Mladen Matić (Gornja Trešnjica)

KONGRUENCIJE

Izlaganje o kongruenciji brojeva odnosi se na skup celih brojeva i deljivost istih. Zato se ovde nužno pretpostavlja da je čitalac već upoznat sa izvesnim osnovnim svojstvima celih brojeva i međusobnom povezanošću deljenika, delioca, količnika i ostatka pri deljenju u Z.

Definicija 1. Neka su a i b celi brojevi i neka je m prirodan broj. Tada se kaže da je broj a kongruentan po modulu m sa brojem b ako i samo ako pri deljenju sa m brojevi a i b daju isti ostatak, što pišemo $a \equiv b \pmod{m}$.

Drugim rečima, brojevi a i b međusobno su kongruentni po modulu m ako i samo ako je $a = mq_1 + r$ i $b = mq_2 + r$, gde $a, b, q_1, q_2 \in Z$, a $m, r \in N$ i $0 \leqslant r < m$.

Ako a nije kongurentno sa b po modulu m, onda ćemo pisati $a \not\equiv b \pmod{m}$.

Primer 1. Pošto je $37 = 8 \cdot 4 + 5$ i $13 = 8 \cdot 1 + 5$, kažemo da su 37 i 13 kongruentni po modulu 8 i pišemo: $37 \equiv 13 \pmod{8}$.

Odnosno, pošto je $15 = 7 \cdot 2 + 1$ i $10 = 7 \cdot 1 + 3$, kažemo da je 15 i 10 nisu kongruentni po modulu 7 i pišemo: $15 \not\equiv 10 \pmod{7}$.

Na osnovu definicije kongruentnosti dva broja neposredno se uviđa da ova relacija ima svojstvo refleksivnosti, simetrije i tranzitivnosti, tj. da je $a \equiv a \pmod{m}$, da iz $a \equiv b \pmod{m}$ sleduje $b \equiv a \pmod{m}$ i da iz $a \equiv b \pmod{m}$ i $b \equiv c \pmod{m}$ sleduje $a \equiv c \pmod{m}$.

Teorema 1. Broj a je kongruentan sa brojem b po modulu m ako i samo ako je razlika ova dva broja deljiva sa m.

Dokaz. Dokažimo najpre prvi deo ove teoreme, tj. da deljivost razlike ima za posledicu modularnu kongruentnost brojeva a i b, što možemo zapisati ovako: $m \mid a - b \Rightarrow a \equiv b \pmod{m}$.

Zaista, neka je $a = mq_1 + r_1$ i $b = mq_2 + r_2$. Tada, pošto je $a - b = m(q_1 - q_2) + (r_1 - r_2)$, iz $m \mid a - b$ proizilazi da je $m \mid m(q_1 - q_2) + (r_1 - r_2)$, a to može biti samo ako je $m \mid (r_1 - r_2)$. No, kako je $0 \leqslant r_1 < m$ i $0 \leqslant r_2 < m$, to ova razlika može biti deljiva sa m samo ako je $r_1 - r_2 = 0 \Rightarrow r_1 = r_2$; a u tom slučaju je $a \equiv b \pmod{m}$.

Isto tako se može dokazati i drugi deo ove teoreme, tj da a i b ne mogu biti dva međusobno kongruentna broja ako razlika

$a-b$ nije deljiva sa m. Jer, ako $m \nmid (a-b)$, znači da $m \nmid m(q_1-q_2) + (r_1-r_2)$, a to može biti samo ako je $r_1 \neq r_2$, tj. ako $a \not\equiv b \pmod{m}$.

Na taj način smo se uverili da je $m \mid a-b$ dovoljan i potreban uslov da bude $a \equiv b \pmod{m}$, a na sličan način se može dokazati da je i, obratno, $a \equiv b \pmod{m}$ potreban i dovoljan uslov da bude $m \mid a-b$.

Zbog toga se kaže da su relacije $a \equiv b \pmod{m}$ i $m \mid a-b$ međusobno ekvivalentne, što se zapisuje ovako: $a \equiv b \pmod{m} \Leftrightarrow m \mid a-b$.

Primer 2. Odrediti da li su istiniti iskazi: a) $438 \equiv 15 \pmod{9}$ i b) $825 \equiv 3 \pmod{9}$.

Rešenje. a) $438-15=423$. Pošto je 423 deljivo sa 9, to je, prema teoremi 1, $438 \equiv 15 \pmod{9}$. — b) Pošto razlika $425-3=422$ nije deljiva sa 9, to i $825 \not\equiv 3 \pmod{9}$.

Primer 3. Relacija $a \equiv 1 \pmod{2}$ znači da je $a-1$ deljivo brojem 2, tj. da postoji takav broj m da je $a-1=2m$, odnosno da je $a=2m+1$. Važi i obrnuto. Prema tome, $a \equiv 1 \pmod{2}$ znači isto što i iskaz: a je neparan broj.

Primer 4. Relacija $a \equiv 0 \pmod{2}$ znači da je $a-0=a$ deljivo sa 2, tj. da je $a=2m$. Važi i obrnuto. Prema tome $a \equiv 0 \pmod{2}$ znači isto što i: a je paran broj.

Napomena. Očigledno je da za proizvoljne cele brojeve a i b važi uvek: $a \equiv b$ (mod 1.)

Teorema 2. Neka su a, b, c celi brojevi i neka je m prirodan broj. Ako je $a \equiv b \pmod{m}$, onda je $a \cdot c \equiv bc \pmod{m}$, a takođe je i $a \cdot c \equiv b \cdot c \pmod{mc}$.

Dokaz. Iz relacije $a \equiv b$ sleduje $m \mid a-b$, tj. $mk=a-b$ ($k \in Z$, $k \not\equiv 0$). Ako ovu jednakost pomnožimo sa c dobijamo $mck=ac-bc$, što pokazuje da je $ac \equiv bc \pmod{m}$, a isto tako i da je $ac \equiv bc \pmod{mc}$; a to je i trebalo dokazati.

Tako, na primer, iz $3 \equiv 5 \pmod{2}$ sleduje $3 \cdot 7 \equiv 5 \cdot 7 \pmod{2}$ i $3 \cdot 7 \equiv 5 \cdot 7 \pmod{14}$; i, zaista $21 \equiv 35 \pmod{2}$ i $21 \equiv 35 \pmod{14}$.

Teorema 3. Neka su a, b, c i d celi brojevi i neka je m prirodan broj. Ako je $a \equiv b \pmod{m}$ i $c \equiv d \pmod{m}$, onda je $a+c \equiv b+d \pmod{m}$ i $a-c \equiv b-d \pmod{m}$.

Dokaz. Ako je $a \equiv b \pmod m$ i $c \equiv d \pmod m$, onda postoje brojevi q_1 i q_2 takvi da je $mq_1 = a - b$ i $mq_2 = c - d$. Ako saberemo ove jednakosti, dobijamo $m(q_1 + q_2) \equiv a + c - (b + d)$, a ako drugu od njih oduzmemo od prve, dobijamo $m(q_1 - q_2) = a - b - (c - d)$. Odavde se vidi da su navedeni zbir i razlika deljivi sa m, i time je dokaz završen.

Tako, na primer iz $2 \equiv 5 \pmod 3$ i $5 \equiv 8 \pmod 3$ sleduje $2 + 5 \equiv 5 + 8 \pmod 3$ i $2 - 5 \equiv 5 - 8 \pmod 3$; i, zaista $7 \equiv 13 \pmod 3$ i $-3 \equiv -3 \pmod 3$.

Teorema 4. Za cele brojeve a, b, c, d i m prirodan broj iz relacije $a \equiv b \pmod m$ i $c \equiv d \pmod m$ sleduje $ac \equiv bd \pmod m$.

Dokaz. Na osnovu Teoreme 2 proizilazi da je $ac \equiv bc \pmod m$ i $bc \equiv bd \pmod m$, a odatle proizilazi da je i $ac \equiv bd \pmod m$, što je i trebalo dokazati.

Tako, na primer, iz $1 \equiv 5 \pmod 4$ i $9 \equiv 13 \pmod 4$ sleduje $1 \cdot 9 \equiv 5 \cdot 13$, i zaista, $9 \equiv 65 \pmod 4$.

Kao neposredna posledica ove teoreme dobija se da iz $a \equiv b \pmod m$ sleduje $a^n \equiv b^n \pmod m$, gde je $n \in N$. Poslednja relacija je tačna i za $n = 0$, jer se tada dobija $1 \equiv 1 \pmod m$.

Primer 5. Svaki višecifreni broj kongruentan je sa svojom cifrom jedinica po modulu 2,5 i 10. Dokazati.

Dokaz. Neka je dati višecifreni broj $a = \overline{C_k C_{k-1} \cdots C_2 C_1 C_0}$. Formirajmo razliku tog broja i broja koji se nalazi na mestu njegovih jedinica, tj.

$$\begin{aligned} a - C_0 &= \overline{C_k C_{k-1} \cdots C_2 C_1 C_0} - C_0 = \overline{C_k C_{k-1} \cdots C_2 C_1 0} = \\ &= C_k \cdot 10^k + C_{k-1} 10^{k-1} + \cdots C_2 10^2 + C_1 \cdot 10 = \\ &= 10 (C_k 10^{k-1} + C_{k-1} \cdot 10^{k-2} + \cdots C_2 \cdot 10 + C_1). \end{aligned}$$

Odavde se vidi da je razlika $a - C_0$ deljiva sa 2,5 i 10, pa je zato $a \equiv C_0 \pmod 2$, $a \equiv C_0 \pmod 5$ i $a \equiv C_0 \pmod{10}$, što je i trebalo dokazati.

Iz navedenog neposredno proizilazi pravilo: sa 2, odnosno sa 5, odnosno sa 10 je deljiv onaj i samo onaj broj čija je cifra na mestu jedinica deljiva sa 2, odnosno sa 5, odnosno sa 10.

Primer 6. Svaki višecifren broj kongruentan je sa zbirom svojih cifara po modulu 3 i 9. Dokazati.

Dokaz. Neka je višecifreni broj $a=\overline{C_k C_{k-1} \cdots C_2 C_1 C_0}$. Formirajmo razliku

$$a-(C_k+C_{k-1}+\cdots C_2+C_1+C_0)=C_k\cdot 10^k+C_{k-1}10^{k-1}+\cdots C_2 10^2+ +C_1\cdot 10+C_0-C_k-C_{k-1}-\cdots C_2-C_1-C_0=C_k\cdot 99\cdots 9+ +C_{k-1}\cdot 99\cdots 9+\cdots C_2\cdot 99+C_1\cdot 9=9(C_k\cdot 11\cdots 1+ +C_k\cdot 11\cdots 1+\cdots C_2 11+C_1).$$

Ovde se vidi da je razlika $a-(C_k+C_{k-1}+\cdots C_2+C_1+C_0)$ deljiva sa 3 i sa 9, pa je zato: $a\equiv C_k+C_{k-1}+\cdots C_2+C_1+C_0 \pmod 3$ i $a\equiv C_k+C_{k-1}+\cdots C_2+C_1+C_0 \pmod 9$.

Iz navedenog neposredno proizilazi pravilo: sa 3, odnosno sa 9 deljiv je onaj i samo onaj broj kod koga je zbir cifara deljiv sa 3, odnosno sa 9.

Primer 7. Odrediti ostatak koji se dobija pri deljenju broja 3^{100} sa 13.

Rešenje. Da bismo odredili traženi ostatak, pokušaćemo najpre da nađemo neki manji broj koji je kongruentan sa brojem 3^{100} po modulu 13. To ćemo postići ovako:

Vidimo da je $3^3=27$ i da je $27\equiv 1 \pmod{13}$. Otud sleduje:

$$3^3\equiv 1 \pmod{13} \Rightarrow (3^3)^{33}\equiv 1^{33} \pmod{13} \Rightarrow 3^{99}\equiv 1 \pmod{13} \Rightarrow$$
$$\Rightarrow 3\cdot 3^{99}\equiv 1\cdot 3 \pmod{13} \Rightarrow 3^{100}\equiv 3 \pmod{13}.$$

Kako je $3:13=0$ sa ostatkom 3, zaključujemo da je traženi ostatak 3.

Primer 8. Odrediti poslednju cifru u dekadnom zapisu broja 7^{20}.

Rešenje. Poslednja cifra zapisa 7^{20} predstavlja ostatak koji se dobije pri deljenju broja 7^{20} sa 10. Prema tome, treba odrediti taj ostatak.

Kako je $7^2=49$ i kako $49:10=4$ sa ostatkom 91, to je $7^2\equiv -1 \pmod{10} \Rightarrow 7^{20}\equiv(-1)^{10} \pmod{10} \Rightarrow 7^{20}\equiv 1 \pmod{10}$.

Kako je $1:10=0$ sa ostatkom 1, zaključujemo da je traženi ostatak 1.

Zadaci

1. *Odrediti ostatke pri deobi sa 11: brojeva a) 3^{21} b) 1979^2+2^{1979}*

2. Odrediti poslednje dve cifre u zapisu 99^9.

3. Dokazati: ceo broj je deljiv sa 11 ako i samo ako je razlika zbira cifara na parnim i zbira cifara na neparnim mestima njegovog decimalnog zapisa deljiva sa 11.

Статијата прв пат е објавена во списанието Математички лист на ДМ на Србија