ZVEZA MED GCD in LCM

$\gcd(20,30)=10 \quad \mathrm{lcm}(20,30)=60 \quad 10\cdot 60 = 20\cdot 30$

IZREK: $\gcd(a,b)\,\mathrm{lcm}(a,b) = ab \quad \forall a,b \in \mathbb{N}$.

Dokaz: let $d = \gcd(a,b)$ Poten:

$\boxed{a = a_1 d}$ in $\boxed{b = b_1 \cdot d}$. velja $a_1 \perp b_1$

trdimo, da je $\boxed{\dfrac{ab}{d}} = a_1 b_1 d = \mathrm{lcm}(a,b) = a_1 b = ab_1$

skupni večkratnik a in b

recimo $v = \mathrm{lcm}(a,b)$. Potem:

$v = \boxed{ap = bq}$ za neka p, q

$a_1 \cancel{d} p = b_1 \cancel{d} q$

tuji $a_1 p = b_1 q$

$\hookrightarrow b_1 \mid a_1 p$

$b_1 \mid p \sim p = \boxed{b_1 t} \quad t \in \mathbb{N}$

vstavimo

$v = ap = bp = ab_1 t = bb_1 k = a_1 d b_1 k = (a_1 b_1 d) k$

ker je $v = \mathrm{lcm}(a,b)$,

je $t = 1$. $\Rightarrow v = a_1 b_1 d$.

sedaj $d \cdot v \stackrel{?}{=} a \cdot b$

$d \cdot a_1 b_1 d \stackrel{?}{=} a \cdot b$

$\cancel{d} \cdot \dfrac{ab}{\cancel{d}} \stackrel{?}{=} a \cdot b$

$ab = ab$ ✓ □

PRAŠTEVILA

praštevilo je tak $p \in \mathbb{N}$ $\ni$: število deliteljev $(p) = 2$.

očitno 1 ni praštevilo.

sicer je sestavljeno, razen 1.

če sta p in $p+2$ praštevili, jima rečemo praštevilska dvojčka.

TRDITEV 8: let $a,b \in \mathbb{N}$, p praštevilo

velja 1.) $p \perp a$ ali $p | a$
  tuje / deli

2.) $p | ab \Rightarrow p|a$ ali $p|b$

3.) $\forall a \geq 2 \ \exists$ praštevilo $p \ \ni: p|a$

DOKAZ:

1.) pdd $p \not| a \Rightarrow gcd(a,p) \neq 1$

let $d = gcd(a,p) \neq 1 \Rightarrow d|p$ in $d \neq 1 \Rightarrow p = d$.

2.) naj $p|ab$ in $p \nmid a \Rightarrow \exists x,y \in \mathbb{Z} \ni$: (REA) $\boxed{px + ay = 1}$ /$\cdot b$

$\underbrace{pxb}_{\text{deljivo s } p} + \underbrace{ayb}_{\text{deljivo s } p \text{ (predp.)}} = b$

leva stran je deljiva s p, torej mora biti tudi desna $\Rightarrow p|b$.

3.) $\forall a \in \mathbb{N}: \exists p$ prašt. $\ni: p|a$.

Dokaz: let $M = \{2,3,4,\dots,a-1,a\}$.

Vzamemo k = najmanjše ~~tako~~ število iz M, ki deli a.

trdim, da k obstaja. če ne drugega, $a|a$.

trdim, da je k praštevilo. če bi ne bilo, bi imel k net delitelj manjši od k, ki bi bil hkrati delitelj a, zato bi ga našli prej kot a za naš k.

IZREK (Euklid): Praštevil je neskončno: RAA:

pdd jih je končno: $P = p_1, p_2, \dots, p_k$.

tedaj let $n = p_1 p_2 \cdots p_k + 1$.

po trditvi 3.) $\exists$ praštevilo, ki deli n.

to ni niti p_1, niti ..., niti p_k ampak nekaj novo.

Domneva (Polignac): Praštevilskih dvojčkov je neskončno mnogo.

KONGRUENCA PO MODULU m.

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

če $m \mid a-b$, rečemo a in b sta kongruentna po modulu m.

pišemo $\quad a \equiv b \pmod{m}$

lastnost: $\quad a \equiv b \pmod{m} \sim a \bmod m = b \bmod m$

1.) če $a \equiv b \pmod{m}$, $c \in \mathbb{Z}$, potem

$$a+c \equiv b+c \pmod{m}$$
$$ac \equiv bc \pmod{m}$$

2.) $a \equiv b \pmod{m}$ $\quad c \equiv d \pmod{m}$

$$a+c \equiv b+d \pmod{m}$$
$$a-c \equiv b-d \pmod{m}$$
$$ac \equiv bd \pmod{m}$$

$$m \overset{?}{\mid} ac-bd$$
$$m \overset{?}{\mid} ac-bc+bc-bd$$
$$m \mid c\underbrace{(a-b)}_{\mid m} + b\underbrace{(c-d)}_{\mid m} \quad \checkmark$$

DRUGI DOKAZ:

$a = (k+r) \quad b = (l+r)$

$c = (m+p) \quad d = (n+p)$

$(k+r)(m+p) \overset{?}{\equiv} (l+r)(n+p)$

$\cancel{km} + \cancel{kp} + \cancel{rm} + rp \overset{?}{\equiv} \cancel{ln} + \cancel{lp} + \cancel{rn} + rp$

$rp \overset{\checkmark}{\equiv} rp \quad \checkmark$

[domača naloga:]

pokaži

- $a \equiv b \pmod{m}$ in $n \in \mathbb{N}$, tedaj $a^n \equiv b^n \pmod{m}$ $\quad$ (dokaz: večkrat uporabi 2.))
- $ac \equiv bc \pmod{m}$ $\quad c \perp m$
  $\Rightarrow a \equiv b \pmod{m}$ $\quad m \mid ac-bc$
  $m \mid (a-b)c \Rightarrow m \mid (a-b)$

MALI FERMATOV IZREK.

$a \in \mathbb{N}$, $p \in$ prašt.

$8 \equiv 2 \pmod{3}$

velja $a^p \equiv a \pmod{p}$

če $p \mid a$ trivialno

predp.: $p \perp a$:

deliмо z a obe strani

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

[domača naloga]

izračunaj

$3^{2024} \bmod 13$

NALOGA: p, q različni praštevili

naj velja $a \equiv b \pmod p$
$a \equiv b \pmod q$

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

---

dokaz: $p \mid a-b$ (predp.)
$q \mid a-b$

$a-b = px$
$a-b = qy$ $\Rightarrow px = qy$

iz $p \perp q$ sledi $q \mid x \Rightarrow x = qx' \Rightarrow a-b = px = \boxed{pq}x'$

$pq \mid a-b$
$\Leftrightarrow$
$a \equiv b \pmod{pq}$

EULERJEVA FUNKCIJA $\varphi(n)$

let $n \in \mathbb{N}$.

$\varphi(n) := |\{k \leq n \,;\, 1 \leq k \leq n \text{ in } k \perp n\}|$

zdb z n tuja števila, manjša od n.

$\varphi(2) = |\{1,3\}| = 2$ $\quad\quad$ $\varphi(6) = |\{1,5\}| = 2$

$\varphi(5) = |\{1,2,3,4\}| = 4$ $\quad\quad$ $\varphi(10) = |\{1,3,7,9\}| = 4$

$\varphi(9) = |\{1\ 2\ \cancel{3}\ 4\ 5\ \cancel{6}\ 7\ 8\ \cancel{9}\}| = 6$

LASTNOST: za p praštevilo velja

$\varphi(p) = p-1$ $\quad |\{1, 2, \ldots, p-1, \cancel{p}\}|$

TRDITEV: p praštevilo, $n \in \mathbb{N}$

potem $\varphi(p^n) = p^n - p^{n-1} = p^n\left(1 - \frac{1}{p}\right)$

$1 \ldots p^n$: $\underbrace{1, 2, 3, \ldots, p, \ldots, 2p, \ldots, 3p, \ldots, p^2, \ldots, p^n}_{\text{teh je } p^n}$

netujih pa je: $1p, 2p, \ldots p^{n-1}p$

p^{n-1}

$\varphi(3)=2 \quad \varphi(5)=4 \quad \varphi(15)=|\{1\ 2\ \cancel{3}\ 4\ \cancel{5}\ \cancel{6}\ 7\ 8\ \cancel{9}\ \cancel{10}\ 11\ \cancel{12}\ 13\ 14\ \cancel{15}\}|=8$

$\varphi(4)=2 \quad \varphi(5)=4 \quad \varphi(20)=8=|\{1\ \cancel{2}\ 3\ \cancel{4}\ \cancel{5}\ \cancel{6}\ 7\ \cancel{8}\ 9\ \cancel{10}\ 11\ \cancel{12}\ 13\ \cancel{14}\ \cancel{15}\ \cancel{16}\ 17\ \cancel{18}\ 19\ \cancel{20}\}|=8$

IZREK:

$\varphi(a)\varphi(b)=\varphi(ab) \quad \forall a,b: \boxed{a \perp b}$

DOKAZ:

1	2	3	$\dots$	a
$a+1$	$a+2$	$a+3$	$\dots$	$2a$
$2a+1$	$2a+2$	$2a+3$	$\dots$	$3a$
	$\vdots$			$\vdots$
$(b-1)a+1$	$(b-1)a+2$	$(b-1)a+3$	$\dots$	ba

↳ vzemimo $x, y \in$ tega stolpca:

$a \mid x-y$.

$(x-y)/a=3$.

Število je tuje z ab
$\Leftrightarrow$ je tuje za in
je tuje hkrati z b.

Če v m-tem stolpcu $m \nmid a$, tudi elementi stolpca niso tuji za.
$\varphi(a)$ je takih stolpcev, ki jih ne križamo zaradi tega pogoja.

Vsi v istem stolpcu imajo različne ostanke po modulu b.
Zdb ne more se zgoditi, da b deli razliko elementa istega stolpca:

$$b \mid (va+s)-(v'a+s)$$

$$b \mid va-v'a$$

$$b \mid a(v-v')$$

v in v' sta oba v $[1, b]$, zato je nujno $|v-v'|<b$, zato $b \mid a(v-v')$ ne deli.

Kadar je ostanek tuj z b, ne križamo } Prevedi elementa stolpca.