Konstrukcija skupa $\mathbb{Z}$

Skup $\mathbb{N} = \{1, 2, 3, \ldots\}$ nazivamo skupom prirodnih brojeva. Skup prirodnih brojeva uz zbrajanje je komutativna polugrupa (zbrajanje je definirano i jedinstveno za svaki $a, b \in \mathbb{N}$, zatim $a + b \in \mathbb{N}$, za svaki $a, b \in \mathbb{N}$; također vrijedi i asocijativnost). Za sada nećemo ulaziti u detaljnija obrazloženja, no pretpostavit ćemo, ukoliko ne prihvaćamo ova svojstva sama po sebi očitima, da je $\mathbb{N}$ definiran pomoću Peanovih aksioma. Tada se iz njih može formalno definirati zbrajanje i slično. Također, $\mathbb{N}$ uz $\leq$ je potpuno uređen skup. Pretpostavit ćemo kako za svaki $a, b, c \in \mathbb{N}$, gdje je $a > c$ (ili $b > c$), iz $a = b$ slijedi $a - c = b - c$ i obratno. Također pretpostavit ćemo kako je $(a+b)-c = a+(b-c)$, za svaki $a, b, c \in \mathbb{N}$ i $b > c$. Također, neka je $a = a + (b - b)$ i $a = (a - b) + b$, za svaki $a, b \in \mathbb{N}$. Detaljnija pojašnjenja ostavljam za jedan drugi put.

Lema. Neka su $a, b, c, d \in \mathbb{N}$ i neka vrijedi $a + d = b + c$. Neka je $a > b$. Tada je $c > d$.

Dokaz. Kako je $a > b$, tada je i $a + d > b$ pa vrijedi $(a + d) - b = (b + c) - b$. Kako je zbrajanje komutativno, to je $(a + d) - b = (c + b) - b$. Po pretpostavci imamo $(a + d) - b = c + (b - b)$, a to je $(a + d) - b = c$. Opet, po komutativnosti zbrajanja, to je ekvivalentno $(d + a) - b = c$. Po prethodnoj pretpostavci slijedi $d + (a - b) = c$, iz čega imamo $c > d$.

$\square$

Lema. Neka su $a, b, c, d \in \mathbb{N}$ i neka vrijedi $a + d = b + c$. Neka je $a = b$. Tada je $c = d$.

Dokaz. Imamo $a + d = b + c$. Kako je $a = b$ to je $a + d = a + c$. Iz toga slijedi, jer je $(a + d) > a$ i $(a + c) > c$, da je $(a + d) - a = (a + c) - a$. Po komutativnosti imamo $(d + a) - a = (c + a) - a$, tj. $d + (a - a) = c + (a - a)$ i napokon $d = c$, tj. $c = d$.

$\square$

Definicija. Neka je za svaki $(a, b), (c, d) \in \mathbb{N} \times \mathbb{N}$ definirana relacija $(a, b) \sim (c, d)$ ako i samo ako $a + d = b + c$.

Propozicija. Relacija $\sim$ iz prethodne definicije je relacija ekvivalencije.

Dokaz. *Refleksivnost.* Vrijedi $a + b = a + b$ pa je $(a, b) \sim (a, b)$. *Simetričnost.* Neka je $(a, b) \sim (c, d)$. Tada vrijedi $a + d = b + c$, što je ekvivalentno $b + c = a + d$. Kako je zbrajanje komutativno, prethodan izraz ekvivalentan je $c + b = d + a$, što povlači $(c, d) \sim (a, b)$. *Tranzitivnost.* Neka je $(a, b) \sim (c, d)$ i $(c, d) \sim (e, f)$. To znači

$a+d=b+c$ i $c+f=d+e$. Pretpostavimo kako je $a>b$. Tada po prethodnoj lemi imamo $c>d$. To opet povlači $e>f$. Stoga, iz $a+d=b+c$ slijedi $d+a=c+b$, zatim $(d+a)-b=(c+b)-b$ pa $d+(a-b)=c+(b-b)$ i napokon $c=(a-b)+d$. Iz $c+f=d+e$ slijedi $(c+f)-f=(d+e)-f$ te $c+(f-f)=d+(e-f)$, što je $c=(e-f)+d$. Dakle, $(a-b)+d=(e-f)+d$, tj. $a-b=e-f$. Iz toga imamo $(a-b)+b=(e-f)+b$, a to je $a=(e-f)+b$, tj. $a=b+(e-f)$. Zatim iz toga slijedi $a+f=(b+(e-f))+f$, što je po asocijativnosti $a+f=b+((e-f)+f)$. Iz toga napokon dobivamo $a+f=b+e$ što povlači $(a,b)\sim(e,f)$. Dokaz za $a<b$ se provodi analogno. Ukoliko je $a=b$, po prethodnoj lemi mora biti $c=d$, a zatim i $e=f$. Stoga je $a+e=b+e$ pa $a+f=b+e$, pa je opet $(a,b)\sim(e,f)$.

$\square$

Definicija. Neka je $[(a,b)]=\{(c,d)\in\mathbb{N}\times\mathbb{N}:\ (a,b)\sim(c,d)\}$. Neka su $a,m\in\mathbb{N}$. Definiramo:

$$\begin{aligned} m^+: &= [(a+m,a)],\\ 0: &= [(a,a)],\\ m^-: &= [(a,a+m)]. \end{aligned}$$

Nadalje, neka je $\mathbb{Z}:=\{m^+:\ m\in\mathbb{N}\}\cup\{0\}\cup\{m^-:\ m\in\mathbb{N}\}$.

Propozicija. Neka su $a,m\in\mathbb{N}$ i $\pi:\mathbb{N}\to\mathbb{N}$ funkcija definirana s $\pi(x)=x+1$. Tada je $[(a,a+m)]=[(1,\pi(m))]$, $[(a,a)]=[(1,1)]$ i $[(a+m,a)]=[(\pi(m),1)]$.

Dokaz. Direktno slijedi iz svojstva $x\in[y]$ povlači $[x]=[y]$. Imamo $(1,\pi(m))\sim(a,a+m)$ jer $1+(a+m)=\pi(m)+a$, tj. $1+(m+a)=\pi(m)+a$ što nas dovodi do $(1+m)+a=\pi(m)+a$; to je ekvivalentno $(m+1)+a=\pi(m)+a$, tj. $\pi(m)+a=\pi(m)+a$. Stoga, $(1,\pi(m))\in[(a,a+m)]$ pa je $[(a,a+m)]=[(1,1+m)]$. Ostali se dokazi provode analogno.

$\square$

Definicija. Neka su $(x,y),(z,w)\in\mathbb{N}\times\mathbb{N}$. Definiramo binarnu operaciju $+:\mathbb{Z}\to\mathbb{Z}$ kao $[(x,y)]+[(z,w)]:=[(x+z,y+w)]$.

Propozicija. Skup $\mathbb{Z}$ uz operaciju iz prethodne definicije je komutativna grupa.

Dokaz. Zatvorenost i definiranost (uz nasljedstvo definiranosti zbrajanja iz $\mathbb{N}$) vrijede po definiciji; kako je $(x+z,y+w)\in\mathbb{N}\times\mathbb{N}$, imamo $[X]\in\mathbb{Z}$ takav da je $(x+z,y+w)\in[X]$

što povlači $[X] = [(x+z, y+w)]$. Zatim, operacija je jedinstveno definirana, jer, uzmemo li $(x_1, y_1), (x_2, y_2), (z_1, w_1), (z_2, w_2) \in \mathbb{N} \times \mathbb{N}$ takve da je $(x_1, y_1) = (x_2, y_2)$ i $(z_1, w_1) = (z_2, w_2)$, imamo $[(x_1, y_1)] + [(z_1, w_1)] = [(x_1 + z_1, y_1 + w_1)]$ te $[(x_2, y_2)] + [(z_2, w_2)] = [(x_2 + z_2, y_2 + w_2)]$. No, kako je $(x_1, y_1) = (x_2, y_2)$ i $(z_1, w_1) = (z_2, w_2)$, također je i $[(x_1, y_1)] = [(x_2, y_2)]$ te $[(z_1, w_1)] = [(z_2, w_2)]$ (po običnoj supstituciji). Tada imamo $[(x_1, y_1)] + [(z_1, w_1)] = [(x_2 + z_2, y_2 + w_2)]$, tj. $[(x_1 + z_1, y_2 + w_2)] = [(x_2 + z_2, y_2 + w_2)]$. *Asocijativnost.* Imamo $([(x, y)] + [z, w]) + [(p, q)] = [(x+z, y+w)] + [(p, q)] = [((x+z)+p, (y+w)+q)]$. Obzirom da vrijedi asocijativnost u $\mathbb{N}$, imamo $[((x+z)+p, (y+w)+q)] = [(x + (z + p), y + (w + q))] = [(x, y)] + [(z + p, w + q)] = [(x + y)] + ([(z, w)] + [(p, q)])$. *Neutralan element.* Imamo $[(x, y)] + [(1, 1)] = [(x + 1, y + 1)]$. No, kako je $x + (y + 1) = y + (x + 1)$, vrijedi $(x, y) \sim (x + 1, y + 1)$ što implicira $[(x, y)] = [(x + 1, y + 1)]$. Dakle, $[(x, y)] + [(1, 1)] = [(x, y)]$. Isto se pokaže i za $[(1, 1)] + [(x, y)] = [(x, y)]$. Stoga je $[(1, 1)] \in \mathbb{Z}$ neutralan element. *Inverzni elementi.* Neka je $[(x, x + m)] \in \mathbb{Z}$. Tada je $[(x + m, x)] \in \mathbb{Z}$ i imamo $[(x, x + m)] + [(x + m, x)] = [(x + m, x + m)] = [(1, 1)]$ (po prethodnoj propoziciji). Slično se pokaže i za $[(x, x + m)] \in \mathbb{Z}$, te za $[(x, x)] \in \mathbb{Z}$. *Komutativnost.* Neka je $[(x, y)], [(z, w)] \in \mathbb{Z}$. Tada je $[(x, y)] + [(z, w)] = [(x + z, y + w)] = [(z + x, w + y)] = [(z, w)] + [(x, y)]$.

$\square$

Primjedba. Primijetimo kako iz gornje propozicije slijedi da je $0 \in \mathbb{Z}$ neutralan element obzirom na operaciju zbrajanja u $\mathbb{Z}$. Također, uzmemo li $m^+ \in \mathbb{Z}$, njegov inverzan element obzirom na zbrajanje je $m^- \in \mathbb{Z}$, tj. vrijedi $m^+ + m^- = m^- + m^+ = 0$.

Definicija. Neka je $\leq$ relacija na skupu $\mathbb{Z}$ takva da $[(x, y)] \leq [(z, w)]$ ako i samo ako $x + w \leq y + z$, za svaki $[(x, y)], [(z, w)] \in \mathbb{Z}$.

Propozicija. Skup $\mathbb{Z}$ uz $\leq$ je potpuno uređen skup.

Dokaz. Po definiciji relacije, relacija je definirana za svaka dva elementa skupa $\mathbb{Z}$. *Refleksivnost.* Vrijedi $x + y \leq x + y$ pa je $[(x, y)] \leq [(x, y)]$. *Antisimetričnost.* Neka je $[(x, y)] \leq [(z, w)]$ i $[(z, w)] \leq [(x, y)]$. Tada je $x + w \leq y + z$ i $z + y \leq w + x$, iz čega slijedi $x + w = y + z$, tj. $[(x, y)] \sim [(z, w)]$ pa onda $[(x, y)] = [(z, w)]$. *Tranzitivnost.* $[(x, y)] \leq [(z, w)]$ i $[(z, w)] \leq [(p, q)]$ je ekvivalentno $x + w \leq y + z$ i $z + q \leq w + p$. Vrijedi $w \leq y + z - x$ i $z + q - p \leq w$. Stoga imamo $z + q - p \leq y + z - x$ i $q + x \leq y + p$, tj. $x + q \leq y + p$ što povlači $[(x, y)] \leq [(p, q)]$.

$\square$

Primjedba. Slično se definira slabija relacija $<$ uz koju je skup $\mathbb{Z}$ parcijalno uređen skup. Dakle, $[(x, y)] < [(z, w)]$ ako i samo ako $x+w < y+z$, za svaki $[(x, y)], [(z, w)] \in \mathbb{Z}$.

Propozicija. Vrijedi $m^- < 0 < n^+$, za svaki $m^-, n^+ \in \mathbb{Z}$.

Dokaz. Imamo $m^- = [(1, \pi(m))]$, $0 = [(1,1)]$ i $n^+ = [(\pi(m), 1)]$. Vrijedi $1 + 1 < \pi(m) + 1$, tj. $1 < \pi(m)$, što je istinito za svaki $m \in \mathbb{N}$ (jer broj 1 nije sljedbenik nijednom prirodnom broju). Dakle, $m^- < 0$. Također, $1 + 1 < \pi(m) + \pi(n)$, tj. $2 < \pi(m) + \pi(n)$. Obzirom da je $1 < \pi(m)$ i $1 < \pi(n)$ očito je $2 < \pi(m) + \pi(n)$ pa je $m^- < n^+$, za svaki $m^-, n^+ \in \mathbb{Z}$. Također, $1 + 1 < 1 + \pi(m)$, tj. $1 < \pi(m)$ pa je i $0 < n^+$.

$\square$

Napomena. Uvedimo sada oznaku $m := m^+$ i $-m := m^-$.

Propozicija. Neka je $m \in \mathbb{Z}$. Ako je $m < 0$ tada je $-m > 0$ (u smislu aditivnog inverza). Također, ako je $m > 0$ tada je $-m < 0$.

Dokaz. Pretpostavimo da je $m < 0$. Tada je, po prethodnoj propoziciji, $m = [(1, \pi(m))]$, $0 = [(1, 1)]$ pa zbog $m < 0$ vrijedi $1+1 < \pi(m)+1$, tj. $1 < \pi(m)$. Pretpostavimo kako je $-m \leq 0$. Tada bi, zbog $-m = [(\pi(m), 1)]$ vrijedilo $\pi(m) + 1 \leq 1 + 1$, tj. $\pi(m) \leq 1$, što je u suprotnosti s $\pi(m) > 1$. Dakle, $m < 0$ povlači $-m > 0$. Po rezultatu iz teorije grupa, kako je $-m$ aditivni inverz od m, vrijedi $-(-m) = m$. Dokaz za $m > 0$ se provodi analogno.

$\square$

Propozicija. Neka su $m, n \in \mathbb{Z}$. Ako je $m \leq n$, tada $-n \leq -m$ (u smislu aditivnih inverza).

Dokaz. Pretpostavimo kako je $m > 0$ i $n > 0$. Tada je $m = [(\pi(m), 1)]$ i $n = [(\pi(n), 1)]$. Tada je $-m = [(1, \pi(m))]$ i $-n = [(1, \pi(n))]$. Iz $[(\pi(m), 1)] \leq [(\pi(n), 1)]$ slijedi $\pi(m) + 1 \leq \pi(n) + 1$, tj. $\pi(m) \leq \pi(n)$. Pretpostavimo da je $-m < -n$. Tada vrijedi $1 + \pi(n) < 1 + \pi(m)$, tj. $\pi(n) < \pi(m)$. No, to je u suprotnosti s pretpostavkom $\pi(m) \leq \pi(n)$. Dokaz za $m < 0$ i $n < 0$ slijedi analogno. Slučaj kada je $m > 0$ i $n < 0$ uz $m \leq n$ je nemoguć po prethodnoj propoziciji. Pretpostavimo kako je $-n < -m$. No, tada je $-n > 0$ i $-m < 0$. No, uz $-n < -m$ to je nemoguće pa može biti samo $-m \leq -n$.

$\square$

Teorem (Well Ordering of $\mathbb{Z}^+$). Neka je $A \subseteq \mathbb{Z}^+$ i $A \neq \emptyset$. Tada postoji $m \in A$ takav da je $m \leq a$ za svaki $a \in A$.

Dokaz. Dokaz se provodi matemematičkom indukcijom. Prvo pokažimo kako tvrdnja vrijedi za sve konačne podskupove od $\mathbb{Z}^+$. Neka je $|A_1| = 1$ i $A_1 \subseteq \mathbb{Z}^+$, i.e. $A_1 = \{a\}$. Tada je očito $\min A_1 = a$. Pretpostavimo kako tvrdnja vrijedi za neki $k \in \mathbb{N}$; neka za svaki skup $A_k \subseteq \mathbb{Z}^+$, gdje je $|A_k| = k$, postoji $m \in A$ takav da je $m \leq a$, za svaki $a \in A_k$. Neka je $A_{k+1} \subseteq \mathbb{Z}^+$ takav da je $|A_{k+1}| = k + 1$. Neka je $a' \in A_{k+1}$. Tada je $|A - \{a'\}| = k$ pa postoji $m \in A - \{a'\}$ takav da je $m \leq a$, za svaki $a \in A - \{a'\}$. Vrijedi $m \leq a'$ ili $m \leq a'$. U prvom slučaju je očito $\min A_{k+1} = m$ (jer je tada i dalje $m \leq a$, za svaki $a \in A_{k+1}$), a u drugom slučaju je $\min A_{k+1} = a'$ (jer je tada $a' \leq m \leq a$, za svaki $a \in A_{k+1}$). Stoga tvrdnja vrijedi za sve skupove veličine $n \in \mathbb{N}$.

Pokažimo sada kako tvrdnja vrijedi i za beskonačne podskupove od $\mathbb{Z}^+$. Neka je $A \in \mathbb{Z}^+$. Neka je $A_x = \{0, \ldots, x\}$, za $x \in \mathbb{Z}^+$. Tada je $A \cap A_x$ konačan skup i vrijedi kako postoji $m \in A \cap A_x$ takav da je $m \leq a$, za svaki $a \in A \cap A_x$. Po definiciji presjeka, ako je $a \in A \cap A_x$ tada je $a \in A$ i $a \cap A_x$. Stoga, slabljenjem tvrdnje, postoji $m \in A$ takav da je $m \leq a$, za svaki $a \in A$.

$\square$

Djeljivost

Definicija. Neka je $x \in \mathbb{R}$. Tada funkciju $|\cdot| : \mathbb{R} \to \mathbb{R}_0^+$ definiranu formulom

$$|x| = x\mathcal{I}_{[0,\infty]}(x) + (-x)\mathcal{I}_{\langle -\infty,0\rangle}(x),$$

gdje je $\mathcal{I}_S : \mathbb{R} \to \{0,1\}$ indikator funkcija za skup S, nazivamo apsolutna vrijednost (broja x).

Primjedba. Iz definicije je lako vidjeti kako vrijedi $|x| \geq 0$, za svaki $x \in \mathbb{R}$.

Propozicija. Za svaki $a \in \mathbb{R}$ vrijedi $a \leq |a|$.

Dokaz. Ako je $a \geq 0$ tada je $|a| = a$, po definiciji. Ako je $a < 0$ tada je $|a| = -a$ i vrijedi $|a| > 0$ pa tako i $|a| > a$ (jer je $a < 0$). Uzevši oba slučaja u obzir to je $|a| \geq a$.

$\square$

Propozicija. Neka su $a, b \in \mathbb{R}$. Ako je $a = b$ tada je $|a| = |b|$. Obrat općenito ne vrijedi.

Dokaz. Neka je $a = b$. Uzmimo prvo $a \geq 0$. Tada je i $b \geq 0$ pa je $|a| = a$ i $|b| = b$. Iz pretpostavke propozicije direktno slijedi $|a| = a = b = |b|$, tj. $|a| = |b|$ (ako su $a, b \in \mathbb{R}_0^+$). Dalje, uzmimo $a < 0$. Tada je i $b < 0$ pa je $|a| = -a$ i $|b| = -b$. Vrijedi $-(-a) = a$ i $-(-b) = b$. Iz pretpostavke je $-|a| = -(-a) = a = b = -(-b) = -|b|$, i.e. $-|a| = -|b|$. To je $|a| = |b|$ za $a < 0$ i $b < 0$ pa uzevši i prvi slučaj u obzir vrijedi $|a| = |b|$, za svaki $a, b \in \mathbb{R}$.

$\square$

Propozicija. Neka su $a, b \in \mathbb{Z}$. Vrijedi $|a| \cdot |b| = |a \cdot b|$.

Dokaz. Neka je $a \geq 0$ i $b \geq 0$. Tada je $ab > 0$ i stoga $|ab| = ab$. Isto tako je i $|a| = a$ i $|b| = b$ pa je $|a||b| = ab$. Iz oba izraza slijedi $|ab| = |a||b|$ za $a, b \geq 0$. Ukoliko su $a, b < 0$ vrijedi $ab > 0$ pa je $|ab| = ab$. Isto tako je $|a| = -a$ i $|b| = -b$ pa je $|a||b| = -a \cdot (-b) = ab = |ab|$. Ako je $a \geq 0$ i $b < 0$ (isto se pokaže i za $a < 0$ i $b \geq 0$), vrijedi $ab < 0$ pa je $|ab| = -ab$. No, isto tako $|a| = a$ i $|b| = -b$ pa je $|a||b| = a \cdot (-b) = -ab = |ab|$. Time smo iscrpili sve mogućnosti i vrijedi tvrdnja propozicije.

$\square$

Definicija. Neka je $a \in \mathbb{Z}$ i $b \in \mathbb{Z}\backslash\{0\}$. Reći ćemo kako b dijeli a, odnosno da je a djeljiv s b (i to zapisati kao $b|a$) ukoliko postoji $k \in \mathbb{Z}$ takav da vrijedi $a = bk$. Također tada kažemo da je b **djelitelj** od a ili da je a **višekratnik** broja b.

Primjer. Pogledajmo par primjera kako bi nam bilo jasnije. Broj 6 je djeljiv s 3 jer vrijedi $6 = 3 \cdot 2$ (ovdje je $k = 2$ i vrijedi $3|6$). No što ako imamo -6 i 3? Tada je $k = -2$ pa će vrijediti $3|(-6)$ jer je $-6 = 3 \cdot (-2)$. Slično, ako imamo -6 i -3 vrijedit će $-3|(-6)$ jer je $-6 = -3 \cdot 2$ (dakle, ovdje je opet $k = 2$).

Propozicija. Ako je $b \in \mathbb{Z}\backslash\{0\}$ djelitelj od $a \in \mathbb{Z}$ vrijedi $b \leq |b| \leq |a|$.

Dokaz. Po prethodnoj propoziciji, ako je $a = kb$ tada je i $|a| = |kb| = |k||b|$. Kako su $|a|$, $|k|$ i $|b|$ nenegativni (što je lako uočiti iz definicije apsolutne vrijednosti), tada je $|b| \leq |a|$. Po prethodnoj propoziciji je $b \leq |b|$ pa je $b \leq |b| \leq |a|$.

$\square$

Propozicija. Postoji konačno mnogo djelitelja za svaki $a \in \mathbb{Z}$.

Dokaz. Za svaki b koji je djelitelj od a vrijedi, po prethodnoj propoziciji, da je $b \leq |a|$. To je $-a \leq b \leq a$, tj. $b \in [-a, a] \cap \mathbb{Z}$. U ovom intervalu ima konačno mnogo cijelih brojeva (najviše $2a$ jer 0 ne može biti djelitelj, po definiciji).

$\square$

Teorem (o dijeljenju s ostatkom). Za svaki $a, b \in \mathbb{Z}$, $b \neq 0$, postoje jedinstveni $q \in \mathbb{Z}$ (**kvocijent**) i $r \in \mathbb{N}_0$ (**ostatak**) takvi da vrijedi $a = bq + r$ i $0 \leq r < |b|$.

Dokaz. *Egzistencija.* Promotrimo prvo koje slučajeve moramo uzeti u obzir. Prvo može biti $a, b > 0$, zatim $a, b < 0$. No, isto tako može biti i $a < 0$, $b > 0$ te $a > 0$ i $b < 0$. Pogledajmo neke primjere prije nego prosudimo što nam je činiti. Uzmimo brojeve čije su apsolutne vrijednosti 7 i 3. Vrijedit će $7 = 3 \cdot 2 + 1$. Zatim, $-7 = 3 \cdot (-3) + 2$ (želimo da r bude pozitivan i manji od $|b|$, što ne bismo dobili u slučaju da smo uzeli 3; ostatak bi morao biti negativan). Također, $7 = -3 \cdot (-2) + 1$ i $-7 = -3 \cdot 3 + 2$. Vidimo kako slučajevi kada su ili oboje pozitivni ili $a > 0$, a $b < 0$ nisu problem. Dakle, slučaj ako je $a > 0$ i $b < 0$ možemo lako svesti na prvi tako da jednostavno uzmemo $b' = -b$ i $a' = a$. Tada će vrijediti (ukoliko dokažemo za slučaj kada su oba pozitivna) $a' = b'q' + r$, gdje je $0 \leq r < |b'|$ a time i $a = -bq' + r$, gdje je $0 \leq r < |-b| = |b|$. Uzmemo li $q = -q'$ lako dobivamo $a = -b \cdot (-q) + r$, tj. $a = bq + r$. No, uzmimo još jedan primjer za ostale slučajeve. Znamo kako je $27 = 6 \cdot 4 + 3$. No, tako je $-27 = 6 \cdot (-5) + 3$ (ne može biti -4 jer bi ostatak bio negativan). Slično i kada su oba negativna vrijedi $-27 = -6 \cdot 5 + 3$. Dakle, ako je $a < 0$, a $b > 0$ uzmemo $a' = -a$ i $b' = b$. Imat ćemo (opet, uz pretpostavku da dokažemo za oba pozitivna) $a' = b'q' + r'$ te $0 \leq r' < |b'|$. Tada je i $-a = bq' + r'$ i vrijedi $0 \leq r' < b$, te $q' \geq 0$. Pomnožimo jednakost s -1 i dobivamo $a = -bq' - r'$. Želimo se riješiti minusa uz b, a za to će nam trebati negativan kvocijent. Uzmemo li, po uzoru na primjer, supstituciju $q' = -(q+1)$ imat ćemo $a = b(q+1) - r'$, to je $a = bq + b - r'$. Vidimo da je dovoljno uzeti $r = b - r'$. Naš r' je manji od b pa vrijedi $r > 0$, a time i $r \geq 0$. Kako je $r' \geq 0$ i $r + r' = b$ vrijedi $r < b$. Tako je zadovoljen i uvjet da je $0 \leq r < b = |b|$. Ukoliko imamo $a, b < 0$, uzimamo $a' = -a$ i $b' = -b$. Tada je $a' = b'q' + r'$, gdje je $q' \geq 0$ i $0 \leq r' < b' = -b$. Tada vrijedi i $-a = -bq' + r'$. Pomnožimo jednakost s -1 i dobivamo $a = bq' - r'$. No, opet, ne možemo imati negativan ostatak, pa uzimamo $q' = (q-1)$. Tada je $a = bq - b - r'$. Isto kao i u prethodnom primjeru, kako je $r' < -b$, tako je $0 < -r' - b = r$, a time i $r \geq 0$. Slično, $r' \geq 0$ i $r + r' = -b$ (zapamtimo $-b$ je pozitivan), vrijedi i $r < -b$, a zbog $b < 0$, to je $r < |b|$. Stoga imamo $a = bq + r$, gdje je $0 \leq r < |b|$. Ovim smo pokazali kako se oba slučaja mogu svesti na prvi, kada su oba pozitivna.

Pokažimo sada da tvrdnja vrijedi za slučaj kada je $a > 0$ i $b > 0$. Uzmimo $R = \{a - bm : \ m \in \mathbb{Z}\} \cap \mathbb{Z}_0^+$ i $r = \min R$. Po *well-ordering* principu, ako je R neprazan i sadrži samo nenegativne elemente, tada ima i najmanji element, odnosno minimum. Kako je R zapravo definiran kao presjek sa skupom nenegativnih cijelih brojeva, on će sadržavati samo nenegativne cijele brojeve - ukoliko takvi postoje u presjeku. Pokažimo da postoje, tj. da je R neprazan. Uzmemo li $m = -1$, imat ćemo $a - b \cdot (-1) \in \mathbb{Z}_0^+$ a tako i $a + b \in R$. Dakle, skup R sadrži barem $a + b$ (oba su nenegativna pa im je i zbroj nenegativan). Dakle, R ima minimum, a tako i njemu pridružen broj $m \in \mathbb{Z}$ takav da vrijedi $r = a - bm$. Obzirom da je $r \in R$, vrijedi $r \geq 0$. Sada pretpostavimo da je $r \geq b$. Tada bi vrijedilo $a - bm \geq b$, a time i $a - b(m+1) \geq 0$. No, $bm < bm + b = b(m+1)$ (jer je, ne zaboravimo, $b > 0$) pa je $-bm > -b(m+1)$. Iz toga slijedi kako je $a - bm > a - b(m+1) \geq 0$, a tako i $a - b(m+1) \in R$. No, to je u suprotnosti s pretpostavkom da je $a - bm$ minimum skupa R ($a - b(m+1)$ ne može biti manji). Stoga mora biti $r < b$, a time i $0 \leq r < b = |b|$. Promotrimo samo još slučaj kada je $a = 0$. Za primjer uzmimo $0 = 7 \cdot 0 + 0$. Dakle, u tom slučaju, $q = 0$ i $r = 0$ pa vrijedi i dalje $a = bq + r$, gdje je $0 \leq r < |b|$.

Jedinstvenost. Pretpostavimo da postoji neki $q' \neq q$ i $r' \neq r$ takvi da vrijedi $a = bq + r$ i $a = bq' + r'$, gdje je $r, r' \in [0, b\rangle \cap \mathbb{N}_0$. To implicira $bq + r = bq' + r'$. Prebacimo sve na desnu stranu i imamo $0 = bq' + r' - bq - r$, tj. $0 = b(q - q') + (r' - r)$. Kako je $b \neq 0$ i $b|0$, vrijedi $0 = b \cdot 0 + 0$. Stoga mora biti $q - q' = 0$, tj. $q = q'$ i $r' - r = 0$, tj. $r = r'$.

$\square$

Primjedba. (i) Neka za neke $a, b \in \mathbb{Z}$, $b \neq 0$ vrijedi $a = qb + r$ gdje je $q, r \in \mathbb{Z}$ i $0 \leq r < |b|$. Ako je $r = 0$ lako je vidjeti kako $b \mid a$; tada postoji $q \in \mathbb{Z}$ takav da je $a = bq$. Ako je $r > 0$, tada možemo vidjeti kako $b \nmid a$, tj. ne postoji $k \in \mathbb{Z}$ za koji bi vrijedilo $a = bk$. To se vidi iz definicije skupa $R = \{a - bm : \ m \in \mathbb{Z}\} \cap \mathbb{N}_0$ i definicije $r = \min R$. Ako bi postojao neki $m \in \mathbb{Z}$ takav da je $a = bm$ tada bi bilo $a - bm = 0$ pa bi i ostatak bio jednak nuli, tj. bilo bi $r = 0$ jer za svaki $x \in R$ po definiciji skupa R vrijedi $x \geq 0$. No, to je u suprotnosti s pretpostavkom da je $r > 0$ pa ne postoji $m \in \mathbb{Z}$ takav da bude $a = bm$. (ii) Ako su $a, b, q, r \in \mathbb{Z}$, $b \neq 0$, $0 \leq r < |b|$ takvi da vrijedi $a = bq + r$. Tada je očito kako $b|(a - r)$ jer je $a - r = bq$, a $q \in \mathbb{Z}$.

Korolar. Neka je $x \in \mathbb{Q}$. Tada postoje jedinstveni $k \in \mathbb{Z}$, $m \in \mathbb{N}_0$, i $n \in \mathbb{N}$, takvi da vrijedi $x = k + \frac{m}{n}$ i $0 \leq m < n$ (tj. $\frac{m}{n}$ je pravi razlomak).

Dokaz. *Egzistencija.* Kako je $x \in \mathbb{Q}$, možemo ga zapisati u obliku $x = \frac{a}{b}$ gdje je $a \in \mathbb{Z}$ i $b \in \mathbb{N}$. Tada, po teoremu o dijeljenju s ostatkom postoje jedinstveni $q, r \in \mathbb{Z}$ takvi da je $a = bq + r$ i $0 \leq r < |b| = b$ (pretpostavili smo kako je $b \in \mathbb{N}$). Podijelimo li izraz za a s b dobivamo $\frac{a}{b} = q + \frac{r}{b}$. Uzmemo $k = q$, $r = m$ i $b = n$ te zbog $x = \frac{a}{b}$ i $\frac{a}{b} = q + \frac{r}{b}$ imamo $x = k + \frac{m}{n}$, gdje, zbog $0 \leq r < b$, dobivamo i $0 \leq m < n$.

Jedinstvenost. Prepostavimo kako $x = k + \frac{m}{n}$ i $x = k' + \frac{m'}{n'}$ i $0 \leq m, m' < n, n'$. Uzmimo $r = \frac{m}{n}$ i $r' = \frac{m'}{n'}$. Tada je $0 \leq r, r' < 1$ (zbog $m < n$ i $m' < n'$. Izjednačimo li obzirom na x ove dvije jednakosti dobivamo $k + r = k' + r'$ i iz toga $r = k' + r' - k$, tj. $r = (k' - k) + r'$. Kako je $r < 1$ i $r' < 1$ mora biti i $|k' - k| < 1$, a to je jedino moguće samo kada je $k - k' = 0$, tj. $k = k'$. Tada imamo $r = 0 + r'$ i napokon $r = r'$.

$\square$

Definicija. Neka su zadani $a, b \in \mathbb{Z} \backslash \{0\}$. Prirodan broj $x \in \mathbb{N}$ za koji vrijedi da $x|a$ i $x|b$ zovemo **zajednički djelitelj** od a i b. Najveći takav broj zovemo **najveći zajednički djelitelj** (eng. *greatest common divisor*) od a i b. Činjenicu da je x najveći zajednički djelitelj od a i b zapisujemo kao $\gcd(a, b) = x$ (dakle, $\gcd(a, b) = \min\{x \in \mathbb{N} : \ x|a \ \wedge \ x|b\}$.).

Definicija. Brojeve $a, b \in \mathbb{Z} \backslash \{0\}$ za koje vrijedi $\gcd(a, b) = 1$ kažemo da su **relativno prosti**. Za broj $p \in \mathbb{N} \backslash \{1\}$ kažemo da je **prost** ukoliko ne postoji $n \in \mathbb{N} \backslash \{1, p\}$ takav da $n|p$. U suprotnom kažemo da je **složen**.

Propozicija. Neka su $a, b, c \in \mathbb{Z}$, takvi da $c|a$ i $c|b$. Tada $c|(ax + by)$, za svaki $x, y \in \mathbb{Z}$.

Dokaz. Kako $c|a$ i $c|b$, postoje $k_1, k_2 \in \mathbb{Z}$ takvi da vrijedi $a = ck_1$ i $b = ck_2$. Neka su $x, y \in \mathbb{Z}$. Pokažimo da postoji $k \in \mathbb{Z}$ takav da je $ax + by = ck$. Uzmemo $w = ax + by$ i zamijenimo a i b s jednakostima iz početka dokaza. Dobivamo $w = ck_1 x + ck_2 y$.

Po distributivnosti množenja prema zbrajanju, to je $w = c(k_1x + k_2y)$. Pronašli smo $k_1x + k_2y = k \in \mathbb{Z}$ takav da vrijedi $w = ck$, tj. $ax + by = ck$ pa $c|(ax + by)$.

$\square$

Propozicija. Neka su $a, b, q, r \in \mathbb{Z}$ te $a, b, r \neq 0$, $0 < r < |b|$ takvi da vrijedi $a = bq+r$. Tada je $\gcd(a, b) = \gcd(b, r)$.

Dokaz. Uzmimo $a = bq + r$ pa je to $r = a - bq$. Neka je $g = \gcd(a, b)$. Tada $g|a$ i $g|b$ i to je najveći takav cijeli broj. Tada g po prethodnoj propoziciji dijeli i svaku cjelobrojnu kombinaciju od a i b, tj. vrijedi da $g|(ax + by)$, za svaki $x, y \in \mathbb{Z}$. Tako vrijedi i za $x = 1$ i $y = -q$, tj. $g|(a - bq)$. To je jednako ostatku pa $g|r$. Dakle, g je zajednički djelitelj od b i r. Uzmimo $g' = \gcd(b, r)$. Očito vrijedi $g' \geq g$. No, $g'|b$ i $g'|(a - bq)$ pa tako i $g'|a$. Stoga je g' zajednički djelitelj od a i b. No, kako je g najveći zajednički djelitelj od a i b vrijedi $g \geq g'$. Dakle, $g = g'$.

$\square$

Teorem (Bezoutova lema). Neka su $a, b \in \mathbb{Z}\backslash\{0\}$. Vrijedi:

$$\gcd(a, b) = \min\{ax + by :\ x, y \in \mathbb{Z}\} \cap \mathbb{N}.$$

Dokaz. Neka je $L = \{ax + by :\ x, y \in \mathbb{Z}\} \cap \mathbb{N}$. Uzmimo $g_1 = \gcd(a, b)$ i $g_2 = \min L$. Pokažimo da je $g_1 = g_2$. No, prvo moramo pokazati da g_2 postoji. Ako su $a, b > 0$, dovoljno je uzeti $x = 1$ i $y = 1$ jer će tada biti $a + b > 0$, a time i $(a + b) \in L$. Ako je $a, b < 0$, uzimamo $x = y = -1$ i tada je $-a - b > 0$ i $-a - b \in L$. Ako je $a > 0$ i $b < 0$ (ili obratno) možemo uzeti $x = 1$ i $y = -1$ pa će biti $a - b > 0$ i $a - b \in L$ (ako je obratno, tj. $a < 0$ i $b > 0$ tada je $b - a \in L$). Dakle, skup L je neprazan i sadrži samo pozitivne brojeve pa po *well-ordering* principu, ima i najmanji element $g_2 = \min L$.

Pretpostavimo da g_2 ne dijeli a (ili g_2 ne dijeli b). Tada postoje jedinstveni $q, r \in \mathbb{Z}$ takvi da vrijedi $a = g_2q + r$, gdje je $0 < r < g_2$ (ako bi bilo $0 \leq r$, uzeli bismo u obzir i to da je a djeljiv s g_2). To znači da je $a = aqx + bqy + r$. Imamo $a - aqx - bqy = r$. Izlučimo faktore tako da bude $a(1 - qx) + b(-qy) = r$. Kako su $1 - qx, -qy \in \mathbb{Z}$ vrijedi da je $r = a(1 - qx) + b(-qy) \in L$. No, kako je $0 < r < g_2 = ax + by$, tj. $0 < a(1 - qx) + b(-qy) < ax - by$, došli smo u kontradikciju s pretpostavkom da je $ax - by$ najmanji element u L. Dakle, $g_2|a$ i $g_2|b$.

Promotrimo sada $g_1 = \gcd(a, b)$. Kako $g_2|a$ i $g_2|b$ oboje su zajednički djelitelji od a i b. No, g_1 je najveći zajednički djelitelj pa vrijedi $g_1 \geq g_2$. Ipak, vrijedi i da $g_1|a$ i $g_1|b$. Po definiciji djeljivosti postoje $k_1, k_2 \in \mathbb{Z}$ takvi da $a = k_1g_1$ i $b = k_2g_1$. Za neke $x, y \in \mathbb{Z}$ imamo $g_2 = ax + by = k_1g_1x + k_2g_1y$. Nakon izlučivanja to je $g_2 = g_1(k_1x + k_2y)$, dakle $g_1|g_2$ te je $g_2 \geq g_1$. Kako imamo $g_2 \geq g_1$ i $g_1 \geq g_2$, slijedi da je $g_1 = g_2$, tj. $\gcd(a, b) = \min(\{ax + by :\ x, y \in \mathbb{Z}\} \cap \mathbb{N})$.

$\square$

Korolar. Neka su $a, b \in \mathbb{Z}\backslash\{0\}$. Cijeli broj n jednak je linearnoj kombinaciji od a i b ako i samo ako je višekratnik od $\gcd(a, b)$.

Dokaz. Neka je $g = \gcd(a, b)$. *Nužnost.* Neka je $n \in \mathbb{Z}$ te neka je $ax + by = n$, za neki $x, y \in \mathbb{Z}$. Treba pokazati kako postoji $k \in \mathbb{Z}$ takav da je $n = gk$. Vrijedi $g|a$ i $g|b$ pa možemo zapisati $a = ga'$ i $b = gb'$, za $a', b' \in \mathbb{Z}$. Stoga imamo $n = a'gx + b'gy$. To je $n = g(a'x + b'y)$ pa $g|n$, tj. postoji $k \in \mathbb{Z}$ takav da je $n = gk$.

Dovoljnost. Neka je $n = gk$, za neki $k \in \mathbb{Z}$. Za g po Bezoutovoj lemi vrijedi $g = ax + by$ za neki $x, y \in \mathbb{Z}$. Pomnožimo li taj izraz s k dobivamo $gk = axk + byk$, tj. $n = a(xk) + b(yk)$. Kako su $xk, yk \in \mathbb{Z}$, radi se o linearnoj kombinaciji brojeva a i b koja je jednaka broju n.

$\square$

Teorem (Euklidova lema). Neka su zadani brojevi $a, b, c \in \mathbb{Z}$ takvi da vrijedi $\gcd(a, b) = 1$ i $a|bc$. Tada $a|c$.

Dokaz. Budući da $a|bc$, tada postoji $k \in \mathbb{Z}$ takav da vrijedi $bc = ka$. Kako je $\gcd(a, b) = 1$, tada postoje $x, y \in \mathbb{Z}$ takvi da je $ax+by = 1$, tj. $by = 1-ax$. Pomnožimo $bc = ka$ s y i imamo $bcy = kay$. Uvršavajući izraz za by dobivamo $c(1 - ax) = kay$. To je $c - cax = kay$. Premjestimo članove tako da bude $c = kay + cax$. Izlučimo s desne strane a i imamo $c = a(ky + cx)$. Kako su $k, y, c, x \in \mathbb{Z}$ tako je i $l = (ky + cx) \in \mathbb{Z}$ pa smo pronašli $l \in \mathbb{Z}$ takav da vrijedi $c = al$ što znači da $a|c$.

$\square$

Korolar. Neka je p prost broj i $a, b \in \mathbb{Z}$ i neka $p|ab$. Tada $p|a$ ili $p|b$ (ili oboje).

Dokaz. Pretpostavimo da $p \nmid a$. Tada je $\gcd(p, a) = 1$, što po Euklidovoj lemi znači da $p|b$. Slično, pretpostavimo da $p \nmid b$. Tada je $\gcd(p, b) = 1$ što znači da $p|a$. Pretpostavimo da je $a = b$. Tada je očito kako, ukoliko $p|a^2$, onda (po prethodna dva dokazana slučaja) $p|a$ (a time i $p|b$).

$\square$

Korolar. Neka su $p, q, r \in \mathbb{N}$ prosti brojevi. Ako $p \mid qr$ tada vrijedi ili $p = q$ ili $p = r$ (ili oboje).

Dokaz. Kako su p, q i r prosti brojevi, tako su i u parovima relativno prosti pa vrijedi $\gcd(p, q) = 1$ i $\gcd(p, r) = 1$. Tako po prethodnom korolaru slijedi da $p \mid q$ odnosno $p \mid r$. No, kako je $p \neq 1$, a q i r su djeljivi samo s jedan ili sami sa sobom, ostaje da mora biti ili $p = r$ ili $p = q$. U slučaju da je $r = q$ vrijedi $p = r = q$.

$\square$

Propozicija. Neka je $a \in \mathbb{Z}\backslash\{-1, 0\}$. Tada vrijedi $\gcd(a, a+1) = 1$.

Dokaz. Pretpostavimo da je $g = \gcd(a, a+1)$ i $g > 1$. Tada $g|a$ i $g|(a+1)$. To znači da postoje $k, l \in \mathbb{Z}$ takvi da je $a = gk$ i $a + 1 = gl$. Odatle slijedi kako mora biti $gk + 1 = gl$, a to je $gk - gl = -1$. Dakle, $g(l - k) = 1$. No, kako $g > 1$ ne mogu postojati cijeli brojevi k i l takvi da vrijedi $g(l - k) = 1$. Zato mora biti $g = 1$, tj. $\gcd(a, a+1) = 1$.

$\square$

Lema. Neka je $a \in \mathbb{Z}\backslash\{0\}$. Najveći djelitelj od a je $|a|$, a najmanji 1.

Dokaz. Uzmimo $S = \{d \in \mathbb{Z}\backslash\{0\} : \ a = kd\} \cap \mathbb{N}$. Očito je kako je $\min S = 1$ jer $a = a \cdot 1$. Upravo iz toga slijedi i $\max S = |a|$ jer $a = -|a|$ za $a < 0$ i $a = |a|$ za $a > 0$. Nijedan drugi cijeli broj k ne postoji u intervalu $\langle -1, 1\rangle\backslash\{0\}$, za koje bi $\max S$ bio veći, a $\min S$ manji.

$\square$

Lema. Neka su $a, b \in \mathbb{Z}\backslash\{0\}$ takvi da $a|b$. Tada je $\gcd(a, b) = |a|$. Vrijedi i obrat.

Dokaz. *Nužnost.* Znamo kako $a|b$, ali i da $a|a$. To je najveći broj koji dijeli a i vrijedi $a|b$ i $a|a$ pa je $\gcd(a, b) = |a|$ (dodajemo apsolutnu vrijednost kako bismo osigurali da je $\gcd(a, b) \in \mathbb{N}$).

Dovoljnost. Pretpostavimo kako je $\gcd(a, b) = |a|$. To znači kako $|a|$ dijeli a i $|a|$ dijeli b, tj. postoji $k \in \mathbb{Z}$ takav da je $b = |a|k$. Ukoliko je b negativan, tada mora biti da je k negativan. Stoga, ako je a negativan, uzimamo $b = ak'$, gdje je $k' \in \mathbb{Z}$ i $k' = |k|$ pa vrijedi $a|b$. Ukoliko je a pozitivan, jednostavno imamo $b = ak$ i vrijedi $a|b$. Ako je b pozitivan, mora biti i da je k pozitivan pa za pozitivan a uzimamo $b = ak$ i onda $a|b$. Ako je a pak negativan, dovoljno je uzeti $k' = -k$ i imamo $b = ak'$, gdje je $k' \in \mathbb{Z}$ pa opet $a|b$. Kako smo u svim slučajevima dobili $a|b$ vrijedi pretpostavka obrata tvrdnje.

$\square$

Teorem (Euklidov algoritam). Neka su zadani $a, b \in \mathbb{Z}\backslash\{0\}$. Tada, postupkom

$$
\begin{aligned}
a &= bq_0 + r_1, \\
b &= r_1 q_1 + r_2, \\
r_1 &= r_2 q_2 + r_3, \\
&\vdots \\
r_{n-2} &= r_{n-1} q_{n-1} + r_n, \\
r_{n-1} &= r_n q_n,
\end{aligned}
$$

gdje je $0 < r_i < r_{i-1}$, za $i \in \{2, \dots, n\}$ te $0 < r_1 < |a|$, dobivamo $\gcd(a, b) = r_n$.

Dokaz. Ovaj postupak traje konačno upravo zbog uzastopne primjene teorema o dijeljenju s ostatkom. Obzirom da je $0 < r_1 < |a|$ i $0 < r_i < r_{i-1}$, za $i \in \{2, \dots, n\}$ zbog *well-ordering* svojstva skupa $\mathbb{Z}^+$, moramo doći do nule (što se vidi u $r_{n-1} = r_n q_n$). Zatim, po prethodnoj propoziciji vrijedi $\gcd(a, b) = \gcd(b, r_1)$. No, tako vrijedi i, po drugom koraku, $\gcd(b, r_1) = \gcd(r_1, r_2)$. Tako za n-ti ostatak vrijedi $\gcd(r_{n-2}, r_{n-1}) = \gcd(r_{n-1}, r_n)$. Tako je $\gcd(a, b) = \gcd(r_{n-1}, r_n)$. No, kako $r_n | r_{n-1}$, po prethodnoj lemi vrijedi $\gcd(r_{n-1}, r_n) = r_n$. Tako je $\gcd(a, b) = r_n$.

□

Propozicija. Neka su $a, b \in \mathbb{Z}^*$. Iz Euklidovog algoritma možemo dobiti $x, y \in \mathbb{Z}$ takve da je $\gcd(a, b) = ax + by$.

Dokaz. Primijenimo li Euklidov algoritam na a i b, dobivamo:

$$\begin{aligned}
a &= bq_0 + r_1, \\
b &= r_1 q_1 + r_2, \\
r_1 &= r_2 q_2 + r_3, \\
&\vdots \\
r_{n-3} &= r_{n-2} q_{n-2} + r_{n-1}, \\
r_{n-2} &= r_{n-1} q_{n-1} + r_n, \\
r_{n-1} &= r_n q_n.
\end{aligned}$$

Uzmemo $r_n = r_{n-2} - r_{n-1} q_{n-1}$. Zatim, $r_n = r_{n-2} - (r_{n-3} - r_{n-2} q_{n-2}) q_{n-1}$, tj. $r_n = r_{n-2}(1 + q_{n-2}) - r_{n-3} q_{n-1}$. Pretpostavimo kako $r_n = r_{i+1} x' + r_i y'$. Tada, jer je $r_{i-1} = r_i q_i + r_{i+1}$ imamo $r_n = x'(r_{i-1} - r_i q_i) + r_i y'$, tj. $r_n = x' r_{i-1} + r_i (y' - q_i x')$. Dakle, nastavimo li tom analogijom, dolazimo i da $r_n = x' r_2 + y' r_1$. No, $r_2 = b - r_1 q_1$ pa imamo $r_n = x'(b - r_1 q_1) + y' r_1$, tj. $r_n = x' b + r_1 (y' - q_1 x')$. Uzmimo $y' - q_1 x' = x$. Dalje, $r_1 = a - bq_0$ pa je $r_n = x' b + (a - bq_0) x$, tj. $r_n = b(x' - q_0 z) + ax$. Uzemo li $y = (x' - q_0 z)$ imamo $r_n = ax + by$, tj. $\gcd(a, b) = ax + by$ za $x, y \in \mathbb{Z}$.

□

Propozicija. Neka je $a \in \mathbb{Z}$. Tada je $\gcd(a, 0) = a$.

Dokaz. Vrijedi da $a | a$ i $a | 0$. To je najveći takav broj koji dijeli a pa je $\gcd(a, 0) = a$.

□

Propozicija. Za $a, b, k \in \mathbb{Z}$, $a, b \neq 0$, vrijedi $\gcd(a, b) = \gcd(a, b + ak)$.

Dokaz. Uzmimo $g = \gcd(a, b)$. Tada $g|a$ i $g|b$ i to je najveći takav broj. Tada g dijeli i cjelobrojnu kombinaciju od a i b pa i $b + ak$. Stoga $g|a$ i $g|(b + ak)$. Uzmimo $g' = \gcd(a, b + ak)$. Tada vrijedi $g' \geq g$ jer je g djelitelj od a i $b + ak$, a g' je najveći takav. No, kako $g'|a$ i $g'|(b+ak)$, tada je $a = g'x$, za neki $x \in \mathbb{Z}$ i $b+ak = g'y$, za neki $y \in \mathbb{Z}$. Tako je $b + g'xk = g'y$, tj. $b = g'y - g'xk = g'(y - xk)$. Dakle, $g'|b$. Kako $g'|a$ i $g'|b$ on je zajednički djelitelj od a i b pa je $g' \leq g$ jer je g najveći takav. No, imamo $g' \leq g$ i $g' \geq g$ pa je $g' = g$.

Drugi način da se pokaže ova propozicija je ovisan o prethodno dokazanoj propoziciji. Uzmemo li $c = b + ak$, očito je kako je b ostatak pri dijeljenju c s a. Pa ako je $g = \gcd(a, c)$ tada je, po prethodno dokazanoj propoziciji $\gcd(a, c) = \gcd(a, b)$. To je $\gcd(a, b + ak) = \gcd(a, b)$.

□

Propozicija. Neka su $m, n, k \in \mathbb{Z}^*$ takvi da $\gcd(m, n) = 1$ i $k|n$. Tada je $\gcd(m, k) = 1$.

Dokaz. Kako $k|n$, postoji $q \in \mathbb{Z}$ takav da je $n = qk$. Pretpostavimo kako postoji $r, m', k' \in \mathbb{Z}$ tako da vrijedi $m = rm'$ i $k = rk'$. Kako je $\gcd(m, n) = 1$, postoje $x, y \in \mathbb{Z}$ takvi da je $xm + yn = 1$. No, tada imamo $xrm' + yqrk' = 1$, tj. $r(xm' + yqk') = 1$. No kako je $r \in \mathbb{Z}$ i $(xm' + yqk') \in \mathbb{Z}$, oba broja moraju biti jednaka ili 1 ili -1. Dakle $r = \pm 1$, što znači da su brojevi m i k relativno prosti.

□

Propozicija. Neka su $m, n, k \in \mathbb{Z}^*$ takvi da $\gcd(mn, k) = 1$. Tada $\gcd(m, k) = 1$ i $\gcd(n, k) = 1$.

Dokaz. Imamo $\gcd(mn, k) = 1$. Neka je $\gcd(m, k) = q$. To znači kako postoje $u, v \in \mathbb{Z}$ takvi da je $m = qu$ i $k = qv$. Iz toga slijedi kako je $mn = qun$. Jer je $\gcd(mn, k) = 1$, postoje $w, z \in \mathbb{Z}$ takvi da vrijedi $mnw + kz = 1$. Imamo $qunw + qvz = 1$, tj. $q(unw + vz) = 1$ pa je $q = \frac{1}{unw+vz}$. No, $(unw + vz) \in \mathbb{Z}$ pa stoga mora biti i $unw + vz = 1$ i imamo $q = 1$. Dakle, jedini zajednički djelitelj od m i k je 1 pa mora biti $\gcd(m, k) = 1$. Analogno se dokazuje i za $\gcd(n, k) = 1$.

□

Propozicija. Neka su $k, n, m \in \mathbb{Z}^*$ takvi da je $\gcd(n, m) = 1$. Tada je $\gcd(kn, km) = k$.

Dokaz. Neka je $g = \gcd(kn, km)$. Pokažimo da je $g = k$. Očito je kako $k|(kn)$ i $k|(km)$, stoga je k zajednički djelitelj od kn i km pa $k|g$. Pokažimo da $g|k$. Vrijedi da $g|(kn)$ i $g|(km)$. Imamo $kn = gx$ i $km = gy$, za $x, y \in \mathbb{Z}$. Pomnožimo li prvu jednadžbu s y dobivamo $kny = gxy$ te je $kny = kmx$, tj. $ny = mx$. To znači kako $n|(mx)$. No, po Euklidovoj lemi mora biti da $n|x$, tj. $\frac{x}{n} \in \mathbb{Z}$. Uzmimo $c = \frac{x}{n}$. Stoga iz $kn = gx$ imamo $k = g\frac{x}{n}$, i.e. $k = gc$, za $c \in \mathbb{Z}$ pa po definiciji $g|k$. Stoga je $g = k$.

$\square$

Propozicija. Neka su $m, n \in \mathbb{Z}^*$. Tada je $\gcd(mn, m) = m$.

Dokaz. Uzmimo $g = \gcd(mn, m)$. Pokažimo kako je $g = m$. Očito $g|(mn)$ i $g|m$ (iz toga slijedi $g \leq m$). No, isto tako $m|(mn)$ i $m|m$ pa je m zajednički djelitelj od mn i m te vrijedi, obzirom da je g po pretpostavci najveći, $m \leq g$. Kako imamo $g \leq m$ i $m \leq g$, vrijedi $g = m$.

$\square$

Propozicija. Neka su $k, l, n \in \mathbb{Z}^*$ takvi da je $\gcd(k, n) = 1$ i $\gcd(l, n) = 1$. Tada je $\gcd(kl, n) = 1$.

Dokaz. Pretpostavimo da postoji $q \in \mathbb{Z}$ takav da $q|(kl)$ i $q|n$ te $q \neq \pm 1$. To znači kako je $kl = qx$ i $n = qy$, za $x, y \in \mathbb{Z}$. Pomnožimo li prvu jednadžbu s y dobivamo $kly = nx$. To znači kako $n|(kly)$. No, po Euklidovoj lemi, $n \nmid k$ stoga $n|(ly)$. Ali, opet po Euklidovoj lemi, $n \nmid l$ pa $n|y$. Stoga je $\frac{y}{n} \in \mathbb{Z}$. Iz $n = qy$ dobivamo $1 = q\frac{y}{n}$. No, to znači da $q|1$ i $\frac{y}{n}|1$, a to može biti samo ako $q = \frac{y}{n} = \pm 1$ (fali preciznosti, ali bit je tu). To je u suprotnosti s pretpostavkom da je $\gcd(kl, n) \neq \pm 1$.

$\square$

Napomena. Od sada ćemo u tekstu uzeti oznaku $\mathbb{Z}^* = \mathbb{Z} \backslash \{0\}$.

Definicija. Neka je $a, b \in \mathbb{Z}^*$. Svaki broj $m \in \mathbb{Z}^*$ takav da $m|a$ i $m|b$ zovemo **zajednički višekratnik** od a i b. Najmanji takav broj zovemo **najmanji zajednički višekratnik** od a i b te pišemo $m = \operatorname{lcm}(a, b)$.

Propozicija. Za svaki $a, b \in \mathbb{Z}^*$ ne postoji najveći zajednički višekratnik.

Dokaz. Pretpostavimo da je m zajednički višekratnik od a i b i to najveći takav. No, uzmemo li $m' = m|a|$, vrijedi da $m'|m$ i $m'|a$, pa tako i $m'|b$. Stoga je m' zajednički višekratnik od a i b. No, kako je $m' = m|a|$, vrijedi $m \leq m'$ što je u suprotnosti s pretpostavkom da je m najveći zajednički višekratnik.

$\square$

Propozicija. Za svaki $a, b \in \mathbb{Z}^*$ vrijedi:

$$\mathrm{lcm}(a, b) = \frac{|ab|}{\gcd(a, b)}.$$

Dokaz. Neka je $l = \mathrm{lcm}(a, b)$ i $l' = \frac{|ab|}{\gcd(a,b)}$. Po definiciji vrijedi $a|l$, $b|l$ i $l \leq l'$ (jer je to najmanji zajednički višekratnik - ukoliko je l' zajednički višekratnik). Pokažimo kako je l' uistinu zajednički višekratnik od a i b, tj. da $a|l$ i $b|l$. Uzmimo $g = \gcd(a, b)$. Tada po definiciji najvećeg zajedničkog djelitelja $g|a$ i $g|b$, tj. $\exists x, y \in \mathbb{Z}$ takvi da $a = gx$ i $b = gy$. Uzmemo li $l' = \frac{|ab|}{g} = \frac{|agx|}{g}$. Kako je g pozitivan, vrijedi $l' = |ax|$ pa $a|l'$. Na isti način se pokaže da $b|l'$ pa je l' zajednički višekratnik od a i b. Pokažimo da $l|l'$. Uzmemo li $\frac{l}{l'}$ imamo:

$$\frac{l}{l'} = \frac{lg}{|ab|}.$$

Po prethodno dokazanoj propoziciji vrijedi $g = az + bw$ za neki $z, w \in \mathbb{Z}^*$. Tada je $lg = alz + blw$. Kako $a|l$ i $b|l$ postoje $m, n \in \mathbb{Z}$ takvi da je $l = am$ i $l = bn$. Stoga je $lg = abnz + abmw = ab(nz + mw)$ pa $(ab)|(lg)$. Stoga je $\frac{l}{l'} = u$, gdje je $u \in \mathbb{Z}$ takav da je $lg = abu$. Dakle, $l = l'u$, i.e. $l'|l$ pa mora biti $l' \leq l$ (ne moramo paziti na apsolutnu vrijednost jer uzimamo u obzir samo pozitivne višekratnike). Kako je $l \leq l'$ (l je najmanji zajednički višekratnik) i $l' \leq l$ vrijedi $l = l'$ i time je dokazana propozicija.

$\square$

Korolar. Ako za $a, b \in \mathbb{Z}^*$ vrijedi $\gcd(a, b) = 1$ tada je $\mathrm{lcm}(a, b) = |ab|$.

Dokaz. Slijedi direktno iz prethodne propozicije. Ako je $\gcd(a, b) = 1$, tada je:

$$\text{lcm(a,b)} = \frac{|ab|}{\gcd(a, b)} = \frac{|ab|}{1} = |ab|.$$

$\square$

Korolar. Neka su $a, b \in \mathbb{Z}^*$ takvi da $b|a$. Tada je $\mathrm{lcm}(a, b) = |a|$.

Dokaz. Vrijedi da je, po prethodnoj lemi, $\gcd(a, b) = |b|$ (ako $b|a$) pa direktnim uvršavanjem u formulu iz prethodne propozicije dobivamo:

$$\mathrm{lcm}(a,b) = \frac{|ab|}{\gcd a, b} = \frac{|a| \cdot |b|}{|b|} = |a|.$$

$\square$

Teorem (Fundamentalni teorem aritmetike). Svaki se prirodan broj veći od 2 može prikazati kao umnožak prostih brojeva (ili je prost broj) na jedinstven način do na poredak.

Dokaz. *Egzistencija* Dokaz se provodi jakom matematičkom indukcijom. Neka je $n = 2$. Tada je n prost broj pa vrijedi baza indukcije. Pretpostavimo da se svaki $k < n$ može prikazati kao umnožak prostih brojeva ili je sam prost broj. Ako je n prost, tada smo gotovi. Ako n nije prost, tada postoji neki n_1 i n_2, različiti od 1, takvi da je $n = n_1 n_2$. No, $n_1 < n$ i $n_2 < n$, pa se po pretpostavci indukcije mogu prikazati kao umnošci prostih brojeva.

Jedinstvenost. Pretpostavimo da je $p_1 p_2 \cdots p_n = q_1 q_2 \cdots q_m$, gdje su $m, n \in \mathbb{N}$ i $m > n$. Po Euklidovoj lemi, ukoliko podijelimo cijeli izraz s p_1, i kako su svi p_i i q_j prosti, mora biti da je p_1 jednak nekom q_j (bez smanjenja općenitosti možemo pretpostaviti kako je to upravo q_1). Tako dijeleći sa svakim p_i (isto, bez smanjenja općenitosti možemo pretpostaviti da će odgovarati upravo broju q_i), dobivamo $1 = q_{n+1} q_{n+2} \cdots q_m$. No, tada $q_{n+1}, q_{n+2}, \ldots, q_m$ moraju biti jednaki 1. Po tome imamo $p_i = q_i$, za svaki $i \in \{1, \ldots, n\}$ dok su ostali $q_j = 1$ i time nebitni.

$\square$

Lema. Neka su $p \neq q$ prosti brojevi te $i, j \in \mathbb{N}$. Tada je $\gcd(p^i, q^j) = 1$.

Dokaz. Očito je kako $p^i = \underbrace{p \cdot p \cdots p}_{i \text{ puta}}$ i $q^j = \underbrace{q \cdot q \cdots q}_{j \text{ puta}}$ ne sadrže nijedan zajednički djelitelj.

$\square$

Propozicija. Neka je $n \in \mathbb{N}$. Ako $p^i | n$ i $q^j | n$, za neke proste brojeve $p \neq q$, te prirodne brojeve i, j. Tada $p^i q^j | n$.

Dokaz. Kako $p^i | n$, postoji $k \in \mathbb{N}$ (radimo u skupu prirodnih brojeva, i p^i i n su prirodni pa mora biti i k) takav da je $n = p^i k$. Također, za $q^j | n$ postoji $l \in \mathbb{N}$ takav da je $n = q^j l$. Primijetimo kako odavdje trivijalno slijedi $p^i \nmid k$ i $q^j \nmid l$. Također, bitna opaska jeste da su p^i i q^j relativno prosti. Imamo $p^i k = q^j l$. Ukoliko podijelimo jednadžbu s p^i, po Euklidovoj lemi (i prethodnoj opasci) mora biti $p^i | l$. Za neki $l' \in \mathbb{N}$ je $l = l' p^i$. Tada je $n = q^j l' p^i$, za neki $l' \in \mathbb{N}$, pa stoga $p^i q^j | n$.

$\square$

Teorem (Euklidov teorem). Postoji beskonačno mnogo prostih brojeva.

Dokaz. Pretpostavimo da postoji n prostih brojeva $p_1, p_2, \ldots, p_n$. Tada postoji složen broj $a = p_1 p_2 \cdots p_n$. Uzmimo $b = a + 1$. Tada je po prethodno dokazanoj propoziciji $\gcd(a, b) = 1$, tj. a i b nemaju zajedničkih djelitelja. No, kako se svaki prirodan broj, po fundamentalnom teoremu aritmetike, može prikazati kao umnožak prostih faktora ili je sam prost broj, vrijedi da je ili b prost ili je b umnožak nekih prostih faktora. Ukoliko je b prost, a nijedan $p_i \nmid b$, tada b mora biti prost broj različit od svih p_i. Ako b nije prost, a nijedan $p_i \nmid b$, b mora biti umnožak nekih prostih faktora različitih od p_i.

$\square$

Kongruencija

Definicija. Neka su $a, b \in \mathbb{Z}$, $m \in \mathbb{N} \backslash \{1\}$. Kažemo kako je a kongruentan b modulo m i pišemo $a \equiv b \pmod{m}$ ako vrijedi $m|(a-b)$.

Primjer. Očito je $17 \equiv 2 \pmod{5}$ jer $5|(17-2)$. Isto tako i $2 \equiv 17 \pmod{5}$ jer $5|(2-17)$. Slično, $-17 \equiv -2 \pmod{5}$ i $-2 \equiv -17 \pmod{5}$, ali nije $-17 \equiv 2 \pmod{5}$ i nije $-2 \equiv 17 \pmod{5}$. Ipak bi bilo npr. $-13 \equiv 2 \pmod{5}$.

Primjedba. Iako jeste $15 \equiv 0 \pmod{5}$ u biti ekvivalentno izjavi $5|15$, ipak nije preporučljivo gledati na to u istom svjetlu.

Propozicija. Relacija kongruencije je relacija ekvivalencije.

Dokaz. (i) *Refleksivnost.* Znamo kako $m|0$ jer za $0 \in \mathbb{Z}$ vrijedi $0 = 0 \cdot m$. Kako je, očito, $a - a = 0$ za svaki $a \in \mathbb{Z}$, vrijedi da $m|(a-a)$. Tako $a \equiv a \pmod{m}$ što dokazuje reflektivnost relacije kongruencije.

(ii) *Simetričnost.* Ukoliko imamo $a \equiv b \pmod{m}$ to znači da $m|(a-b)$, dakle postoji $k \in \mathbb{Z}$ takav da je $a - b = mk$. To je $-(b-a) = mk$ pa pomnoživši sve s -1 dobivamo $b - a = m \cdot (-k)$. Stoga postoji $k' \in \mathbb{Z}$, $k' = -k$ takav da $b - a = k'm$ pa $m|(b-a)$. Tj. $b \equiv a \pmod{m}$. Simetričnost, dakle, vrijedi.

(iii) *Tranzitivnost.* Ako je $a \equiv b \pmod{m}$ i $b \equiv c \pmod{m}$, tada vrijedi $m|(a-b)$ i $m|(b-c)$. To znači kako postoje $k, l \in \mathbb{Z}$ takvi da $a - b = mk$ i $b - c = ml$. Zbrojimo li te dvije jednakosti dobivamo $a - c = m(k+l)$. Uzevši $k' = k + l$ imamo $a - c = k'm$ pa $m|(a-c)$. To znači da $a \equiv c \pmod{m}$. Time je dokazana i tranzitivnost relacije kongruencije.

$\square$

Propozicija. Neka su $a, b, c \in \mathbb{Z}$ i $m \in \mathbb{N}$. Ako je $a \equiv b \pmod{m}$, tada je

(i) $ac \equiv bc \pmod{m}$,

(ii) $a + c \equiv b + c \pmod{m}$.

Dokaz. Kako je $a \equiv b \pmod{m}$ to znači da $m|(a-b)$, tj. da postoji $k \in \mathbb{Z}$ takav da je $a - b = km$. (i) Pomnožimo li tu jednakost s c dobivamo $(a-b)c = kmc$, što možemo grupirati tako da bude $ac - bc = m(kc)$. Uzmemo li $k' \in \mathbb{Z}$ takav da je $k' = kc$ imamo $ac - bc = k'm$ pa $m|(ac-bc)$. To znači da je $ac \equiv bc \pmod{m}$. (ii) Dodamo li jednakosti $a - b = km$ broj c tada je $a - b + c = km + c$, tj. $a - b + c - c = km$. Nakon grupiranja to je $(a+c) - (b+c) = km$ pa $m|((a+c)-(b+c))$. Stoga je $a + c \equiv b + c \pmod{m}$.

$\square$

Propozicija. Vrijedi $a \equiv a + km \pmod{m}$, za svaki $a, k \in \mathbb{Z}$ i $m \in \mathbb{N}$.

Dokaz. Vrijedi $m|(a - km)$ a to je ekvivalentno $m|(a - a - km)$, tj. $m|(a - (a + km))$ pa je $a \equiv a + km \pmod{m}$.

$\square$

Propozicija. Neka su $a, b, k \in \mathbb{Z}$ i $m \in \mathbb{N}$. Tada, $a \equiv b + km \pmod{m}$ ako i samo ako $a \equiv b \pmod{m}$.

Dokaz. *Nužnost.* Ako je $a \equiv b + mk \pmod{m}$, tada $m|(a - b - mk)$, tj. postoji $q \in \mathbb{Z}$ takav da je $a - b - mk = mq$. Iz toga dobivamo $a - b = m(q + k)$ pa $m|(a - b)$, tj. $a \equiv b \pmod{m}$. *Dovoljnost.* Ako je $a \equiv b \pmod{m}$, tada postoji $q \in \mathbb{Z}$ takav da je $mq = a - b$. Uzmimo $k \in \mathbb{Z}$. Tada je $mq = a - b + km - km$. Iz toga dobivamo $m(q - k) = a - b - km$, tj. $m(q - k) = a - (b + km)$. Iz toga slijedi $a \equiv b + km \pmod{m}$.

$\square$

Propozicija. Neka su $a, b \in \mathbb{Z}$ i $k, m \in \mathbb{N}$. Tada iz $a \equiv b \pmod{k)m}$ slijedi $a \equiv b \pmod{m}$.

Dokaz. Po definiciji $km|(a-b)$, tj. postoji $q \in \mathbb{Z}$ takav da je $a-b = kmq$. To možemo zapisati kao $a - b = m(kq)$ pa očito $m|(a - b)$, tj. $a \equiv b \pmod{m}$.

$\square$

Propozicija. Neka su $a, b \in \mathbb{Z}$ i $0 \leq a, b < m$. Tada iz $a \equiv b \pmod{m}$ slijedi $a = b$.

Dokaz. Iz $a \equiv b \pmod{m}$ slijedi $m|(a - b)$, tj. postoji $q \in \mathbb{Z}$ takav da je $a - b = mq$. Drugim riječima, $a = mq + b$. Kako je $0 \leq b < m$, imamo $mq \leq mq + b < m$, iz čega slijedi $mq \leq a < m$, što je moguće samo ako je $q = 0$. Stoga, mora biti $a = m \cdot 0 + b$ pa je $a = b$.

$\square$

Propozicija. Neka su $a, b, c, d \in \mathbb{Z}$ i $m \in \mathbb{N}$ Ako je $a \equiv b \pmod{m}$ i $c \equiv d \pmod{m}$ tada je $a + c \equiv b + d \pmod{m}$.

Dokaz. Kako je $a \equiv b \pmod{m}$ tada $m|(a-b)$ pa postoji $k \in \mathbb{Z}$ takav da je $a-b = mk$. Isto tako postoji $l \in \mathbb{Z}$ takav da je $c - d = ml$. Zbrojimo li ova dva izraza dobivamo $(a + c) - (b + d) = m(k + l)$ pa $m|((a + c) - (b + d))$. Stoga je $a + c \equiv b + d \pmod{m}$.

$\square$

Propozicija. Neka su $a, b, c, d \in \mathbb{Z}$ i $m \in \mathbb{N}$ Ako je $a \equiv b \pmod m$ i $c \equiv d \pmod m$ tada je $ac \equiv bd \pmod m$.

Dokaz. Kako je $a \equiv b \pmod m$ i $c \equiv d \pmod m$, postoje $k, l \in \mathbb{Z}$ takvi da je $a - b = mk$ i $c - d = ml$. Iz zadnje jednakosti imamo $c = d + ml$. Pomnožimo prvu jednadžbu s c i dobivamo $ac - bc = mkc$. Zatim, uvrstimo izraz za c tako da dobijemo $ac - bd - ml = mkc$. To je pak ekvivalentno izrazu $ac - bd = mkc + ml$. Zajednički faktor m možemo izlučiti te dobivamo $ac - bd = m(kc + l)$. Kako su $k, c, l \in \mathbb{Z}$, tada je i $(kc + l) \in \mathbb{Z}$ pa vrijedi $m|(ac - bd)$ što je po definiciji kongruencije $ac \equiv bd \pmod m$.

$\square$

Propozicija. Neka su $x, y \in \mathbb{Z}$ i $a \in \mathbb{Z}^*$. Ako je $ax \equiv ay \pmod a m$, tada je $x \equiv y \pmod m$.

Dokaz. Imamo $am|(ax - ay)$, tj. postoji $q \in \mathbb{Z}$ takav da je $ax - ay = amq$. Izlučimo zajednički faktor a i dobivamo $a(x - y) = a(mq)$. Obzirom da je $a \neq 0$ po pretpostavci propozicije, cijeli izraz možemo podijeliti s a i dobiti $x - y = mq$. Po definiciji to je $x \equiv y \pmod m$.

$\square$

Propozicija. Neka su $x, y \in \mathbb{Z}$ i $a \in \mathbb{Z}^*$. Ako je $ax \equiv ay \pmod m$ i $\gcd(a, m) = 1$ vrijedi $x \equiv y \pmod m$.

Dokaz. Iz $ax \equiv ay \pmod m$ dobivamo $m|(ax - ay)$, tj. $m|a(x - y)$. Po Euklidovoj lemi, obzirom da je $\gcd(m, a) = 1$, mora biti $m|(x - y)$, tj. $x \equiv y \pmod m$.

$\square$

Propozicija. Neka je $m \in \mathbb{Z}$. Tada $m|(qm + 1)^n - 1$, za svaki $q \in \mathbb{Z}$ i $n \in \mathbb{N}$.

Dokaz. Neka je $m, q \in \mathbb{Z}$ i $n \in \mathbb{N}$. Pokažimo da $m|(qm + 1)^n - 1$. Neka je $n = 1$. Imamo $(qm + 1)^1 - 1 = qm + 1 - 1 = qm$, iz čega je očito kako $m|qm$. Pretpostavimo kako tvrdnja vrijedi za $n = k$, tj. neka postoji $q' \in \mathbb{Z}$ takav da je $(qm + 1)^k - 1 = q'm$. Dokažimo da tvrdnja vrijedi za $n = k + 1$. Imamo:

$$(qm + 1)^{k+1} - 1 = (qm + 1)^k (qm + 1) - 1 = qm(qm + 1)^k + (qm + 1)^k - 1.$$

Primijetimo kako iz pretpostavke indukcije možemo iskoristiti $(qm+1)^k - 1 = q'm$. Stoga je:

$$(qm+1)^{k+1} - 1 = qm(qm+1)^k + q'm.$$

Gornjem izrazu možemo dodati i oduzeti m pa je:

$$(qm+1)^{k+1} - 1 = qm(qm+1)^k - m + m + q'm = m\left((qm+1)^k - 1 + 1 + q'\right).$$

Opet iskoristimo pretpostavku indukcije i dobivamo:

$$(qm+1)^{k+1} - 1 = m(q'm + 1 + q') = m\left(q'(m+1) + 1\right).$$

Iz toga slijedi kako $m|(qm+1)^{k+1}$ te je tvrdnja dokazana za svaki $n \in \mathbb{N}$. Stoga iz $a^n - 1 = (qm+1)^n - 1$ imamo $m|(qm+1)^n - 1$, a tako i $m|a^n - 1$, što je ekvivalentno, po definiciji kongruencije, $a^n \equiv 1 \pmod{m}$.

$\square$

Propozicija. Neka je $a \equiv b \pmod{m}$. Tada je $a^n \equiv b^n \pmod{m}$, za svaki $n \in \mathbb{N}$.

Dokaz. Za $n = 1$ očito vrijedi $a \equiv b \pmod{m}$, po pretpostavci propozicije. Pretpostavimo kako je $a^k \equiv b^k \pmod{m}$, za neki $k \in \mathbb{N}$. Pokažimo kako tvrdnja vrijedi za $k+1$. Koristeći prethodno dokazanu propoziciju, pretpostavku i bazu indukcije, slijedi $aa^k \equiv bb^k \pmod{m}$, tj. $a^{k+1} \equiv b^{k+1} \pmod{m}$.

$\square$

Propozicija. Ako je $a \equiv 1 \pmod{m}$, tada je $a^n \equiv 1 \pmod{m}$, za svaki $n \in \mathbb{N}$.

Dokaz. Iz prethodne propozicije, uvrštavanjem $b = 1$ i koristeći činjenicu kako je $1^n = 1$, direktno slijedi $a^n \equiv 1 \pmod{m}$.

$\square$

Propozicija. Neka je $x \equiv y \pmod{m}$. Tada vrijede sljedeće tvrdnje:

1. Ako je $z \equiv x + w \pmod{m}$, tada je $z \equiv y + w \pmod{m}$.
2. Ako je $z \equiv xw \pmod{m}$, tada je $z \equiv yw \pmod{m}$.

Dokaz. *Ad* 1. Postoje $k, l \in \mathbb{Z}$ takvi da je $mk = x - y$ i $ml = z - (x + w)$. Imamo $x = mk + y$ i $ml = z - x - w$. Iz toga slijedi kako je $ml = z - mk - y - w$, tj. $m(l + k) = z - (y + w)$ što je ekvivalentno $z \equiv y + w \pmod{m}$.

Ad 2. Postoje $k, l \in \mathbb{Z}$ takvi da je $mk = x - y$ i $ml = z - xw$. Tada je $x = mk + y$ pa uvrštavanjem dobivamo $ml = z - (mk + y)w$, tj. $ml = z - mkw - yw$. To je ekvivalentno $m(l + kw) = z - yw$ što implicira $z \equiv yw \pmod{m}$.

$\square$

Propozicija. Neka je $a \in \mathbb{Z}^*$ i $m \in \mathbb{N}$. Tada, $\gcd(a, m) = 1$ ako i samo ako postoji $b \in \mathbb{Z}$ takav da je $ab \equiv 1 \pmod{m}$.

Dokaz. *Nužnost.* Neka je $\gcd(a, m) = 1$. Tada po Bezoutovoj lemi postoje $x, y \in \mathbb{Z}$ takvi da je $ax + my = 1$. To je ekvivalentno izrazu $my = 1 - ax$, što znači kako $m|(1 - ax)$ pa je po definiciji $1 \equiv ax \pmod{m}$. Po simetričnosti relacije kongruencije vrijedi $ax \equiv 1 \pmod{m}$. Uzmemo li $b = x$, imamo da postoji $b \in \mathbb{Z}$ takav da je $ab \equiv 1 \pmod{m}$.

Dovoljnost. Neka postoji $b \in \mathbb{Z}$ takav da je $ab \equiv 1 \pmod{m}$. Tada, po definiciji kongruencije, $m|(ab-1)$, tj. postoji $q \in \mathbb{Z}$ takav da je $ab-1 = mq$. Uzmemo li $q' = -q$, imamo $1 - ab = mq'$ i to je ekvivalentno $1 = mq' + ab$. Uzmimo $\gcd(a, b) = g$. Tada $g|m$ i $g|a$, te postoje $m', a' \in \mathbb{Z}$ takvi da je $m = m'g$ i $a = a'g$. Uvrštavajući to u prethodnu jednakost dobivamo $m'gq' + a'gb = 1$. Izlučimo zajednički faktor te imamo $g(m'q' + a'b) = 1$, što znači da $g|1$. Dakle, $|g| = 1$, što znači kako su a i m relativno prosti.

$\square$

Napomena. Primijetimo kako, ukoliko je $\gcd(a, m) = 1$, te $ab \equiv 1 \pmod{m}$, mora biti i $\gcd(b, m) = 1$. Jer, kada dobijemo $ab \equiv 1 \pmod{m}$, to je ekvivalentno $ab - 1 = mq$, za $q \in \mathbb{Z}$, pa je $1 = mq' + ab$, za $q' = -q$. Pretpostavimo li $\gcd(b, m) = g$, imamo $1 = m'gq' + ab'g$, za $m', b' \in \mathbb{Z}$. Tada je $g(m'q' + ab') = 1$ pa mora biti $g|1$ i $|g| = 1$ pa su b i m također relativno prosti.

Propozicija. Neka su $a, b \in \mathbb{Z}^*$ i $m \in \mathbb{N}$. Ako je $ab \equiv 1 \pmod{m}$, tada je $a(b+km) \equiv 1 \pmod{m}$, za svaki $k \in \mathbb{Z}$.

Dokaz. Neka je $ab \equiv 1 \pmod{m}$. To znači kako je $ab - 1 = mq$, za neki $q \in \mathbb{Z}$. Uzmemo li $a(b + km) = ab + akm$ imamo $a(b + km) = mq + 1 + akm$, a iz toga $a(b + km) = 1 + m(q + ak)$. To je pak ekvivalentno $a(b + km) - 1 = m(q + ak)$, pa je $a(b + km) \equiv 1 \pmod{m}$.

$\square$

Propozicija. Neka je $a \in \mathbb{Z}^*$ i $m \in \mathbb{N}$. Ako je $\gcd(a, m) \neq 1$, onda ne postoji $b \in \mathbb{Z}^*$ takav da je $ab \equiv 1 \pmod m$.

Dokaz. Neka je $g = \gcd(a, m)$ i $g \neq 1$. Tada je $a = a'g$ i $m = m'g$ za $a', m' \in \mathbb{Z}$. Pretpostavimo da postoji $b \in \mathbb{Z}^*$ takav da je $ab \equiv 1 \pmod m$. Imamo $ab - 1 = mq$, za neki $q \in \mathbb{Z}$. No, također $a'gb - 1 = m'gq$. Iz toga dobivamo $g(a'b - m'q) = 1$. No, to znači kako mora biti $g = \pm 1$, što je u suprotnosti s pretpostavkom da je $g \neq 1$. Dakle, ne postoji $b \in \mathbb{Z}^*$ takav da je $ab \equiv 1 \pmod m$.

$\square$

Propozicija. Neka je $x \in \mathbb{Z}^-$ i $m \in \mathbb{N}$. Tada postoji $k \in \mathbb{N}$ takav da je $0 \leq x + km < m$.

Dokaz. Po teoremu o dijeljenju s ostatkom $x = qm + r$, gdje je $0 \leq r < |m| = m$. Dovoljno je uzeti $q = -k$ te dobivamo $x = -km + r$. Iz toga je $r = x + km$ i $0 \leq r < m$.

$\square$

Napomena. Primijetimo kako pomoću Euklidovog algoritma možemo dobiti $x, y \in \mathbb{Z}$ takve da je $ax + my = \gcd(a, m)$, tj. $ax + my = 1$. Tada je $ax \equiv 1 \pmod m$. Ukoliko je $x < 0$, koristeći prethodnu propoziciju, lagano možemo uzeti $b = x + km$. Po prethodnoj propoziciji također možemo uzeti takav b, po teoremu o dijeljenju s ostatkom, tako da bude $0 \geq b < m$. Ovo je jedan efikasan algoritam za pronalaženje (multiplikativnog) inverza u $(\mathbb{Z}/n\mathbb{Z})^*$.

Propozicija. Neka je $n \in \mathbb{N} - 2\mathbb{N}$. Tada vrijedi $(n+1)^2 \equiv n + 1 \pmod{2n}$.

Dokaz. Kako je $n \in \mathbb{Z}^+ - 2\mathbb{Z}$, možemo uzeti $n = 2k + 1$, gdje je $k \in \mathbb{Z}_0^+$. Imamo:

$$(n+1)^2 = ((2k+1)+1)^2 = (2k+2)^2 = 4k^2 + 8k + 4.$$

Također imamo $n + 1 = (2k + 1) + 1 = 2k + 2$ i $2n = 2(2k + 1) = 4k + 2$. Pokazat ćemo kako $4k + 2 | (4k^2 + 8k + 4) - (2k + 2)$, tj. kako $4k + 2 | 4k^2 + 6k + 2$. Po formuli za rješenja kvadratne jednadžbe imamo:

$$\begin{aligned} k_{1,2} &= \frac{-6 \pm \sqrt{6^2 - 4 \cdot 4 \cdot 2}}{2 \cdot 4} \\ &= \frac{-6 \pm \sqrt{36 - 32}}{8} = \frac{-6 \pm \sqrt{4}}{8} \\ &= \frac{-6 \pm 2}{8}. \end{aligned}$$

Iz toga dobivamo:

$$\begin{aligned} k_1 &= \frac{-6-2}{8} = \frac{-8}{8} = -1 \\ k_2 &= \frac{-6+2}{8} = \frac{-4}{8} = -\frac{1}{2}. \end{aligned}$$

Po tome je:

$$4k^2 + 6k + 2 = 4\left(k+1\right)\left(k+\frac{1}{2}\right) = \left(k+1\right)\left(4k+2\right).$$

Iz gornjeg rezultata vidljivo je kako $(4k+2)|(4k^2+6k+2)$ te je time propozicija dokazana.

$\square$

Propozicija. Neka je $n, k \in \mathbb{Z}^+$ i $n > k$. Tada je:

$$\binom{n}{k} = \binom{n-1}{k-1} + \binom{n-1}{k}.$$

Dokaz. Primijetimo kako po ograničenjima propozicije na n i k, u nijednom retku ispod nećemo dobiti negativan faktorijel. Imamo:

$$\begin{aligned} \binom{n-1}{k-1} + \binom{n-1}{k} &= \frac{(n-1)!}{(n-(k-1))!(k-1)!} + \frac{(n-1)!}{(n-k)!k!} \\ &= \frac{(n-1)!}{(n-(k-1))(n-k)!(k-1)!} + \frac{(n-1)!}{(n-k)!k(k-1)!} \\ &= \frac{(n-1)!k + (n-1)!(n-k)}{(n-k)!k!} = \frac{(n-1)!(k+(n-k))}{(n-k)!k!} \\ &= \frac{(n-1)!n}{(n-k)!k!} = \frac{n!}{(n-k)!k!} = \binom{n}{k}. \end{aligned}$$

$\square$

Propozicija. Neka je $n \in \mathbb{Z}_0^+$. Tada je:

$$\binom{n}{0} = \binom{n}{k} = 1.$$

Dokaz. Po definiciji je:

$$\begin{aligned}\binom{n}{0} &= \frac{n!}{(n-0)!0!} = \frac{n!}{n!0!} = 1,\\ \binom{n}{n} &= \frac{n!}{(n-n)!n!} = \frac{n!}{0!n!} = 1.\end{aligned}$$

□

Propozicija. Neka su $n, k \in \mathbb{Z}_0^+$ i $n \leq k$. Tada je $\binom{n}{k} \in \mathbb{Z}^+$.

Dokaz. Dokaz se provodi matematičkom indukcijom. Ako je $n = k$ ili $k = 0$, imamo $\binom{n}{0} = \binom{n}{n} = 1$ pa je $\binom{n}{0}, \binom{n}{n} \in \mathbb{Z}^+$. Za $n = 0$ imamo $\binom{0}{k} = 1 \in \mathbb{Z}^+$, za svaki $0 \leq k \leq n$ (tj. za $k = 0$). Pretpostavimo kako je tvrdnja istinita za neki $n \in \mathbb{Z}_0^+$ (i za sve $0 \leq k \leq n$; po bazi indukcije smo pokazali kako je točno za $n = 0$ i sve $0 \leq k \leq n$, tj. za $k = 0$). Za $n+1$, obzirom da ćemo promatrati $0 < k < n$ (za $k = 0$ i $k = n$ je dokazano) i jer je $n + 1 \in \mathbb{Z}^+$, po prethodnoj propoziciji imamo:

$$\binom{n+1}{k} = \binom{n}{k-1} + \binom{n}{k}.$$

Po pretpostavci indukcije, oba su člana pozitivni cijeli brojevi pa je i njihov zbroj pozitivan cijeli broj te je $\binom{n+1}{k} \in \mathbb{Z}^+$.

□

Propozicija. Neka je $p \in P$ i $n \in \mathbb{N}$, $n < p$. Tada:

$$\binom{p}{n} \equiv 0 \pmod{p}.$$

Dokaz. Po formuli za binomni koeficijent imamo:

$$\binom{p}{n} = \frac{p!}{(p-n)!n!} = \frac{p(p-1)\cdots(p-n+1)(p-n)!}{(p-n)!n!} = \frac{p(p-1)\cdots(p-n+1)}{n!}.$$

Obzirom da u nazivniku imamo n faktora, a svi su strogo manji od p i manji od n, oni ne mogu dijeliti p, jer je p prost broj (osim u slučaju kada je $n = 1$, no tada je binomni koeficijent očito jednak p). No, jer je binomni koeficijent cijeli broj, po Euklidovoj lemi, $n!$ mora dijeliti preostale članove, tj. $n! | (p-1)\cdots(p-n+1)$. Dakle, razlomak $\frac{(p-1)\cdots(p-n+1)}{n!} = k$ je cijeli broj pa imamo:

$$\binom{p}{n} = pk.$$

Po definiciji djeljivosti, $p|\binom{p}{n}$. Drugim riječima, $p|\binom{p}{n}-0$ pa je po definiciji kongruencije:

$$\binom{p}{n} \equiv 0 \pmod{p}.$$

$\square$

Rješavanje kongruencija

Propozicija. Neka je $m \in \mathbb{N}$ i $a \in \mathbb{Z}$. Rješenje od $x \equiv a \pmod{m}$ je svaki $x \in \{a + km : k \in \mathbb{Z}\}$.

Dokaz. Za svaki $k \in \mathbb{Z}$ definiramo $x_k = a + km$. Tada, uvrstimo to u kongruenciju i dobivamo $x_k \equiv a \pmod{m}$, tj. $a + km \equiv a \pmod{m}$. Po prethodnoj propoziciji to je ekvivalentno $a \equiv a \pmod{m}$.

□

Propozicija. Neka je $m \in \mathbb{N}$ i $a, b \in \mathbb{Z}$ takvi da je $\gcd(a, m) = 1$. Linearna kongruencija $ax \equiv b \pmod{m}$ tada ima jedinstveno rješenje modulo m.

Dokaz. *Postojanje.* Kako je $\gcd(a, m) = 1$, po Bezoutovoj lemi postoje $a', m' \in \mathbb{Z}$ takvi da je $a'a + m'm = 1$, tj. $m'm = 1 - a'a$. To je ekvivalentno, po definiciji kongruencije, $1 \equiv a'a \pmod{m}$. Uzmemo li dakle $ax \equiv b \pmod{m}$ i pomnožimo li tu kongruenciju s dobivenim $a' \in \mathbb{Z}$, dobivamo $a'ax \equiv a'b \pmod{m}$. No, $a'a \equiv 1 \pmod{m}$ pa imamo $x \equiv a'b \pmod{m}$.

Jedinstvenost. Pretpostavimo kako postoji $x' \in \mathbb{Z}$ takav da je $ax' \equiv b \pmod{m}$, ali x' nekongruentno s x_0. To znači kako $m \nmid x' - x_0$ tj. po teoremu o dijeljenju s ostatkom postoje $q, r \in \mathbb{Z}$, takvi da je $x' - x_0 = qm + r$, gdje je $0 \leq r < |m| = m$. Stoga je $x' - x_0 \equiv r \pmod{m}$. No, obzirom da je $ax' \equiv b \pmod{m}$, dobivamo $x' \equiv a_0 b \pmod{m}$ (po prethodnom postupku). No $x_0 = a_0 b$ pa imamo $0 \equiv r \pmod{m}$, tj. $r = mr'$, za neki $r' \in \mathbb{Z}$. Stoga imamo $x' - x_0 = qm + mr'$, tj. $x' - x_0 = m(q + r')$. Dakle, $x' \equiv x_0 \pmod{m}$, što je u kontradikciji s pretpostavkom da $m \nmid x' - x_0$.

□

Teorem (Kineski teorem o ostatcima). Neka su $a, b \in \mathbb{Z}$ i $m, n \in \mathbb{Z}^+$ takvi da je $\gcd(m, n) = 1$. Tada sustav $x \equiv a \pmod{m}$, $x \equiv b \pmod{n}$ ima jedinstveno rješenje modulo mn.

Dokaz. *Postojanje.* Kako je $\gcd(m, n) = 1$, po Bezoutovoj lemi postoje $p, q \in \mathbb{Z}$ takvi da je $mp + nq = 1$. Odatle slijedi $mp \equiv 1 \pmod{n}$ i $nq \equiv 1 \pmod{m}$. Uzmemo li $x_0 = mpb + nqa$, lako se vidi kako će takav x_0 zadovoljavati obje kongruencije. Prvo, $mpb + nqa \equiv a \pmod{m}$ daje $mpb + nqa - a = ms$, za neki $s \in \mathbb{Z}$. Iz toga slijedi $nqa - a = m(s - pb)$, tj. $nqa \equiv a \pmod{m}$. No, zbog $nq \equiv 1 \pmod{m}$, imamo $a \equiv a \pmod{m}$. Slično, $mpb + nqa \equiv b \pmod{n}$ daje $mpb + nqa - b = nt$, za neki $t \in \mathbb{Z}$. Tada je $mpb - b = n(t - qa)$ što je ekvivalentno kongruenciji $mpb \equiv b \pmod{n}$. Zbog

$mp \equiv 1 \pmod{n}$ imamo $b \equiv b \pmod{n}$. Dakle, $x_0 = mpb + nqa$ je rješenje sustava, a brojevi p i q se mogu dobiti pomoću Euklidovog algoritma.

Jedinstvenost. Pretpostavimo kako postoji i $y_0 \in \mathbb{Z}$ takav da je $y_0 \equiv a \pmod{m}$ i $y_0 \equiv b \pmod{n}$. Iz toga slijedi $x_0 \equiv y_0 \pmod{m}$ i $x_0 \equiv y_0 \pmod{n}$. To znači kako $m|x_0 - y_0$ i $n|x_0 - y_0$. Iz prvog uvjeta dobivamo da postoji $q \in \mathbb{Z}$ takav da je $x_0 - y_0 = mq$. No, kako $n|x_0 - y_0$, tj. $n|mq$, obzirom da je $\gcd(m,n) = 1$, po Euklidovoj lemi imamo $n|q$, tj. postoji $p \in \mathbb{Z}$ takav da je $mq = mnp$. Stoga je $x_0 - y_0 = mnp$, tj. $x_0 \equiv y_0 \pmod{mn}$.

□

Korolar. Neka je $k \in \mathbb{Z}^+ - \{1\}$ i neka su $a_1, \dots, a_k \in \mathbb{Z}$ i $m_1, \dots, m_k \in \mathbb{Z}$ takvi da je $\gcd(m_i, m_j) = 1$, za svaki $i \neq j$, $i, j \in \{1, \dots, k\}$. Tada sustav $x \equiv a_1 \pmod{m_1}, \dots, x \equiv a_k \pmod{m_k}$ ima jedinstveno rješenje modulo $m_1 \cdots m_k$.

Dokaz. Provodi se po indukciji. Neka je $k = 2$. Tada sustav $x \equiv a_1 \pmod{m_1}$, $x \equiv a_2 \pmod{m_2}$ po prethodnom teoremu ima jedinstveno rješenje x_0 modulo $m_1 m_2$. Prepostavimo kako tvrdnja vrijedi za neki $k \in \mathbb{Z}$. Pokažimo da vrijedi za $k+1$. Imamo $x \equiv a_1 \pmod{m_1}, \dots, x \equiv a_k \pmod{m_k}, x \equiv a_{k+1} \pmod{m_{k+1}}$. Po pretpostavci indukcije, sustav $x \equiv a_1 \pmod{m_1}, \dots, x \equiv a_k \pmod{m_k}$ ima jedinstveno rješenje x_0 modulo $M = m_1 \cdots m_k$. Kako je $\gcd(m_{k+1}, m_i) = 1$, za svaki $i \in \{1, \dots, k\}$, tada je i $\gcd(M, m_{k+1}) = 1$. Iz toga imamo $Mq + m_{k+1}p = 1$. Uzmemo:

$$y_0 = Mqa_{k+1} + m_{k+1}px_0.$$

Vidimo kako će biti $Mqa_{k+1} + m_{k+1}px_0 \equiv a_i \pmod{m_i}$, za svaki $i \in \{1, \dots, k\}$ jer $Mqa_{k+1} + m_{k+1}px_0 - a_i = m_i s_i$, gdje je $s_i \in \mathbb{Z}$. No, obzirom da $m_i|M$ (po definiciji broja M), imamo $M = m_i t_i$, za neki $t_i \in \mathbb{Z}$. Stoga imamo $m_i t_i q a_{k+1} + m_{k+1}px_0 - a_i = m_i s_i$ što je ekvivalentno $m_{k+1}px_0 - a_i = m_i(s_i - t_i q a_{k+1})$, odnosno $m_{k+1}px_0 \equiv a_i \pmod{m_i}$. Sada još moramo primijetiti kako je, zbog $Mq + m_{k+1}p = 1$, zapravo $1 - m_{k+1}p = Mq$, tj. $1 - m_{k+1}p = m_i t_i q$. Iz toga dobivamo $m_{k+1}p \equiv 1 \pmod{m_i}$ pa iz $m_{k+1}px_0 \equiv a_i \pmod{m_i}$ slijedi $x_0 \equiv a_i \pmod{m_i}$, što je u skladu s pretpostavkom. Nadalje, pokazat ćemo i kako $y_0 \equiv a_{k+1} \pmod{m_{k+1}}$. Imamo $Mqa_{k+1} + m_{k+1}px_0 \equiv a_{k+1} \pmod{m_{k+1}}$, tj. $Mqa_{k+1} + m_{k+1}px_0 - a_{k+1} = m_{k+1}s_{k+1}$, gdje je $s_{k+1} \in \mathbb{Z}$. To je pak ekvivalentno $Mqa_{k+1} - a_{k+1} = m_{k+1}(s_{k+1} - px_0)$, tj. $Mqa_{k+1} \equiv a_{k+1} \pmod{m_{k+1}}$. Još ostaje primijetiti kako iz $Mq + m_{k+1}p = 1$ slijedi $1 - Mq = m_{k+1}p$, tj. $Mq \equiv 1 \pmod{m_{k+1}}$. Stoga iz $Mqa_{k+1} \equiv a_{k+1} \pmod{m_{k+1}}$ slijedi $a_{k+1} \equiv a_{k+1} \pmod{m_{k+1}}$, što je istinito. Dakle y_0 je rješenje zadanog sustava. Pretpostavimo još kako postoji $z_0 \in \mathbb{Z}$ takav da je $z_0 \equiv a_1 \pmod{m_1}, \dots, z_0 \equiv a_{k+1} \pmod{m_{k+1}}$. No, tada je i $z_0 \equiv y_0 \pmod{m_1}, \dots, z_0 \equiv y_0 \pmod{m_{k+1}}$ pa $m_i|z_0 - y_0$ za svaki $i \in \{1, \dots, k+1\}$. To naravno povlači kako $m_1 \cdots m_{k+1} | z_0 - y_0$, tj. $z_0 \equiv y_0 \pmod{m_1 \cdots m_{k+1}}$. Time je jedinstvenost rješenje modulo $m_1 \cdots m_{k+1}$ dokazana i tvrdnja vrijedi za svaki $k \in \mathbb{Z}$.

$\square$

Eulerova funkcija

Definicija. Neka je $x \in \mathbb{R}$. Definiramo $\lfloor x \rfloor = \max\{k \in \mathbb{Z} : \ k \leq x\}$.

Primjedba. Neka je $\frac{n}{m} \in \mathbb{Q}$. Tada je:

$$\left\lfloor \frac{n}{m} \right\rfloor = \max\left\{k \in \mathbb{Z} : \ k \leq \frac{n}{m}\right\}.$$

No, obzirom da je $m \in \mathbb{Z}^+$ (ako i nije, možemo namjestiti da bude; za sada nećemo biti toliko precizni niti ćemo dokazivati postojanje maksimuma i slično), imamo:

$$\left\lfloor \frac{n}{m} \right\rfloor = \max\{k \in \mathbb{Z} : \ km \leq n\}.$$

Lako se vidi kako je $\left\lfloor \frac{n}{m} \right\rfloor$ jednak koeficijentu k koji daje najveći višekratnik broja m manji od n. Stoga je najveći višekratnik broja m manji od n u stvari $m \left\lfloor \frac{n}{m} \right\rfloor$.

Propozicija. Neka je $m \in \mathbb{Z}^+$. Broj višekratnika od m u skupu $\{1, \ldots, n\}$, gdje je $n \in \mathbb{N}$, je $\left\lfloor \frac{n}{m} \right\rfloor$.

Dokaz. Neka je $S = \{1, \ldots, n\}$ i $m \in \mathbb{Z}^+$. Višekratnici broja m iz skupa S se tada nalaze u skupu $V = \{km \in S : \ k \in \mathbb{Z}\}$. Želimo znati $|V|$. Znamo kako je najveći višekratnik broja m manji od n jednak $v = m \left\lfloor \frac{n}{m} \right\rfloor$. Stoga je $\max V = v$. Ukoliko $m \notin V$, tada je (jer V ne sadrži nulu, tj. $0 \cdot m$), vrijedi $V = \emptyset$ pa je $|V| = 0$. Ako $m \notin V$, to znači u biti $n < m$ pa je lako uočiti kako je $\left\lfloor \frac{n}{m} \right\rfloor = 0$ (jer je $\frac{n}{m} < 1$ za $n < m$). Ako $m = n$, očito je $v = 1$. No, ako je $m > n$, sigurno je i $m \in V$ i $\min\{V\} = m$. Tada je broj višekratnika u V (ne zaboravimo uključiti i najveći) jednak

$$|V| = \frac{m \left\lfloor \frac{n}{m} \right\rfloor - m}{m} + 1 = \left\lfloor \frac{n}{m} \right\rfloor.$$

□

Definicija. Neka je zadan skup:

$$\varphi_m = \{n \in \mathbb{Z}^+ : \ (\gcd(m, n) = 1) \wedge (n \leq m)\}.$$

Tada je Eulerova funkcija $\varphi : \mathbb{Z}^+ \to \mathbb{Z}^+$ definirana kao $\varphi(m) = |\varphi_m|$.

Teorem (Euler[1]). Neka su $a \in \mathbb{Z} - \{0\}$ i $m \in \mathbb{Z}^+ - \{1\}$ takvi da je $\gcd(a, m) = 1$. Tada vrijedi:

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

Dokaz. Neka je $S = \{k \in \mathbb{Z}^+ \cap [1, m-1] : \gcd(a, k) = 1\}$. Očito je kako je $|S| = \varphi(m)$ jer za svaka dva $k_1 \neq k_2$, $k_1, k_2 \in S$, vrijedi $k_1 \not\equiv k_2 \pmod{m}$ (ako bi bili jednaki modulo m, obzirom da su oba manji od m, bilo bi $k_1 = k_2$, što je u suprotnosti s pretpostavkom da su različiti). No, promotrimo sada skup $aS = \{ak \in \mathbb{Z}^+ : k \in S\}$. Svi su elementi u aS različiti modulo m jer, ako to ne bi bilo tako, postojali bi $k_1 \neq k_2$, $k_1, k_2 \in S$, $k \leq \varphi(m)$ takvi da je $ak_1 \equiv ak_2 \pmod{m}$. No, obzirom da je $\gcd(a, m) = 1$, po Bezoutovoj lemi postoje $x, y \in \mathbb{Z}^+$ takvi da je $ax + my = 1$, tj. $my = 1 - ax$, što implicira $1 \equiv ax \pmod{m}$. Stoga, pomnožimo li $ak_1 \equiv ak_2 \pmod{m}$ dobivamo $axk_1 \equiv axk_2 \pmod{m}$, tj. $k_1 \equiv k_2 \pmod{m}$. No, obzirom da su $k_1, k_2 \in S$, vrijedi $0 < k_1, k_2 < m$, pa mora biti $k_1 = k_2$, što je u suprotnosti s pretpostavkom da su različiti. Stoga vrijedi da su svi elementi u aS različiti modulo m pa je $|aS| = |S| = \varphi(m)$. To znači kako se svi elementi iz S nalaze u aS modulo m i obratno. Dakle, elementi iz S i aS su jednaki modulo m pa su produkti tih elemenata opet jednaki modulo m. Ako je $S = \{a_1, \ldots, a_{\varphi(m)}\}$ imamo:

$$a_1 a_2 \cdots a_{\varphi(m)} \equiv (aa_1)(aa_2) \cdots (aa_{\varphi(m)}) \pmod{m}.$$

Ukoliko preuredimo te elemente s desne strane, dobivamo produkt od $\varphi(m)$ elemenata a, pa je:

$$a_1 a_2 \cdots a_{\varphi(m)} \equiv a^{\varphi(m)} a_1 a_2 \cdots a_{\varphi(m)} \pmod{m}.$$

No, obzirom da je $\gcd(a_i, m) = 1$, tada je također $\gcd(A, m) = 1$, gdje je $A = a_1 \cdots a_{\varphi(m)}$. Po Bezoutovoj lemi postoje $p, q \in \mathbb{Z}$ takvi da je $Ap + mq = 1$, što implicira $Ap \equiv 1 \pmod{m}$. Stoga, pomožimo li obje strane gornje kongruencije s p, dobivamo:

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

No, to je zbog simetričnosti relacije kongruencije isto što i $a^{\varphi(m)} \equiv 1 \pmod{m}$, što je i trebalo dokazati.

[1] Ovaj teorem sam dokazao pomoću teorije grupa u svojoj skripti *Abstract Algebra*. Dokaz je, uz poznavanje teorije grupa, vrlo izravan i očigledan.

$\square$

Lema. Neka je $p \in P$ te $m, n \in \mathbb{Z}^+$. Tada, $\gcd(p^m, n) = 1$ ako i samo ako $\gcd(p, n) = 1$.

Dokaz. *Nužnost.* Neka je $\gcd(p^m, n) = 1$. Tada postoje $x, y \in \mathbb{Z}$ takvi da je $p^m x + ny = 1$. Iz toga dobivamo $p(p^{m-1}x) + ny = 1$. Pretpostavimo li da $\gcd(p, n) = g$ i $g \neq 1$, tada je $p = p'g$ i $n = n'g$. No iz toga slijedi, obzirom da je p prost i $g \neq 1$, kako je $g = p$ pa je $n = n'p$. Stoga imamo $p(p^{m-1}x) + n'py = 1$. Tada je $p\,(p^{m-1}x + n'y) = 1$ i mora biti $p = 1$, što je nemoguće jer $1 \notin P$. Dakle, $\gcd(p, n) = 1$. *Dovoljnost.* Neka je $\gcd(p, n) = 1$. Pretpostavimo li kako je $\gcd(p^m, n) = g$, gdje je $g \neq 1$, tada $g | p^m$ i $g | n$. Iz $g | p^m$, po Euklidovoj lemi, slijedi kako je $g = p^k$, gdje je $1 < k \leq m$. Iz toga bi slijedilo kako $p^k | n$ i da postoji $n' \in \mathbb{Z}$ takav da je $n = n'p^k$, tj. $n = p(n'p^{k-1})$. Stoga $p | n$. No, kako i $p | p$ slijedi $\gcd(p, n) = p$, što je u suprotnosti s pretpostavkom.

$\square$

Teorem. Vrijedi $\varphi(p^m) = p^{m-1}(p-1)$, za svaki $p \in P$ i $m \in \mathbb{Z}^+$.

Dokaz. Promotrimo skup:

$$\varphi_{p^m} = \{n \in \mathbb{Z}^+ : \ (\gcd(p^m, n) = 1) \wedge (n \leq p^m)\}.$$

Po prethodnoj lemi, $\gcd(p^m, n) = 1$ ako i samo ako $\gcd(p, n) = 1$. Stoga prethodni skup zapisati na ekvivalentan način:

$$\varphi_{p^m} = \{n \in \mathbb{Z}^+ : \ (\gcd(p, n) = 1) \wedge (n \leq p^m)\}.$$

Skup φ_{p^m} ne sadrži samo višekratnike broja p manje od p^m (i veće od 1). Po prethodnoj propoziciji, broj višekratnika u $\{1, \ldots, p^m\}$ je $\left\lfloor \frac{p^m}{p} \right\rfloor = \lfloor p^{m-1} \rfloor$. No, jer je $m \geq 1$, tada je $p^{m-1} \in \mathbb{Z}^+$ pa mora biti $\lfloor p^{m-1} \rfloor = p^{m-1}$. Kako skup $\{1, \ldots, p^m\}$ sadrži p^m članova, broj članova u tom skupu koji nisu višekratnici broja p je $p^m - p^{m-1}$. Dakle,

$$|\varphi_{p^m}| = p^m - p^{m-1} = p^{m-1}(p-1).$$

Dakle, $\varphi(p^m) = p^{m-1}(p-1)$.

$\square$

Primjedba. Primijetimo da zbog ovog svojstva, multiplikativnosti Eulerove funkcije (tj. $\varphi(mn) = \varphi(m)\varphi(n)$ ako i samo ako $\gcd(m, n) = 1$; dokaz ću ostaviti za svoje spise iz algebre) i fundamentalnog teorema aritmetike, Eulerovu funkciju možemo računati kao:

$$\varphi(n) = \varphi\left(\prod_{\substack{p \in P \\ \alpha(p) \geq 1}} p^{\alpha(p)}\right) = \prod_{\substack{p \in P \\ \alpha(p) \geq 1}} \varphi\left(p^{\alpha(p)}\right) = \prod_{\substack{p \in P \\ \alpha(p) \geq 1}} \left(p^{\alpha(p)-1}(p-1)\right).$$

Propozicija. Neka su $m, n \in \mathbb{Z}^+$. Ako $n|m$ tada $\varphi(n)|\varphi(m)$.

Dokaz. Zapišimo kvocijent brojeva m i n po fundamentalnom teoremu aritmetike kao:

$$\frac{m}{n} = \frac{\prod_{\substack{p \in P \\ \alpha(p) \geq 1}} p^{\alpha(p)}}{\prod_{\substack{p \in P \\ \beta(p) \geq 1}} p^{\beta(p)}}.$$

Slično, možemo promotriti i kvocijent:

$$\frac{\varphi(m)}{\varphi(n)} = \frac{\prod_{\substack{p \in P \\ \alpha(p) \geq 1}} p^{\alpha(p)-1}(p-1)}{\prod_{\substack{p \in P \\ \beta(p) \geq 1}} p^{\beta(p)-1}(p-1)}.$$

Obzirom da $n|m$, tada za svaki $p \in P$ vrijedi $\alpha(p) - \beta(p) \geq 0$. Također, $\alpha(p) - 1 - (\beta(p) - 1) = \alpha(p) - \beta(p) \geq 0$. Članovi $(p - 1)$ se također pokrate uz odgovarajuće $p \in P$, pa je $\frac{\varphi(m)}{\varphi(n)} = q$, gdje je $q \in \mathbb{Z}^+$. Iz toga slijedi $\varphi(m) = q\varphi(n)$, tj. $\varphi(n)|\varphi(m)$.

$\square$

Primitivni korijen

Definicija. Neka je $m \in \mathbb{Z}^+ - \{1\}$ i $g \in \mathbb{Z}$, $\gcd(g, m) = 1$. Ako za svaki $a \in \mathbb{Z}$, gdje je $\gcd(a, m) = 1$, postoji $k \in \mathbb{Z}$ takav da vrijedi $g^k \equiv a \pmod{m}$, kažemo da je g **primitivan korijen** modulo m.

Primjedba. Kroz teoriju grupa, mogli bismo reći kako je primitivan korijen generator grupe $(\mathbb{Z}/m\mathbb{Z})^*$, tj. $g \in \mathbb{Z}/m\mathbb{Z}$ takav da vrijedi $\langle g \rangle = (\mathbb{Z}/m\mathbb{Z})^*$ (gdje $\langle g \rangle$ označava cikličku grupu generiranu elementom g, a ne principalan ideal polja $\mathbb{Z}/m\mathbb{Z}$ generiran elementom g).

Definicija. Neka je $m \in \mathbb{Z}^+ - \{1\}$. **Redom elementa** $a \in \mathbb{Z}$ nazivamo nenegativan broj $n = \min\{k \in \mathbb{Z}^+ : \ a^k \equiv 1 \pmod{m}\}$ i pišemo $\operatorname{ord}_m(a) = n$. Ukoliko takav broj ne postoji pišemo $\operatorname{ord}_m(a) = 0$ i kažemo kako je element a **beskonačnog reda**.

Propozicija. Neka je $m \in \mathbb{Z}^+ - \{1\}$. Tada, $\operatorname{ord}_m(a) > 0$ ako i samo ako $\gcd(a, m) = 1$.

Dokaz. *Nužnost.* Neka je $\operatorname{ord}_m(a) > 0$. Tada je $\operatorname{ord}_m(a) \neq 0$ i postoji $k \in \mathbb{Z}^+$ takav da je $a^k \equiv 1 \pmod{m}$. Po definiciji relacije kongruencije, postoji $q \in \mathbb{Z}$ takav da je $a^k - 1 = qm$. Pretpostavimo kako je $\gcd(a, m) = g > 1$. Tada $a = bg$ i $m = ng$, za neke $b, n \in \mathbb{Z}$. Iz $a^k - 1 = qm$ dobivamo $(bg)^k - 1 = q(ng)$. To je pak ekvivalentno izrazu $b^k g^k - 1 = qng$, tj. $g(g^{k-1}b^k - qn) = 1$. Obzirom da je $g \in \mathbb{Z}^+$ i $g^{k-1}b^k - qn \in \mathbb{Z}$, može samo biti $g = 1$, što je u kontradikciji s pretpostavkom da je $\gcd(a, m) > 1$ i mora biti $\gcd(a, m) = 1$. *Dovoljnost.* Pretpostavimo kako je $\gcd(a, m) = 1$. Po Eulerovom teoremu, $a^{\varphi(m)} \equiv 1 \pmod{m}$. Kako je $\varphi(m) > 0$, za svaki $m \in \mathbb{Z}^+$, postoji barem jedan element skupa $\min\{k \in \mathbb{Z}^+ : \ a^k \equiv 1 \pmod{m}\}$, pa red elementa a ne može biti nula. Stoga, $\operatorname{ord}_m(a) > 0$.

$\square$

Teorem. Neka je $m \in \mathbb{Z}^+ - \{1\}$ i $a \in \mathbb{Z}$. Ako je $a^k \equiv 1 \pmod{m}$, za neki $k \in \mathbb{Z}$, tada $\operatorname{ord}_m(a) \mid k$.

Dokaz. Pretpostavimo kako je $a^k \cong 1 \pmod{m}$, gdje je $k \in \mathbb{Z}$. Po teoremu o dijeljenju s ostatkom postoje $q, r \in \mathbb{Z}$ takvi da je $k = q\operatorname{ord}_m(a) + r$, gdje je $0 \leq r < \operatorname{ord}_m(a)$. Tada je $a^k = a^{q\operatorname{ord}_m(a)+r} = a^{q\operatorname{ord}_m(a)}a^r = \left(a^{\operatorname{ord}_m(a)}\right)^q a^r$. Kako je $a^k \equiv 1 \pmod{m}$, tada je $\left(a^{\operatorname{ord}_m(a)}\right)^q a^r \equiv 1 \pmod{m}$. Također, obzirom da je $a^{\operatorname{ord}_m(a)} \equiv 1 \pmod{m}$, imamo $1^q a^r \equiv 1 \pmod{m}$, tj. $a^r \equiv 1 \pmod{m}$. No, obzirom da je $0 \leq r < \operatorname{ord}_m(a)$, a $\operatorname{ord}_m(a)$ je po definiciji najmanji takav broj da je $a^{\operatorname{ord}_m(a)} \equiv 1 \pmod{m}$, mora biti $r = 0$. Tada iz $k = q\operatorname{ord}_m(a) + r$ slijedi $k = q\operatorname{ord}_m(a)$, tj. $\operatorname{ord}_m(a) \mid k$.

□

Korolar. Neka su $m \in \mathbb{Z}^+ - \{1\}$ i $a \in \mathbb{Z}$ takvi da je $\gcd(a,m) = 1$. Tada $\text{ord}_m(a) | \varphi(m)$.

Dokaz. Kako je $\gcd(a,m) = 1$, po Eulerovom teoremu vrijedi $a^{\varphi(m)} \equiv 1 \pmod{m}$. Po prethodnom teoremu tada $\text{ord}_m(a) | \varphi(m)$.

□

Teorem. Neka je $m \in \mathbb{Z}^+ - \{1\}$ i $a \in \mathbb{Z}$ takvi da je $\gcd(a,m) = 1$. Tada, $\text{ord}_m(a) = \varphi(m)$ ako i samo ako za svaki $p \in P$ takav da $p|\varphi(m)$ vrijedi:

$$a^{\frac{\varphi(m)}{p}} \not\equiv 1 \pmod{m}.$$

Dokaz. *Nužnost.* Pretpostavimo kako je $\text{ord}_m(a) = \varphi(m)$, ali kako postoji $p \in P$ takav da $p|\varphi(m)$ i $a^{\frac{\varphi(m)}{p}} \equiv 1 \pmod{m}$. Obzirom da je $\frac{\varphi(m)}{p} \in \mathbb{Z}^+$ i kako je $\frac{phi(m)}{p} < \varphi(m) = \text{ord}_m(a)$, dolazimo u kontradikciju s činjenicom da je $\varphi(m)$ red od a. Stoga mora biti $a^{\frac{\varphi m}{p}} \not\equiv 1 \pmod{m}$, za svaki $p \in P$ takav da $p|\varphi(m)$.

Dovoljnost. Pretpostavimo da je $a^{\frac{\varphi(m)}{p}} \not\equiv 1 \pmod{m}$ za svaki $p \in P$ takav da $p|\varphi(m)$. Po korolaru prethodnog teorema, jer je $\gcd(a,m) = 1$, slijedi $\text{ord}_m(a) | \varphi(m)$, tj. postoji $q \in \mathbb{Z}$ takav da je $\varphi(m) = q\text{ord}_m(a)$. Ako je $q = 1$, tada je $\varphi(m) = \text{ord}_m(a)$ pa smo gotovi. Ako je $q > 1$, tada $q|\varphi(m)$ pa postoji $p \in P$ takav da $p|q$ i $p|\varphi(m)$. Stoga imamo:

$$a^{\frac{\varphi(m)}{p}} = a^{\frac{q\text{ord}_m(a)}{p}}.$$

Obzirom da $p|q$, možemo to preslagati tako da bude:

$$a^{\frac{\varphi(m)}{p}} = \left(a^{\text{ord}_m(a)}\right)^{\frac{q}{p}}.$$

Kako je $a^{\text{ord}_m(a)} \equiv 1 \pmod{m}$, tada je $\left(a^{\text{ord}_m(a)}\right)^{\frac{q}{p}} \equiv 1^{\frac{q}{p}} \pmod{m} \equiv 1 \pmod{m}$ te dobivamo:

$$a^{\frac{\varphi(m)}{p}} = \left(a^{\text{ord}_m(a)}\right)^{\frac{q}{p}} \equiv 1 \pmod{m}.$$

Iz toga naravno slijedi $a^{\frac{\varphi(m)}{p}} \equiv 1 \pmod{m}$, što je u suprotnosti s pretpostavkom da za svaki $p \in P$ takav da $p|\varphi(m)$ vrijedi $a^{\frac{\varphi(m)}{p}} \not\equiv 1 \pmod{p}$. Dakle, mora biti $q = 1$ pa opet dobivamo $\text{ord}_m(a) = \varphi(m)$.

$\square$

Korolar. Neka su $m \in \mathbb{Z}^+ - \{1\}$ i $a \in \mathbb{Z}$ takvi da je $\gcd(a, m) = 1$. Tada, $\operatorname{ord}_m(a) = \varphi(m)$ ako i samo ako je a primitivni korijen modulo m.

Dokaz. *Nužnost.* Neka je $\operatorname{ord}_m(a) = \varphi(m)$. Prisjetimo se kako je $(\mathbb{Z}/m\mathbb{Z})^*$ grupa s $\varphi(m)$ elemenata. Obzirom da je $\gcd(a, m) = 1$, vrijedi $\overline{a} \in (\mathbb{Z}/m\mathbb{Z})^*$. Tada je $\overline{a}^{\operatorname{ord}_m(a)} = \overline{1}$, jer je $a^{\operatorname{ord}_m(a)} \equiv 1 \pmod{m}$. To znači kako $\operatorname{ord}(\overline{a}) | \operatorname{ord}_m(a)$. No, također, $\overline{a}^{\operatorname{ord}(\overline{a})} = \overline{1}$ što implicira $a^{\operatorname{ord}(\overline{a})} \equiv 1 \pmod{m}$ pa vrijedi $\operatorname{ord}_m(a) | \operatorname{ord}(\overline{a})$ i na kraju $\operatorname{ord}(\overline{a}) = \operatorname{ord}_m(a) = \varphi(m)$. Stoga, uzmemo li $\langle\overline{a}\rangle \leq (\mathbb{Z}/m\mathbb{Z})^*$, vrijedi $|\langle\overline{a}\rangle| = \varphi(m)$. Zbog prethodne dvije jednakosti, i jer su $\langle a\rangle$ i $(\mathbb{Z}/m\mathbb{Z})^*$ konačni skupovi, slijedi $\langle\overline{a}\rangle = (\mathbb{Z}/m\mathbb{Z})^*$. Uzmimo $b \in \mathbb{Z}$, $\gcd(b, m) = 1$ i pokažimo kako postoji $k \in \mathbb{Z}$ takav da je $a^k \equiv b \pmod{m}$. Kako je $\gcd(b, m) = 1$, vrijedi $\overline{b} \in (\mathbb{Z}/m\mathbb{Z})^*$ pa je i $\overline{b} \in \langle\overline{a}\rangle$. To znači kako postoji $k \in \mathbb{Z}$ takav da je $\overline{a}^k = \overline{b}$, drugim riječima $a^k \equiv b \pmod{m}$. Dakle a je primitivni korijen modulo m.

Dovoljnost. Neka je a primitivni korijen modulo m. Tada je $\overline{a} \in (\mathbb{Z}/m\mathbb{Z})^*$. Uzmimo $\langle\overline{a}\rangle \leq (\mathbb{Z}/m\mathbb{Z})^*$. Pretpostavimo kako postoji $\overline{b} \in (\mathbb{Z}/m\mathbb{Z})^* - \langle a\rangle$. To bi značilo kako ne postoji $k \in \mathbb{Z}$ takav da vrijedi $\overline{b} = \overline{a}^k$, tj. $a^k \equiv b \pmod{m}$, što je u suprotnosti s pretpostavkom da je a primitivni korijen modulo m. To znači da je $\langle\overline{a}\rangle = (\mathbb{Z}/m\mathbb{Z})^*$. No, to povlači i $|\langle\overline{a}\rangle| = |(\mathbb{Z}/m\mathbb{Z})^*| = \varphi(m)$, a također i $\operatorname{ord}(\overline{a}) = \varphi(m)$. Kako je $a^{\operatorname{ord}_m(a)} \equiv 1 \pmod{m}$, to znači da je $\overline{a}^{\operatorname{ord}_m(a)} = \overline{1}$, pa slijedi da $\operatorname{ord}(\overline{a}) | \operatorname{ord}_m(a)$, tj. $\varphi(m) | \operatorname{ord}_m(a)$. No, po prethodnoj propoziciji imamo $\operatorname{ord}_m(a) | \varphi(m)$, pa to implicira $\operatorname{ord}_m(a) = \varphi(m)$.

$\square$

Primjedba. Prethodni teorem uz korolar govori također kako je a primitivni korijen modulo m ako i samo ako za svaki $p \in P$ takav da $p | \varphi(m)$ vrijedi $a^{\frac{\varphi(m)}{p}} \not\equiv 1 \pmod{m}$. Ovu činjenicu koristimo za provjeru je li a primitivni korijen modulo m.

Teorem. Neka su $m \in \mathbb{Z}^+ - \{1\}$ i $a \in \mathbb{Z}$ takvi da je $\gcd(a, m) = 1$. Neka je $k \in \mathbb{Z}^+$. Tada vrijedi:

$$\operatorname{ord}_m\left(a^k\right) = \frac{\operatorname{ord}_m(a)}{\gcd(\operatorname{ord}_m(a), k)}.$$

Dokaz. Kako je $\left(a^k\right)^{\operatorname{ord}_m\left(a^k\right)} \equiv 1 \pmod{m}$, vrijedi $\left(a^k\right)^{\operatorname{ord}_m\left(a^k\right)} = a^{k\operatorname{ord}_m\left(a^k\right)} \equiv 1 \pmod{m}$. Stoga po prethodnom teoremu $\operatorname{ord}_m(a) | k\operatorname{ord}_m\left(a^k\right)$ pa postoji $q \in \mathbb{Z}$ takav da je $k\operatorname{ord}_m\left(a^k\right) = q\operatorname{ord}_m(a)$. Neka je $g = \gcd(\operatorname{ord}_m(a), k)$. Tada je $k = k'g$ i $\operatorname{ord}_m(a) = o'g$. Tada iz $k\operatorname{ord}_m\left(a^k\right) = q\operatorname{ord}_m(a)$ dobivamo $k'g\operatorname{ord}_m\left(a^k\right) = qo'g$, tj. $k'\operatorname{ord}_m\left(a^k\right) = qo'$. Kako je $\gcd(k', o') = 1$, i kako $o' | k'\operatorname{ord}_m\left(a^k\right)$, po Euklidovoj lemi mora biti $o' | \operatorname{ord}_m\left(a^k\right)$. Dalje, $\left(a^k\right)^{o'} = a^{ko'} = a^{k'o'g} = a^{k'\operatorname{ord}_m(a)} \equiv 1 \pmod{m}$. Po prethodnom teoremu, $\text{ord}_m\left(a^k\right)|o'$. To, uz $o'|\text{ord}_m\left(a^k\right)$, implicira $\text{ord}_m\left(a^k\right) = o'$. Iz $\text{ord}_m(a) = o'g$ vidimo kako je $\text{ord}_m\left(a^k\right) = o' = \frac{\text{ord}_m(a)}{g}$.

$\square$

Lema. Neka su $m \in \mathbb{Z}^+ - \{1\}$ i $a \in \mathbb{Z}$ takvi da je $\gcd(a, m) = 1$. Ako je

$$a^{\frac{\varphi(m)}{p}} \not\equiv 1 \pmod{m},$$

za neki $p \in P$ takav da $p|\varphi(m)$, tada je

$$a^{\frac{\varphi(m)}{p^k}} \not\equiv 1 \pmod{m},$$

za svaki $k \in \mathbb{Z}^+$ takav da $p^k|\varphi(m)$.

Dokaz. Pretpostavimo kako je:

$$a^{\frac{\varphi(m)}{p}} \not\equiv 1 \pmod{m},$$

ali da za neki $p^k|\varphi(m)$ vrijedi:

$$a^{\frac{\varphi(m)}{p^k}} \equiv 1 \pmod{m}.$$

Primijetimo kako je $k \geq 1$, pa je $k - 1 \geq 0$. Tada imamo:

$$\left(a^{\frac{\varphi(m)}{p^k}}\right)^{p^{k-1}} \equiv 1 \pmod{m}.$$

No, to je u kontradikciji s

$$\left(a^{\frac{\varphi(m)}{p^k}}\right)^{p^{k-1}} = a^{\frac{\varphi(m)}{p}} \not\equiv 1 \pmod{m},$$

pa naša pretpostavka nije bila valjana.

$\square$

Teorem. Neka su $m \in \mathbb{Z}^+ - \{1\}$ i $a \in \mathbb{Z}$ takvi da je $\gcd(a, m) = 1$. Ako je

$$a^{\frac{\varphi(m)}{p}} \not\equiv 1 \pmod{m},$$

za neki $p \in P$ takav da $p|\varphi(m)$, tada je

$$\operatorname{ord}_m\left(a^{\frac{\varphi(m)}{p^{\alpha}}}\right) = p^{\alpha}.$$

Dokaz. Neka je po fundamentalnom teoremu aritmetike $\varphi(m) = \prod_{i=1}^{n} p_i^{\alpha_i}$. Uzmimo $p = p_1$ i $\alpha = \alpha_1$. Tada $\operatorname{ord}_m(a)\,|\varphi(m)$ pa je $\operatorname{ord}_m(a) = p_1^{\beta_1} \cdots p_n^{\beta_n}$. Vidimo kako je:

$$\operatorname{ord}_m\left(a^{\frac{\varphi(m)}{p^{\alpha_1}}}\right) = \frac{p_1^{\beta_1} \cdots p_n^{\beta_n}}{p_2^{m_2} \cdots p_n^{m_n}},$$

gdje je $m_i = \min\{\alpha_i, \beta_i\}$. Ako je $m_i = \alpha_i$ tada je $\alpha_1 \leq \beta_1$ pa ne može biti $p^{\beta_1}|p^{\alpha_1}$. Dakle, mora biti $m_i = \beta_i$. Stoga je:

$$\operatorname{ord}_m\left(a^{\frac{\varphi(m)}{p^{\alpha_1}}}\right) = \frac{p_1^{\beta_1} \cdots p_n^{\beta_n}}{p_2^{\beta_2} \cdots p_n^{\beta_n}} = p_1^{\beta_1}.$$

Pretpostavimo kako je $\beta_1 < \alpha_1$. Tada je:

$$\left(a^{\frac{\varphi(m)}{p^{\alpha_1}}}\right)^{p_1^{\beta}} = a^{\frac{\varphi(m)}{p^{\alpha_1-\beta_1}}} \equiv 1 \pmod{m}.$$

Po prethodnoj lemi, obzirom da je $\alpha_1 - \beta_1 > 0$ i jer je

$$a^{\frac{\varphi(m)}{p_1}} \not\equiv 1 \pmod{m},$$

slijedi kako je:

$$a^{\frac{\varphi(m)}{p^{\alpha_1-\beta_1}}} \not\equiv 1 \pmod{m}.$$

Dakle, ne može biti $\beta_1 < \alpha_1$ pa mora biti $\beta_1 \geq \alpha_1$, što uz $\beta_1 \leq \alpha_1$ daje $\beta_1 = \alpha_1$. Stoga je:

$$\operatorname{ord}_m\left(a^{\frac{\varphi(m)}{p^{\alpha_1}}}\right) = p_1^{\alpha_1}.$$

□

Primjedba. Gornji teorem je osnova postupka za pronalaženje primitivnih korijena modulo m. No, ostaje još pitanje postoji li primitivan korijen modulo m, za svaki $m \in \mathbb{Z}^+ - \{1\}$ te, ukoliko postoji, koliko ih postoji? Ukoliko m nije prost broj, primitivni korijeni modulo m ne moraju nužno postojati. No, ako je m prost broj, postojat će, i o tome, kao i o njihovom broju, govorit će sljedeći teorem.

Lema. Neka je $m \in \mathbb{Z}^{+} - \{1\}$ i neka su $a, b \in \mathbb{Z}$ takvi da je $\gcd\{\mathrm{ord}_m(a), \mathrm{ord}_m(b)\} = 1$. Tada vrijedi $\mathrm{ord}_m(ab) = \mathrm{ord}_m(a)\,\mathrm{ord}_m(b)$.

Dokaz. Uzmimo $\mathrm{ord}_m(a) = p$ i $\mathrm{ord}_m(b) = q$. Također, neka je $l = \mathrm{lcm}(p, q) = pq$. Tada je $(ab)^l = a^l b^l = a^{pq} b^{pq} = (a^p)^q (b^q)^p \equiv 1 \pmod{p}$, jer su p i q redovi elemenata a i b, istim redoslijedom. To povlači kako $\mathrm{ord}_m(ab) \,|\, l$, tj. postoji $t \in \mathbb{Z}$ takav da je $l = t\mathrm{ord}_m(ab)$. Iz toga dobivamo $\mathrm{ord}_m(ab) = \frac{pq}{t}$. Neka je $t_1 = \gcd(t, p)$. Tada $t_1 | t$ pa postoji $t_2 \in \mathbb{Z}$ takav da je $t = t_1 t_2$. Kako je $\mathrm{ord}_m(ab) \in \mathbb{Z}$, tada je $\frac{p}{t_1} \in \mathbb{Z}$ i $\frac{q}{t_2} \in \mathbb{Z}$. Pretpostavimo da je $\gcd(t_1, t_2) = t'$. Tada je $t_1 = t' s_1$ i $t_2 = t' s_2$. To bi impliciralo, jer $t_1 | p$ i $t_2 | q$, da $t' | p$ i $t' | q$, što je u suprotnosti s pretpostavkom da su p i q relativno prosti. Dakle, $\gcd(t_1, t_2) = 1$. Tada imamo:

$$(ab)^{\frac{pq}{t_1 t_2}} \equiv 1 \pmod{p}.$$

No, također vrijedi i:

$$\begin{aligned} (ab)^{t_1 \frac{pq}{t_1 t_2}} &\equiv 1 \pmod{p}, \\ (ab)^{t_2 \frac{pq}{t_1 t_2}} &\equiv 1 \pmod{p}. \end{aligned}$$

Iz tih kongruencija, istim redoslijedom, dobivamo:

$$\begin{aligned} a^{p \frac{q}{t_2}} b^{p \frac{q}{t_2}} &\equiv 1 \pmod{p}, \\ a^{q \frac{p}{t_1}} b^{q \frac{p}{t_1}} &\equiv 1 \pmod{p}. \end{aligned}$$

No, kako je p red od a, a q red od b, te dvije kongruencije možemo, istim redoslijedom zapisati kao:

$$\begin{aligned} b^{p \frac{q}{t_2}} &\equiv 1 \pmod{p}, \\ a^{q \frac{p}{t_1}} &\equiv 1 \pmod{p}. \end{aligned}$$

No, to znači kako $q|p\frac{q}{t_2}$ i $p|q\frac{p}{t_1}$. Po Euklidovoj lemi, zbog $\gcd(p,q) = 1$, i jer je $\frac{q}{t_2}, \frac{p}{t_1} \in \mathbb{Z}$, imamo $q|\frac{q}{t_2}$ i $p|\frac{p}{t_1}$, tj. postoje $r_1, r_2 \in \mathbb{Z}$ takvi da je $\frac{q}{t_2} = r_1 q$ i $\frac{p}{t_1} = r_2 p$. To implicira $r_1 t_2 = 1$ i $t_1 r_2 = 1$, što je moguće samo ako je $r_1 = t_2 = r_2 = t_1 = 1$. Dakle, $\operatorname{ord}_m(ab) = \frac{pq}{t} = \frac{pq}{t_1 t_2} = pq = \operatorname{ord}_m(a)\operatorname{ord}_m(b)$.

$\square$

Teorem. Neka je $p \in P$. Tada je $(\mathbb{Z}/p\mathbb{Z})^*$ ciklička grupa[2].

Dokaz. Neka su $\{p_1, \cdots, p_m\} \subset P$ djelitelji od $\varphi(p) = p-1$. Neka je $p_i \in \{p_1, \cdots, p_m\}$. Pretpostavimo kako ne postoji element $a \in \mathbb{Z}$, $\gcd(a,p) = 1$, takav da je:

$$a^{\frac{p-1}{p_i}} \not\equiv 1 \pmod{p}.$$

Tada, za svaki $a \in \mathbb{Z}$ vrijedi:

$$a^{\frac{p-1}{p_i}} \equiv 1 \pmod{p}.$$

No, obzirom da je $(\mathbb{Z}/p\mathbb{Z})^*$ polje, možemo uzeti $\overline{a} \in (\mathbb{Z}/p\mathbb{Z})^*$ i tada bi

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

bilo ekvivalentno upravo

$$\overline{a}^{\frac{p-1}{p_i}} - \overline{1} = \overline{0}.$$

To implicira kako je svaki $\overline{a} \in (\mathbb{Z}/p\mathbb{Z})^*$ korijen polinoma:

$$p(x) = x^{\frac{p-1}{p_i}} - \overline{1}.$$

No, kako je $|(\mathbb{Z}/p\mathbb{Z})^*| = p-1$, to bi značilo da $p(x)$ ima $p-1$ korijena, što je nemoguće jer je $\deg p(x) = \frac{p-1}{p_i} < p-1$. Dakle, mora postojati $\overline{a_i} \in (\mathbb{Z}/p\mathbb{Z})^*$ takav da vrijedi:

$$\overline{a_i}^{\frac{p-1}{p}} \neq \overline{1}$$

što je ekvivalentno izrazu:

[2]Obzirom da je ciklička, postoji element $\overline{g} \in (\mathbb{Z}/p\mathbb{Z})^*$ takav da je $\langle \overline{g} \rangle = (\mathbb{Z}/p\mathbb{Z})^*$, tj. za svaki $\overline{a} \in (\mathbb{Z}/p\mathbb{Z})^*$ postoji $k \in \mathbb{Z}$ takav da je $\overline{g}^k = \overline{a}$, tj. $g^k \equiv a \pmod{p}$.

$$a_i^{\frac{p-1}{p_i}} \not\equiv 1 \pmod{p}.$$

Po prethodnom teoremu je tada:

$$\mathrm{ord}_p\left(a_i^{\frac{p-1}{p_i^{\alpha}}}\right) = p_i^{\alpha},$$

gdje je $\alpha = \max\{k \in \mathbb{Z} : \ p_i^k | p-1\}$. Obzirom da je izbor p_i bio arbitraran, za svaki p_i postoji a_i čiji je red jednak najvećoj potenciji p_i koja dijeli $p-1$. Po prethodnoj lemi, jer je $\gcd\left(p_i^{\alpha_i}, p_j^{\alpha_j}\right) = 1$, za svaki $i \neq j$, $i, j \in \{1, \ldots, m\}$, vrijedi:

$$\mathrm{ord}_p\left(a_1 \cdots a_m\right) = p^{\alpha_1} \cdots p^{\alpha_m} = p-1.$$

$\square$

Korolar. Neka je $p \in P$. Tada, za svaki $d \in \mathbb{Z}$ takav da $d|p-1$ postoji $a \in \mathbb{Z}$ takav da je $\mathrm{ord}_p\left(a\right) = d$.

Dokaz. Po prethodnom teoremu, postoji $a \in \mathbb{Z}$ takav da je $\mathrm{ord}_p\left(a\right) = p-1$. Kako $d|p-1$, postoji $q \in \mathbb{Z}$ takav da je $p-1 = qd$. Primijetimo kako je, jer $q|p-1$, tada $\gcd\left(p-1, q\right) = q$. Po formuli za red potencije elementa a imamo:

$$\mathrm{ord}_p\left(a^q\right) = \frac{p-1}{\gcd\left(p-1, q\right)} = \frac{p-1}{q} = d.$$

$\square$

Korolar. Neka je $p \in P$. Tada, za svaki $d \in \mathbb{Z}$ takav da $d|p-1$, postoji $\varphi(d)$ elemenata, nekongruentnih p, reda d modulo p.

Dokaz. Po prethodnom korolaru, postoji $a \in \mathbb{Z}$ takav da je $\mathrm{ord}_p\left(a\right) = d$. Promotrimo skup $C(a) = \{a^k : \ k \in \{0, \ldots, d-1\}\}$. Pretpostavimo kako je $a^i \equiv a^j \pmod{p}$, za neki $i \neq j$, $i, j \in \{0, \ldots, d-1\}$. Bez smanjenja općenitosti pretpostavimo $i > j$. Obzirom da je $0 \leq i, j < d$, tada je $0 \leq i - j < d = \mathrm{ord}_p\left(a\right)$. Tada iz $a^i \equiv a^j \pmod{p}$ slijedi $a^{i-j} \equiv 1 \pmod{p}$. No, to bi značilo kako $\mathrm{ord}_p\left(a\right)|i-j$, tj. postoji $q \in \mathbb{Z}$ takav da je $i - j = q\mathrm{ord}_p\left(a\right) < \mathrm{ord}_p\left(a\right)$. Kako je $\mathrm{ord}_p\left(a\right) > 0$ dobivamo $i - j = q < 1$, što je moguće, obzirom da je $i - j \in \mathbb{Z}_0^+$, samo ako je $i - j = 0$. No iz toga bi slijedilo $i = j$, što je u suprotnosti s pretpostavkom da je $i \neq j$. Dakle, svi elementi u $C(a)$ su nekongruentni modulo p i ima ih upravo d. Po prethodnoj formuli imamo:

$$\mathrm{ord}_p\left(a^k\right) = \frac{\mathrm{ord}_p\left(a\right)}{\gcd\left(\mathrm{ord}_p\left(a\right), k\right)}.$$

Lako je vidjeti kako će biti $\text{ord}_p\left(a^k\right) = \text{ord}_p(a)\,(= d)$ ako i samo ako je:

$$\gcd\left(\text{ord}_p(a), k\right) = 1,$$

tj. $\gcd(d, k) = 1$. Takvih elemenata nekongruentno p (koji se nalaze u $C(a)$) ima upravo, najmanje, $\varphi(d)$ (očigledno iz same definicije Eulerove funkcije). No, postoji li mogućnost da postoji neki element reda d modulo p a da nije u $C(a)$? Promotrimo jednadžbu $x^d - 1 \equiv 0 \pmod{p}$. Očito je kako $(a^k)^d \equiv 1 \pmod{p}$ (jer je $\text{ord}_p(a) = d$, pa je $(a^d)^k \equiv 1 \pmod{p}$). Dakle, svi elementi iz $C(a)$ su rješenja kongruencije $x^d - 1 \equiv 0 \pmod{p}$. No, obzirom da se i dalje radi o polju $\mathbb{Z}/p\mathbb{Z}$, polinom $x^d - \overline{1}$ takvih rješenja može imati najviše d. Stoga, sva su rješenja u $C(a)$ i ne mogu biti u nijednom drugom skupu. To implicira kako je broj elemenata reda d modulo p točno $\varphi(d)$.

$\square$