MLADI NADARENI MATEMATIČARI
Marin Getaldić

Kongruencije

18.10.2015.

Uvod/teorijske osnove

Neka je $n \in \mathbb{N}$ i $a, b \in \mathbb{Z}$. Kažemo da je a **kongruentan** b **modulo** n i pišemo

$$a \equiv b \pmod{n}$$

ako je razlika brojeva a i b djeljiva sa n, $n|a-b$. Dakle, a je kongruentan b modulo n ako i samo ako brojevi a i b daju isti ostatak pri dijeljenju sa n.

Primjer 1. *Vrijedi:*

$$15 \equiv 7 \pmod{8},\ 15 \equiv 23 \pmod{8},\ 15 \equiv -17 \pmod{8},$$
$$-23 \equiv 5 \equiv 19 \equiv 75 \equiv -37 \pmod{14},$$
$$11 \equiv 121 \equiv -33 \equiv 0 \pmod{11}.$$

Uočimo da za svaki $n \in \mathbb{N}$ i sve $a, b, c \in \mathbb{Z}$ direktno iz definicije kongruentnosti slijedi

- $a \equiv a \pmod{n}$,
- ako je $a \equiv b \pmod{n}$, onda je $b \equiv a \pmod{n}$,
- ako je $a \equiv b \pmod{n}$ i $b \equiv c \pmod{n}$, onda je $a \equiv c \pmod{n}$.

Sljedeći teorem nam govori kako računamo s kongruencijama:

Teorem 1. *Za svaki $n \in \mathbb{N}$ i sve $a, a_1, a_2, b, b_1, b_2 \in \mathbb{Z}$ vrijede sljedeće tvrdnje:*

(a) *ako je $a_1 \equiv b_1 \pmod{n}$ i $a_2 \equiv b_2 \pmod{n}$, onda $a_1 + a_2 \equiv b_1 + b_2 \pmod{n}$,*

(b) *ako je $a_1 \equiv b_1 \pmod{n}$ i $a_2 \equiv b_2 \pmod{n}$, onda $a_1 \cdot a_2 \equiv b_1 \cdot b_2 \pmod{n}$,*

(c) *ako je $a \equiv b \pmod{n}$ i $m \in \mathbb{N}$, onda je $a^m \equiv b^m \pmod{n}$,*

(d) *ako je $ac \equiv bc \pmod{n}$ i $(c, n) = 1$, onda je $a \equiv b \pmod{n}$; općenito vrijedi $ac \equiv bc \pmod{n}$ ako i samo ako je $a \equiv b \pmod{\frac{n}{(c,n)}}$, pri čemu s (c, n) označavamo najveći zajednički djelitelj brojeva c i n,*

(e) *ako je f polinom s cjelobrojnim koeficijentima i $a \equiv b \pmod{n}$, onda je $f(a) \equiv f(b) \pmod{n}$.*

Dokaz teorema. Najprije uočimo da je tvrdnja (c) direktna posljedica tvrdnje (b), dok je tvrdnja (e) direktna posljedica tvrdnji (a) i (b). Ovdje ćemo dokazati samo tvrdnju (d), i to drugi, općenitiji dio te tvrdnje. Uočimo da ova tvrdnja sadrži frazu "ako i samo ako". Općenito, tvrdnja "A vrijedi ako i samo ako vrijedi B" označava dvije tvrdnje: "ako vrijedi A, onda vrijedi B" i "ako vrijedi B, onda vrijedi A". Zato ćemo tvrdnju dokazati u dva koraka: u prvom koraku pretpostavimo da vrijedi prvi dio tvrdnje i dokazivati da vrijedi drugi, a u drugom ćemo koraku dokazivati obrat, pretpostavit ćemo da vrijedi drugi dio tvrdnje, a dokazivat ćemo da vrijedi prvi dio (u dokazu smo te korake označili uokvirenim strelicama kako bismo znali koji smjer tvrdnje dokazujemo). A sada možemo sprovesti dokaz.
Stavimo $n_1 = \frac{n}{(c,n)}$, $c_1 = \frac{c}{(c,n)}$ i uočimo da su brojevi c i n relativno prosti, tj. $(c_1, n_1) = 1$.

$\boxed{\Rightarrow}$ Pretpostavimo da vrijedi $ac \equiv bc \pmod{n}$. Tada je, prema definiciji, broj $ac - bc = (a-b)c$ djeljiv sa n, pa postoji prirodan broj k takav da $(a-b)c = kn$. Dijeljenjem ove relacije s (c, n) dobivamo $(a-b)c_1 = kn_1$. Dakle, n_1 dijeli broj $(a-b)c_1$, a kako su brojevi n_1 i c_1 relativno prosti, slijedi da n_1 dijeli $a-b$. Zato, ponovno prema definiciji, slijedi $a \equiv b \pmod{n}$.

$\boxed{\Leftarrow}$ Pretpostavimo sada obratno, tj. $a \equiv b \pmod{n_1}$. Tada, prema definiciji, $n_1 | a-b$, pa slijedi $n_1 c | (a-b)c$. No, budući da je

$$n_1 c = \frac{n}{(c,n)} \cdot c = \frac{c}{(c,n)} \cdot n = c_1 n,$$

imamo $c_1 n | (a-b)c$. Posebno, $n | a-b$, pa po definiciji slijedi $a \equiv b \pmod{n}$.

Zadatci i rješenja

Zadatak 1.
Dokažite tvrdnje (a) i (b) teorema 1.

Zadatak 2.
Nađite ostatak pri dijeljenju broja $3^{100} + 5^{100}$ brojem 7.

Rješenje.
Uočimo da je $3^2 \equiv 2 \pmod{7}$ pa je $3^6 \equiv 2^3 \equiv 1 \pmod{7}$. Zato je $3^{96} \equiv 1^{16} \equiv 1 \pmod{7}$, pa je $3^{100} \equiv 3^4 \equiv 2^2 \equiv 4 \pmod{7}$.
Nadalje, $5 \equiv -2 \pmod{7}$, pa $5^3 \equiv -8 \equiv -1 \pmod{7}$. Zato $5^{99} \equiv (-1)^{33} \equiv -1 \pmod{7}$, a odavde slijedi $5^{100} \equiv -5 \equiv 2 \pmod{7}$. Konačno, $3^{100} + 5^{100} \equiv 4 + 2 \equiv 6 \pmod{7}$.

Zadatak 3.
Nađite posljednju znamenku broja 7^{7^7}.

Zadatak 4.
Nađite ostatak pri dijeljenju broja $(7^{2014})^{2015} - (3^{2014})^{2015}$ brojem 11.

Zadatak 5.
Nađite sve prirodne brojeve m, n koji zadovoljavaju jednadžbu

$$4^m - 9n = 5.$$

Zadatak 6.
Dokažite sljedeći kriterij djeljivosti brojem 11: prirodan broj je djeljiv brojem 11 ako i samo ako mu je razlika zbroja znamenki na parnim i zbroja znamenki na neparnim mjestima djeljiva s 11.

Zadatak 7.
Nađite sve cijele brojeve x, y koji zadovoljavaju sljedeću **diofantsku jednadžbu**:

$$3x + 5y = 8.$$

Rješenje.
Ako izrazimo x preko y, dobivamo $x = \frac{8-5y}{3}$. Budući da je x cijeli broj, mora biti $8 - 5y \equiv 0 \pmod{3}$, odnosno $5y \equiv 5 \pmod{3}$. Budući da je $(5,3) = 1$, dijeljenjem ove kongruencije s 5 (koristimo tvrdnju (c) teorema 1) slijedi $y \equiv 1 \pmod{3}$. Dakle, $y = 3t + 1$ za $t \in \mathbb{Z}$. Uvrštavanjem u gornji izraz za x dobivamo $x = \frac{8-5(3t+1)}{3} = 1 - 5t$. Dakle, jednadžbu zadovoljavaju svi parovi oblika $(x, y) = (1 - 5t, 3t + 1)$, $t \in \mathbb{Z}$.

Zadatak 8.
Nađite sve cijele brojeve a, b koji zadovoljavaju diofantsku jednadžbu:

$$3x + 4y = 29.$$

Zadatak 9.
Nađite sve cijele brojeve x i y koji zadovoljavaju jednadžbu

$$x^2 + y^2 = 2015$$

Rješenje.
Hint: odredite čemu sve može biti kvadrat cijelog broja kongruentan modulo 4, tzv. *kvadratne ostatke modulo 4.*

Zadatak 10.
Dokažite da jednadžba

$$15x^2 - 7y^2 = 9$$

nema rješenja u skupu prirodnih brojeva.

Zadatak 11.
Nađite sve prirodne brojeve n takve da je $n! + 5$ potpun kub.
Napomena: broj $n!$ čitamo "n faktorijela" i on označava umnožak svih prirodnih brojeva od 1 do n: $n! = 1 \cdot 2 \cdot \cdots \cdot (n-1) \cdot n$.

Rješenje.
Hint: uočite da je broj $n!$ za $n \geqslant 6$ djeljiv s 9 te odredite čemu sve može biti kub cijelog broja kongruentan modulo 9, tzv. *kubne ostatke modulo 9.*

Rješenja nekih zadataka

Rješenje zadatka 1. Neka je $a_1 \equiv b_1 \pmod{n}$ i $a_2 \equiv b_2 \pmod{n}$. Tada $n|a_1 - b_1$ i $n|a_2 - b_2$. Zato $n|(a_1 - b_1) + (a_2 - b_2)$, tj. $n|(a_1 + b_1) - (a_2 + b_2)$, pa $a_1 + b_1 \equiv a_2 + b_2 \pmod{n}$, što je tvrdnja (a).
Nadalje,

$$a_1b_1 - a_2b_2 = a_1b_1 - a_1b_2 + a_1b_2 - a_2b_2 = a_1(b_1 - b_2) + b_2(a_1 - a_2),$$

pa zbog $n|a_1 - b_1$ i $n|a_2 - b_2$ slijedi $n|a_1b_1 - a_2b_2$. Dakle, $a_1b_1 \equiv a_2b_2 \pmod{n}$, što je tvrdnja (c) teorema.

Rješenje zadatka 3. Uočimo da trebamo naći ostatak pri dijeljenju broja 7^{7^7} brojem 10.Vrijedi

$$7 \equiv 7,\ 7^2 \equiv 9,\ 7^3 \equiv 7 \cdot 9 \equiv 3,\ 7^4 \equiv 7 \cdot 3 \equiv 1,\ 7^5 \equiv 7,\ \ldots \pmod{10}$$

Dakle, ostatci potencija broja 7 pri dijeljenju s 10 će se ponavljati, i to na sljedeći način

$$7^{4k} \equiv 3 \pmod{10},$$
$$7^{4k+1} \equiv 1 \pmod{10},$$
$$7^{4k+2} \equiv 7 \pmod{10},$$
$$7^{4k+3} \equiv 9 \pmod{10}.$$

Dakle, da bismo odredili posljednju znamenku broja 7^{7^7}, trebamo odrediti ostatak pri dijeljenju eksponenta 7^7 s 4. No, $7 \equiv -1 \pmod{4}$, pa $7^7 \equiv (-1)^7 \equiv -1 \equiv 3 \pmod{4}$. Dakle, $7^{7^7} \equiv 9 \pmod{10}$, pa je posljednja znamenka ovog broja 9.

Rješenje zadatka 5. Jednadžbu možemo zapisati u obliku $4^m = 9n + 5$. Odredimo sada sve moguće ostatke potencije broja 4 pri dijeljenju brojem 9:

$$4 \equiv 4,\ 4^4 \equiv 16 \equiv 7,\ 4^3 \equiv 28 \equiv 1,\ 4^4 \equiv 4,\ \ldots \pmod{9}$$

Dakle,

$$4^{3k} \equiv 1 \pmod{9},$$
$$4^{3k+1} \equiv 4 \pmod{9},$$
$$4^{3k+2} \equiv 7 \pmod{9}.$$

Odavde vidimo da ne postoji prirodan broj m takav da $4^m \equiv 5 \pmod{9}$, pa zaključujemo kako zadana jednadžba nema rješenja u skupu prirodnih brojeva.

Rješenje zadatka 6. Uzmimo neki prirodan broj i zapišimo ga kao

$$n = \overline{a_k a_{k-1} \cdots a_1 a_0} = a_k \cdot 10^k + a_{k_1} \cdot 10^{k-1} + \ldots + a_1 \cdot 10 + a_0,$$

gdje su $a_k, \ldots, a_0$ znamenke broja n. Uočimo da vrijedi $10 \equiv -1 \pmod{11}$, pa je $10^m \equiv -1 \pmod{11}$ za neparan m i $10^m \equiv 1 \pmod{11}$ za paran m. Zato imamo

$$\begin{aligned} n &\equiv a_0 + a_1 \cdot 10 + a_2 \cdot 10^2 + a_3 \cdot 10^3 + a_4 \cdot 10^4 + a_5 \cdot 10^5 + \ldots \pmod{11} \\ &\equiv a_0 + a_1 \cdot (-1) + a_2 \cdot 1 + a_3 \cdot (-1) a_4 \cdot 1 + a_5 \cdot (-1) + \ldots \pmod{11} \\ &\equiv (a_0 + a_2 + a_4 + \ldots) - (a_1 + a_3 + a_5 + \ldots) \pmod{11} \end{aligned}$$

Odavde slijedi navedeni kriterij; zapravo možemo zaključiti i nešto više: ostatak pri dijeljenju prirodnog broja brojem 11 jednak je ostatku pri dijeljenju razlike zbroja njegovih znamenki na parnim i neparnim mjestima brojem 11.

Rješenje zadatka 9. Imamo

$$\begin{aligned} n &\equiv 0 \pmod 4 \Rightarrow n^2 \equiv 0 \pmod 4, \\ n &\equiv 1 \pmod 4 \Rightarrow n^2 \equiv 1 \pmod 4, \\ n &\equiv 2 \pmod 4 \Rightarrow n^2 \equiv 0 \pmod 4, \\ n &\equiv 3 \pmod 4 \Rightarrow n^2 \equiv 1 \pmod 4. \end{aligned}$$

Dakle, svi kvadratni ostatci modulo 4 su 0 i 1. Zato vidimo da zbroj kvadrata dvaju cijelih brojeva može biti kongruentan 0, 1 ili 2 modulo 4. Budući da je $2015 \equiv 3 \pmod 4$, zadana jednadžba nema rješenja u skupu cijelih brojeva.

Rješenje zadatka 10. Pretpostavimo suprotno. Uočimo da u tom slučaju mora biti $3|y^2$, odnosno $3|y$. Ako je $y = 3y_1$, dijeljenjem jednadžbe s 3 dobivamo

$$5x^2 - 21y_1^2 = 3.$$

No sada mora biti $3|x$, pa uz $x = 3x_1$ ponovnim dijeljenjem jednadžbe s 3 imamo

$$15x_1^2 - 7y_1^2 = 1.$$

No, odavde bi slijedilo (zbog $7y_1^2 \equiv y_1^2 \pmod 3$)

$$7y_1^2 \equiv -1 \equiv 2 \pmod 3 \Rightarrow y_1^2 \equiv 2 \pmod 3.$$

No, 2 nije kvadratni ostatak modulo 3. Kontradikcija.