Najveći zajednički djeljitelj i najmanji zajednički višekratnik

Miljen Mikić

Definicija 1. *Najveći zajednički djeljitelj ili mjera dva prirodna broja a i b je najveći prirodan broj koji dijeli i a i b, te ga označavamo s (a, b) ili $M(a, b)$. U slučaju kada vrijedi $M(a, b) = 1$, kažemo da su a i b relativno prosti.*

Napomena. *Definicija najvećeg zajedničkog djeljitelja se na prirodan način generalizira i na više od dva prirodna broja. Međutim, ako je $M(a_1, a_2, \ldots, a_n) = 1$, to ne znači nužno da su svi a_i i a_j međusobno relativno prosti za $i \neq j$, npr. $M(4, 5, 12) = 1$, iako 4 i 12 nisu relativno prosti. Ako pak dodatno vrijedi da su svi a_i i a_j relativno prosti, onda kažemo da su brojevi a_i u parovima relativno prosti.*

Definicija 2. *Najmanji zajednički višekratnik dva prirodna broja a i b je najmanji prirodan broj koji je djeljiv i s a i s b, te ga označavamo s $[a, b]$ ili $V(a, b)$.*

Propozicija 1. *Neka su a i b prirodni brojevi takvi da je $a > b$. Vrijedi $M(a, b) = M(a - b, b)$.*

Propozicija 2. *Neka su a i b prirodni brojevi takvi da je $a = bq + r$. Tada je $M(a, b) = M(b, r)$.*

Dokaz. Neka je $d = M(a, b)$ i $d' = M(b, r)$. Budući da $d \mid a$ i $d \mid b$, slijedi da $d \mid r$, pa stoga $d \mid d'$. S druge strane, iz $d' \mid b$ i $d' \mid r$, slijedi $d' \mid a$, pa $d' \mid d$. Zaključujemo $d = d'$. □

Najveći zajednički djeljitelj nije teško odrediti kad znamo faktorizirati oba zadana broja, ali za velike brojeve to može biti težak problem - na tome se primjerice temelji kriptografija. Efikasan način za nalaženje najvećeg zajedničkog djeljitelja u općenitom slučaju je **Euklidov algoritam**.

Algoritam se sastoji od uzastopne primjene dijeljenja:

$$\begin{aligned}
m &= nq_1 + r_1, \quad 1 \leq r_1 < n \\
n &= r_1 q_2 + r_2, \quad 1 \leq r_2 < r_1 \\
&\ldots \\
r_{k2} &= r_{k1} q_k + r_k, \quad 1 \leq r_k < r_{k1} \\
r_{k1} &= r_k q_{k+1} + r_{k+1}, \quad r_{k+1} = 0.
\end{aligned}$$

Ovaj lanac nejednakosti je konačan zbog $n > r_1 > r_2 > \cdots > r_k$. Zadnji ne-nul ostatak, r_k, je najveći zajednički djeljitelj od m i n, što je rezultat višestruke primjene Propozicije 2:

$$M(m, n) = M(n, r_1) = M(r_1, r_2) = \cdots = M(r_{k1}, r_k) = r_k.$$

Primjer Izračunaj $M(2002 + 2, 2002^2 + 2, 2002^3 + 2, \ldots)$.

Neka je g traženi najveći zajednički djeljitelj. Uočimo da je $2002^2+2 = 2002(2000+2)+2 = 2000(2002+2)+6$. Prema Euklidovom algoritmu, imamo $M(2002+2, 2002^2+2) = M(2004, 6) = 6$. Stoga $g \mid M(2002+2, 2002^2+2) = 6$. Svaki broj u nizu $2002+2, 2002^2+2, \ldots$ je paran. Nadalje, budući da je $2002 = 2001+1 = 667 \cdot 3 + 1$, za sve prirodne brojeve k, $2002^k = 3a_k + 1$ za neki cijeli broj a_k. Stoga je $2002^k + 2$ djeljiv s 3. Budući da su 2 i 3 relativno prosti, svaki broj u ovom nizu djeljiv je sa 6, pa je $g = 6$.

Lema 3. *Neka su a i b cijeli brojevi, od kojih bar jedan nije nula. Tada je $\{xa + yb \mid x, y \in \mathbb{Z}\}$ skup svih cjelobrojnih višekratnika od $M(a, b)$. Posebno, $M(a, b)$ je najmanji pozitivni broj u tom skupu.*

Dokaz. Neka je S skup svih brojeva oblika $xa + yb$, gdje su $x, y \in \mathbb{Z}$. Uočimo da ako je k u S, tada je svaki višekratnik od k također u S, a ako su k i l u S, tada je $k - l$ također u S. Lako se vidi da S sadrži neke prirodne brojeve, neka je d najmanji prirodni broj među njima. Tada je S skup svih višekratnika od d. U suprotnom, mogli bismo pronaći $s \in S$, koji podijeljen s d daje $\frac{s}{d} = q + \frac{r}{d}$, pri čemu $0 < r < d$, a to je nemoguće budući da je $r = s - qd \in S$, i d je najmanji prirodni broj u S. Budući da je $a, b \in S$, imamo $d \mid a$ i $d \mid b$. S druge strane, kako je $d = x_0 a + y_0 b$ za neke $x_0, y_0 \in \mathbb{Z}$, svaki broj koji dijeli i a i b dijeli i d. Iz toga je očito $d = M(a, b)$.

□

Korolar 4. *(Bezout) Za prirodne brojeve a i b postoje cijeli brojevi x i y takvi da je $ax + by = M(a, b)$.*

Korolar 5. *Prirodni brojevi a i b su relativno prosti ako i samo ako postoje cijeli brojevi x i y takvi da je $ax + by = 1$.*

Propozicija 6. *Neka je m prirodan broj, i neka su a i b cijeli brojevi koji su relativno prosti s m. Ako su x i y cijeli brojevi takvi da*

$$a^x \equiv b^x \pmod{m}, \quad a^y \equiv b^y \pmod{m},$$

tada

$$a^{M(x,y)} \equiv b^{M(x,y)} \pmod{m}.$$

Dokaz. Prema Bezoutovom identitetu, postoje nenegativni cijeli brojevi u i v takvi da je $M(x, y) = ux - vy$. Prema zadanim uvjetima, imamo

$$a^{ux} \equiv b^{ux} \pmod{m}, \quad b^{vy} \equiv a^{vy} \pmod{m},$$

što povlači da je $a^{ux} b^{vy} \equiv a^{vy} b^{ux} \pmod{m}$. Budući da je $M(a, m) = M(b, m) = 1$, prema pravilu o dijeljenju kongruencija imamo $a^{M(x,y)} \equiv a^{ux-vy} \equiv b^{ux-vy} \equiv b^{M(x,y)} \pmod{m}$.

□

Propozicija 7. *Za sve prirodne brojeve a i b vrijedi $ab = M(a, b)V(a, b)$.*

Dokaz. Neka je $a = p_1^{\alpha_1} \cdots p_k^{\alpha_k}$, $b = p_1^{\beta_1} \cdots p_k^{\beta_k}, \alpha_i, \beta_i \geq 0$, $i = 1, \ldots, k$. Kako je $M(a, b) = p_1^{min(\alpha_1,\beta_1)} \cdots p_k^{min(\alpha_k,\beta_k)}$, te $V(a, b) = p_1^{max(\alpha_1,\beta_1)} \cdots p_k^{max(\alpha_k,\beta_k)}$, vrijedi

$$\begin{aligned} M(a, b)V(a, b) &= p_1^{min(\alpha_1,\beta_1)+max(\alpha_1,\beta_1)} \cdots p_k^{min(\alpha_k,\beta_k)+max(\alpha_k,\beta_k)} \\ &= p_1^{\alpha_1+\beta_1} \cdots p_k^{\alpha_k+\beta_k} = mn. \end{aligned}$$

□

Napomena. *Prethodna propozicija ne može se poopćiti, npr. ne vrijedi*

$$M(a,b,c)V(a,b,c) = abc.$$

Primjer Neka je a najmanji, a A najveći od n različitih prirodnih brojeva. Dokažite da je najmanji zajednički višekratnik tih brojeva veći ili jednak na, te da je najveći zajednički djeljitelj manji ili jednak $\frac{A}{n}$.

Neka su $a = a_1 < a_2 < a_3 < \cdots < a_n = A$ zadani brojevi, m njihov najmanji zajednički višekratnik, te d najveći zajednički djeljitelj. S jedne strane $\frac{m}{a_n} < \frac{m}{a_{n1}} < \cdots < \frac{m}{a_1} = \frac{m}{a}$, a s druge strane $\frac{a_1}{d} < \frac{a_2}{d} < \cdots < \frac{a_n}{d} = \frac{A}{d}$. Kako su brojevi u oba ova niza prirodni, oba $\frac{m}{a}$ i $\frac{A}{d}$ moraju biti barem n, što povlači $m \geq na$ i $d \leq \frac{A}{n}$.

Zadaci

1. Prirodni brojevi a i b takvi su da je

   $$\frac{a+1}{b} + \frac{b+1}{a}$$

   cijeli broj. Dokažite da najveći zajednički djeljitelj od a i b nije veći od $\sqrt{a+b}$. *(Španjolska 1996.)*

2. Neka su m i n prirodni brojevi takvi da

   $$M(m,n) + V(m,n) = m + n.$$

   Dokažite da je jedan od ta dva broja djeljiv s drugim. *(Rusija 1995.)*

3. Na ploči je napisano nekoliko prirodnih brojeva. Bilo koja dva različita broja možemo obrisati s ploče i umjesto njih napisati njihov najveći zajednički djeljitelj i najmanji zajednički višekratnik. Dokažite da se nakon konačno mnogo koraka brojevi na ploči više neće mijenjati.
   (St Petersburg 1996.)

4. a) Za koje vrijednosti $n > 2$ postoji skup od n uzastopnih prirodnih brojeva takav da je najveći element u tom skupu djeljitelj najmanjeg zajedničkog višekratnika od preostalih $n-1$ brojeva?
   b) Za koje vrijednosti $n > 2$ postoji jedinstven skup koji ima navedeno svojstvo? *(IMO 1981.)*

5. Neka su x, y i z prirodni brojevi takvi da

   $$\frac{1}{x} - \frac{1}{y} = \frac{1}{z}.$$

   Neka je h najveći zajednički djeljitelj od x, y, z. Dokažite da su $hxyz$ i $h(y-x)$ potpuni kvadrati. *(UK 1998.)*

6. Odredite sve konačne neprazne skupove S prirodnih brojeva takvih da je

$$\frac{i+j}{M(i,j)}$$

element od S za sve i i j (ne nužno različite) iz S. *(APMO 2004.)*

7. Neka su a, b i n prirodni brojevi. Dokažite:
a) $M(n^a-1, n^b-1) = n^{M(a,b)} - 1$
b) $M(n^a+1, n^b+1) \mid n^{M(a,b)} + 1$.

8. Neka su a i b različiti prirodni brojevi takvi da je $ab(a+b)$ djeljivo s $a^2 + ab + b^2$. Dokažite da je $|a-b| > \sqrt[3]{ab}$. *(Rusija 2001.)*

9. Dokažite da za sve prirodne brojeve $m > n$ vrijedi

$$V(m,n) + V(m+1, n+1) > \frac{2mn}{\sqrt{m-n}}.$$

(St.Petersburg 2001.)

10. Pronađite najveći prirodan broj n koji je djeljiv sa svim prirodnim brojevima manjima od $\sqrt[3]{n}$. *(APMO 1998.)*

11. Počevši od točke $(1,1)$, kamen se miče po koordinatnoj ravnini prema sljedećim pravilima:
a) Iz bilo koje točke (a,b) kamen se može pomaknuti u $(2a,b)$ ili $(a,2b)$.
b) Iz bilo koje točke (a,b), kamen se može pomaknuti u $(a-b,b)$ ako $a > b$, odnosno u $(a, b-a)$, ako $a < b$.
Za koje prirodne brojeve x, y se kamen može pomaknuti u (x,y)?