod{n}$ i $c \equiv d \pmod{n}$

(a)
$$\left.\begin{array}{l} a \equiv b \pmod{n} \Leftrightarrow n \mid a-b \\ c \equiv d \pmod{n} \Leftrightarrow n \mid c-d \end{array}\right\} \Rightarrow n \mid \underset{(a+c)-(b+d)}{\underset{\shortparallel}{(a-b)+(c-d)}}$$

$$\Rightarrow n \mid (a+c)-(b+d) \Rightarrow a+c \equiv b+d \pmod{n}$$

(b) DZ

(c)
$$\left.\begin{array}{l} n \mid a-b \Rightarrow n \mid c(a-b) \\ n \mid c-d \Rightarrow n \mid b(c-d) \end{array}\right\} \Rightarrow n \mid ca - \cancel{cb} + \cancel{bc} - bd$$

$$\Rightarrow n \mid ac-bd \Rightarrow ac \equiv bd \pmod{n}$$

(d) DZ, (Uputa: indukcija po k, iskoristiti (c) u koraku)

■

Nap Ako je $a \equiv b \pmod{n}$, onda je i

$$a+c \equiv b+c \pmod{n}$$

$$a \cdot c \equiv b \cdot c \pmod{n}$$

za bilo koji $c \in \mathbb{Z}$.

Nap $6 \equiv 18 \pmod{4}$ $[4 \mid 6-18 = -12]$

Je li $1 \equiv 3 \pmod{4}$? NE! $(4 \nmid 1-3 = -2)$

$\Rightarrow$ Ne možemo „kratiti" kongruencije!

Prop Ako je $ma \equiv mb \pmod{n}$ i $M(m,n) = 1$, onda je $a \equiv b \pmod{n}$

DOKAZ: $ma \equiv mb \pmod{n} \Rightarrow n \mid ma - mb \Rightarrow n \mid m(a-b)$

$$n \mid m(a-b) \wedge M(m,n) = 1 \xRightarrow{(\text{Lema})} n \mid a-b$$

$$\Rightarrow a \equiv b \pmod{n}$$

■

Zad 10 Odredite ostatak pri dijeljenju

$$325 \cdot 837 - 258 \cdot 392 =: N$$

brojem 9

Rj Tražimo $r \in \{0,1,2,\dots,8\}$ t.d. $N \equiv r \pmod 9$

$N = q \cdot 9 + r \Rightarrow 9 \mid 9q = N - r \Rightarrow N \equiv r \pmod 9$

$325 : 9 = 36$
55
①
$\Rightarrow 325 \equiv 1 \pmod 9$

$837 : 9 = 93$
27
⓪
$\Rightarrow 837 \equiv 0 \pmod 9$

$258 : 9 = 28$
78
⑥
$\Rightarrow 258 \equiv 6 \pmod 9$

$392 : 9 = 43$
32
⑤
$\Rightarrow 392 \equiv 5 \pmod 9$

$N = 325 \cdot 837 - 258 \cdot 392 \equiv 1 \cdot 0 - 6 \cdot 5 = -30$

$0 \equiv 36 \pmod 9$

$N + 0 \equiv -30 + 36 = 6 \pmod 9$ $\qquad \underline{\underline{N \equiv 6 \pmod 9}}$

N pri dijeljenju s 9 daje ost. 6

(DZ) Odredite zadnju znamenku broja

$$43567 \cdot 23408 \cdot 32147 - 2543 =: N$$

Uputa: zadnja znamenka = ost. pri dijeljenju s 10

tražimo $0 \leq r \leq 9$ t.d. $N \equiv r \pmod{10}$

Zad 11 Odredite ostatak pri dijeljenju 3^{71} s 41

Rj Ideja: Tražimo potenciju od 3 koja daje „lijep" ostatak pri dijeljenju s 41

$3^0 = 1 \rightarrow$ ok ali ne pomaže nam puno

$3^1 = 3,\ 3^2 = 9,\ 3^3 = 27,\ 3^4 = 81 \equiv 40 \pmod{41}$

$40 \equiv 40 - 41 = -1 \pmod{41}$

↳ $3^4 \equiv -1 \pmod{41}$

$71 : 4 = 17$
31
$③$

$$3^{71} = 3^{4\cdot 17+3} = (3^4)^{17}\cdot 3^3 \equiv (-1)^{17}\cdot 27$$

$$= -1\cdot 27 \equiv -27 + 41 = \underline{\underline{14}} \qquad 0 \le 14 < 41$$

Dakle, ostatak je 14.

Zad 12 Odredite ostatak pri dijeljenju broja

$$225^{52}\cdot 113^{23}\cdot 557^{29} + 240^{157}\cdot 518^{258} =: N$$

brojem 37.

Rj $225 : 37 = 6$
-222
$③$

$113 : 37 = 3$
-111
$②$

$557 : 37 = 15$
187
$②$

$225 \equiv 3 \pmod{37}$ $\quad 113 \equiv 2 \pmod{37}$ $\quad 557 \equiv 2 \pmod{37}$

$240 : 37 = 6$
$⑱$

$240 \equiv 18 \pmod{37}$

$518 : 37 = 14$
148
$⓪$

$518 \equiv 0 \pmod{37}$

$6^2 = 36$
$\equiv 36 - 37 = -1$

$$\Rightarrow N \equiv 3^{52}\cdot 2^{23}\cdot 2^{29} + 18^{157}\cdot 0^{258} = 3^{52}\cdot 2^{52}$$

$$= 6^{52} = (6^2)^{26} = (36)^{26} \equiv (-1)^{26} = 1 \pmod{37}$$

Traženi ostatak je 1.

Zad 13 Odredite zadnje dvije znamenke broja

$$205^{205}$$

Rj Tražimo ostatak pri dijeljenju sa 100

$$205 \equiv 5 \pmod{100}$$

$$\begin{aligned}205^{205} &\equiv 5^{205} \equiv 5^{202} \cdot 5^3 = 5^{202} \cdot 125\\ &\equiv 5^{202} \cdot 25 = 5^{201} \cdot 125 \equiv 5^{201} \cdot 25\\ &= 5^{200} \cdot 125 \equiv 5^{200} \cdot 25 = 5^{199} \cdot 125\\ &\equiv \ldots \equiv 125 \equiv 25 \pmod{100}\end{aligned}$$

$\Rightarrow$ zadnje dvije znamenke su 25

Zad 14 Dokažite: $3 \mid n \iff 3 \mid (\text{zbroj znamenaka od } n)$

Rj Neka je $n = \overline{a_k a_{k-1} \cdots a_1 a_0}$.

Dovoljno je dokazati da je $n \equiv a_0 + a_1 + \cdots + a_k \pmod{3}$

Uočimo: $10 \equiv 1 \pmod{3}$

$$\Rightarrow 10^m \equiv 1^m = 1 \pmod{3}, \ \forall m \in \mathbb{N}$$

$$\begin{aligned}n &= a_0 + 10 a_1 + 10^2 a_2 + \cdots + 10^k a_k\\ &\equiv a_0 + 1 \cdot a_1 + 1 \cdot a_2 + \cdots + 1 \cdot a_k\\ &= a_0 + a_1 + \cdots + a_k \pmod{3}\end{aligned}$$

(DZ) $9 \mid n \iff 9 \mid (\text{zbroj znam. od } n)$

TEORIJA BROJEVA

$\mathbb{N} := \{1, 2, 3, 4, \dots\}$ osnovne računske operacije: $+, \cdot$

$\mathbb{Z} := \{\dots, -2, -1, 0, 1, 2, \dots\}$ osnovne računske operacije: $+, -, \cdot$ ← univerzalni skup

eorem (dijeljenje s ostatkom) Neka su $k \in \mathbb{Z}$, $l \in \mathbb{N}$. Tada postoje jedinstveni q i r

KVOCIJENT ↑ q ↑ r OSTATAK.

koji zadovoljavaju $\begin{cases} k = q \cdot l + r \\ 0 \leq r < l \end{cases}$

$k \equiv q$ (DIV l)
$k \equiv r$ (MOD l)

Oznake: $q =: k$ DIV l
$r =: k$ MOD l

NE MORA BITI $l > 0$

PAZITI NA REDOSLIJED!

efinicija Za proizvoljne k, l kažemo da l dijeli k (k je djeljiv s l), i pišemo $l | k$, ako postoji m takav da je $k = l \cdot m$.

rimjer
$2 | 4$ jer je $4 = 2 \cdot 2$
$-2 | 4$ jer je $4 = (-2) \cdot (-2)$
$2 | -4$ jer je $-4 = 2 \cdot (-2)$
$5 | -5$ jer je $-5 = 5 \cdot (-1)$
$7 | 0$ jer je $0 = 7 \cdot 0$
$0 | 0$ jer je $0 = 0 \cdot 31$ ☺

Kako dokazati $l \nmid k$? Ako je $l = 0$, jednostavno metodom kontradikcije.

$r \neq 0 \Leftrightarrow k \not\equiv 0$ (MOD l)

$0 \nmid 7$, jer bi inače bilo $7 = 0 \cdot m = 0$ ↯

Ako je $l > 0$, po teoremu: ako nađemo $r \neq 0$ koji zadovoljava uvjete, znamo da je jedinstven.

$3 \nmid 8$ jer je 8 MOD $3 = 2 \neq 0$ (jer je $\underline{8 = 3 \cdot 2 + 2}$ i $\underline{0 \leq 2 < 3}$)

$5 \nmid -17$ jer je (-17) MOD $5 = 3 \neq 0$ (jer je $-17 = 5 \cdot (-4) + 3$ i $0 \leq 3 < 5$)

Ako je $l < 0$, znamo da je $l | k$ ekvivalentno s $-l | k$ ($k = l \cdot m = (-l) \cdot (-m)$)

$-5 \nmid 16$ jer $5 \nmid 16$ (jer $16 = 5 \cdot 3 + 1$ i $0 < 1 < 5$)

ako je $r = k$ MOD $l \neq 0$, tada je $(-k)$ MOD $l = l - r$ KORISNO!

adatak Ispitajte svojstva relacije $|$ na ⓐ $\mathbb{Z}$, ⓑ $\mathbb{N}$.

ⓐ & ⓑ: refl ✓ jer za svaki k, $k | k$ (jer $k = k \cdot 1$)

trans ✓ jer $a | b | c$ povlači $b = a \cdot k$ i $c = b \cdot l$, a tada je
$c = b \cdot l = (a \cdot k) \cdot l = a \cdot \underbrace{(k \cdot l)}_{\in \mathbb{Z}}$, pa $a | c$.

sim ✗ jer $2 | 6$, ali $6 \nmid 2$
($6 = 2 \cdot 3$) (2 MOD $6 = 2 \neq 0$)

irefl ✗ jer $3 | 3$ ($3 = 3 \cdot 1$)

ⓐ antisim ✗ jer $5 | -5$ i $-5 | 5$, ali $5 \neq -5$
($-5 = 5 \cdot (-1)$) ($5 = (-5) \cdot (-1)$)

VAŽNO!

ⓑ antisim ✓ jer $a | b | a$ povlači
$a = b \cdot k$ i $b = a \cdot l$, pa je
$a = a \cdot l \cdot k$ $/ : a \, (\neq 0)$, odnosno $l \cdot k = 1$
Iz $a, b > 0$ dobijemo $l, k > 0$ $\Rightarrow$

adatak ⓐ Ako $k | l$ i $k | m$, tada $k | l + m$ i $k | l - m$.

DZ ⓑ Ako $k | l$ ili $k | m$, tada $k | l \cdot m$.

Obrati ovih tvrdnji NE VRIJEDE! ⓐ $2 | 3 - 1$ i $2 | 3 + 1$, ali $2 \nmid 3$.
ⓑ $6 | 2 \cdot 3$, ali $6 \nmid 2$ i $6 \nmid 3$.

[illegible]tak Dokažite: $3 \mid n^3 - n$ (~~za~~ svaki cijeli broj n)

$n^3 - n = n(n^2-1) = n(n-1)(n+1) = (n-1)n(n+1) \longleftrightarrow$ PRODUKT 3 UZASTOPNA BROJA

Od 3 uzastopna broja, jedan je sigurno djeljiv s 3 (zašto? jer ostaci pri dijeljenju s 3 su im točno 0, 1, 2, pa je jedan od njih 0), pa je produkt djeljiv s 3.

$\boxed{\text{II}}$ 1°) $n \text{ MOD } 3 = 0$: $n = 3k$ za neki k

$n^3 - n = (3k)^3 - 3k = 27k^3 - 3k = 3 \cdot \overbrace{(9k^3 - k)}^{\in \mathbb{Z}}$

2°) $n \text{ MOD } 3 = 1$: $n = 3k+1$ za neki k

$n^3 - n = (3k+1)^3 - (3k+1) = 27k^3 + 27k^2 + 9k + \cancel{1} - 3k - \cancel{1} = 3 \cdot \overbrace{(9k^3 + 9k^2 + 2k)}^{\in \mathbb{Z}}$

3°) $n \text{ MOD } 3 = 2$: $n = 3k+2$ za neki k

$n^3 - n = (3k+2)^3 - (3k+2) = 27k^3 + 54k^2 + 36k + 8 - 3k - 2 = 3 \overbrace{(9k^3 + 18k^2 + 11k + 2)}^{\in \mathbb{Z}}$

[illegible]tak Dokažite: $5 \mid n^5 - n$

$n^5 - n = n(n^4 - 1) = n(n^2+1)(n^2-1) = n(n-1)(n+1)(n^2+1)$ [illegible] produkt ✓

1°) $n \text{ MOD } 5 \in \{0, 1, 4\}$ [illegible] $= 5\overbrace{(5k^2 + 4k + 1)}^{\in \mathbb{Z}}$ ✓

2°) $n \text{ MOD } 5 = 2$: $n = 5k+2$ [illegible] $+1 = n^2 + 1$, pa je djeljivo s 5 ✓

3°) $n \text{ MOD } 5 = 3$: kao gore [illegible] ✓

DZ $7 \mid n^7 - n$

Definicija Za $n \geq 2$ kažemo da je prim broj (prost broj) ako $k \mid n$ povlači $k \in \{1, n, -1, -n\}$.

Primijetimo da ~~[illegible]~~ uvijek vrijedi: $1 \mid n$, $-1 \mid n$, $n \mid n$, $-n \mid n$. Dakle, prim brojevi su oni koji imaju točno 4 djelitelja (ostali više od 4, 1 i −1 imaju 2, a 0 ima beskonačno mnogo).

VAŽNE ČINJENICE: • Euklidov teorem: prostih brojeva ima beskonačno mnogo

• Osnovni teorem aritmetike: svaki prirodan broj se može na jedinstven način zapisati kao produkt prim brojeva, zanemarujući poredak

$105 = 3 \cdot 5 \cdot 7$

$24 = 2 \cdot 2 \cdot 2 \cdot 3$

$899 = 29 \cdot 31$

$17 = 17$ ← produkt 1 prim broja

1 ← produkt 0 prim brojeva

Zadatak Neka je n produkt prvih 100 prim brojeva.

ⓐ Odredite zadnju znamenku od n.

$n = \overbrace{2 \cdot 3 \cdot 5}\, 7 \cdots p_{100} = 10 \cdot 3 \cdot 7 \cdots$

Dakle, $10 \mid n$, pa je zadnja znamenka od n jednaka 0.

ⓑ Odredite n MOD 4.

$n = 2 \cdot \underline{[illegible]} = 2 \cdot (2k+1) = 4k+2$

[illegible] neparni, pa im je i produkt nepa[illegible]

Dakle, n MOD $4 = 2$

Zadatak Može li zbroj 4 uzastopna ~~[illegible]~~ broja biti prim broj?

Pretpostavimo: $n + (n+1) + (n+2) + (n+3) = 4n + 6 = \underbrace{2(2n+3)}_{\text{paran}}$ je prim broj $\Rightarrow 2(2n+3) = 2$ / : 2

JEDINI PARAN [illegible]

$2n + 3 = 1$

$n = -1$

Dakle, jedini takav zbroj je $(-1) + 0 + 1 + 2 = 2$. MOŽE!

Oznaka: $\mathbb{P} = \{n \geq 2 : n \text{ prim broj}\} = \{2, 3, 5, 7, 11, 13, 17, 19, 23, 29, 31, 37, \ldots\}$

Zadatak: Ako je n neparan, odredite n^2 MOD 8.

$n^2=(2k+1)^2=4k^2+4k+1=4\underbrace{k(k+1)}_{\text{UMNOŽAK 2 UZASTOPNA BROJA} \Rightarrow \text{PARAN}}+1=4\cdot 2l+1=8l+1$, $0\leq 1<8$

$\hookrightarrow n^2$ MOD 8 = 1

Zadatak: Ako su $n_1=\overline{abc}$ i $n_2=\overline{def}$ dva troznamenkasta prirodna broja čiji je zbroj djeljiv s 37, tada je i $n=\overline{abcdef}$ djeljiv s 37.

Pretpostavimo $37|n_1+n_2$, dakle $n_1+n_2=37k$ za neki k. Tada

$n=\overline{abcdef}=\overline{abc}\cdot 1000+\overline{def}=1000n_1+n_2=1000n_1+37k-n_1=999n_1+37k=37\overbrace{(k+27n_1)}^{\in\mathbb{Z}}$

Definicija: Neka su $a,b\in\mathbb{Z}$ i nisu oba 0. Za $d\boxed{\in\mathbb{N}}$ (VAŽNO!) kažemo da je najveća zajednička mjera (NZM) od a i b, i pišemo $d=NZM(a,b)$, ako ima sljedeća svojstva:

- $d|a$ i $d|b$
- $c|a$ i $c|b$ povlači $c|d$

ako su d i d' dvije NZM, tada $d|d'$ i $d'|d$ pa $d=d'$ jer su prirodni brojevi, a [illegible] je [illegible] na $\mathbb{N}$

Teorem: $NZM(a,b)$ je najmanji prirodni broj oblika $ka+lb$.

- postoji prirodan broj tog oblika (npr., $a\cdot a+b\cdot b=a^2+b^2>0$ jer a i b nisu oba 0)

pa postoji i najmanji takav (zbog principa indukcije, kasnije)

Označimo $d=NZM(a,b)$ i $c=\min(\mathbb{N}\cap\{ka+lb: k,l\in\mathbb{Z}\})\in\mathbb{N}$

$\boxed{d|c}$ $c=k_0a+l_0b$, a $d|a$ i $d|b$, dakle $d|k_0a$ i $d|l_0b$, pa $d|c$ ✓

$\boxed{c|d}$ Dovoljno je dokazati $c|a$. Tada analogno $c|b$, pa $c|d$. Pretpostavimo suprotno, da

Označimo $r=a$ MOD c, $q=a$ DIV c, tada $\left\{\begin{array}{l} 0<r<c \text{ (r je prirodan broj manji od c)} \\ a=qc+r \\ r=a-qc=a-q(k_0a+l_0b)=\overbrace{(1-qk_0)}^{\in\mathbb{Z}}a+\overbrace{(-ql_0)}^{\in\mathbb{Z}}b \end{array}\right\}$ Kontradikcija (jer je c bio najmanji)

Zadatak: Dokazati $\underbrace{NZM(a,b)}_{d}=\underbrace{NZM(b,a+b)}_{e}$. Tada $d,e\in\mathbb{N}$. Dokažimo $e|d$ i $d|e$ pa slijedi $e=d$.

$\boxed{d|e}$ Imamo $d|a$, $d|b$ $\Rightarrow$ $d|a+b$ $\Rightarrow$ $d|e$

$\boxed{e|d}$ Imamo $e|b$, $e|a+b$ $\Rightarrow$ $e|a$ $\Rightarrow$ $e|d$ ✓

Zadatak $\boxed{DZ}$ Dokazati: $NZM(a,b)=NZM(b,a-b)=NZM(b,a \text{ MOD } b)$ [illegible]

VAŽNO!

Primjer: $NZM(420,195)=NZM(195,\underbrace{420 \text{ MOD } 195}_{195\cdot 2+30})=NZM(\underbrace{195,30}_{=30\cdot 6+15})=NZM(\underbrace{30,15}_{=15\cdot 2})=NZM(15,0)=15$

Koliko je $NZM(a,0)$? Djelitelji 0 su svi cijeli brojevi.

Zajednički djelitelji 0 i a su dakle djelitelji od a.

$\boxed{NZM(a,0)=|a|}$ Najveći od njih je upravo $|a|$.

Euklidov algoritam: dijeli veći broj manjim, a zamijeni veći broj ostatkom.

To radimo dok ostatak ne postane 0 – tada je 1. broj traženi NZM.

(Ovdje zanemarujemo predznake jer $NZM(a,b)=NZM(|a|,|b|)$)

datak: Odredite NZM(3094, 19950) Euklidovim algoritmom.

a	b	a MOD b
	a DIV b	

→ XXIV

19950	3094	1386	322	98	28	$\boxed{14}$	0
	6	2	4	3	3	2 ← NZM	

z Euklidovog algoritma možemo dobiti i zapis NZM(a,b) = k·a + l·b, ovako:

$$NZM(3094, 19950) = 14 = 98 \text{ MOD } 28 = 98 - 3 \cdot 28 = 98 - 3 \cdot (322 \text{ MOD } 98) = 98 - 3 \cdot (322 - 3 \cdot 98) =$$

$$= 98 - 3 \cdot 322 + 3 \cdot 3 \cdot 98 = (1 + 3 \cdot 3) \cdot 98 - 3 \cdot 322 = 10 \cdot 98 - 3 \cdot 322 = 10 \cdot (1386 \text{ MOD } 322) - 3 \cdot 322 =$$

$$= 10 \cdot (1386 - 4 \cdot 322) - 3 \cdot 322 = 10 \cdot 1386 - (10 \cdot 4 + 3) \cdot 322 = 10 \cdot 1386 - 43 \cdot 322 = \text{[I TAKO DALJE]}$$

$$= 10 \cdot 1386 - 43 \cdot (3094 - 2 \cdot 1386) = (10 + 43 \cdot 2) \cdot 1386 - 43 \cdot 3094 = 96 \cdot \underbrace{(19950 - 6 \cdot 3094)}_{=1386} -$$

$$- 43 \cdot 3094 = 96 \cdot 19950 + (-619) \cdot 3094$$

$$14 = 1 \cdot 14 + 0 \cdot 28 =$$
$$= 1 \cdot 98 - 3 \cdot 28 =$$
$$= 10 \cdot 98 - 3 \cdot 322 =$$
$$= 10 \cdot 1386 - 43 \cdot 322 =$$
$$= 96 \cdot 1386 - 43 \cdot 3094 =$$
$$= 96 \cdot 19950 - 619 \cdot 3094$$

Bolji zapis

$$14 = 0 \cdot 28 + 1 \cdot 14$$
$$= 1 \cdot 98 + (-3) \cdot 28$$
$$= (-3) \cdot 322 + 10 \cdot 98$$
$$= 10 \cdot 1386 + (-43) \cdot 322$$
$$= (-43) \cdot 3094 + 96 \cdot 1386 =$$
$$= 96 \cdot 19950 + (-619) \cdot 3094$$

	6	2	4	3	3	2
−619	96	−43	10	−3	1	0

←

	2	
y−2·x	x	y

Sve skupa

19950	3094	1386	322	98	28	$\boxed{14}$	0
	6	2	4	3	3	2	
−619	96	−43	10	−3	1	0	

datak: Odredite NZM(483327, 226304) i prikažite je kao linearnu kombinaciju argumenata.

483327	226304	30719	11271	8177	3094	1989	1105	884	$\boxed{221}$	0
	2	7	2	1	2	1	1	1	4	
472	−221	30	−11	8	−3	2	−1	1	0	

$$NZM = 221 = 472 \cdot 226304 - 221 \cdot 483327$$

Z 7. NZM(3050, 2107) = k·3050 + l·2107. Odredite k i l.

Definicija: Za brojeve a i b kažemo da su relativno prosti ako je NZM(a,b) = 1

datak: Dokažite da se razlomak $\frac{7n+1}{21n+4}$ ne može skratiti ni za koji n.

Dokazujemo da su 7n+1 i 21n+4 relativno prosti, za svaki n.

$$NZM(7n+1, 21n+4) = NZM(7n+1, 21n+4-(7n+1)) = NZM(7n+1, 14n+3) = NZM(7n+1, 7n+$$

$$= NZM(7n+1, 1) = d \quad \text{Znamo } d \mid 1,\ d \in \mathbb{N} \Rightarrow \text{dakle } \boxed{d = 1} \checkmark \quad \text{Općenito } \boxed{NZM(a,1) =$$

elativno prosti brojevi imaju svojstvo da je neka njihova linearna kombinacija jednaka 1

obrnuto, ako takva postoji, očito je 1 njihov djelitelj, pa je NZM = 1). To je vrlo korisno