Mali Fermat, Euler, Kineski teorem o ostacima

Grgur Valentić

MEMO pripreme, lipanj 2019.

Uvod

Neka je $n = p_1^{\alpha_1} p_2^{\alpha_2} \dots p_k^{\alpha_k}$ rastav prirodnog broja n na proste faktore. Označimo sa $\varphi(n)$ broj brojeva manjih ili jednakih od n koji su relativno prosti s n. Tada vrijedi

$$\varphi(n) = n(1 - \frac{1}{p_1})(1 - \frac{1}{p_2}) \dots (1 - \frac{1}{p_k})$$

dokaz:

Za $n = p^\alpha$, gdje je p prost broj, tvrdnja se svodi na $\varphi(n) = p^\alpha - p^{\alpha-1}$. No to je očito, jer svi brojevi manji od p^α su relativno prosti s njim, osim brojeva $p, 2p, \dots, p^\alpha$ kojih ima točno $p^{\alpha-1}$. Ukoliko dokažemo da vrijedi $\varphi(mn) = \varphi(m)\varphi(n)$, za brojeve m i n koji su relativno prosti, šro ćemo označavati s $M(m, n) = 1$, dokazat ćemo tvrdnju. Pokušajte se u to uvjeriti indukcijom po broju prostih faktora broja n.

Neka je $R = \{r_1, \dots r_{\varphi(m)}\}$ skup brojeva relativno prostih s m manjih ili jednakih m. Inače, taj skup se naziva reducirani sustav ostataka modulo m. Neka je $S = \{s_1, \dots s_{\varphi(n)}\}$ reducirani sustav ostatak modulo n. Označimo $T = \{nr + ms : r \in R, s \in S\}$. Tvrdimo da je T reducirani sustav ostataka modulo mn.

Pokažimo prvo da su svi iz T relativno prosti s mn. Pretpostavimo suprotno, neka neki p koji dijeli mn, dijeli $nr + ms$, za neke $r \in R$ i $s \in S$. Zbog simetrije, uzmimo $p|m$, pa kako $p|nr + ms$, dobivamo $p|nr$. No, $M(n, m) = 1$ povlači da p ne dijeli n, a kako je $r \in R$ ne može p dijeliti r jer je $M(r, m) = 1$. Dakle, pretpostavka je kriva, odnosno svi iz T su relativno prosti s mn.

Pokažimo sada da ako je neki k relativno prost s mn, da je tada $k \in T$. Poznata je činjenica da za $M(m, n) = 1$ postoje $a, b \in \mathbb{Z}$ takvi da je $am + bn = 1$. To je naprosto posljedica Euklidovog algoritma. Dakle, $akm + bkn = k$. Uzmimo dakle $r = bk$, $s = ak$. Preostaje pokazati da su $r \in R$ i $s \in S$. Zbog simetrije, pokažimo $r \in R$. Pretpostavimo suprotno, neka neki p dijeli i r i m. No iz $sm + rn = k$, dobivamo $p|k$, što je u kontradikciji sa $M(k, mn) = 1$.

Preostaje vidjeti da su svi elementi iz T različiti za različite r i s. Neka je $nr + ms \equiv nr' + ms' \pmod{mn}$. Tada je $n(r - r') \equiv m(s' - s) \pmod{mn}$, pa dobivamo $n(r - r') \equiv 0 \pmod{m}$. Kako je $M(m, n) = 1$, dobivamo $r \equiv r' \pmod{m}$. Na ekvivalentan način dobivamo i $s \equiv s' \pmod{n}$.

Obzirom da je broj elemenata skupa T jasno $\varphi(m)\varphi(n)$, tvrdnja je dokazana.

Eulerov teorem: Neka su $a, n \in \mathbb{N}$ takvi da je $M(a, n) = 1$. Tada je

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

dokaz:

Neka je $R = \{r_1, \ldots, r_{\varphi(n)}\}$ reducirani sustav ostataka modulo n. Tada je i $S = \{ar_1, \ldots, ar_{\varphi(n)}\}$ reducirani sustav ostataka modulo n. Jasno je da $M(ar, n) = 1$, za sve $r \in R$. Pretpostavimo da je $ar \equiv ar' \pmod{n}$. Tada je $a(r - r') \equiv 0 \pmod{n}$, pa kako je $M(a, n) = 1$, dobivamo $r \equiv r' \pmod{n}$. Drugim riječima, svi elementi skupa S jesu relativno prosti s n, i svi su međusobno različiti, dakle oni čine reducirani sustav ostataka modulo n.

Kako su dakle, skupovi R i S jednaki (modulo n), vrijedi

$$r_1 \ldots r_{\varphi(n)} \equiv ar_1 \ldots ar_{\varphi(n)} \pmod{n}$$

, pa je

$$(a^{\varphi(n)} - 1)(r_1 \ldots r_{\varphi(n)}) \equiv 0 \pmod{n}$$

Odnosno, kako su svi r_i relativno prosti s n, dobivamo

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

Mali Fermatov teorem: Neka je $a \in \mathbb{N}$ i $p \in \mathbb{N}$ prost. Tada je $a^p \equiv a \pmod{p}$.

Ovo je posebni slučaj Eulerovog teorema, jer ako p dijeli a, tvrdnja je trivijalna, a u suprotnom imamo $a^{p-1} \equiv 1 \pmod{p}$, što je upravo Eulerov teorem obzirom da je $\varphi(p) = p - 1$.

Kineski teorem o ostacima: Neka su $m_1, \ldots, m_k \in \mathbb{N}$ u parovima relativno prosti, te $a_1, \ldots, a_k \in \mathbb{N}$ proizvoljni. Tada postoji jedinstveni $x \in \mathbb{N}$, do na modulo $m_1 \ldots m_k$, koji zadovoljava sustav kongruencija $x \equiv a_i \pmod{m_i}$, za $1 \leq i \leq k$.

dokaz:

Napravit ćemo samu slučaj $k = 2$, jer ilustrira sve ideje dokaza, a u generalni slučaj se uvjerite indukcijom. Neka su dakle m i n relativno prosti, te tražimo x koji zadovoljava $x \equiv a \pmod{m}$ i $x \equiv b \pmod{n}$. Promotrimo brojeve $a, a + m, \ldots, a + (n-1)m$. Tvrdimo da su to upravo svi mogući ostaci modulo n. Naime, kad bi neka dva bila jednaka tada bismo imali $a + km \equiv a + lm \pmod{n}$, odnosno $m(k - l) \equiv 0 \pmod{n}$, što zbog $M(m, n) = 1$ i $0 \leq k, l \leq n - 1$, daje $k = l$.

Vrijedi i nešto generalnija verzija teorema koja se jednostavno svodi na osnovnu. Neka su $m_1, \ldots, m_k \in \mathbb{N}$, te $a_1, \ldots, a_k \in \mathbb{N}$ proizvoljni. Neka je još $a_i \equiv a_j \pmod{M(m_i, m_j)}$, za sve i, j. Tada postoji jedinstveni $x \in \mathbb{N}$, do na modulo $NZV(m_1, \ldots, m_k)$, koji zadovoljava sustav kongruencija $x \equiv a_i \pmod{m_i}$, za $1 \leq i \leq k$.

Zadaci

1. Nađite ostatak pri dijeljenju 2^{100} sa 11, 25 i 39.
2. Dokažite da za svaki $n \in \mathbb{N}$ postoji $a \in \mathbb{N}$, tako da za sve $k \in \{1 \dots n\}$ postoji $b \in \mathbb{N}$ takav da $b^2 | a + k$.
3. Dokažite da za sve $m, n \in \mathbb{N}$ vrijedi $21 | mn(m^6 - n^6)$.
4. Neka je $\omega(n)$ broj različitih prostih faktora broja n. Dokažite da postoji točno $2^{\omega(n)}$ brojeva djeljivih s n među brojevima $1 \cdot 2, 2 \cdot 3, \dots, n \cdot (n+1)$.
5. Neka je n paran prirodan broj. Dokažite da postoji neparni djelitelj od $3^n + 1$ koji je kongruentan 5 modulo 6.
6. Dokažite da za svaki $n \in \mathbb{N}$ postoji n u parovima relativno prostih prirodnih brojeva $k_1, \dots, k_n$ različitih od 1 takvih da je $k_1 \dots k_n - 1$ produkt 2 uzastopna prirodna broja.
7. Nađite sve proste p takve da $p | 4^p + 5^p$.
8. Dokažite da za svaki $n \in \mathbb{N}$ postoji $a \in \mathbb{N}$, tako da se za sve $k \in \{1 \dots n\}$ broj $a + k$ ne može prikazati kao zbroj kvadrata dva prirodna broja.
9. Nađite sve proste p takve da $p^2 | 5^{p^2} + 1$.
10. Dokažite da za sve p, q različite proste brojeve vrijedi $pq | p^{q-1} + q^{p-1} - 1$.
11. Neka je $f : \mathbb{N} \to \mathbb{N}$ takva da ako je $M(m, n) = 1$, tada je $M(f(m), f(n)) = 1$, te vrijedi $n \leq f(n) \leq n + 100$, za sve $n \in \mathbb{N}$. Dokažite da ako za neki prosti p vrijedi $p | f(n)$, tada vrijedi $p | n$.
12. Dokažite da za sve $n \in \mathbb{N}$ postoje $a, b \in \mathbb{N}$ takvi da $n | 4a^2 + 9b^2 - 1$.
13. Dokažite da za sve $n \in \mathbb{N}$ postoje različiti $a, b \in \mathbb{N}$ takvi da $a + i | b + i$, za sve $i \in \{1, \dots n\}$. Dokažite da ne postoje različiti $a, b \in \mathbb{N}$ takvi da $a + i | b + i$, za sve $i \in \mathbb{N}$.