The Title

The Author

The Date

Contents

Part I

Cijeli brojevi

1. Definirajte relaciju djeljivosti | i ispitajte strukture (N,|) i (Z,|)

Osnovni pojam elementarne teorije brojeva je djeljivost. Neka su a i b cijeli brojevi.

Kažemo da a **dijeli** b ako je $a \neq 0$ i b je višekratnik od a, tj:
$(\exists k)(b = ka), \;\; k \in Z$

U tom slučaju pišemo $a|b$ i čitamo "a dijeli b"

U izrazu $a|b$ a se zove djelitelj, b djeljenik. a je mjera od b, a b je mjera od a.

Relacija djeljivosti ima sljedeća tri osnovna svojstva:

a) *refleksivnost:* za svaki cijeli broj $a \neq 0$ vrijedi $a|a$

b) *antisimetričnost* za svaka dva cijela broja it $a|b$ i $b|a$ slijedi $a = \pm b$.
Ako su a i b prirodni brojevi, onda slijedi $a = b$.

c) *tranzitivnost:* ako su $a|b$ i $b|c$, onda je $a|c$.

Teorem:

a) Relacija djeljivosti | je relacija poretka na N.

b) Relacija djeljivosti | nije relacija poretka na Z. $(-2|2 \wedge 2| - 2 \nRightarrow -2 = 2)$

2. Teorem o djeljivosti. Citirajte ga i dokažite.

U vezi s relacijom | značajan je **teorem o djeljivosti:**
Neka su svi brojevi koji se pojavljuju u teoremu cijeli:

a) $m|a \wedge m|b \Rightarrow m|(a \pm b)$

b) $m|a \Rightarrow m|ka$

c) $(m|a \vee m|b) \Rightarrow m|(ab)$

d) $(m|a \wedge n|b) \Rightarrow (mn)|(ab)$

e) $m|a \Rightarrow m|a^k$

f) $m|a \Rightarrow m^k|a^k$

Dokazi:

a) $a = k_1 m \wedge b = k_2 m$
$\Rightarrow a \pm b = k_1 m \pm k_2 m = (k_1 \pm k_2)m = lm$
$\Rightarrow m|(a \pm b)$

b) $m|a \Rightarrow m|ka$
$a = lm \quad / \cdot k$
$a \cdot k = lm \cdot k$
$a \cdot k = l \cdot k \cdot m = b \cdot m \Rightarrow m|ak$

c) $m|a \vee m|b \Rightarrow m|ab$
$a = km \wedge b = lm \Rightarrow a \cdot b = km \cdot lm = klm \cdot m = cm \Rightarrow m|ab$

d) $a = km \wedge b = ln$ / pomnožimo ih
$\Rightarrow (ab) = klmn$
$\Rightarrow (ab) = p(mn) \Rightarrow (mn)|(ab)$

e) $m|a \Rightarrow m|a^k$
$a = lm \;\; / \cdot a$

$a \cdot a = l \cdot m \cdot a = n_1 \cdot m$
$a \cdot a \cdot a = n_2 \cdot m$ itd.
$a \cdot ... \cdot a_k = n_k \cdot m \Rightarrow a^k = n_k \cdot m \Rightarrow m|a^k$

f) $m|a \Rightarrow m^k|a^k$
$a = lm \quad /^k$
$a^k = (lm)^k$
$a^k = l^k \cdot m^k$
$a^k = b \cdot m^k$ *uzmemo da je $(l^k = b)$
$\Rightarrow m^k|a^k$

3. Teorem o dijeljenju. Citirajte ga i dokažite.

Neka je $a \in Z$, $b \in N$. Tada postoji samo jedan cijeli broj q i samo jedan prirodan broj r iz N_0 $(r < b, r \in \{0, 1, 2, ..., b-1\})$ takav da vrijedi: $a = bq + r$. Broj q naziva se cjelobrojni kvocijent (količnik), a r se naziva ostatak dijeljenja (eng. modulus). Ostatak prij dijeljenju obično označavamo sa mod. $v = \mathrm{mod}(a, b)$.

Primjer:
$a = 16$
$b = 5$
$\Rightarrow q = 3$, $r = 1$
$16 = 3 \cdot 5+$

Dokaz:
Prvo ćemo dokazati da se cijeli broj može prikazati u obliku $a = bg + r$. (dokaz egzistencije)
Drugo ćemo pokazati da je to jedini način. (dokaz jedinstvenosti)

Definirati skupove:
$I_k = \{z \in Z \mid k \in Z,\ z \in [kb, (k+1)\rangle\ \}$
$I_0 = [0, b\rangle$
$I_1 = [b, 2b\rangle$
$I_{-1} = [-b, 0\rangle$
$I_2 = [2b, 3b\rangle$
Napravili smo particiju skupa cijelih brojeva u uniju dosjunktnih poluintervala: $Z = \bigcup_{k \in Z} I_k$

$a \in Z$, $\exists k : a \in I_k = [kb, (k+1)b\rangle$
Označimo k sa q.
$qb \leq a < (q+1)b$
$qb \leq a < qb + b$
$0 \leq a - qb < b \Rightarrow a - qb = r \Rightarrow a = qb + r$, $a \leq r < b$

Indirektan dokaz:

Pretpostavimo da postoji još jedan takav dokaz, i iz te pretpostavje izvedimo kontra dokaz.

$a = qb + r$, $r \in \{0, 1, 2, ..., b-1\}$

$a = q_1 b + r_1$, $r_1 \in \{0, 1, 2, ..., b-1\}$

$r - r_1 = (a - qb) - (a - q_1 b) = a - qb - a + q_1 b = (q_1 - q)b$

Ovo znači da $b|(r - r_1)$

Kako su r i r_1 iz skupa $\{0, 1, 2, ..., b-1\}$:

iz $b|(r - r_1)$ i $r - r_1 \in \{-(b-1), (-b-2), ..., 0, ..., b-2, b-1\}$ dobijemo kontradikciju jer b ne može dijeliti brojeve koji su po mofulu manjo od njega, jedino može ako je 0.

Ako je 0, onda:

$b|0 \Rightarrow r = r_1$

Tada je:

$a = bg + r$

$a = bq + r$

Ako to oduzmemo, dobijemo:

$0 = bq - bq_1 = b(q - q_1) = 0 \Rightarrow q - q_1 = 0 \Rightarrow q = q_1$

Dokazali smo jedinstvenost.

Teorem je važan jer omogućava da se skup cijelih brojeva u odnosu na djelitelj podijeli u klase.

4. Pojam mjere i višekratnika. NZM i nzv. Neke propozicije o NZM i nzv.

Ako d dijeli a $(a|b)$ i d dijeli b $(d|b)$, tada se d naziva zajednički djelitelj ili zajednička mjera a i b. Najveći zajednički djelitelj brojeva a i b naziva se **najveća zajednička mjera.** To označavamo $NZM(a, b)$. Postoji najmanja zajednička mjera, i to je 1.

Na sličan način, ako a dijeli v $(a|v)$ i b dijeli v $(b|v)$, tada je v najveći zajednički višekratnik od a i b. Najmanji zajednički višekratnik označavamo sa $nzv(a, b)$. Najveći zajednički višekratnik ne postoji.

Primjer:

$nzv(6, 8) = 24$

$NZM(6, 8) = 2$

Može se promatrati NZM i nzv i od više brojeva. Općenito:

$NZM(a_1, a_2, ..., a_m)$ ili $nzv(a_1, a_2, ..., a_m)$

U slučaju da su brojevi cijeli, dovoljno je promatrati samo pozitivne brojeve:

$NZM(-6, 8) = NZM(6, 8) = 2$

Specijalno, ako je $NZM(a_1, a_2, ..., a_m) = 1$, tada kažemo da su brojevi $(a_1, a_2, ..., a_m)$ uzajamno relativno prosti.

5. Euklidov algoritam. Citirajte ga i dokažite pripadni teorem.

Ovo je jedan od najvažnijih i najjednostavnijih algoritama za traženje NZM dva (ili više) cijelih brojeva. Mislilo se da ne postoji efikasniji algoritam od ovoga, ali nedavno su otkriveni neki neznatno efikasniji.

Neka je $a \in Z$ i neka je $b \in N$. Prema teoremu o djeljenju, vrijedi: $a = bq_1 + r_2$, gdje je q_1 vocijent dijeljenja a sa b ($q_1 \in Z$), a r_2 je ostatak i za njega vrijedi: $0 \leq r_2 < b$.

Kako je $b > r_2$, b se može podijeliti sa r_2:

$b = r_2q_2 + r_3$, $q_2 \in Z$, $0 \leq r_3 \leq r_2$

$= r_3q_3 + r_4$, $q_3 \in Z$, $0 \leq r_4 \leq r_3$

Postupak dijeljenja se nastavlja dok se može i dok se ne odredi $r_k > 0$ i $r_{k+1} = 0$, i tada je $NZM(a, b) = r_k$

Imamo dva slučaja:

1) $b|a \Rightarrow a = qb + 0 \Rightarrow NZM(a, b) = b$

2) $b \nmid a \Rightarrow a = bq_1 + r_2$, $b > r_2 > 0$

Iz postupaka dijeljenja navedenog u Euklidovom algoritmu, vidmo da niz ostataka stalno opada i ograničen je odozdo:

$0 \leq ...r_4 < r_3 < r_2 < b$

Mora postojati neki $r_{k+1} = 0$ i neki $r_k > 0$, tako da je:

$r_{k+1} = 0 \leq r_k < ... < r_3 < r_2 < b$

Posljednji član u nizu dijeljenja je sljedeći:

$r_{k-1} = r_kq_k + r_{k+1}$, $r_{k+1} = 0$

Sada iskoristimo prethodni teorem:

$NZM(a, b) = NZM(b, r_2)$

$NZM(b, r_2) = NZM(r_2, r_3)$, itd...

$NZM(r_{k-2}, r_{k-1}) = NZM(r_{k-1}, r_k) = r_k$

Iz tranzitivnosti jednakosti slijedi: $NZM(a, b) = r_k$

Primjedba:

1) Pretpostavili smo u teoremu da je b prirodan broj, ali isti postupak bi bio da je b cijeli broj. To smo radili jer se mjera definira kao prirodan broj.

2) Pretpostavka da je $a > b$. Što ako je $b > a$? Vrijedi: $NZM(a, b) = NZM(b, a)$

Euklidova algoritam može se koristiti i sa više od 2 cijela beojda. Može se pokazato da vrijedi rekurzivna relacija:

$NZM(a_1, a_2, ..., a_{n-1}, a_n) = NZM(NZM(a_1, a_2, ..., a_{n-1}), a_n)$

Još se koristi i indirektno za određivanje najmanjeg zajedničkog višekratnika, vrijdi formula:

$nzv(a, b) \cdot NZM(a, b) = |ab| \;\Rightarrow\; nzv(a, b) = \frac{|ab|}{NZM(a,b)}$

Jasno je da se prethodne dvije relacije mogu kombinirati i tako odrediti nzv za više brojeva. No, i ovde postoji rekurzivna relacija:

$nzv(a_1, a_2, ..., a_{n-1}, a_n) = nzv(nzv(a_1, a_2, ..., a_{n-1}), a_n)$

6. Bezoutov teorem. Citirajte ga i dokažite.

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

Poznat je prošireni Euklidov algoritam ili **Bezoutov teorem**: Ako su a i b cijeli brojevi, tada postoje i cijeli brojevi s i t, tako da vrijedi: $s \cdot a + t \cdot b = NZM(a, b)$

Specijalno, ako su a i b relativno prosti, tada je $s \cdot a + t \cdot b = 1$.

Primjetimo da se u Euklidovu algoritmu nigdje ne koriste rezultati q_k.

Dokaz:

Prema teoremu o dijeljenju i Euklidovom algoritmu $a = bq + r$, $0 \leq r_2 < b$. Imamo dva koraka.

Korak 1:

Izračunajmo $r_2 \;\Rightarrow\; r_2 = a - bq_1 = 1 \cdot a + (-q_1) \cdot b$

Korak 2 (ako r_2 nije mjera):

Dijelimo: $b = r_2q_2 + r_3 \Rightarrow r_3 = b - r_2q_2$

$$\begin{aligned} &= b - (a - bq_1) \cdot q_2 \\ &= \underbrace{-a}_{s=-1} + \underbrace{(1 + q_1q_2)}_{t} \cdot b \end{aligned}$$

Ako r_3 nije mjera, tada ide korak 3:

$r_2 = r_3q_3 + r_4 \Rightarrow r_4 = r_2 - r_3q_3$

$$\begin{aligned} &= (a - bq_1) - q_3(-a + (1 - q_1q_2)b) \\ &= \underbrace{(1 + q_2q_3)}_{s} \cdot a + \underbrace{(-q_1 - q_3 - q_1q_2q_3)}_{t} \cdot b \end{aligned}$$

Ako je ovo kraj algoritma, r_4 je mjera.

Opisani postupak se nastavlja dok se ne dođe do izraza $r_k = s \cdot a + t \cdot b$, znači dok se ne dođe do r_k.

Primjer:

$a = 6$, $b = 9$

$NZM(6, 9) = NZM(9, 6) = 3$

$s \cdot 6 + t \cdot 9 = 3 \quad / : 3$

$2s + 3t = 1$

$\Rightarrow t = 1$, $s = -1$

$\Rightarrow t = 5$, $s = 7$

Iz ovoga možemo naslutiti da rješenja s i t kojima se može prikazati relacija $sa + tb = NZM(a, b)$ ima beskonačno.

Prikaz NZM kao linearne kombinacije (dvaju) cijelih brojeva može se proširiti i na prikaz linearne kombinacije više od 2 broja:

$u \cdot a + v \cdot b + w \cdot c = NZM(a, b, c)$

Vidjeli smo da Euklidov algoritam daje jedan od beskonačno mnogo takvih predočavanja. Pretpostavimo da smo našli jedan prikaz oblika $sa+tb = NZM(a, b)$.

Tada očito vrijedi i sljedeći prikaz:

$(s + \frac{bk}{d})a + (t - \frac{ak}{d})b = d$

$sa + \frac{bka}{d} + tb - \frac{bak}{d} = d$

$sa + tb = d$

Ova relacija pomaže da odredimo sva moguća rješenja s i t u linernoj kombinaciji $sa + tb = d$. Ima ih beskonačno mnogo.

7. Pojam diofantske jednadžbe. Neki primjeri diofantskih jednadžbi. Teorem o rješivosti diofantske jednadžbe ax+by=c.

Diofantske jednadžbe su jednadžbe oblika $f(x_1, x_2, ..., x_n) = b$, pri čemu je f polinom, čiji su koeficijenti realni brojevi. Rješenja se traže u cijelim brojevima. Riješiti Diofantsku jednadžbu znači naći samo cijele brojeve koji zadovoljavaju jednadžbu. Često ih susrećemo u rješavanju problema praktične prirode gdje se barata objektima koji se ne mogu dijeliti na sastavne djelove, koji imaju cijeli broj primjera.

Stupanj Diofantske jednadžbe je stupanj polinoma. Tako imamo Diofantsku jednadžbu prvoga stupnja (linearna Diofantska jednadžba), drugoga reda (kvadratna Diofantska jednadžba), trećeg stupnja (kubna Diofantska jednadžba), ...

Poznat je postupak za rješavanje linearnih i kvadratnih.

Najpoznatija kvadratna naziva se Pellova, npr.

$991x^2 - y^2 = 1$ -> metodom promašaja i pokušaja

Za Diofantsku jednadžbu 3. stupnja ne zna se postupak rješavanja, a za Diofantske jednadžbe 4,5 ili višeg stupnja je Rus Ignjašević pokazao da algoritmam za rješavanje ne postoji.

Primjeri Diofantske linearne jednadžbe:

$2s + 3t = 1$ -> Diofantska jednadžba sa 2 nepoznanice

$a + 2b + 5c = 10$ -> Diofantska jednadžba sa 3 nepoznanice

Primjetimo da je problem rješavanja Diofantske jednadžbe sa dvije nepoznanice ekvivalentan problemu određivanja parametara s i t u Bezoutovu teoremu. Iz toga zaključujemo da se Diofantksa jednadžba rješava Euklidovim algoritmom. Rješenja s i t se mogu pogoditi, a zatim se na opisani način dobiju sva moguća rješenja:

$(s + \frac{bk}{d})a + (t - \frac{ak}{d})b = d$

Postoji još jedan način rješavanja koji se naziva Eulerova metoda, ali postoje i druge metode. Ponekad se stavaljaju ograničenja rješenja Diofantskih jednadžbi. Najčešće se traži da rješenja budu prirodni brojevi ili iz nekog intervala. Tada rješenja može biti konačno mnogo.

Teorem: zadana je Diofantska jednadžba $ax + by = c \Leftarrow NZM(a, b)|c$

Ovaj izraz znači da jednadžba ima rješenja samo ako $NZM(a, b)|c$. Vrijedi i obratno.

8. Metode rješavanja diofantske jednadžbe ax+by=c. Detaljno obrazložite postupke.

$NZM(a, b)|c \Rightarrow c = k \cdot NZM(a, b)$

Prema Bezoutu, postoje rješenja s i t takvi da:

$sa + tb = NZM(a, b) \quad / \cdot k$

$ksa + ktb = k \cdot NZM(a,b) = c$

Posljednja relacija znači da postoje rješenja jednadžbe $ax + by = c$, i da su ta rješenja $x = ks$ i $y = kt$.

Definicija: Pojedinačna rješenja x_0 i y_0 Diofantske jednadžbe $ax + by = NZM(a,b)$ nazivaju se partiularna rješenja Diofantske jednadžbe, a rješenja $x = x_0 + bt$ i $y = y_0 - at$ $(t \in Z)$ nazivaju se opća rješenja Diofantske jednadžbe. I općih i partiklarnih rješenja ima beskonačno mnogo. Ova metoda rješavanja zasniva se na proširenom Euklidovom algoritmu (Bezoutov teorem). Postoji još i Eulerova metoda koja je algoritamski neupotrebljiva iako se lako koristi.

Diofantska jednadžba se može riješiti i na sljedeći način:

Imamo jednadžbu $ax + by = c$. Rješenja se ne trebaju tražiti Euklidovim algoritmom, mogu se pogoditi. I ta rješenja zovemo partikularna rješenja, tj. x_p i y_p (oni su rješenja tzv. partikularne jednadžbe).

Nadalje, uzmemo jednadžbu $ax + by = 0$, tj. stavimo umjesto c da je jednadžba jednaka nuli. Odredimo opća rješenja za tu jednadžbu i dobijemo rješenja x_H i y_H koja zovemo homogenim rješenjima (rješenjima tzv. homogene jednadžbe).

Opća rješenja jednadžbe $ax + by = c$ dobijemo:

$x_0 = x_H + x_p$

$y_0 = y_H + y_p$

U slučaju da je Diofantska jednadžba sa 3 ili više nepoznanica, tada je općenito oblika: $a_1x_1 + a_2x_2 + ... + a_nx_n = b$.

Postupak:

Prvo, kao i u slučaju sa 2 nepoznanice, treba provjeriti ima li jednadžba rješenja, tj. da li $NZM(a_1, a_2, ..., a_n)|b$. Ako je to zadovoljeno, tada cijelu jednadžbu podijelimo sa $NZM(a_1, ..., a_n)$ i dobijemo: $a'_1x_1 + a'_2x_2 + ... + a'_nx_n = b'$

Sada napišemo jednadžbu: $a'_1x_1 + a'_2x_2 + ... + a'_{n-1}x_{n-1} = b' - a'_nx_n$

Sada Diofantsku jednadžbu gledamo kao da ima $n-1$ nepoznanica, pri čemu nepoznanicu x_n sada gledamo kao parametar.

Ova jednadžba mora opet biti rješiva, tj. mora važiti:

$NZM(a'_1, a'_2, ..., a'_{n-1})|(b' - a'_n \cdot x_n)$, što vrijedi kada je $(b' - a'_n \cdot x_n) = k \cdot (a'_1, a'_2, ..., a'_{n-1})$

Ovo se može shvatiti kao Diofantska jednadžba sa 2 nepoznanice, x_n i k, i može se riješiti ranije opisanim načinima. Nama je važno dobiti rješenje za x_n, koje uvrstimo u prethodnu Diofantsku jednadžbu i tako sada imamo Diofantsku jednadžbu sa $n-1$ nepoznaznicom. Opisanim postupkom je objašnjeno kako se Diofantska jednadžba sa više nepoznanica reducira na Diofantsku jednadžbu sa jednom nepoznanicom manje. Taj postupak je rekurzivan, pa se nastavlja dok ne nađemo rješenja svih nepoznanica.

9. Multinomni teorem.

On govori kako se potencira polinom prirodnim brojem: $(x_1 + x_2 + ... + x_n)^n$. Znamo formulu za potenciranje binoma, npr. $(x + y)^2$ ili $(x + y)^3$.

$(x+y)^n$ -> binomni teorem.

Formula za potenciranje polinoma prirodnim brojem n:

$(x+y)^n = \sum_{k=0}^{n} \binom{n}{k} x^{n-k} y^k$ –>binomni teorem, kojemu je $\binom{n}{k}$ binomni koeficijent

$\binom{n}{k} = \frac{n\ !}{k\ !\ (n-k)\ !} = \binom{n}{k,\ n-k}$

$(x_1+x_2+...+x_m)^n = \sum_{i_1+i+...+i_m=n} \binom{n}{i_1,i_2,...,i_m} x_1^{i_1} x_x^{1_2} ... x_m^{i_m}$, $0 \leq i_1, i_2, ..., i_m \leq n$

$\binom{n}{i_1,i_2,...,i_m} = \frac{n!}{k!(n-k)!}$

Primjer:

$(x-2y+3z)^3$

$= \sum_{i+j+k=3} \binom{3}{i,\ j,\ k} x^i (-2y)^j (3z)^k$, $0 \leq i, j, k \leq 3$

$= \binom{3}{300} x^3 (-2y)^0 (3z)^0 + \binom{3}{210} x^2 (-2y)^1 (3z)^0 + ... + \binom{3}{111} x^1 (-2y)^1 (3z)^1$