Teorija brojeva

Matko Ljulj

18. lipnja 2019.

Kongruencije, mali Fermatov teorem i Eulerov teorem

Za dva cijela broja a i b kažemo da su kongruentni po modulu n ako je njihova razlika $a - b$ djeljiva s n. Može se reći i da su a i b kongruentni ako daju isti ostatak pri dijeljenju s n. Pišemo:

$$a \equiv b \pmod{n} \Leftrightarrow n \mid a - b$$

Kongruencijama se služimo jako slično kao i znakom jednako, tj. možemo ih zbrajati, oduzimati, množiti, potencirati. Dakle, ako je $a \equiv b \pmod{n}$ i $c \equiv d \pmod{n}$, vrijedi:

- $a + c \equiv b + d \pmod{n}$
- $a - c \equiv b - d \pmod{n}$
- $ac \equiv bd \pmod{n}$
- $a^m \equiv b^m \pmod{n}$, za bilo koji $m \in \mathbb{N}$. **Oprez:** obrat ne vrijedi, npr: $1^6 \equiv 2^6 = 64 \pmod{7}$, ali $1 \not\equiv 2 \pmod{7}$.
- $am \equiv bm \pmod{n} \Rightarrow a \equiv b \pmod{\frac{n}{M(n,m)}}$, gdje $M(m,n)$ označava najveću zajedničku mjeru (djelitelj) brojeva m i n.

Fermatov (mali) teorem. Neka su a i p prirodni brojevi pri čemu je p prost. Tada vrijedi $a^p \equiv a \pmod{p}$.
Ekvivalentna formulacija: Neka su a i p cijeli brojevi pri čemu je p prost. Ako $M(a,p) = 1$, tada vrijedi $a^{p-1} \equiv 1 \pmod{p}$.

Eulerov teorem. Neka su a i n prirodni brojevi takvi da je $M(a,n) = 1$. Neka je $\varphi(n)$ broj prirodnih brojeva manjih ili jednakih n koji su relativno prosti s n. Tada vrijedi $a^{\varphi(n)} \equiv 1 \pmod{p}$.

Primijetiti: $\varphi(p) = p - 1$, za proste p, pa je Eulerov teorem generalizacija Fermatovog teorema.

Eulerova φ funkcija ima i zatvorenu formulu:

$$\varphi(n) = n\left(1 - \frac{1}{p_1}\right)\left(1 - \frac{1}{p_2}\right)\ldots\left(1 - \frac{1}{p_k}\right) = p_1^{a_1-1}\cdots p_k^{a_k-1}(p_1 - 1)\cdots(p_k - 1),$$

te je multiplikativna: vrijedi $\varphi(1) = 1$ i $\varphi(mn) = \varphi(m)\varphi(n)$, za bilo koja dva **relativno prosta** prirodna m, n.

Kod kongruencija korisno je znati česte kvadratne, kubne i ostale ostatke koje koristimo. Npr: kvadrat broja pri dijeljenju s 3 i 4 daje ostatke $0, 1$, modulo 8 daje $0, 1, 4$; kub prirodnog broja modulo 7 daje $0, 1, 6$. Općenito, m-ta potencija prirodnog broja daje "malo" ostataka modulo n ako je $m = \varphi(n)$ (ti ostatci su 0 i 1) ili $2m = \varphi(n)$ (ti ostatci su 0 i ± 1).

Zadatci

1. Dani su cijeli brojevi a, b takvi da je $a^2 + b^2$ djeljivo s 11. Dokaži da je tada djeljivo i s 121.
2. Nađi nenegativna cijela rješenja jednadžbe $5^m \cdot 7^n + 5^m + 7^{n+1} = 89$.
3. Nađi prirodna rješenja jednadžbe $6^m + 2^n + 2 = x^2$.
4. Nađi sve prirodne x, y takve da je $\dfrac{xy^2}{x+y}$ prost broj.
5. Nađi prirodna rješenja jednadžbe $x! + y! + z! = 2^{u!}$.
6. Dokaži da je za sve prirodne brojeve n izraz $n^{19} - n^7$ djeljiv s 30.
7. Nađi sve prirodne n takve da je $n! + 5$ potpun kub.
8. Nađi cjelobrojna rješenja jednadžbe $x^{10} - y^2 = 12600$.
9. Dokaži da postoji prirodan broj n takav da broj 3^n završava s 2019 nula i jednom jedinicom.
10. Dokaži da ne postoji prirodan broj n takav da $41 \mid 3^{3^n} + 1$.
11. Nađi sve prirodne a, b, c takve da je $3^a + 4^b = 5^c$.
12. Dani su prirodni brojevi a, b, c. Neka je d najveća zajednička mjera brojeva a, b, c. Neka vrijedi $\dfrac{1}{a} - \dfrac{1}{b} = \dfrac{1}{c}$. Dokaži da su brojevi $abcd$ i $d(b-a)$ potpuni kvadrati.
13. Dani su prirodni brojevi x, y takvi da je $2x^2 + x = 3y^2 + y$. Dokaži da su brojevi $x - y$, $2x + 2y + 1$ i $3x + 3y + 1$ potpuni kvadrati.