Prsten cijelih brojeva

Pravdić, Marijana

Master's thesis / Diplomski rad

2017

Degree Grantor / Ustanova koja je dodijelila akademski / stručni stupanj: **Josip Juraj Strossmayer University of Osijek, Department of Mathematics / Sveučilište Josipa Jurja Strossmayera u Osijeku, Odjel za matematiku**

Permanent link / Trajna poveznica: https://urn.nsk.hr/urn:nbn:hr:126:456788

SVEUČILIŠTE JOSIPA JURJA STROSSMAYERA U OSIJEKU
ODJEL ZA MATEMATIKU

Marijana Pravdić

Prsten cijelih brojeva

Diplomski rad

Osijek, 2017.

SVEUČILIŠTE JOSIPA JURJA STROSSMAYERA U OSIJEKU
ODJEL ZA MATEMATIKU

Marijana Pravdić

Prsten cijelih brojeva

Diplomski rad

Mentor:
izv. prof. dr. sc. I. Matić

Osijek, 2017.

Veliku zahvalnost dugujem svom mentoru doc.dr.sc. Matić koji mi je omogućio sve potrebne materijale i pomogao svojim savjetima pri izradi ovog diplomskog rada.

Također, zahvaljujem se svim svojim prijateljima i prijateljicama, koji su uvijek bili uz mene i bez kojih cijeli ovaj tijek mog studiranja ne bi prošao tako lako i zabavno.

I na kraju, najveću zaslugu za ono što sam postigla pripisujem svojim roditeljima, koji su uvijek bili tu bez obzira da li se radilo o teškim ili sretnim trenutcima i bez kojih sve ovo što sam dosad postigla ne bi bilo moguće.

Veliko HVALA svima!

Sadržaj

Uvod

Jedinstvenost faktorizacije prostim brojevima je jedna od najvažnijih tema algebre i baš zbog toga su je mnogobrojni teoretičari nazvali osnovnim teoremom aritmetike. Jedinstvenost faktorizacije prostim brojevima je svojstvo koje nam govori da se bilo koji cijeli broj može izraziti u obliku produkta prostih brojeva na jedinstven način. Ideja o jedinstvenoj faktorizaciji prostim brojevima je toliko važna da je brojni teoretičari proučavaju i u drugim sustavima osim cijelih brojeva. Neki brojevni sustavi nemaju jedinstvenu faktorizaciju stupnja prostih brojeva.

U matematici, prsten je algebarska struktura u kojoj su definirani zbrajanje i množenje, i imaju svojstva opisana niže. Prsten je generalizacija skupa cijelih brojeva. Drugi primjeri prstena su polinomi i cijeli brojevi modulo n. Grana apstraktne algebre koja proučava prstenove se naziva teorijom prstena.

1 Osnove teorije brojeva

Teorija brojeva je grana matematike koja se ponajprije bavi proučavanjem svojstva skupa prirodnih brojeva. Jedno od osnovnih svojstva skupa $\mathbb{N}$ je da su na njemu definirane operacije zbrajanja i množenja koje zadovoljavaju pravila komutativnosti, asocijativnosti i distributivnosti.

Za razliku od većine ostalih područja matematike, seže više od 4500 godina u prošlost. Unatoč njenoj starosti, još uvijek postoje pitanja koja čak i do danas nisu odgovorena. Veliki broj načela tog područja otkriven je eksplicitnim eksperimentima.

Od svog nastanka u klasičnom razdoblju, kroz razvoj od 1600. do 1800. godine, teorija brojeva je većinu vremena bila odvojena od ostalih područja matematike. Pitanja teorije brojeva nisu bitna samo matematičarima. Danas, kao i u ranim danima, ovi su problemi privlačni i mnogim laicima te je teorija brojeva zabilježena kao područje matematike u kojemu su prijedlozi i slutnje amatera zaslužne za mnoge cijenjene rezultate.

1.1 Prsten cijelih brojeva

U ovom poglavlju ćemo pogledati apstraktna algebarska svojstva cijelih brojeva i što skup $\mathbb{Z}$ čini jedinstvenim kao algebarsku strukturu.

Podsjetimo se da je **prsten** R skup na kojem su definirane dvije binarne operacije, zbrajanje i množenje, koje smo označavali sa $+$ i $\cdot$, definiranim tako da zadovoljava sljedećih 6 aksioma:

(1) Zbrajanje je komunitativno: $a + b = b + a$, za svaki $a, b \in R$

(2) Zbrajanje je asocijativno: $a + (b + c) = (a + b) + c$, za $a, b, c \in R$

(3) Postoji element 0 tako da je $a + 0 = a$ za svaki $a \in R$

(4) Za svaki $a \in R$ postoji aditivni inverz, označen s $-a$, tako da je $a + (-a) = 0$

(5) Množenje je asocijativno: $a \cdot (b \cdot c) = (a \cdot b) \cdot c$, za $a, b, c \in R$

(6) Množenje je distributivno s obzirom na zbrajanje: $a \cdot (b + c) = a \cdot b + a \cdot c$, za $a, b, c \in R$.

Ako R dodatno zadovoljava i svojstvo

(7) množenje je komutativno: $ab = ba$, za svaki $a, b \in R$,

onda je R **komutativni prsten**, dok ako R zadovoljava svojstvo

(8) postoji multiplikativna jedinica, označena s 1 (različit od 0), tako da vrijedi $a \cdot 1 = 1 \cdot a = a$, za svaki $a \in R$

onda R nazivamo **prsten s jedinicom**. Ako R zadovoljava svojstva (1)-(8) tada je R **komutativan prsten s jedinicom**.

Prsten ima dvije operacije. Skup G s jednom operacijom označenom sa $\cdot$ naziva se **grupa** ako zadovoljava sljedeća tri svojstva:

(1) $\cdot$ je asocijativno. To jest, $(g_1 \cdot g_2) \cdot g_3 = g_1 \cdot (g_2 \cdot g_3)$ za $g_1, g_2, g_3 \in G$.

(2) Postoji neutralan element za $\cdot$, označen s 1. To jest, $g \cdot 1 = 1 \cdot g = g$ za sve $g \in G$.

(3) Svaki $g \in G$ ima inverz u odnosu na $\cdot$. To jest, za svaki $g \in G$ postoji g^{-1} tako da $g \cdot g^{-1} = g^{-1} \cdot g = 1$.

Ako je, osim toga, $\cdot$ komutativno, G se naziva **Abelova grupa**. Grupe, a posebno Abelova grupa, će igrati važnu ulogu u teoriji brojeva. Reći ćemo mnogo više o njima kasnije.

Polje K je komutativan prsten s jedinicom sa svojstvom da svaki element različit od nule ima inverz s obzirom na množenje, tj. za svaki $a \in K$, $a \neq 0$ postoji $b \in K$ tako da $ab = ba = 1$. U ovom slučaju skup $K^* = K \setminus \{0\}$ tvori Abelovu grupu s obzirom na množenje u K. Skup K^* s množenjem se zove **multiplikativna grupa** od K.

Prsten se može smatrati kao najosnovnija algebarska struktura u kojoj može biti izvršeno zbrajanje, oduzimanje i množenje. U svakom prstenu jednadžba $x + b = c$ se uvijek može riješiti.

Nadalje, polje se može smatrati kao najosnovnija algebarska struktura u kojoj zbrajanje, oduzimanje, množenje i dijeljenje može biti izvršeno. Dakle, u bilo kojem polju jednadžba $ax + b = c$ se uvijek može riješiti.

Kombinirajući ovu definiciju s našim znanjem o skupu $\mathbb{Z}$ dobili smo sljedeću važnu tvrdnju o strukturama cijelih brojeva.

Lema 1. *Cijeli brojevi $\mathbb{Z}$ tvore komutativan prsten s jedinicom.*

Postoje mnogi primjeri takvih prstenova, a da bi definirali $\mathbb{Z}$ na jedinstven način moramo uvesti određena svojstva. Ako se množe dva cijela broja različita od nule, onda je umnožak različit od nule.

To nije uvijek istina u prstenu. Na primjer, promotrimo skup funkcija definiranih na intervalu $[0, 1]$. Prema običnom množenju i zbrajanju one tvore prsten s elementom nula iz čega slijedi da je funkcija istovjetno nula.

Neka je funcija $f(x)$ takva da je nula na segmentu $\left[0, \frac{1}{2}\right]$ i različita od nule inače, te funkcija $g(x)$ nula na $\left[\frac{1}{2}, 0\right]$ i različita od nule inače. Tada je $f(x) \cdot g(x) = 0$, ali ni f ni g nisu nul-funkcije. Definiramo **integralnu domenu** tako da R bude komutativan prsten s

jedinicom sa svojstvom ako je $ab = 0$ za $a, b \in R$ onda su ili $a = 0$ ili $b = 0$. Dva elementa različita od nule koji u umnošku daju nulu zovu se **djelitelji nule**, a time i integralna domena je komutativan prsten s jedinicom i bez djelitelja nule. Stoga, $\mathbb{Z}$ je integralna domena.

Sve ovo ćemo sažeti na drugi način. Kažemo da je integralna domena D **uvjetna integralna domena** ako postoji karakterističan skup D^+, koji nazivamo **skup pozitivnih brojeva** sa sljedećim svojstvima:

1. Skup D^+ je zatvoren s obzirom na zbrajanje i množenje.
2. Ako je $x \in D$ tada je jedna od sljedećih tvrdnji istinita:
   (a) $x = 0$,
   (b) $x \in D^+$,
   (c) $-x \in D^+$.

Ako su $x, y \in D$ tada pišemo $x < y$ ako je $y - x$ iz D^+. Uz taj uvjet D^+ se jasno može identificirati s elementima $x \in D$ tako da je $x > 0$. Tada ćemo dobiti sljedeći rezultat.

Lema 2. *Ako je D uvjetna integralna domena onda*

(1) $x < y$ i $y < z$ povlači $x < z$.

(2) Ako su $x, y \in D$ onda samo jedno vrijedi: $x = y$ ili $x < y$ ili $y < x$.

Iz toga slijedi da su $\mathbb{Z}$ cijeli brojevi uvjetna integralna domena. Njihova posebnost među takvim strukturama ovisi o dodatna dva svojstva, koja su ekvivalentna.

Pravilo indukcije. Neka je S podskup prirodnih brojeva $\mathbb{N}$. Pretpostavimo da je $1 \in S$ i S ima svojstvo da ako je $n \in S$ onda je $n + 1 \in S$. Tada je $S = \mathbb{N}$.

Svojstvo dobre uređenosti. Neka je S neprazan podskup prirodnih brojeva $\mathbb{N}$. Tada S sadrži najmanji element.

Lema 3. *Pravilo indukcije je ekvivalentno svojstvu dobre uređenosti.*

Dokaz. Da bi to dokazali najprije moramo pretpostaviti pravilo indukcije i pokazati da vrijedi svojstvo dobre uređenosti i obrnuto.

Pretpostavimo da vrijedi pravilo indukcije i neka je S neprazan podskup od $\mathbb{N}$. Moramo pokazati da S sadrži najmanji element. Neka je T skup definiran s

$$T = \{x \in \mathbb{N} : x \leq s, \forall s \in S\}.$$

Slijedi $1 \in T$ budući je $S \subset \mathbb{N}$. Ako za bilo koji $x \in T$, $x + 1 \in T$ tada prema pravilu indukcije $T = \mathbb{N}$, ali bi tada S bio prazan što je u kontradikciji s pretpostavkom da je S neprazan. Zato postoji jedan $a \in T$ tako da $a + 1 \notin T$. Bez smanjenja općenitosti, uzmimo da je a najmanji element od S.

Sada imamo, $a \leq s$ za sve $s \in S$ dok je $a \in T$. Ako $a \notin S$ tada bi svaki $s \in S$ zadovoljavao da je $a + 1 \leq s$. To bi značilo da je $a + 1 \in T$, što je kontradikcija. Stoga $a \in S$ i $a \leq s$ za sve $s \in S$ pa je a i najmanji element. Tada prema pravilu indukcije slijedi svojstvo dobre uređenosti.

S druge strane pretpostavimo da vrijedi svojstvo dobre uređenosti i pretpostavimo da je $1 \in S$ te za bilo koji $n \in S$ vrijedi $n + 1 \in S$. Moramo pokazati da je $S = \mathbb{N}$. Ako je $S = \mathbb{N}$ tada je $\mathbb{N} \setminus S$ neprazan podskup od $\mathbb{N}$. Stoga on mora sadržavati najmanji element. Također vrijedi $n - a \in S$, ali tada slijedi da je $(n - 1) + 1 = n \in S$ što je kontradikcija. To znači da je onda $\mathbb{N} \setminus S$ prazan skup i tada vrijedi da je $S = \mathbb{N}$. □

Pravilo indukcije je naravno temelj za induktivne dokaze, koji igraju veliku ulogu u teoriji brojeva. Kao podsjetnica, u induktivnom dokazivanju želimo dokazati iskaze $P(n)$ koji ovise o pozitivnom cijelom broju n. U indukciji ćemo pokazati da ako je $P(1)$ istina, onda $P(n + 1)$ proizilazi iz istinitosti $P(n)$. Iz pravila indukcije, $P(n)$ je istina za sve pozitivne cijele brojeve (prirodne brojeve) n.

Primjer: Pokažite da vrijedi $1 + 2 + \cdots + n = \frac{(n)(n+1)}{2}$.

Za $n = 1$ imamo da je

$$1 = \frac{(1)\,(2)}{2} = 1.$$

Pretpostavimo da vrijedi za $n = k$

$$1 + 2 + \cdots + k = \frac{k\,(k+1)}{2}$$

pa promotrimo za $n = k + 1$

$$1 + 2 + \cdots + k + (k+1) = (1 + 2 + \cdots k)\,(k+1) = \frac{k\,(k+1)}{2} + (k+1) = \frac{(k+1)\,(k+2)}{2}.$$

Dakle ako tvrdnja vrijedi za $n = k$, onda vrijedi i za $n = k + 1$, a time prema principu matematičke indukcije vrijedi za sve $n \in \mathbb{N}$.

1.2 Djeljivost, prosti i složeni brojevi

Početna točka teorije brojeva je upravo djeljivost.

Definicija 1. *Za cijele brojeve a i b kažemo da a **dijeli** b, ili da je a **djelitelj** od b, ako postoji cijeli broj q tako da $b = a \cdot q, a \neq 0$. Označavat ćemo to s $a \mid b$. Tada je b **višekratnik** od a. Ako je $b > 1$ cijeli broj čiji su jedini djelitelji $\pm 1, \pm b$ tada je b **prost** broj, inače, $b > 1$ je **složen** broj.*

Teorem 1. *Sljedeća svojstva djeljivosti su direktna posljedica definicije:*

(1) $a \mid b \Rightarrow a \mid bc$ *za bilo koji cijeli broj* c.

(2) $a \mid b$ *i* $b \mid c$, *slijedi* $a \mid c$.

(3) $a \mid b$ *i* $a \mid c$, *slijedi da* $a \mid (bx + cy)$ *za bilo koje cijele brojeve* x *i* y.

(4) $a \mid b$ *i* $b \mid a$, *slijedi da je* $a = \pm b$.

(5) Ako $a \mid b$ *i* $a > 0$, $b > 0$ *tada je* $a < b$.

(6) $a \mid b$ *ako i samo ako* $ca \mid cb$ *za bilo koji cijeli broj* $c \neq 0$.

(7) $a \mid 0$ *za sve* $a \in \mathbb{Z}$ *i* $0 \mid a$ *samo za* $a = 0$.

(8) $a \mid \pm 1$ *samo za* $a = \pm 1$.

(9) $a_1 \mid b_1$ *i* $a_2 \mid b_2$ *slijedi da* $a_1 a_2 \mid b_1 b_2$.

Dokaz. Dokazat ćemo (2), tj. ako $a \mid b$ i $b \mid c$, onda $a \mid c$.

Pretpostavimo $a \mid b$ i $b \mid c$. Tada postoje x i y takvi da $b = a \cdot x$ i $c = b \cdot y$. Ako uvrstimo $b = a \cdot x$ imamo da je $c = a \cdot x \cdot y = a \cdot (x \cdot y)$ i iz tog slijedi da $a \mid c$. □

Ako su b, c, x i y cijeli brojevi tada cijeli broj $b \cdot x + c \cdot y$ zovemo **linearna kombinacija** brojeva b i c.

Svojstvo (3) Teorema 1 kaže da zajednički djelitelj brojeva b i c dijeli i svaku linearnu kombinaciju od b i c. Nadalje, ako je $b > 1$ složen broj onda postoji $x > 0$ i $y > 0$ takvi da $b = x \cdot y$ i prema (5) iz Teorema 1 vrijedi $1 < x < b$, $1 < y < b$.

U običnoj aritmetici su uvijek zadani a i b da bi se moglo podijeliti b s a. Sljedeći teorem, teorem o dijeljenju s ostatkom, kaže da ako je $a > 0$, bilo da a dijeli b ili postoji ostatak pri dijeljenju bit će manji od a.

Teorem 2 (**Teorem o dijeljenju s ostatkom**). *Za dane* a *i* b *gdje je* $a > 0$ *postoje jedinstveni cijeli brojevi* q *i* r *takvi da je* $b = qa + r$, *gdje je* $r = 0$ *ili* $0 < r < a$. *Kažemo da je* q *kvocijent,* a r *je ostatak.*

Dokaz. Za dane a, b, $a > 0$ promotrimo skup $S = \{b - q \cdot a \geq 0; q \in \mathbb{Z}\}$. Ako je $b > 0$ tada $b + a \geq 0$ i zbroj je u skupu S. Ako je $b \leq 0$ onda postoji $q > 0$ s $-qa < b$. Tada $b + qa > 0$ i pripada skupu S. Dakle, u oba slučaja, skup S nije prazan.

Stoga je S neprazan podskup skupa $\mathbb{N} \cup \{0\}$ i zbog toga sadrži najmanji element r. Ako je $r \neq 0$, moramo pokazati da je $0 < r < a$. Pretpostavimo da je $r \geq a$, onda je $r = x + a$ gdje je $x \geq 0$ i $x < r$ budući da je $a > 0$. Tada $b - qa = r = a + x \Rightarrow b - (q + 1) \cdot a = x$. To znači da $x \in S$. Budući je $x < r$ to je u kontradikciji s prethodnim da je r najmanji element. Stoga ako je $r \neq 0$ onda je $0 < r < a$.

Još je ostalo pokazati jedinstvenost od q i r. Pretpostavimo također da je $b = q_1 a_1 + r_1$. Prema prethodno navedenom i r_1 mora biti najmanji element iz skupa S. Dakle, $r_1 \leq r$

i $r \leq r_1$, pa prema tome $r = r_1$. Sada $b - qa = b - q_1 a \Rightarrow (q_1 - q)\, a = 0$, a budući da je $a > 0$ slijedi da je $q_1 - q = 0$, a to znači da je $q = q_1$. □

Sljedeće ideje su potrebne za definiranje **najvećeg zajedničkog djelitelja** i **najmanjeg zajedničkog višekratnika**.

Definicija 2. *Dani su cijeli brojevi a, b različiti od nule. Njihov* ***najveći zajednički djelitelj*** *$d > 0$ je pozitivan cijeli broj koji je zajednički djelitelj, tj. $d \mid a$ i $d \mid b$ i ako je d_1 bilo koji drugi zajednički djelitelj tada $d_1 \mid d$. Najveći zajednički djelitelj od a i b označavat ćemo s (a, b).*

Sljedeći teorem kaže da svi cijeli brojevi različiti od nule, imaju najveći zajednički djelitelj koji je jedinstven.

Teorem 3. *Za cijele brojeve a i b različite od nule, njihov najveći zajednički djelitelj postoji, jedinstven je, a može biti karakteriziran kao najmanja pozitivna linearna kombinacija od a i b.*

Dokaz. Za dane a, b različite od nule promatramo skup $S = \{ax + by > 0 : x, y \in \mathbb{Z}\}$. Očito je $a^2 + b^2 > 0$, pa je S neprazan podskup od $\mathbb{N}$ pa ima najmanji element $d > 0$. Pokažimo da je d njihov najveći zajednički djelitelj.

Prvo moramo pokazati da je d zajednički djelitelj. Neka je $d = ax + by$ najmanja pozitivna linearna kombinacija. Prema Teoremu o dijeljenju s ostatkom, $a = qd + r$, $0 \leq r < d$. Pretpostavimo da je $r \neq 0$. Tada je $r = a - qd = a - q\,(ax + by) = (1 - qx)\, a - qby > 0$. Stoga je r pozitivna linearna kombinacija od a i b i zato je iz skupa S, ali $r < d$ pa je u kontradikciji s prethodnim da je d najmanji element iz S. Prema tome $r = 0$, i tako $a = q \cdot d$ i $d \mid a$. Analogno se pokaže da $d \mid b$, pa je d zajednički djelitelj od a i b. Neka je d_1 bilo koji drugi zajednički djelitelj od a i b. Zatim d_1 dijeli svaku linearnu kombinaciju od a i b. Potom $d_1 \mid d$ iz toga slijedi da je d najveći zajednički djelitelj od a i b. Na kraju moramo pokazati da je d jedinstven. Pretpostavimo da je i d_1 najveći zajednički djelitelj od a i b. Dakle, $d = \pm d_1$ iz čega slijedi da je $d = d_1$ jer su oni oba pozitivni. □

Ako $(a, b) = 1$ tada možemo reći da su a i b **relativno prosti** ako i samo ako je 1 linearna kombinacija od a i b. Imamo sljedeća tri rezultata.

Lema 4. *Ako je $d = (a, b)$ tada je $a = a_1 d$ i $b = b_1 d$ takvi da je $(a_1 b_1) = 1$.*

Dokaz. Ako je $d = (a, b)$ onda $d \mid a$ i $d \mid b$. Dakle, $a = a_1 d$ i $b = b_1 d$. Imamo $d = ax + by = a_1 dx + b_1 dy$. Dijeljenjem obje strane jednadžbe s d, dobijemo $1 = a_1 x + b_1 y$.

Dakle, $(a_1, b_1) = 1$. □

Lema 5. *Za bilo koji cijeli broj c vrijedi $(a, b) = (a, b + ac)$.*

Dokaz. Pretpostavimo $(a, b) = d$ i $(a, b + ac) = d_1$. Iz tog imamo da je d najmanja pozitivna linearna kombinacija od a i b. Pretpostavimo $d = ax + by$. Budući da je d_1 linearna kombinacija od a i $b + ac$ imamo $d_1 = ar + (b + ac)\, s = a\,(cs + r) + bs$.

Stoga je d_1 linearna kombinacija od a i b i time $d_1 \geq d$. S druge strane, $d_1 \mid a$ i $d_1 \mid b + ac$ pa $d_1 \mid b$. Stoga $d_1 \mid d$, pa vrijedi da je $d_1 \leq d$. Iz prethodne dvije nejednakosti dobivamo $d_1 = d$. □

Sljedeći rezultat koji zovemo **Euklidov algoritam** pruža tehniku za pronalaženje najvećeg zajedničkog djelitelj za dva broja i prikaz najvećeg zajedničkog djelitelja kao linearne kombinacije.

Teorem 4 (**Euklidov algoritam**). *Za dana dva cijela broja b i $a > 0$ uzastopnom primjenom teorema o dijeljenju s ostatkom se dobivaju jednakosti*

$$b = q_1 a + r_1, 0 < r_1 < a$$

$$a = q_2 r_1 + r_2, 0 < r_2 < r_1$$

$$\dots$$

$$r_{n-2} = q_n r_{n-1} + r_n, 0 < r_n < r_{n-1}$$

$$r_{n-1} = q_{n+1} r_n.$$

Posljednji ostatak koji nije nula, r_n, je najveći zajednički djelitelj od a i b.

Dokaz. U izvršavanju uzastopne podjele kao što je navedeno u iskazu teorema svaki ostatak r_i je strogo manji od prethodnog dok je nenegativan. Dakle, slijedi $r_i s$ konačno mora završiti sa ostatkom nula. Stoga je posljednji ostatak r_n različit od nule. Moramo pokazati da je to najveći zajednički djelitelj. Iz Leme 5 najveći zajednički djelitelj $(a, b) = (a, b - q_1 a) = (a, r_1) = (r_1, a - q_2 r_1) = (r_1, r_2)$. Nastavimo li dalje imamo $(a, b) = (r_{n-1}, r_n) = r_n$ jer r_n dijeli r_{n-1}. Time smo pokazali da je r_n najveći zajednički djelitelj od a i b.

Kako bi izrazili r_n kao linearnu kombinaciju od a i b označimo prvo

$$r_n = r_{n-2} - q_n r_{n-1}.$$

Zamjenom dobijemo

$$= r_{n-2} - q_n \left(r_{n-3} - q_{n-1} r_{n-2}\right) = \left(1 + q_n q_{n-1}\right) r_{n-2} - q_n r_{n-3}.$$

Nastavimo li ovim slijedom u konačnici ćemo izraziti r_n kao linearnu kombinaciju od a i b. □

Primjer: Pronađimo najveći zajednički djelitelj za 270 i 2412 i najveći zajednički djelitelj izrazi kao linearnu kombinaciju od 270 i 2412.

Primjenjujemo Euklidov algoritam:

$$2412 = 8 \cdot 270 + 252$$
$$270 = 1 \cdot 252 + 18$$
$$252 = 14 \cdot 18.$$

Tu je posljednji nenul ostatak 18, što je najveći zajednički djelitelj za 270 i 2412. Sada trebamo 18 izraziti kao linearnu kombinaciju od 270 i 2412. Iz prve jednadžbe,

$$252 = 2412 - 8 \cdot 270,$$

što u drugoj jednadžbi daje,

$$270 = 2412 - 8 \cdot 270 + 18 \Rightarrow 18 = -1 \cdot 2412 + 9 \cdot 270,$$

a to je željena linearna kombinacija.

Sada pretpostavimo da je $d = (a, b)$, gdje su $a, b \in \mathbb{Z}$ i $a \neq 0$ i $b \neq 0$. Zatim primjetimo da za jedno cjelobrojno rješenje jednadžbe

$$ax + by = d,$$

lako možemo odrediti i ostala rješenja.

Pretpostavimo, bez smanjenja općenitosti, da je $d = 1$, tj. da su a i b relativno prosti. Ako ne, možemo podijeliti s $d > 1$. Pretpostavimo da su x_1, y_1 i x_2, y_2 dva cjelobrojna rješenja jednadžbe $ax + by = 1$, to jest,

$$ax_1 + by_1 = 1,$$
$$ax_2 + by_2 = 1.$$

Tada

$$a\,(x_1 - x_2) = -b\,(y_1 - y_2).$$

Budući da je $(a, b) = 1$, prema Lemi 6, $b \mid (x_1 - x_2)$ i stoga

$$x_2 = x_1 + bt$$

za neki $t \in \mathbb{Z}$. Uvrštavanjem natrag u jednadžbu dobili bismo $ax_1 + by_1 = a\,(x_1 + bt) + by_2 \Rightarrow by_1 = abt + by_2$ od $b \neq 0$.

Dakle, $y_2 = y_1 - at$. Stoga su sva rješenja dana s

$$x_2 = x_1 + bt,$$
$$y_2 = y_1 - at.$$

za neki $t \in \mathbb{Z}$. Konačna ideja ovog poglavlja je najmanji zajednički višekratnik.

Definicija 3. *Za dane cijele brojeve a i b različite od nule, njihov* ***najmanji zajednički višekratnik*** *$m > 0$ je pozitivan cijeli broj koji je zajednički višekratnik, tj. $a \mid m$ i $b \mid m$, i ako je m_1 bilo koji drugi zajednički višekratnik tada vrijedi da $m \mid m_1$. Označavat ćemo ga s $[a, b]$.*

Kao i za najveći zajednički djelitelj svaka dva cijela broja imaju najmanji zajednički višekratnik i on je jedinstven. Prvo nam treba sljedeći rezultat poznat kao Euklidova lema.

Lema 6 (**Euklidova lema**)**.** *Pretpostavimo da $a \mid bc$ i $(a, b) = 1$. Onda $a \mid c$.*

Dokaz. Neka je $(a, b) = 1$, tada se 1 može izraziti u obliku linearne kombinacije a i b. To jest,

$$ax + by = 1.$$

Pomnožimo li sve s c dobit ćemo

$$acx + bcy = c.$$

Sada imamo $a \mid a$ i $a \mid bc$, prema čemu slijedi da a dijeli i linearnu kombinaciju $acx + bcy$, a time i da $a \mid c$. □

Teorem 5. *Za dane cijele brojeve a i b različite od nule, njihov najmanji zajedniči višekratnik postoji i jedinstven je. Nadalje vrijedi,*

$$(a, b)\,[a, b] = ab.$$

Dokaz. Neka je $d = (a, b)$ i $m = \frac{ab}{d}$. Pokazat ćemo da je m najmanji zajednički višekratnik brojeva a i b. Imamo, $a = a_1 d, b = b_1 d$ tako da $(a_1, b_1) = 1$. Tada vrijedi $m = a_1 b_1 d$. Budući da je $a = a_1 d, m = b_1 a$, tada $a \mid m$. Analogno, $b \mid m$ pa je m zajednički višekratnik od a i b. Dalje, pretpostavimo da je m_1 drugi zajednički višekratnik od a i b pa je $m_1 = ax = by$. Iz toga ćemo dobiti

$$a_1 dx = b_1 dy \Rightarrow a_1 x = b_1 y \Rightarrow a_1 \mid b_1 y.$$

Ipak, $(a_1 b_1) = 1$ pa prema Lemi 6, $a_1 \mid y$. Dakle, $y = a_1 z$. Iz toga slijedi da je

$$m_1 = b_1 d\,(a_1 z) = a_1 b_1 dz = mz$$

i stoga $m \mid m_1$. Dakle, m je najmanji zajedniči višekratnik. Jedinstvenost se dokaže kao i u dokazu za jedinstvenost najvećeg zajedničkog djelitelja. Pretpostavimo da je m_1 drugi najmanji zajednički višekratnik, zatim iz $m \mid m_1$ i $m_1 \mid m$ slijedi da je $m = \pm m_1$, a budući su oba pozitivna onda su jednaki, $m = m_1$. □

Primjer: Pronađimo najmanji zajedniči višekratnik za 270 i 2412.

Iz prethodnog primjera našli smo da je to $(270, 2412) = 18$. Prema tome,

$$[270, 2412] = \tfrac{270 \cdot 2412}{(270,2412)} = \tfrac{270 \cdot 2412}{18} = 36180.$$

1.3 Osnovni teorem aritmetike

U ovom poglavlju ćemo dokazati osnovni teorem aritmetike koji je fundamentalni rezultat teorije brojeva i temeljno svojstvo skupa cijelih brojeva. Taj rezultat kaže da svaki cijeli broj $n > 1$ možemo rastaviti na proste faktore i taj rastav je jedinstven. Prvo ćemo pokazati da uvijek postoji rastav na proste faktore.

Lema 7. *Svaki cijeli broj $n > 1$ može biti izražen kao produkt prostih brojeva, barem sa samo jednim faktorom.*

Dokaz. Dokaz slijedi induktivno. Budući da je $n = 2$ prost, tvrdnja vrijedi za najmanji broj faktora. Pretpostavit ćemo da za svaki cijeli broj $k < n$ postoji rastav na proste faktore. Moramo pokazati da onda i n također ima rastav na proste faktore.

Ako je n prost broj, onda je dokaz gotov. Pretpostavimo da je n složen broj. Neka je $n = m_1 m_2$ takav da je $1 < m_1 < n, 1 < m_2 < n$. Induktivno možemo zaključiti da m_1 i m_2 također možemo izraziti kao produkte prostih brojeva. Tada i n možemo izraziti u obliku umnoška prostih brojeva koristeći upravo te proste brojeve od m_1 i m_2. Time je dokaz gotov. □

Prije nego krenemo na osnovni teorem aritmetike, treba naglasiti da se ovaj rezultat može koristiti za dokaz beskonačnosti prostih brojeva.

Teorem 6. *Postoji beskonačno mnogo prostih brojeva.*

Dokaz. Pretpostavimo da ima konačno mnogo prostih brojeva $p_1, \ldots, p_n$. Svaki od njih je pozitivan pa vrijedi $N = p_1 p_2 \cdots p_n + 1$. Prema Lemi 7 N ima rastav na proste faktore. Konkretno, postoji prost broj p koji dijeli N. Pa vrijedi $p \mid p_1 p_2 \cdots p_n + 1$.

Budući su to samo prosti brojevi koji predstavljaju $p_1, p_2, \ldots, p_n$ slijedi da je $p = p_i$ za $i = 1, \ldots, n$. Vrijedi da $p \mid p_1 p_2 \cdots p_i \cdots p_n$ pa ne može dijeliti i $p_1 \cdots p_n + 1$, što je kontradikcija. Stoga p nije jedan od navedenih prostih brojeva pa prema tome zaključujemo da prostih brojeva ima beskonačno mnogo. □

Ovaj se teorem može dokazati i na drugi način.

Dokaz. Pretpostavimo da postoji konačno mnogo prostih brojeva $p_1, \ldots, p_n$. Znači $n \geq 2$. Označimo s P skup svih tih prostih brojeva, $P = \{p_1, \ldots, p_n\}$. Podijelimo P u dva disjunktna neprazna podskupa P_1 i P_2. Pretpostavimo da je $m = q_1 + q_2$, gdje je q_1 umnožak prostih brojeva iz P_1 i q_2 je umnožak prostih brojeva iz P_2. Neka je p prosti djelitelj od m. Budući da je $p \in P$, slijedi da p dijeli ili q_1 ili q_2, ali nikada oboje. A to znači da p ne dijeli m, što je kontadikcija. Stoga p nije jedan od navedenih prostih brojeva i broj prostih brojeva mora biti beskonačan. □

Iako postoji beskonačno mnogo prostih brojeva, pogled na listu prostih brojeva pokazuje da su oni rijeđi jer cijelih brojeva ima više. Ako nam je

$$\pi(x) = \text{prost broj} \leq x,$$

osnovno pitanje je kakvo je asimptotsko ponašanje ove funkcije? Ovo pitanje je osnova teorema o prostim brojevima.

Teorem 7. *Za bilo koji pozitivan cijeli broj k postoji k uzastopnih složenih cijelih brojeva.*

Dokaz. Promotrimo niz

$$(k+1)!+2, (k+1)!+3, \ldots, (k+1)!+k+1.$$

Pretpostavimo da je n cijeli broj takav da je $2 \leq n \leq k+1$. Zatim $n \mid (k+1)!+n$. Stoga svaki od prirodnih brojeva u gornjem nizu je složen. □

Lema 8 (**Euklidova lema**). *Ako je p prost i $p \mid ab$, onda $p \mid a$ ili $p \mid b$.*

Dokaz. Pretpostavimo da $p \mid ab$. Ako p ne dijeli a, onda je jasno da a i p moraju biti relativno prosti, to jest $(a,p) = 1$. Onda na osnovu Leme 6, $p \mid b$. □

Sada ćemo navesti i dokazati osnovni teorem aritmetike.

Teorem 8 (**Osnovni teorem aritmetike**). *Za svaki cijeli broj $n \neq 0$ postoji faktorizacija*

$$n = cp_1p_2\cdots p_k,$$

gdje je $c = \pm 1$ i $p_1, \ldots, p_n$ su prosti brojevi. Nadalje, ova faktorizacija je jedinstvena do na poredak faktora.

Dokaz. Pretpostavimo da $n \geq 1$. Ako $n \leq -1$ koristimo $c = -1$ i dokaz je isti. Također isto vrijedi i za $n = 1$, $k = 0$. Sada pretpostavimo $n > 1$. Iz Leme 7, n ima rastav na proste faktore

$$n = p_1p_2\cdots p_m.$$

Moramo pokazati da je ovo jedinstven način faktorizacije. Pretpostavimo onda da n ima još jednu faktorizaciju $n = q_1q_2\cdots q_k$ gdje su q_i prosti brojevi. Moramo pokazati da je $m = k$ i da se radi o istim prostim brojevima. Sada imamo

$$n = p_1p_2\cdots p_m = q_1\cdots q_k.$$

Pretpostavimo da je $k \geq m$. Iz $n = p_1p_2\cdots p_m = q_1\cdots q_k$ slijedi da $p_1 \mid q_1q_2\cdots q_k$. Po Euklidovoj lemi, moramo imati $p_1 \mid q_i$ za neko i. Ali q_i je prost i $p_1 > 1$, slijedi da je $p_1 = q_i$. Stoga možemo eliminirati p_1 i q_i s obje strane faktorizacije pa dobijemo

$$p_2\cdots p_m = q_1\cdots q_{i-1}q_{i+1}\cdots q_k.$$

Nastavljajući na ovaj način, možemo eliminirati sve p_i s lijeve strane faktorizacije i tako dobiti

$$1 = q_{m+1}\cdots q_k.$$

Ako su $q_{m+1}, \ldots, q_k$ prosti brojevi, ovo bi bilo nemoguće. Zato $m = k$ i svaki prosti broj p_i je uključen u prostim brojevima $q_1, \ldots, q_m$. Zato se faktorizacija razlikuje samo u poretku faktora, čime smo završili dokaz. □

Za bilo koji pozitivni cijeli broj $n > 1$, možemo kombinirati sve iste proste brojeve u faktorizaciji broja n i napisati kao

$$n = p_1^{m_1} p_2^{m_2} \cdots p_k^{m_k} \text{ sa } p_1 < p_2 < \cdots < p_k.$$

Ovo se naziva **standardni rastav na proste brojeve**. Primjetimo da bilo koja dva pozitivna cijela broja a i b uvijek možemo napisati preko rastava na proste faktore.

Postoji nekoliko posljedica osnovnog teorema aritmetike.

Teorem 9. *Neka su a i b pozitivni cijeli brojevi veći od 1. Pretpostavimo*

$$a = p_1^{e_1} \cdots p_k^{e_k} \ ,$$
$$b = p_1^{f_1} \cdots p_k^{f_k},$$

gdje smo uključili eksponente koji mogu biti jednaki nuli i različite proste brojeve. Tada je

$$(a, b) = p_1^{min(e_1,f_1)} \cdot p_2^{min(e_2,f_2)} \cdots p_k^{min(e_k,f_k)},$$
$$[a, b] = p_1^{max(e_1,f_1)} \cdot p_2^{max(e_2,f_2)} \cdots p_k^{max(e_k,f_k)}.$$

Korolar 1. *Neka su a i b pozitivni cijeli brojevi veći od 1. Tada $(a, b)\,[a, b] = ab$.*

Primjer: Pronađimo standardne proste dekompozicije od 270 i 2412 i iskoristite ih kako bi odredili najveći zajednički djelitelj i najmanji zajednički višekratnik.

Podsjetimo se da smo našli najveći zajednički djelitelj i najmanji zajednički višekratnik ovih brojeva u prethodnom dijelu korištenjem Euklidovog algoritma.

Da bi pronašli rastav na proste faktore, moramo raspisivati broj u obliku umnoška i nastaviti faktorizaciju dok ne ostanu samo prosti faktori:

$$270 = 27 \cdot 10 = 3^3 \cdot 2 \cdot 5 = 2 \cdot 3^3 \cdot 5,$$

a to je standardni rastav na proste faktore broja 270. Slično tome,

$$2412 = 4 \cdot 603 = 4 \cdot 3 \cdot 201 = 4 \cdot 3 \cdot 3 \cdot 67 = 2^2 \cdot 3^2 \cdot 67,$$

što je standardni rastav na proste faktore broja 2412. Iz toga imamo

$$270 = 2 \cdot 3^3 \cdot 5 \cdot 67^0,$$
$$2412 = 2^2 \cdot 3^2 \cdot 5^0 \cdot 67,$$

iz kojeg smo zaključili da

$$(a, b) = 2 \cdot 3^2 \cdot 5^0 \cdot 67^0 = 2 \cdot 3^2 = 18,$$

i

$$[a, b] = 2^2 \cdot 3^3 \cdot 5 \cdot 67 = 36180.$$

Primjetimo da osnovni teorem aritmetike možemo proširiti na racionalne brojeve. Pretpostavimo da je $r = \frac{a}{b}$ pozitivan racionalni broj. Onda

$$r = \frac{p_1^{e_1} \cdots p_k^{e_k}}{p_1^{f_1} \cdots p_k^{f_k}} = p_1^{e_1 - f_1} \cdots p_k^{e_k - f_k}.$$

Zato bilo koji pozitivan racionalan broj ima standardni rastav na proste faktore

$$p_1^{t_1} \cdots p_k^{t_k} \text{ gdje su } t_1, \ldots, t_k \text{ cijeli brojevi.}$$

Tako na primjer,

$$\tfrac{15}{49} = 3 \cdot 5 \cdot 7^{-2}.$$

Lema 9. *Ako je a cijeli broj kojem n-ta potencija nije potpuna, onda je n-ti korijen od a iracionalan.*

Dokaz. Ovaj rezultat govori, na primjer, da ako cijeli broj nije potpun kvadrat onda je kvadratni korijen tog broja iracionalan. Činjenica da je kvadratni korijen od 2 iracionalan bio je poznat i Grcima. Pretpostavimo da je b cijeli broj sa standardnim rastavom na proste faktore

$$b = p_1^{e_1} \cdots p_k^{e_k}.$$

Onda

$$b^n = p_1^{ne_1} \cdots p_k^{ne_k},$$

i to mora biti standardni rastav na proste faktore broja b^n. Slijedi da je cijeli broj a n-ta potencija ako i samo ako ima standardni rastav na proste faktore

$$a = q_1^{f_1} \cdots q_t^{f_t} \text{ uz uvjet } n \mid f_i \text{ za svaki } i.$$

Pretpostavimo da a nije n-ta potencija. Zatim

$$a = q_1^{f_1} \cdots q_t^{f_t},$$

gdje n ne dijeli f_i za sve i. Uzimajući n-ti korijen dobivamo

$$a^{1/n} = q_1^{f_1/n} \cdots q_i^{f_i/n} \cdots q_t^{f_t/n}.$$

Međutim, f_i/n nije cijeli broj, tako da $a^{1/n}$ ne može biti racionalan, prema osnovnom teoremu aritmetike na skup racionalnih brojeva. □

Koncept djelitelja i faktora može se proširiti na svaki prsten. Kažemo da $a \mid b$ u prstenu R ako postoji $c \in R$ tako da $b = ac$. Ograničit ćemo se na integralnu domenu. Invertibilan element u integralnoj domeni je element e koji ima multiplikativni inverz. To znači da postoji element e_1 iz R tako da vrijedi $ee_1 = 1$. Tako su jedini invertibilni elementi u prstenu cijelih brojeva $\mathbb{Z}$ ± 1. Dva elementa r i r_1 u integralnoj domeni su asocirani ako je $r = er_1$ za neki invertibilni element e. Prost element u integralnoj domeni je element kojem su jedini djelitelji 1 i on sam. S ovim definicijama možemo pričati o faktorizaciji na proste faktore.

Kažemo da je integralna domena D **domena jedinstvene faktorizacije** ako za svaki $d \in D$, ili je $d = 0$, ili je d jedinica, ili d ima rastav na proste faktore jedinstven do na poredak i asociranost. To znači da ako je

$$r = p_1 \cdots p_m = q_1 \cdots q_k$$

tada je $m = k$ i svaki p_i je asociran odgovarajućem q_j.

Osnovni teorem aritmetike u algebarskoj terminologiji kaže da je prsten cijelih brojeva domena jedinstvene faktorizacije. Međutim, daleko od toga da su jedini.

Teorem 10. *Neka je F polje i $F[x]$ prsten polinoma jedne varijable nad poljem F. Tada je $F[x]$ domena jedinstvene faktorizacije.*

Ovaj teorem je zapravo slučaj mnogo općenitijeg rezultata. Integralna domena D se zove euklidska domena ako postoji funkcija $N : D \setminus \{0\} \to \mathbb{N} \cup \{0\}$ koja zadovoljava: Za sve $a, b \in D$, $a \neq 0$ postoje $r, q \in D$ takvi da $b = aq + r$ i ili je $r = 0$ ili $r \neq 0$ i $N(r) < N(a)$.

Teorem 11. *Svaka euklidska domena je domena jedinstvene faktorizacije.*

Gaussovi cijeli brojevi $\mathbb{Z}[i]$ su kompleksni brojevi oblika $a + bi$ gdje su $a, b \in \mathbb{Z}$.

Lema 10. *Cijeli brojevi $\mathbb{Z}$, Gaussovi cijeli brojevi $\mathbb{Z}[i]$ i prsten polinoma $F[x]$ nad poljem F su Euklidske domene.*

Korolar 2. *$\mathbb{Z}[i]$ i $F[x]$ nad poljem F su domene jedinstvene faktorizacije.*

2 Kongruencija i modularna aritmetika

2.1 Osnovna teorija kongruencija

Definicija 4. *Neka je m pozitivan cijeli broj. Ako su x, y cijeli brojevi tako da $m \mid (x-y)$ kažemo da je x* ***kongruentno*** *y* ***modulo*** *m što označavamo s $x \equiv y \pmod{m}$. Ako m ne dijeli $x-y$ onda su x i y* ***nekongruentni modulo*** *m.*

Ako $x \equiv y \pmod{m}$ onda se y zove **ostatak** od x modulo m. Za dani $x \in \mathbb{Z}$ skup cijelih brojeva $\{y \in \mathbb{Z}; x \equiv y \pmod{m}\}$ naziva se **klasa ostatka** od x modulo m. Označavamo ju s $[x]$. Primjetimo da je $x \equiv 0 \pmod{m}$ ekvivalentno $m \mid x$.

Teorem 12. *Ako je $m > 0$, onda je biti kongurentno modulo m relacija ekvivalencije u odnosu na cijele brojeve. Stoga klase ostataka čine particiju skupa cijelih brojeva.*

Dokaz. Podsjetimo se da je relacija $\sim$ na skupu S relacija ekvivalencije ako je refleksivna, tj. $s \sim s$ za sve $s \in S$; simetrična, tj. ako je $s_1 \sim s_2$, onda je $s_2 \sim s_1$; i tranzitivna, tj. ako je $s_1 \sim s_2$ i $s_2 \sim s_3$, onda je $s_1 \sim s_3$. Ako je $\sim$ relacija ekvivalencije tada skup svih klasa ekvivalencije $[s] = \{s_1 \in S; s_1 \sim s\}$ daje particiju skupa S.

Promotrimo $\equiv \pmod{m}$ u $\mathbb{Z}$. Za dani $x \in \mathbb{Z}$, $x - x = 0 = 0 \cdot m$ tako da $m \mid (x-x)$ i $x \equiv x \pmod{m}$. Tada je $\equiv \pmod{m}$ refleksivna.

Pretpostavimo da je $x \equiv y \pmod{m}$. Tada $m \mid (x-y) \Rightarrow x - y = am$ za neki $a \in \mathbb{Z}$. Potom $y - x = -am$ pa $m \mid (y-x)$ i $y \equiv x \pmod{m}$. Tada je $\equiv \pmod{m}$ simetrična.

Na kraju, pretpostavit ćemo $x \equiv y \pmod{m}$ i $y \equiv z \pmod{m}$. Zatim $x - y = a_1 m$ i $y - z = a_2 m$. No međutim, $x - z = (x-y) + (y-z) = a_1 m + a_2 m = (a_1 + a_2)\, m$. Stoga, $m \mid (x-z)$ i $x \equiv z \pmod{m}$. Pa je $\equiv \pmod{m}$ tranzitivan, i teorem je dokazan. □

Dakle, za $m > 0$, svaki cijeli broj pripada jednoj i samo jednoj klasi ostataka. Stoga, pokažimo da postoji točno m klasa ostataka modulo m.

Teorem 13. *Za dani $m > 0$ postoji točno m klasa ostataka modulo m. Posebno, $[0], [1], \ldots, [m-1]$ daje kompletan skup klasa ostataka.*

Dokaz. Pokažimo da za dani $x \in \mathbb{Z}$, x mora biti kongruentan modulo m za jedan od $0, 1, 2, \ldots, m-1$. Pored toga, nijedan drugi nije kongruentan modulo m. Kao posljedica,

$$[0], [1], \ldots, [m-1]$$

daje kompletan skup klasa ostataka modulo m i ima ih m. Da bi se vidjele te tvrdnje pretpostavit ćemo $x \in \mathbb{Z}$. Prema Teoremu o dijeljenju s ostatkom imamo

$$x = qm + r, \text{ gdje je } 0 \leq r < m.$$

To znači da $r = x - qm$, ili u smislu kongurencije, da $x \equiv r \pmod{m}$. Stoga x je kongruentan jednom iz skupa $0, 1, 2, \ldots, m-1$. Pretpostavimo $0 \leq r_1 < r_2 < m$. Tada m ne dijeli $r_2 - r_1$, pa su r_1 i r_2 nekongruentni modulo m. Tada je svaki cijeli broj kongruentan jednom i samo jednom elementu skupa $0, 1, 2, \ldots, m-1$, i stoga $[0], [1], \ldots, [m-1]$ daje kompletan skup klasa ostataka modulo m. □

Postoji mnogo skupova sa potpunim sustavom ostatka modulo m. Posebno, skup od m cijelih brojeva $x_1, x_2, \ldots, x_m$ će predstavljati **potpun sustav ostataka** modulo m ako je $x_i \not\equiv x_j \pmod{m}$ osim ako $i = j$. Iz danog jednog potpunog sustava ostataka lako je dobiti i drugi.

Lema 11. *Ako $\{x_1, \ldots, x_m\}$ formiraju potpun sustav ostataka modulo m i $(a, m) = 1$, onda $\{ax_1, \ldots, ax_m\}$ također formira potpun sustav ostataka modulo m.*

Dokaz. Pretpostavimo $ax_i \equiv ax_j \pmod{m}$. Zatim $m \mid a(x_i - x_j)$. Iz $(a, m) = 1$ prema Euklidovoj lemi $m \mid x_i - x_j$ i stoga $x_i \equiv x_j \pmod{m}$. □

Lema 12. *Ako $x \equiv y \pmod{m}$, onda je $(x, y) = (y, m)$.*

Dokaz. Pretpostavimo $x - y = am$. Zatim bilo koji zajednički djelitelj od x i m je i zajednički djelitelj od y. Iz toga slijedi dokaz. □

2.2 Prsten cijelih brojeva modulo n

Možda je najlakši način za rukovanje rezultatima kongruencija ako ih se promatra u okviru apstraktne algebre. Da bismo to učinili izgradili smo za svaki $n > 0$ prsten pod nazivom prsten cijelih brojeva modulo n. Mi ćemo slijediti ovaj pristup. Međutim, napomenimo da, iako ovaj pristup pojednostavljuje i objašnjava mnoge od dokaza, povijesno gledano, dani dokazi su isključivo numeričko-teorijski. Često su ovi potpuno numeričko-teorijski dokazi inspiracija algebarskim dokazima.

Lema 13. *Ako je $a \equiv b \pmod{n}$ i $c \equiv d \pmod{n}$, onda*

(1) $a + c \equiv b + d \pmod{n}$,

(2) $ac \equiv bd \pmod{n}$.

Dokaz. Pretpostavimo $a \equiv b \pmod{n}$ i $c \equiv d \pmod{n}$. Onda $a - b = q_1 n$ i $c - d \equiv q_2 n$ za neke cijele brojeve q_1, q_2. To znači da $(a + c) - (b + d) = (q_1 + q_2) n$, ili da $n \mid (a + c) - (b + d)$. Stoga $a + c \equiv b + d \pmod{n}$. □

Definicija 5. *Promotrimo potpun sustav ostataka $x_1, \ldots, x_n$ modulo n. Na skupu klasa ostataka $[x_1], \ldots, [x_n]$ definiramo*

1. $[x_i] + [x_j] = [x_i + x_j]$,

2. $[x_i]\,[x_j] = [x_i x_j]$.

Teorem 14. *Za dani pozitivan cijeli broj* $n > 0$*, skup klasa ostataka formira komutativni prsten s jedinicom s operacijama iz prethodne definicije. Ovo se zove* ***prsten cijelih brojeva modulo*** n *i označava sa* $\mathbb{Z}_n$*. Neutralan element je* $[0]$ *i jedinica je* $[1]$.

Dokaz. Iz Leme 13 proizilazi da su ove operacije dobro definirane na skupu klasa ostataka, tj. ako uzmemo dva različita predstavnika klase ostataka, operacije su i dalje iste.

Moramo pokazati da je $\mathbb{Z}_n$ komutativni prsten s jedinicom, i moramo pokazati da zadovoljava, u odnosu na definirane operacije, sva svojstva prstena. Zapravo, $\mathbb{Z}_n$ nasljeđuje ova svojstva iz $\mathbb{Z}$. Pokazat ćemo komutativnost zbrajanja. Pretpostavimo $[a], [b] \in \mathbb{Z}_n$. Tada

$$[a] + [b] = [a + b] = [b + a] = [b] + [a],$$

gdje je $[a + b] = [b + a]$ naslijeđeno iz $\mathbb{Z}$. □

Ovaj teorem je zapravo poseban slučaj općeg rezultata u apstraktnoj algebri. U prstenu cijelih brojeva $\mathbb{Z}$, skup višekratnika cijelog broja n čini ideal koji se obično označava kao $n\mathbb{Z}$. Prsten $\mathbb{Z}_n$ je kvocijentni prsten od $\mathbb{Z}$ modulo ideal $n\mathbb{Z}$, tj. $\mathbb{Z}/n\mathbb{Z} \cong \mathbb{Z}_n$.

Obično smatramo da se $\mathbb{Z}_n$ sastoji od $0, 1, \ldots, n-1$ sa zbrajanjem i množenjem modulo n. Da ne bi došlo do zabune element $[a]$ u $\mathbb{Z}_n$ označavat ćemo samo s a.

Primjer: Promotrimo zbrajanje i množenje u $\mathbb{Z}_5$.

Na primjer, kada imamo modulo 5, tada $3 \cdot 4 = 12 \equiv 2 \pmod 5$ pa u $\mathbb{Z}_5$ imamo $3 \cdot 4 = 2$. Zbrajanje izgleda ovako: $4 + 2 = 6 \equiv 1 \pmod 5$, pa u $\mathbb{Z}_5$ imamo $4 + 2 = 1$.

Teorem 15. *(1)* $\mathbb{Z}_n$ *je integralna domena ako i samo ako je* n *prost broj.*

(2) $\mathbb{Z}_n$ *je polje ako i samo ako je* n *prost broj.*

Dokaz. Budući je $\mathbb{Z}_n$ komutativan prsten s jedinicom za bilo koji n, to će biti integralna domena ako i samo ako ne postoje djelitelji nule. Pretpostavimo prvo, da je n prost broj i pretpostavimo da

$$ab = 0$$

u $\mathbb{Z}_n$. Zatim u $\mathbb{Z}$ imamo

$$ab \equiv 0 \pmod n \Rightarrow n \mid ab.$$

Ako je n prost broj, prema Euklidovoj lemi $n \mid a$ ili $n \mid b$. U terminima kongruencija je onda

$$a \equiv 0 \pmod n \Rightarrow a = 0 \text{ u } \mathbb{Z}_n$$

ili

$$b \equiv 0 \pmod{n} \Rightarrow b = 0 \text{ u } \mathbb{Z}_n.$$

Stoga je $\mathbb{Z}_n$ integralna domena, ako je n prost broj.

Zatim, pretpostavimo da n nije prost broj. Onda $n = m_1 m_2$ gdje su $1 < m_1 < n$ i $1 < m_2 < n$. Tada $n \nmid m_1$, $n \nmid m_2$, ali $n | m_1 m_2$. Prevođenjem u $\mathbb{Z}_n$ imamo

$$m_1 m_2 = 0 \text{ ili}$$
$$m_1 \neq 0 \text{ ili } m_2 \neq 0.$$

Stoga $\mathbb{Z}_n$ nije integralna domena ako n nije prost broj. Time je dokazan prvi dio.

Budući je polje integralna domena, $\mathbb{Z}_n$ ne može biti polje osim ako je n prost broj. Da bi dokazali drugi dio moramo pokazati da ako je n prost broj onda je $\mathbb{Z}_n$ polje. Pretpostavimo da je n prost broj. $\mathbb{Z}_n$ je komutativan prsten s jedinicom, a da bi pokazali da je polje moramo pokazati da svaki nenul element ima multiplikativni inverz.

Pretpostavimo $a \in \mathbb{Z}_n$, $a \neq 0$. Tada u $\mathbb{Z}$ postoji x, y tako da $ax + ny = 1$. U smislu kongruencije imamo

$$ax \equiv 1 \pmod{n},$$

ili u $\mathbb{Z}_n$

$$ax = 1.$$

Zbog toga a ima inverz u $\mathbb{Z}_n$ i stoga je $\mathbb{Z}_n$ polje. □

Primjer: Pronađimo 6^{-1} u $\mathbb{Z}_{11}$.

Korištenjem Euklidovog algoritma,

$$11 = 1 \cdot 6 + 5$$

$$6 = 1 \cdot 5 + 1$$

$$\Rightarrow 1 = 6 - (1 \cdot 5) = 6 - (1 \cdot (11 - 1 \cdot 6)) \Rightarrow 1 = 2 \cdot 6 - 1 \cdot 11.$$

Prema tome, inverz od 6 modulo 11 je 2, to jest, u $\mathbb{Z}_{11}$, $6^{-1} = 2$.

Primjer: Riješimo linearnu jednadžbu $6x + 3 = 1$ u $\mathbb{Z}_{11}$.

Rješenje je

$$x = 6^{-1} \cdot (1 - 3).$$

U $\mathbb{Z}_{11}$ imamo

$$1 - 3 = -2 = 9$$

i

$$6^{-1} = 2 \Rightarrow x = 2 \cdot 9 = 18 = 7.$$

Stoga je rješenje u $\mathbb{Z}_{11}$ $x = 7$. Brza provjera pokazuje da u Z_{11} vrijedi

$$6 \cdot 7 + 3 = 42 + 3 = 45 = 1.$$

Linearna jednadžba u $\mathbb{Z}_{11}$ naziva se linearna kongruencija modulo 11. Mi ćemo komentirati rješenja takvih kongruencija u narednom potpoglavlju.

Teorem 16 (**Wilsonov teorem**). *Ako je p prost broj, onda*

$$(p-1)! \equiv -1 \pmod{p}.$$

Dokaz. Pišemo $(p-1)! = (p-1)\,(p-2)\cdots 1$. Budući je $\mathbb{Z}_p$ polje, svaki $x \in \{1, 2, \ldots, p-1\}$ ima multiplikativni inverz modulo p. Dalje, pretpostavimo $x = x^{-1}$ u $\mathbb{Z}_p$. Tada je $x^2 = 1$, iz čega slijedi $(x-1)\cdot(x+1) = 0$ u $\mathbb{Z}_p$ i stoga je $x = 1$ ili $x = -1$ budući je $\mathbb{Z}_p$ integralna domena. Dakle, u $\mathbb{Z}_p$ su samo 1 i -1 jednaki svom multiplikativnom invezu. Nadalje, $-1 = p-1$ budući $p - 1 \equiv -1 \pmod{p}$. Stoga, u umnošku $(p-1)\cdot(p-2)\cdots 1$, gledajući u polju $\mathbb{Z}_p$, svaki element ima multiplikativni inverz različit od samog sebe osim 1 i $p-1$. Nadalje, umnožak svakog elementa sa svojim inverzom je 1. Stoga u $\mathbb{Z}_p$ imamo $(p-1)\cdot(p-2)\cdots 1 = p-1$. Pišemo u obliku kongruencije

$$(p-1)! \equiv p-1 \equiv -1 \pmod{p}.$$

□

Obrat Wilsonovog teorema također vrijedi, ako $(n-1)! \equiv -1 \pmod{n}$, onda n mora biti prost broj.

Teorem 17. *Ako je $n > 1$ prirodan broj i vrijedi*

$$(n-1)! \equiv -1 \pmod{n},$$

onda je n prost broj.

Dokaz. Pretpostavimo $(n-1)! \equiv -1 \pmod{n}$. Ako je n složen, onda $n = mk$ gdje su $1 < m < n-1$ i $1 < k < n-1$. Stoga m i k su uračunati u $(n-1)!$. Slijedi da je, $(n-1)!$ djeljiv s n tako da $(n-1)! \equiv 0 \pmod{n}$, što je u kontradikciji s tvrdnjom da je $(n-1)! \equiv -1 \pmod{n}$. Stoga n mora biti prost broj. □

2.3 Invertibilni elementi i Eulerova funkcija

U polju F svaki nenul element ima multiplikativni inverz. Ako je R komutativan prsten s jedinicom, a ne nužno polje, tada je invertibilan element svaki koji posjeduje multiplikativni inverz. U ovom slučaju njegov inverz je invertibilan. Na primjer, u prstenu cijelih

brojeva su jedini invertibilni elementi ± 1. Skup invertibilnih elemenata u komutativnom prstenu s jedinicom formira Abelovu grupu i naziva se grupa invertibilnih elemenata od R. Podsjetimo se da je grupa G skup s jednom operacijom koja je asocijativna, ima neutralni element za tu operaciju takav da svaki element ima inverz u odnosu na ovu operaciju. Ako je operacija komutativna, onda je G Abelova grupa.

Lema 14. *Ako je R komutativan prsten s jedinicom, onda skup invertibilnih elemenata u grupi R formira Abelovu grupu s obzirom na množenje. Tu grupu zovemo* ***unitarna grupa*** *R, označena s $U(R)$.*

Lema 15. *Element $a \in \mathbb{Z}_n$ je invertibilan ako i samo ako $(a, n) = 1$.*

Dokaz. Pretpostavimo $(a, n) = 1$. Onda postoje $x, y \in \mathbb{Z}$ takav da $ax + ny = 1$. To znači da je $ax \equiv 1 \pmod{n}$ što opet implicira $ax = 1$ u $\mathbb{Z}_n$ i stoga je a invertibilan.

Obrnuto, pretpostavimo da je a invertibilan u $\mathbb{Z}_n$. Tada postoji $x \in \mathbb{Z}$ takav da je $ax = 1$. Napisano u obliku kongruencije,

$$ax \equiv 1 \pmod{n} \Rightarrow n \mid ax - 1 \Rightarrow ax - 1 = ny \Rightarrow ax - ny = 1.$$

Stoga je 1 linearna kombinacija od a i n, i tada su $(a, n) = 1$.

□

Ako je a invertibilan u $\mathbb{Z}_n$ onda se linearna jednadžba

$$ax + b = c$$

uvijek može riješiti s jedinstvenim rješenjem $x = a^{-1}(c - b)$. Određivanje ovog rješenja može se postići istim postupkom kao u $\mathbb{Z}_p$, gdje je p prost broj. Ako a nije invertibilan situacija je složenija.

Primjer: Riješimo $5x + 4 = 2$ u $\mathbb{Z}_6$.
Iz $(5, 6) = 1$, 5 je invertibilan element u $\mathbb{Z}_6$, imamo

$$x = 5^{-1}(2 - 4).$$

Sada, $2 - 4 = -2 = 4$ u $\mathbb{Z}_6$. Dalje, $5 = -1$ u prstenu $\mathbb{Z}_6$, tako da $5^{-1} = -1^{-1} = -1$. Zatim imamo

$$x = 5^{-1}(2 - 4) = -1(4) = -4 = 2.$$

Jedinstveno rješenje u $\mathbb{Z}_6$ je $x = 2$.

Budući je element a invertibilan u $\mathbb{Z}_n$ ako i samo ako je $(a,n)=1$, slijedi da je broj invertibilnih elemenata u $\mathbb{Z}_n$ jednak broju prirodnih brojeva manjih ili jednakih n koji su relativno prosti s n. Taj broj je dan kao **Eulerova funkcija**.

Definicija 6. *Za bilo koji prirodan broj n definiramo,*

$$\varphi(n) = \textit{broj prirodnih brojeva manjih ili jednakih } n \textit{ koji su relativno prosti s } n.$$

Primjer: $\varphi(6)$ =2, budući su između 1, 2, 3, 4, 5, 6 samo 1, 5 relativno prosti s 6.

Lema 16. *Broj invertibilnih elemenata u $\mathbb{Z}_n$, što je red unitarne grupe $U(\mathbb{Z}_n)$, je $\varphi(n)$.*

Definicija 7. *Za dani $n>0$, **reducirani sustav ostataka** modulo n je skup cijelih brojeva $x_1,\ldots,x_k$ tako da je svaki x_i relativno prost s n, $x_i \not\equiv x_j \pmod{n}$ osim za $i=j$, i ako $(x,n)=1$ za neki cijeli broj x onda $x \equiv x_i \pmod{n}$ za neki i.*

Zato je reducirani sustav ostataka potpun skup predstavnika onih klasa ostataka cijelih brojeva koji su relativno prosti s n. Reducirani sustav ostataka je čitav skup invertibilnih elemenata u $\mathbb{Z}_n$. Iz toga slijedi da reducirani sustav ostatka modulo n ima $\varphi(n)$ elementa.

Primjer: Reducirani sustav ostataka modulo 6 je $\{1,5\}$.

Razvit ćemo formulu za $\varphi(n)$. U skladu sa temom prvo ćemo utvrditi formulu za proste faktore, a zatim postaviti rezultate zajedno putem osnovnog teorema aritmetike.

Lema 17. *Za bilo koji prosti broj p i $m>0$ vrijedi,*

$$\varphi(p^m) = p^m - p^{m-1} = p^m\left(1-\frac{1}{p}\right).$$

Dokaz. Podsjetimo se, ako je $1 \le a \le p$ onda je ili $a=p$ ili $(a,p)=1$. Iz toga slijedi da su pozitivni cijeli brojevi manji od p^m koji nisu relativno prosti s p^m upravo višekratnici od p, to jest $p, 2p, 3p, \ldots, p^{m-1}p$. Svi ostali pozitivni $a<p^m$ su relativno prosti s p^m. Stoga je broj prirodnih brojeva manjih od p^m koji su relativno prosti s p^m je

$$p^m - p^{m-1}.$$

□

Lema 18. *Ako je $(a,b)=1$, onda $\varphi(a,b)=\varphi(a)\varphi(b)$.*

Dokaz. Neka je $R_a = \left\{x_1,\ldots,x_{\varphi(a)}\right\}$ reducirani sustav ostataka modulo a, neka je $R_b = \left\{y_1,\ldots,y_{\varphi(b)}\right\}$ reducirani sustav ostataka modulo b, i neka je

$$S = \{ay_i + bx_j : i=1,\ldots,\varphi(b), j=1,\ldots,\varphi(a)\}.$$

Tvrdimo da je S reducirani sustav ostataka modulo ab. Budući da S ima $\varphi(a)\varphi(b)$ elementa iz toga će slijediti da je $\varphi(ab) = \varphi(a)\varphi(b)$.

Da bi pokazali da je S reducirani sustav ostataka modulo ab moramo pokazati sljedeće: prvo da je svaki $x \in S$ relativno prost s ab; zatim da su elementi iz S različiti; i konačno da za svaki cijeli broj n takav da je $(n, ab) = 1$ vrijedi $n \equiv s \mod ab$ za neki $s \in S$.

Neka je $x = ay_i + bx_j$. Tada iz $(x_j, a) = 1$ i $(a, b) = 1$ slijedi $(x, a) = 1$. Analogno, $(x, b) = 1$. To pokazuje da je svaki element iz S relativno prost s ab.

Sljedeće pretpostavimo

$$ay_i + bx_j \equiv ay_k + bx_l \pmod{ab}.$$

Tada

$$ab \mid (ay_i + bx_j) - (ay_k + bx_j) \Rightarrow ay_i \equiv ay_k \pmod{b}.$$

Iz $(a, b) = 1$ slijedi da je $y_i \equiv y_k \pmod{b}$. Ali onda $y_i = y_k$ budući je R_b reduciran sustav ostataka. Slično $x_j = x_l$. To pokazuje da su elementi iz S različiti modulo ab. Konačno, pretpostavimo $(n, ab) = 1$. Neka $(a, b) = 1$, postoje x, y takvi da $ax + by = 1$. Onda

$$anx + bny = n.$$

Iz $(x, b) = 1$ i $(n, b) = 1$ slijedi da je $(nx, b) = 1$. Zbog toga je s_i takav da $nx = s_i + tb$. Na isti način $(ny, a) = 1$, tako da je r_j dan s $ny = r_j + ua$. Onda imamo

$$a(s_i + tb) + b(r_j + ua) = n \Rightarrow n = as_i + br_j + (t + u)ab$$

$$\Rightarrow n \equiv ar_i + bs_j \pmod{ab}.$$

□

Teorem 18. *Pretpostavimo $n = p_1^{e_1} \cdots p_k^{e_k}$, gdje su p_i prosti brojevi međusobno različiti, a e_i prirodni brojevi. Tada vrijedi*

$$\varphi(n) = \left(p_1^{e_1} - p_1^{e_1-1}\right) \cdots \left(p_k^{e_k} - p_k^{e_k-1}\right) = n \prod_i (1 - 1/p_i).$$

Dokaz. Na osnovu prethodne leme imamo

$$\begin{aligned} \varphi(n) &= \varphi(p_1^{e_1}) \cdot \varphi(p_2^{e_2}) \cdots \varphi(p_k^{e_k}) \\ &= \left(p_1^{e_1} - p_1^{e_1-1}\right) \cdot \left(p_2^{e_2} - p_2^{e_2-1}\right) \cdots \left(p_k^{e_k} - p_k^{e_k-1}\right) \\ &= p_1^{e_1}(1 - 1/p_1) \cdots p_k^{e_k}(1 - 1/p_k) = p_1^{e_1} \cdots p_k^{e_k} \cdot (1 - 1/p_1) \cdots (1 - 1/p_k) \\ &= n \textstyle\prod_i (1 - 1/p_i). \end{aligned}$$

□

Primjer: Odredimo $\varphi(126)$.

Pišemo $126 = 2 \cdot 3^2 \cdot 7 \Rightarrow \varphi(126) = \varphi(2)\varphi(3^2)\varphi(7) = 1(3^2-3)\cdot 6 = 36$. Znači, u $\mathbb{Z}_{126}$ ima 36 invertibilnih elemenata.

Teorem 19. *Za $n > 1$ i za $d \geq 1$ vrijedi,*

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

Dokaz. Pretpostavimo da $n = p^e$ za p prost broj. Onda su djelitelji od n $1, p, p^2, \ldots, p^e$, pa

$$\begin{aligned}\sum_{d|n} \varphi(d) &= \varphi(1) + \varphi(p) + \varphi\left(p^2\right) + \cdots + \varphi\left(p^e\right) \\ &= 1 + (p-1) + \left(p^2 - p\right) + \cdots + \left(p^e - p^{e-1}\right).\end{aligned}$$

Primjetimo da se ovaj iznos skraćuje, tj. $1 + (p-1) = p + (p^2 - p) = p^2$, i tako dalje. Dakle, suma je samo p^e i rezultat je dokazan za prirodan broj n koji je potencija prostog broja.

Sada ćemo raditi induktivno po broju različitih prostih faktora broja n. Gornji argument pokazuje da je rezultat istinit ako n ima samo jedan prost faktor. Pretpostavimo da je rezultat točan kad god cijeli broj ima manje od k različitih prostih faktora i pretpostavimo da $n = p_1^{e1} \cdots p_k^{ek}$ ima k različitih prostih faktora. Onda $n = p^e c$, gdje $p = p_1$,$e = e_1$, i c ima manje od k različitih prostih faktora. Koristeći pretpostavku indukcije,

$$\sum_{d|c} \varphi(d) = c.$$

Budući je $(c, p) = 1$ djelitelji od n su svi oblika $p^\alpha d_1$, gdje $d_1 \mid c$ i $\alpha = 0, 1, \ldots, e$, slijedi da je

$$\sum_{d|n} \varphi(d) = \sum_{d_1|c} \varphi(c) + \sum_{d_1|c} \varphi(pd_1) + \cdots + \sum_{d_1|c} \varphi\left(p^e d_1\right).$$

Prema $(d_1, p^\alpha) = 1$ za bilo koji djelitelj od c, suma iznosi

$$\sum_{d_1|c} \varphi(c) + \sum_{d_1|c} \varphi(p)\varphi(d_1) + \cdots + \sum_{d_{1|c}} \varphi\left(p^e\right)\varphi(d_1)$$

$$= \sum_{d_1|c} \varphi(c) + (p-1)\sum_{d_1|c} \varphi(d_1) + \cdots + \left(p^e - p^{e-1}\right)\sum_{d_1|c} \varphi(d_1)$$

$$= c + (p-1)c + \left(p^2 - p\right)c + \cdots + \left(p^e - p^{e-1}\right)c.$$

Kao i u slučaju potencije prostog broja, skraćivanjem sume dobije se konačan rezultat

$$\sum_{d|n} \varphi(d) = p^e c = n.$$

□

Primjer:
Neka je $n = 10$. Djelitelji od 10 su 1, 2, 5, 10. Onda $\varphi(1) = 1$, $\varphi(2) = 1$, $\varphi(5) = 4$, $\varphi(10) = 4$. Tada je

$$\varphi(1) + \varphi(2) + \varphi(5) + \varphi(10) = 1 + 1 + 4 + 4 = 10.$$

2.4 Mali Fermatov teorem i red elemenata

Za bilo koji pozitivan cijeli broj n unitarna grupa $U(\mathbb{Z}_n)$ je konačna Abelova grupa. Podsjetimo se da u bilo kojoj grupi G svaki element $g \in G$ generira cikličku podgrupu koja se sastoji od svih različitih potencija od g. Ako je ova ciklička podgrupa konačna reda m, onda se m naziva **red elementa** g. Ekvivalentno, red elementa $g \in G$ se može opisati kao najmanja pozitivna potencija m takva da je $g^m = 1$. Ako takva potencija ne postoji, onda je g beskonačnog reda. Označavat ćemo red skupa G s $|G|$ i red elementa $g \in G$ s $|g|$. Ako je grupa G konačna, onda očigledno svaki element u grupi ima konačan red. Primjenit ćemo ovu ideju na unitarnu grupu $U(\mathbb{Z}_n)$, ali najprije ćemo se podsjetiti na još neke činjenice o konačnim grupama.

Teorem 20 (**Lagrangeov teorem**)**.** *Pretpostavimo da je G konačna grupa reda n. Onda red bilo koje podgrupe dijeli n. Posebno, red bilo kojeg elementa dijeli red grupe.*

Ako je $g \in G$ tako da je $|G| = n$, onda prema Lagrangeovom teoremu postoji m takav da $g^m = 1$ i $m \mid n$. Kako je $n = mk$, vrijedi $g^n = g^{mk} = (g^m)^k = 1^k = 1$.

Korolar 3. *Ako je G konačna grupa reda n i $g \in G$, tada je $g^n = 1$.*

Teorem 21. *Neka je G konačna Abelova grupa i $|G| = n$. Vrijedi*

(1) Ako su $g_1, g_2 \in G$ takvi da je $|g_1| = a, |g_2| = b$, onda je $(g_1 g_2)^{nzv(a,b)} = 1$.

(2) Ako su $g_1, g_2 \in G$ takvi da je $|g_1| = a, |g_2| = b$, i $(a, b) = 1$, onda je $|g_1 g_2| = ab$.

(3) Ako je $n = p_1^{e_1} p_2^{e_2} \cdots p_k^{e_k}$ faktorizacija prostog broja n, onda je

$$G = H_1 \cdot H_2 \cdot H_k,$$

gdje su $H_1, \ldots, H_k$ podgrupe od G takve da je $|H_i| = p_i^{ei}$.

Drugi dio prethodnog teorema je dio osnovnog teorema o konačno generiranim Abelovim grupama, koji igra istu ulogu u teoriji Abelovih grupa kao osnovni teorem aritmetike u teoriji brojeva.

Uz ove činjenice, pretpostavimo da je $a \in \mathbb{Z}_n$ invertibilan. Tada je $a \in U(\mathbb{Z}_n)$ i stoga a ima multiplikativni red, tj. postoji cijeli broj m takav da je $a^m = 1$ u $\mathbb{Z}_n$. U smislu kongruencije to znači da $a^m \equiv 1 \pmod{n}$. Ako $a \in \mathbb{Z}_n$ nije invertibilan onda ne može postojati potencija $m \geq 1$ takva da $a^m \equiv 1 \pmod{n}$, a ako takav m postoji, onda je a^{m-1} inverz od a.

Lema 19. *Neka je $n > 0$, onda za cijeli broj a postoji cijeli broj m takav da $a^m \equiv 1 \pmod{n}$ ako i samo ako $(a, n) = 1$ ili ekvivalentno, a je invertibilan element u $\mathbb{Z}_n$.*

Definicija 8. *Ako je $(a, n) = 1$, tada je red od a modulo n najmanja potencija m takav da vrijedi $a^m \equiv 1 \pmod{n}$. Mi ćemo pisati red(a) ili $|\langle a \rangle|$ ili $|a|$ za red od a.*

Budući je red od $U(\mathbb{Z}_n)$ jednak $\varphi(n)$, time smo dobili da red svakog elemenata modulo n mora dijeliti $\varphi(n)$.

Korolar 4. *Ako je $(a, n) = 1$, onda red $(a) \mid \varphi(n)$.*

Teorem 22 (**Eulerov teorem**). *Ako $(a, n) = 1$ onda*

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

Ako je $n = p$ prost broj onda je bilo koji cijeli broj $a \neq 0$ modulo p invertibilan u $\mathbb{Z}_p$. Dalje, $\varphi(p) = p - 1$, i stoga imamo sljedeći korolar koji se naziva Mali Fermatov teorem.

Korolar 5. *Ako je p prost broj i $p \nmid a$, tada $a^{p-1} \equiv 1 \pmod{p}$.*

Ako je $(a, n) = 1$ i red od a je točno $\varphi(n)$, tada a zovemo **primitivan korijen** modulo n. U ovom slučaju unitarna grupa je ciklička s generatorom a. Za $n = p$ prost broj uvijek postoji primitivan korijen.

Teorem 23. *Za prost broj p uvijek postoji element a reda $\varphi(p) = p - 1$, tj. primitivan korijen. Ekvivalentno, unitarna grupa $\mathbb{Z}_p$ je uvijek ciklička.*

Dokaz. Kako je svaki nenul element u $\mathbb{Z}_p$ invertibilan, unitarna grupa $U(\mathbb{Z}_p)$ je upravo multiplikativna grupa nad poljem $\mathbb{Z}_p$. Činjenica da je $U(\mathbb{Z}_p)$ ciklička slijedi iz općeg rezultata koji ćemo dokazati. □

Teorem 24. *Neka je F polje. Onda bilo koja konačna podgrupa od multiplikativne grupe F mora biti ciklička.*

Dokaz. Pretpostavimo da je G konačna podgrupa multiplikativne grupe F. Pretpostavimo $|G| = n$. Standardno, najprije ćemo dokazati teorem u slučaju da je n potencija prostog broja i onda postaviti rezultat preko osnovnog teorema aritmetike.

Pretpostavimo $n = p^k$ za neki k. Onda je red bilo kojeg elementa iz G je p^α, gdje je $\alpha \leq k$. Pretpostavimo da je maksimalan red p^t gdje je $t < k$. Tada je p^t najmanji zajednički višekratnik redova svih elemenata iz G. Slijedi da za svaki $g \in G$ vrijedi $g^{p^t} = 1$. Tada je svaki $g \in G$ rješenje polinomijalne jednadžbe

$$x^{p^t} - 1 = 0.$$

Međutim, u polju ne može biti više rješenja od stupnja jednadžbe. Kako G ima $n = p^k$ elemenata i $p^t < p^k$, to je kontradikcija. Dakle maksimalan broj reda može biti $p^k = n$. Stoga G ima element reda $n = p^k$ i taj element generira G, i G mora biti ciklička.

Sad ćemo uvesti broj različitih prostih faktora broja $n = |G|$. Gornji argument se bavi slučajem kad postoji samo jedan prost faktor.

Pretpostavimo da je rezultat točan ako red od G ima manje od k različitih prostih faktora.

Neka je $n = p_1^{e_1} \cdots p_k^{e_k}$. Onda $n = p^e c$, gdje c ima manje od k različitih prostih faktora. Stoga je G konačna Abelova grupa s

$$|G| = p^e c,$$

slijedi $G = H \times K$ gdje je

$$|H| = p^e, |K| = c.$$

Po induktivnoj pretpostavci H i K su obje cikličke, pa H ima element h reda p^e i K ima element k reda c. Budući je $(p^e, c) = 1$, element hk ima red $p^e c = n$, čime je dokaz završen. □

Teorem 25. *Cijeli broj n će imati primitivan korijen modulo n ako i samo ako*

$$n = 2, 4, p^k, 2p^k,$$

gdje je p neparan prost broj.

Red elementa, posebno Fermatov teorem, daje metodu za ispitivanje je li broj prost broj. To ispitivanje odnosi se na utvrđivanje zadanog cijelog broja n je li prost broj ili složen. Najjednostavnije ispitivanje je sljedeće. Ako je n složen, onda $n = m_1 m_2$ gdje su $1 < m_1 < n, 1 < m_2 < n$. Najmanje jedan od ovih faktora mora biti manji ili jednak $\sqrt{n}$. Tada provjeramo sve cijele brojeve jesu li manji ili jednaki $\sqrt{n}$. Ako ni jedan od ovih ne dijeli n onda je n prost broj. Ovo se može poboljšati korištenjem osnovnog teorema aritmetike. Ako n ima djelitelj manji ili jednak $\sqrt{n}$ onda ima prost djelitelj manji ili jednak $\sqrt{n}$, tako da se u gornjoj provjeri djeljivosti mora provjeriti samo za proste brojeve manji ili jednak $\sqrt{n}$.

Iako ova metoda uvijek radi, to je često nepraktično za veliki n i ostale metode moraju

biti upotrebljene da se vidi je li broj prost. Po Fermatovom teoremu, ako je n prost i $a < n$, onda $a^{n-1} \equiv 1 \pmod{n}$. Ako se nađe broj a za kojeg ovo ne vrijedi, onda a nije prost broj. Dat ćemo trivijalan primjer.

Primjer: Odredimo je li 77 prost broj.
Ako je 77 prost, onda imamo $2^{76} \equiv 1 \pmod{77}$. Sada,

$$2^{76} = 2^{38 \cdot 2} = 4^{38}.$$

Sada računamo $\pmod{77}$:

$$4^3 = 64 = -13 \Rightarrow 4^6 = 169 = 15 \Rightarrow 4^{12} = 225 = 71 = -6$$

$$\Rightarrow 4^{36} = (-6)^3 = -216 = -62 \Rightarrow 4^{38} = 4^2 (-62) = -992 = -68 \neq 1.$$

Tada 77 nije prost broj.

Ova metoda može odrediti je li broj n složen. Međutim, ne može utvrditi je li broj prost. Postoje brojevi n za koje vrijedi $a^{n-1} \equiv 1 \pmod{n}$ za sve $(a, n) = 1$, ali n nije prost broj. Oni se nazivaju **pseudoprosti brojevi**.

2.5 Cikličke grupe

U teoriji grupa, ciklička grupa je grupa koja može biti generirana samo jednim svojim elementom, u smislu da grupa ima element g ("generator" grupe) takav da, kada se zapiše u obliku umnoška, svaki element grupe je stupanj od g (umnožak od g u slučaju aditivne notacije).

Grupa G se naziva cikličkom ako postoji element g u G, takav da $G = \langle g \rangle = \{gn$ za svaki cijeli broj $n\}$. Kako je svaka grupa generirana elementom grupe podgrupa te grupe, pokazivanjem da je jedina podgrupa grupe G koja sadrži g sama G, pokazuje se da je G ciklička. Za svaki pozitivan cijeli broj n postoji točno jedna ciklička grupa čiji red je n, i postoji točno jedna beskonačna ciklička grupa (cijeli brojevi u odnosu na zbrajanje). Stoga su cikličke grupe najjednostavnije grupe.

Ime 'ciklička' može dovesti do zabune: moguće je generirati beskonačno mnogo elemenata i ne napraviti nijedan ciklus; to jest, svako g^n može biti različito. Grupa generirana na ovaj način je beskonačna ciklička grupa, koja je izomorfna aditivnoj grupi cijelih brojeva $\mathbb{Z}$. Grupe se obično označavaju na sljedeći način: $\mathbb{Z}/n$ ili $\mathbb{Z}/n\mathbb{Z}$.

Lema 20. *(1) Ako je G konačna ciklička grupa reda n onda je G izomorfna $(\mathbb{Z}_n, +)$. Posebno, sve cikličke grupe određenog reda su izmorfne.*

(2) Ako je G beskonačna ciklička grupa onda je G izomorfna s $(\mathbb{Z}, +)$.

Ciklička grupa je Abelova grupa i svaka njena podgrupa je također Abelova. Kao gotovo direktnu posljedicu teorema o dijeljenju s ostatkom dobivamo da svaka podgrupa cikličke grupe mora biti ciklička.

Lema 21. *Neka je G ciklička grupa. Tada je svaka podgrupa G ciklička.*

Dokaz. Pretpostavimo $G = \langle g \rangle$ i $H \subset G$ je podgrupa. Budući se G sastoji od potencija od g, H se također sastoji od određenih potencija od g. Neka je k najmanji pozitivan cijeli broj takav da je $g^k \in H$. Pokazali smo da $H = \langle g^k \rangle$, tj. H je ciklička podgrupa generirana s g^k.

Očito je da je to ekvivalentno s pokazivanjem da svaki $h \in H$ mora biti potencija od g^k.

Pretpostavimo $g^t \in H$. Možemo pretpostaviti da $t > 0$ i da $t > k$ gdje je k najmanji pozitivni cijeli broj takav da $g^k \in H$. Ako je $t < 0$ tada pišemo $-t$. Prema teoremu o dijeljenju s ostatkom imamo

$$t = gk + r$$

gdje je $r = 0$ ili $0 < r < k$.

Ako je $r \neq 0$ onda $0 < r < k$ i $r = t - k$. Stoga $g^r = g^{t-k} = g^t g^{-k}$. Sada je $g^t \in H$ i $g^k \in H$ i stoga H je podgrupa iz čega slijedi $g^{t-k} \in H$. Ali je tada $g^r \in H$, što je u kontradikciji s $0 < r < k$ i s tim da je k najmanja potencija od g u H. Stoga $r = 0$ i $t = qk$. Imamo onda

$$g^t = g^{qk} = \left(g^k\right)^q.$$

što kompletira dokaz. □

Svaki element cikličke grupe G generira svoju cikličku podgrupu. Pitanje je, kada se ciklička podgrupa podudara s cijelom grupom G? Posebno, koje potencije g^k su generatori od G? Odgovor dolazi isključivo iz teorije brojeva.

Lema 22. *(1) Neka $G = \langle g \rangle$ bude konačna ciklička grupa reda n. Onda je g^k s $k > 0$ generator od G ako i samo ako je $(k, n) = 1$, to jest, k i n su relativno prosti.*

(2) Ako je $G = \langle g \rangle$ beskonačna ciklička grupa, onda su g, g^{-1} jedini generatori grupe G.

Dokaz. Pretpostavimo prvo da je $G = \langle g \rangle$ konačna ciklička grupa reda n i pretpostavimo da je $(k, n) = 1$. Onda postoje prirodni brojevi x, y tako da je $kx + ny = 1$. Iz toga slijedi da je

$$g = g^1 = g^{kx+ny} = g^{kx} g^{ny} = \left(g^k\right)^x (g^n)^y.$$

Ali $g^n = 1$ pa $(g^n)^y = 1$ i stoga

$$g = \left(g^k\right)^x.$$

Tada je g potencija od g^k i onda je svaka potencija od g ujedno i potencija od g^k. Cijela grupa G se tada sastoji od potencija g^k i tada je g^k generator grupe G.

Obratno, pretpostavimo da je g^k također generator od G. Tada postoji potencija x tako da $g = (g^k)^x = g^{kx}$. Kako je $kx \equiv 1 \pmod{n}$ i k je invertibilan modulo n, što implicira da su $(k, n) = 1$.

Pretpostavimo sljedeće, da je $G = \langle g \rangle$ beskonačna ciklička. Tada ne postoji potencija od g koja je jednaka neutralnom elementu grupe G. Pretpostavimo da je g^k također generator gdje je $k > 1$. Tada postoji potencija x tako da $g = (g^k)^x = g^{kx}$. Ali iz tog slijedi da $g^{kx-1} = 1$, što je u kontradikciji s činjenicom da nema potencije od g koja je jednaka 1. Stoga je $k = 1$. □

Podsjetimo se da je $\varphi(n)$ broj pozitivnih cijelih brojeva manjih od n koji su relativno prosti s n. To je broj generatora cikličke grupe reda n.

Korolar 6. *Neka je G konačna grupa reda n. Tada ona ima $\varphi(n)$ generatora.*

Prema Lagrangeovom teoremu, za svaku konačnu grupu red podgrupe dijeli red grupe, to znači ako je $|G| = n$ i $|H| = d$ tako da je H podgrupa od G tada $d \mid n$. Međutim, obrat općenito ne vrijedi, tj. da ako je $|G| = n$ i $d \mid n$ ne mora postojati podgrupa reda d. Nadalje, ako postoji podgrupa reda d tada može ili ne mora postojati druga podgrupa reda d. Međutim, za konačnu cikličku grupu G reda n ako $d \mid n$ postoji jedinstvena podgrupa reda d.

Teorem 26. *Neka je G konačna ciklička grupa reda n. Ako vrijedi $d \mid n$ za $d \geq 1$ tada postoji jedinstvena podgrupa H reda d.*

Dokaz. Neka je $G = \langle g \rangle$ i $|G| = n$. Pretpostavimo $d \mid n$. Tada $n = kd$. Promotrimo element g^k. Tada $(g^k)^d = g^{kd} = g^n = 1$. Nadalje, ako je $0 < t < d$ tada $0 < kt < kd$, pa $kt \neq 0$ modulo n i stoga je $g^{kt} = (g^k)^t \neq 1$. Tada je d najmanja potencija od g^k koja je jednaka 1 i tada g^k ima red d i generira cikličku podgrupu reda d. Sada još moramo pokazati da je jedinstvena.

Pretpostavimo da je $H = \langle g^t \rangle$ druga ciklička podgrupa reda d (podsjetimo se da su sve podrupe od G također cikličke). Možemo pretpostaviti da je $t > 0$ i pokazat ćemo da je g^t potencija od g^k, a time i da se podgrupe podudaraju.

Kako je H reda d imamo $g^{td} = 1$, što implicira da je $td \equiv 0 \pmod{n}$. Kako je $n = kd$ slijedi da $t \geq k$. Primjenom teorema o dijeljenju s ostatkom slijedi:

$$t = qk + r \text{ gdje je } 0 \leq r < k.$$

Ako je $r \neq 0$ tada $0 < r < k$ i $r = t - qk$. Tada

$$r = t - qk \Rightarrow rd = td - qkd \equiv 0 \pmod{n}.$$

Dakle, $n \mid rd$, što je nemoguće jer $rd < kd = n$. Stoga, $r = 0$ i $t = qk$. Iz toga dobivamo

$$g^t = g^{qk} = (g^k)^q.$$

Dakle g^t je potencija od g^k i $H = \langle g^k \rangle$. □

Koristeći ovaj rezultat možemo dati alternativni dokaz teorema 19.

Teorem 27. *Za $n > 1$ i za $d \geq 1$ vrijedi,*

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

Dokaz. Promotrimo cikličku grupu G reda n. Ako vrijedi $d \mid n$, $d \geq 1$, tada postoji jedinstvena ciklička podgrupa H reda d. Tada H ima $\varphi(d)$ generatora. Svaki element iz G generira svoju cikličku podgrupu H_1 reda d i stoga mora biti uključen u $\varphi(d)$ generatora od H_1. Tada je

$$\textstyle\sum_{d|n} \varphi(d) = \text{ukupan broj generatora svih cikličkih podgrupa od } G.$$

Ali to mora biti cijela grupa pa je ova suma jednaka n. □

3 Kineski teorem o ostatcima

U ovom poglavlju proučavat ćemo sustave dviju ili više linearnih kongruencija. Za rješavanje takvih sustava koristi se poznati Kineski teorem o ostatcima. Kineski, jer su posebni slučajevi teorema bili poznati još drevnim Kinezima. U suvremenoj algebri je ovaj teorem veoma moćan alat, što ćemo vidjeti u ovom poglavlju. Krenut ćemo sa sustavom dvije linearne kongruencije.

Teorem 28. *Neka su m i n prirodni brojevi veći od 1, i neka su a i b bilo koji cijeli brojevi. Tada je $x = x_0$ rješenje kongruencija*

$$x \equiv a \pmod{m}$$

$$x \equiv b \pmod{n}$$

ako i samo ako najveći zajednički djelitelj od m i n dijeli $b - a$. Ako je $x = x_0$ rješenje, tada skup cijelih brojeva x koji zadovoljavaju dvije kongruencije je isti kao i skup cijelih brojeva x koji zadovoljava kongruenciju

$$x \equiv x_0 \pmod{[m, n]}$$

gdje je $[m, n]$ najmanji zajednički višekratnik od m i n.

Dokaz. Pretpostavimo da je x rješenje obje kongruencije

$$x \equiv a \pmod{m}$$

$$x \equiv b \pmod{n}.$$

Budući je x rješenje prve kongruencije vrijedi $x = a + my$, gdje je y cijeli broj, te vrijedi $x = b + nz$, gdje je z cijeli broj, budući je x rješenje druge kongruencije. Izjednačimo li ta dva izraza dobivamo sljedeće:

$$a + my = b + nz$$

odnosno

$$my - nz = b - a.$$

Sada primjenimo Bezoutov identitet na ove jednadžbe i dobijemo sljedeće rezultate:

- Ako najveći zajednički djelitelj od m i n ne dijeli $b - a$, onda nema cijelih brojeva y i z tako da vrijedi $my - nz = b - a$ (ako je d najveći zajednički djelitelj od m i n, onda d dijeli $my - nz$, stoga mora dijeliti i $b - a$). Stoga, ne postoji cijeli broj x koji je rješenje zadanih kongruencija.
- Ako d najveći zajednički djelitelj od m i n dijeli $b - a$, tako da $b - a = qd$, tada možemo koristiti Bezoutov identitet kako bismo riješili jednadžbu: nađemo cijele brojeve t i w tako da je $mt + nw = d$, tada je $m(tq) + n(wq) = b - a$. Ako označimo s $y = tq$, vidimo da je $x = a + mtq$ rješenje početne kongruencije.

Ovi rezultati dokazuju prvi dio teorema. Za drugi dio, pretpostavimo da su x_0 i x_1 rješenja zadanih kongruencija. Tada je $x_1 - x_0$ rješenje "homogenog" para kongruencija

$$x \equiv 0 \pmod{m}$$

$$x \equiv 0 \pmod{n}.$$

To znači da je $x_1 - x_0$ zajednički višekratnik od m i n, pa je ujedno i višekratnik najmanjeg zajedničkog višekratnika od m i n. (Najveći zajednički višekratnik označavamo s $[m, n]$.) Stoga vrijedi $x_1 - x_0 = [m, n]k$, za neki k odnosno

$$x_1 = x_0 + [m, n]k$$

za neki k.

Obratno, ako je x_0 rješenje zadanog para kongruencija i x zadovoljava kongruenciju $x \equiv x_0 \pmod{[m, n]}$ za neki cijeli broj k, tada je $x \equiv x_0 \pmod{m}$ i $x \equiv x_0 \pmod{n}$, što znači da je x rješenje zadanog para kongruencija.

Skup cijelih brojeva x za koje vrijedi $x = x_0 + [m, n]k$ može se zapisati u obliku

$$x \equiv \quad (\text{mod } [m, n])$$

□

Teorem 29 (Kineski teorem o ostatcima)**.** *Neka su m i n relativno prosti prirodni brojevi veći od 1, te a i b bilo koji cijeli brojevi. Tada je $x = x_0$ rješenje od*

$$x \equiv a \pmod{m}$$

$$x \equiv b \pmod{n}.$$

Skup cijelih brojeva x koji zadovoljavaju obje kongruencije je jednak skupu svih x-ova koji zadovoljavaju

$$x \equiv x_0 \pmod{mn}.$$

Primjer: Razmotrimo

$$x \equiv 38 \pmod{60}$$

$$x \equiv 7 \pmod{11}.$$

Vrijedi $x = 38 + 60r = 7 + 11s$ za neke cijele brojeve r, s. Da bi našli x, ne moramo naći i r i s u jednadžbi $38 + 60r = 7 + 11s$, nego samo jedan od njih. Jednadžbu $38 + 60r = 7 + 11s$ možemo zapisati u obliku $38 + 60r \equiv 7 \pmod{11}$ odnosno

$$5 + 5r \equiv 7 \pmod{11}.$$

Iz toga dobijemo

$$5r \equiv 2 \pmod{11}.$$

Budući je 9 inverz od 5 modulo 11, pomnožimo zadnju kongruenciju s 9:

$$r \equiv 9 \cdot 5r \equiv 9 \cdot 2 \equiv 7 \pmod{11}.$$

Tada je $x = 38 + 7 \cdot 60 = 458$ rješenje zadane kongruencije. Budući je 660 najmanji zajednički višekratnik od 11 i 60, opće rješenje je

$$x \equiv 458 \pmod{660}.$$

Primjer: Nađimo sva rješenja sljedećeg sustava kongruencija:

$$x \equiv 2 \pmod{12}$$

$$x \equiv 8 \pmod{10}$$

$$x \equiv 9 \pmod{13}.$$

Najprije riješimo prve dvije kongruencije:

$$x = 2 + 12r = 8 + 10s.$$

To riješimo kao u prethodnom primjeru i dobijemo da je $x = 38$ rješenje. Najmanji zajednički višekratnik za 12 i 10 je $[12, 10] = 60$ pa opće rješenje za prve dvije kongruencije je $x = 38 + 60k$ za bilo koji cijeli broj k. Dakle, riješiti ove tri kongruencije isto je što i riješiti

$$x \equiv 38 \pmod{60}$$

$$x \equiv 9 \pmod{13}.$$

Iz ove dvije kongruencije dobijemo da je $x = 38 + 60t = 9 + 13u$ odnosno $38 + 60t \equiv 9 \pmod{13}$. Kao i u prethodnom primjeru možemo kratiti s modulo 13, pa imamo:

$$-1 - 5t \equiv 9 \pmod{13}$$

odnosno

$$-5t \equiv 10 \pmod{13}.$$

Tada je

$$t \equiv -2 \equiv 11 \pmod{13},$$

pa je $x = 38 + 60(11) = 698$. Opće rješenje zadanog sustava kongruencija je $x \equiv 698 \pmod{780}$ jer je $[10, 12, 13] = 60 \cdot 13 = 780$.

Ako imamo sustav od n kongruencija čiji su moduli relativno prosti u parovima (ne kao u prethodnom primjeru), tada uvijek postoji rješenje i jedinstveno je. Tada imamo:

Teorem 30 (Kineski teorem o ostatcima)**.** *Neka su $m_1, m_2, \ldots, m_r$ u parovima relativno prosti prirodni brojevi veći od 1 i $a_1, a_2, \ldots, a_r$ bilo koji cijeli brojevi. Tada sustav kongruencija*

$$x \equiv a_1 \pmod{m_1}$$

$$x \equiv a_2 \pmod{m_2}$$

$$\vdots$$

$$x \equiv a_r \pmod{m_r}$$

ima rješenje. Ako je x_0 jedno rješenje, onda su sva rješenja tog sustava dana s $x \equiv x_0 \pmod{m_1 m_2 \cdots m_r}$.

Dokaz. Neka je $m = m_1 m_2 \cdots m_r$ te neka je $n_j = \frac{m}{m_j}$ za $j = 1, \ldots, r$. Tada je $(m_j, n_j) = 1$ pa postoji cijeli broj x_j takav da je $n_j x_j \equiv a_j \pmod{m_j}$. (Postoje cijeli brojevi u i v,

takvi da je $m_j u + n_j v = 1$. Kad pomnožimo ovu jednakost s a_j slijedi navedeni zaključak.) Promotrimo broj

$$x_0 = n_1 x_1 + \ldots + n_r x_r.$$

Svi pribrojnici navedenog zbroja su djeljivi s m_j osim možda $n_j x_j$ pa je $x_0 \equiv n_j x_j \pmod{m_j}$. Dakle, $x_0 \equiv a_j \pmod{m_j}$ pa je x_0 rješenje zadanog sustava kongruencija. Ako su x i y dva rješenje zadanog sustava kongruencija, koristeći svojstvo: Neka su a, b, c, d cijeli brojevi. Ako je $a \equiv b \pmod{m}$ i $c \equiv d \pmod{m}$, tada je $a + c \equiv b + d \pmod{m}$, $a - c \equiv b - d \pmod{m}$, $ac \equiv bd \pmod{m}$., dobivamo $x \equiv y \pmod{m_j}$ za $j = 1, \ldots, m$. Korištenjem činjenice da su $m_1, \ldots, m_r$ u parovima prosti brojevi, dobivamo da je $x \equiv y \pmod{m}$. □

Primjer: Pretpostavimo da želimo riješiti $36x \equiv 29 \pmod{85}$. Broj 85 možemo napisati kao umnožak brojeva 17 i 5 koji su relativno prosti pa je prethodna kongruencija ekvivalentna sljedećim kongruencijama:

$$36x \equiv 29 \pmod{5}$$

$$36x \equiv 29 \pmod{17}.$$

Da bi riješili zadanu kongruenciju, riješit ćemo novi sustav kongruencija. Prvu kongruenciju možemo skratiti pa imamo

$$x \equiv 4 \pmod{5},$$

dok je druga kongruencija ekvivalentna sljedećoj

$$2x \equiv 12 \pmod{17}$$

odnosno

$$x \equiv 6 \pmod{17}.$$

Sada trebamo riješiti par kongruencija

$$x \equiv 4 \pmod{5}$$

$$x \equiv 6 \pmod{17}.$$

Ove dvije kongruencije možemo zapisati i u obliku

$$x = 4 + 5r = 6 + 17s$$

odnosno

$$6 + 17s \equiv 4 \pmod{5}$$

pa sređivanjem dobijemo

$$17s \equiv -2 \pmod 5$$

to jest

$$2s \equiv -2 \equiv 8 \pmod 5$$

iz čega slijedi da je $s = 4$, stoga je $x = 6 + 17 \cdot 4 = 74$. Budući je $36 \cdot 74 \equiv 29 \pmod 5$ i $36 \cdot 74 \equiv 29 \pmod{17}$ dobivamo rješenje $x = 74$ zadane kongruencije $36x \equiv 29 \pmod{85}$.

3.1 Druge metode rješavanja

U ovom ćemo dijelu dati alternativnu metodu za rješavanje sustava od n kongruencija kada su moduli u parovima relativno prosti. Ideja ove metode je rješavanje više posebnih sustava koji kasnije kao linearna kombinacija čine rješenje izvorne kongruencije.

Primjer: Razmotrimo par kongruencija:

$$x \equiv 15 \pmod{20}$$

$$x \equiv 3 \pmod{17}.$$

Znamo da postoji rješenje budući su brojevi 20 i 17 relativno prosti. Da bismo riješili zadani sustav moramo prvo riješiti sljedeće:

$$x \equiv 1 \pmod{20}$$

$$x \equiv 0 \pmod{17}$$

i

$$x \equiv 0 \pmod{20}$$

$$x \equiv 1 \pmod{17}.$$

U prvom sustavu, $x = e_1$ je rješenje sustava ako je

$$e_1 = 1 + 20r = 17s.$$

Rješavanjem ove kongruencije dobijemo

$$17s \equiv 1 \pmod{20}.$$

Iz

$$17 \equiv -3 \pmod{20}$$

i inverz od 3 modulo 20 je 7, pa možemo staviti da je $s = -7$, stoga je $e_1 = -119$. Slično

i u drugom sustavu, $x = e_2$ je rješenje ako je

$$e_2 = 20t = 1 + 17u.$$

Rješavanjem ove kongruencije dobijemo

$$17u \equiv -1 \pmod{20}.$$

Pomnožimo ovu kongruenciju s -1 pa imamo:

$$3u \equiv 1 \pmod{20},$$

pa možemo staviti da je $u = 7$ i $e_2 = 120$.

Kako smo našli e_1 i e_2 možemo naći i konačno rješenje x_0 izvornog sustava tako da je

$$x_0 = 15e_1 + 3e_2 = 15 \cdot (-119) + 3 \cdot 20 = -1425.$$

(Provjera: modulo 20, $x_0 \equiv 15 \cdot (-119) \equiv 15 \cdot 1 = 15$ i modulo 17, $x_0 \equiv 3 \cdot 120 \equiv 3 \cdot 1 = 3$.)

Kao i ranije, budući je $[20, 17] = 20 \cdot 17 = 340$, opće rješenje je $x \equiv -1425 \pmod{340}$ i najmanje pozitivno rješenje je $x = -1425 + 340 \cdot 5 = 275$.

Ova metoda pronalaska rješenja e_1 i e_2 vrijedi samo ukoliko su moduli relativno prosti.

Na primjer, pokušajmo riješiti sustav

$$x \equiv 1 \pmod{20}$$

$$x \equiv 0 \pmod{18}$$

dobijemo da je $x = 1 + 20r = 18s$. Ali jednadžba $20r - 18s = 1$ nema rješenja jer brojevi 20 i 18 nisu relativno prosti.

3.2 Babilonsko množenje

Ovdje prikazujemo korisnu i zanimljivu primjenu ove metode. Zamislite da se vratite u društvo i okolinu drevnih Babilonaca gdje se umjesto papira koriste teške glinene ploče, a brojevni sustav je imao bazu 60. Da bismo pomnožili brojeve kao što su

$$(35, 43, 52) = 35 \cdot 60^2 + 43 \cdot 60 + 52$$

i

$$(14, 2, 47) = 14 \cdot 60^2 + 2 \cdot 60 + 47,$$

prema uobičajenom algoritmu za množenje, trebalo bi zapamtiti tablicu množenja sa bazom 60 koja sadrži $\frac{59\cdot 60}{2} = 1770$ umnožaka ili bismo ih trebali zapisati na glinenu ploču koja je preteška za nositi unaokolo. Postoji li bolje rješenje? Postoji, Kineski teorem o ostatcima.
Za početak primjetimo da su $5 \cdot 8 \cdot 9 \cdot 11 = 3960 > 59 \cdot 59$ i $5, 8, 9$ i 11 u parovima relativno prosti. Vidimo da e_5 zadovoljava

$$e_5 \equiv 1 \pmod 5$$

$$e_5 \equiv 0 \pmod{8 \cdot 9 \cdot 11};$$

e_8 zadovoljava

$$e_8 \equiv 1 \pmod 8$$

$$e_8 \equiv 0 \pmod{5 \cdot 9 \cdot 11};$$

e_9 zadovoljava

$$e_9 \equiv 1 \pmod 9$$

$$e_9 \equiv 0 \pmod{5 \cdot 8 \cdot 11};$$

i e_{11} zadovoljava

$$e_{11} \equiv 1 \pmod{11}$$

$$e_{11} \equiv 0 \pmod{5 \cdot 8 \cdot 9}.$$

Zaključujemo da je $e_5 = -1584, e_8 = -495, e_9 = -440$ i $e_{11} = -1440$.

Da bismo pomnožili

$$52 \cdot 47,$$

vidimo da

$$52 \cdot 47 \equiv 2 \cdot 2 \equiv -1 \pmod 5$$

$$52 \cdot 47 \equiv 4 \cdot (-1) \equiv 4 \pmod 8$$

$$52 \cdot 47 \equiv -2 \cdot 2 \equiv -4 \pmod 9$$

$$52 \cdot 47 \equiv -3 \cdot 3 \equiv 2 \pmod{11}.$$

Slijedi da je modulo 3960,

$$52 \cdot 47 \equiv (-1)e_5 + 4e_8 + -4e_9 + 2e_{11}$$

$$\equiv 1584 - 1980 + 1760 - 2880 \equiv -1516 \equiv 2444 \pmod{3960}.$$

Budući da je $52 \cdot 47 < 3960$ i $52 \cdot 47 \equiv 2444 \pmod{3960}$ mora vrijediti da je $52 \cdot 47 = 2444$.

Možemo napraviti tablicu svih umnožaka koji se mogu pojaviti prilikom ovakvog množenja. Budući da je svaki broj modulo 5 kongruentan $0, 1$,ili 2 ili negativnim vrijednostima tih brojeva u našoj tablici treba biti samo e_5 i $2e_5$. Slično, za modulo $8, 9$ i 11 u tablici treba biti samo $e_8, 2e_8, 3e_8$ i $4e_8$; $e_9, 2e_9, 3e_9$ i $4e_9$; i $e_{11}, 2e_{11}, 3e_{11}, 4e_{11}$ i $5e_{11}$, svi modulo 3960:

$\cdot$	e_5	e_8	e_9	e_{11}
1	-1584	-495	-440	-1440
2	792	-990	-880	1080
3		-1485	-1320	-360
4		-1980	-1760	-1800
5				720

Na primjer, $3e_9$ je kongruentno -1320 modulo 3960, dok je $4e_{11}$ kongruentno -1800 modulo 3960.

Primjer: Koristimo tablicu za pronalaženje $43 \cdot 47$. Promatramo

$$43 \cdot 47 \equiv 1 \pmod{5}$$

$$43 \cdot 47 \equiv -3 \pmod{8}$$

$$43 \cdot 47 \equiv -4 \pmod{9}$$

$$43 \cdot 47 \equiv -3 \pmod{11},$$

tada vrijedi

$$43 \cdot 47 \equiv 1 \cdot e_5 - 3 \cdot e_8 - 4 \cdot e_9 - 3 \cdot e_{11} \pmod{3960}$$

i onda iščitamo te uvjete iz tablice pa dobijemo

$$43 \cdot 47 \equiv -1584 + 1485 + 1760 + 360 \equiv 2021 \pmod{3960}.$$

Kako je $43 \cdot 47 < 3960$, tada je $43 \cdot 47 = 2021$.

Na taj način možemo riješiti naš babilonski problem "pamćenja" stvaranjem glinene ploče s malom tablicom od 15 brojeva na njemu. Pomoću tablice možemo pomnožiti bilo koja dva broja manja od 60 koristeći kongruencije modulo $5, 8, 9$ i 11.

Zaključak

Teorija brojeva je grana matematike koja se ponajprije bavi proučavanjem svojstava skupa prirodnih brojeva $\mathbb{N} = \{1, 2, 3, 4 \ldots\}$. Jedno od osnovnih svojstava skupa $\mathbb{N}$ je da su na njemu definirane operacije zbrajanja i množenja koje zadovoljavaju pravila komutativnosti, asocijativnosti i distributivnosti. Pored toga, na skupu $\mathbb{N}$ imamo uređaj takav da za svaka dva različita elementa m, n iz $\mathbb{N}$ vrijedi ili $m < n$ ili $n < m$.

Teorija brojeva je, pored geometrije, jedna od najstarijih grana matematike. Bavi se proučavanjem svojstava cijelih brojeva, s posebnim osvrtom na osobine prirodnih brojeva. Jedan od glavnih ciljeva joj je otkrivanje zanimljivih i neočekivanih odnosa između različitih vrsta brojeva i dokazivanje istinitosti tvrdnji kojima se ti odnosi iskazuju. Gauss je matematiku nazivao kraljicom nauka, a teoriju brojeva kraljicom matematike. Stariji naziv za teoriju brojeva je bio aritmetika, ali se od početka 20. stoljeća mijenja nazivom teorija brojeva. Za razliku od drugih grana matematike, mnogi problemi i teoremi iz teorije brojeva se mogu iskazati vrlo jednostavnim i lako razumljivim jezikom, iako rješenja tih problema i dokazi teorema često zahtijevaju sofisticiranu matematičku pozadinu. Do sredine 20. stoljeća je teorija brojeva smatrana granom matematike koja nije imala direktnu primjenu u stvarnom svijetu. Međutim, pojavom digitalnih računara i digitalnih komunikacija, došlo se do spoznaje da teorija brojeva pruža jako mnogo odgovora i rješenja u stvarnim problemima.

Teoriju kongruencija uveo je u svom djelu Disquisitiones Arithmeticae iz 1801. godine Carl Friedrich Gauss (1777-1855), jedan od najvećih matematičara svih vremena. On je također uveo i oznaku za kongruenciju koju i danas rabimo.

Literatura

[1] A. Baker, *A Comprehensive Course in Number Theory* New York 2012.

[2] B. Fine, G. Rosenberger, *Number Theory-An Introduction via the Distribution of Primes*, Birkhäuser, 2007.

[3] B. Ibrahimpašić, *Uvodu teoriju brojeva*, Bihać, 2014.

[4] I. Niven, H. S. Zuckerman, H. L. Montgomery, *An Introduction to the Theory of Numbers*, New York, 1991.

Sažetak

Teorija brojeva je grana matematike koja se bavi svojstvima brojeva, posebno cijelih, kao i širih klasa problema koji proizilaze iz ovog pučavanja.

Izraz aritmetika se također koristi u teoriji brojeva. Ovo je stariji izraz koji više nije popularan koliko je nekada bio. Teoriju brojeva su nekada zvali viša aritmetika, ali i ovaj izraz više nije u upotrebi. Pa ipak, izraz aritmetika se i dalje javlja u imenima nekih područja matematike (aritmetičke funkcije, aritmetika eliptičkih krivulja). Ovaj smisao izraza aritmetika ne treba miješati ni sa elementarnom aritmetikom, niti sa granom logike koja proučava Peanovu aritmetiku kao formalni sustav.

Ključne riječi: babilonsko množenje, djeljivost, kineski teorem o ostatcima, kongruencija, osnovni teorem aritmetike, prsten cijelih brojeva.

Title and summary

Number theory is a branch of mathematics dealing with the properties of numbers, especially whole, as well as the broader class of problems that arise from this study.

The term arithmetic is also used in number theory. This is an older term that is no longer as popular as it once was. Number theory was called the higher arithmetic, but this term is no longer in use. However, arithmetic expression persists in the names of some mathematical fields (arithmetic functions, arithmetic of elliptic curves, fundamental theorem of arithmetic). This sense of the term arithmetic should not be confused with elementary arithmetic is not, nor the branch of logic that studies Peano arithmetic as a formal system. Mathematicians who deal with the theory of numbers are called number theorists.

Keywords: Babylonian multiplication, chinese remainder theorem, congruence, divisibility, ring of algebraic integers.

Životopis

Zovem se Marijana Pravdić. Rođena sam 20.10.1992 godine u Frankfurtu na Maini. Završila sam srednju ekonomsku školu u Žepču. Matematiku sam odlučila upisati prvenstveno jer sam je voljela, a drugi razlog je bila moja profesorica iz srednje škole koja mi je pokazala ljubav prema matematici. Matematiku sam upisala 2011.godine na Odjelu za matematiku u Osijeku. Prva godina za mene je bila najteža jer je bila godina prekretnica. No, podrška roditelja, ljubaznost profesora i velika kolegijalnost od strane ljudi koji su skupa sa mnom prolazili kroz sve matematičke zadatke me je dovela do mjesta na kojem se sada nalazim. Kroz praksu sam se susrela sa svojim budućim poslom i nimalo ne žalim što sam završila upravo nastavnički smjer matematike. Praksu sam imala u osnovnim i srednjim školama u Osijeku i u Žepču. Nadam se da ću uvijek uživati u svom poslu sjećajući se kako su na mene utjecali moji nastavnici i profesori.