

# Kongruencije

Matko Šimić, Zagreb

## Uvod

Još u osnovnoj školi učenike se upoznaje s pojmovima djeljivosti, višekratnika te dijeljenja s ostatkom. Kasnije, uvođenjem skupa racionalnih brojeva, pomalo se zanemaruje baratanje s ostacima pri dijeljenju, a time i moćan alat teorije brojeva – **kongruencije**. Kongruencije osim u teorijskoj matematici imaju i široku primjenu u kriptografiji i računalnom otkrivanju grešaka, ali i u svakodnevnom životu. Jedan takav primjer je mjerenje vremena. Dijeljenje dana na 24 sata nakon čega brojenje kreće iznova je zapravo aritmetika u modulu 24. Čak je i zapadni glazbeni sustav utemeljen na modularnoj aritmetici s obzirom na to da raspoznamo 12 tonova, po visini poredani od C do H, nakon čega ponovno krećemo s tonom C.

## Definicije i svojstva

**Definicija.** Za cijele brojeve  $a$  i  $b$  kažemo da  $a$  *dijeli*  $b$  (odnosno da je  $b$  djeljiv s  $a$ ), u oznaci  $a \mid b$ , ako postoji cijeli broj  $k$  takav da vrijedi  $b = a \cdot k$ . Ako  $a \mid b$ , tada kažemo da je  $a$  *djelitelj* od  $b$  te da je  $b$  *višekratnik* od  $a$ .

**Definicija.** Za cijele brojeve  $a$  i  $b$  te prirodan broj  $n$  kažemo da je broj  $a$  **kongruentan** broju  $b$  **modulo**  $n$  ako  $n$  dijeli razliku  $a - b$  te tada pišemo  $a \equiv b \pmod{n}$ . Također,  $a$  je kongruentno  $b$  modulo  $n$  ako i samo ako  $a$  i  $b$  daju isti ostatak pri dijeljenju s  $n$ .



Iz definicije sada vidimo da na primjer:

$$\begin{aligned} 15 &\equiv 7 \pmod{8}, 15 \equiv 31 \pmod{8} \\ 15 &\equiv -17 \pmod{8}, 18 \equiv 0 \pmod{6} \\ 60 &\equiv 18 \pmod{6}, 6 \equiv 600 \pmod{6}. \end{aligned}$$

Relacija *biti kongruentan modulo*  $n$  je relacija ekvivalencije, što nam omogućuje slijedno rješavanje zadataka.

**Definicija.** Neka je  $n$  prirodan broj i  $a_1, a_2, \dots, a_n$  cijeli brojevi takvi da vrijedi:

$$\begin{aligned} a_1 &\equiv 1 \pmod{n} \\ a_2 &\equiv 2 \pmod{n} \\ &\vdots \\ a_{n-1} &\equiv n-1 \pmod{n} \\ a_n &\equiv 0 \pmod{n}. \end{aligned}$$

Tada skup  $\{a_1, a_2, \dots, a_n\}$  zovemo *potpun sustav ostataka modulo*  $n$ .

Za svaki prirodan broj  $n$  i cijele brojeve  $a, a_1, a_2, b, b_1, b_2, c$  direktno iz definicije se pokazuju i sljedeća svojstva:

- Ako je  $a_1 \equiv b_1 \pmod{n}$  i  $a_2 \equiv b_2 \pmod{n}$ , tada  $a_1 + a_2 \equiv b_1 + b_2 \pmod{n}$ .
- Ako je  $a_1 \equiv b_1 \pmod{n}$  i  $a_2 \equiv b_2 \pmod{n}$ , tada  $a_1 \cdot a_2 \equiv b_1 \cdot b_2 \pmod{n}$ , posebno  $a_1 \cdot c \equiv b_1 \cdot c \pmod{n}$ .
- Ako je  $a \equiv b \pmod{n}$  i  $m$  prirodan broj, tada  $a^m \equiv b^m \pmod{n}$ .
- Ako je  $a \cdot c \equiv b \cdot c \pmod{n}$  i ako su  $c$  i  $n$  relativno prosti brojevi, tada  $a \equiv b \pmod{n}$ .
- Ako je  $a \equiv b \pmod{n}$  i  $f$  polinom s cjelobrojnim koeficijentima, tada  $f(a) \equiv f(b) \pmod{n}$ .

## Primjeri

Postoji mnogo tipova zadataka u čijem rješavanju moramo promatrati neke kongruentnosti, ostatke i djeljivosti te ih obično nije teško prepoznati. Na natjecanjima se u takvim zadacima obično eksplicitno traži da se pokaže kako je jedan izraz djeljiv (ili nije) s drugim ili da odredimo ostatak pri dijeljenju. Pronalazak zadnje ili zadnjih nekoliko znamenaka je također čest tip zadatka u kojem trebamo promatrati broj modulo 10 (ili potencija broja 10). Nešto je teže primijetiti da su kongruencije dobra taktika rješavanja zadataka u kojima se traže rješenja neke diofantske ili druge algebarske jednačbe.

Ako vrijedi  $a \equiv b \pmod{n}$  i  $b \equiv c \pmod{n}$ , možemo upotrijebiti ekvivalentan, kraći zapis  $a \equiv b \equiv c \pmod{n}$ .

**Primjer 1.** Pronađite posljednju znamenku broja  $7^{11^5}$ .

*Rješenje.* Možemo primijetiti kako je traženje posljednje znamenke broja jednako traženju ostatka pri dijeljenju s 10 te tražimo uzorak u ostacima pri dijeljenju potencija broja 7 s 10.

Računamo ostatke pri dijeljenju potencija broja 7 s

10:

$$\begin{aligned} 7 &\equiv 7 \pmod{10} \\ 7^2 &\equiv 9 \pmod{10} \\ 7^3 &\equiv 7 \cdot 7^2 \equiv 7 \cdot 9 \equiv 3 \pmod{10} \\ 7^4 &\equiv 7 \cdot 7^3 \equiv 7 \cdot 3 \equiv 1 \pmod{10} \\ 7^5 &\equiv 7 \cdot 7^4 \equiv 7 \cdot 1 \equiv 7 \pmod{10}. \end{aligned}$$

Zbog svojstava kongruencija ostatci će se ponavljati u istom poretku tako da za  $k \in \mathbb{N}_0$ :

$$\begin{aligned} 7^{4k} &\equiv 1 \pmod{10} \\ 7^{4k+1} &\equiv 7 \pmod{10} \\ 7^{4k+2} &\equiv 9 \pmod{10} \\ 7^{4k+3} &\equiv 3 \pmod{10} \end{aligned}$$

stoga moramo pronaći ostatak pri dijeljenju broja  $11^5$  s 4. Vrijedi  $11 \equiv -1 \pmod{4}$  pa  $11^5 \equiv (-1)^5 \equiv -1 \equiv 3 \pmod{4}$  i konačno zaključujemo  $7^{11^5} \equiv 3 \pmod{10}$ .

**Primjer 2.** Dokažite da kvadrat cijelog broja pri dijeljenju s 3 može isključivo dati ostatke 0 ili 1.

*Rješenje.* Prvo možemo primijetiti da broj pri dijeljenju s 3 može dati ostatke 0, 1 ili 2 (odnosno da je skup  $\{0, 1, 2\}$  potpun sustav ostataka modulo 3).

Sada zadatak možemo podijeliti u 3 slučaja, ovisno o tome koji ostatak prirodan broj  $n$  daje pri dijeljenju s 3.

1. slučaj:  $n \equiv 0 \pmod{3}$ . Zaključujemo

$$n^2 \equiv 0^2 \equiv 0 \pmod{3}.$$

2. slučaj:  $n \equiv 1 \pmod{3}$ . Zaključujemo

$$n^2 \equiv 1^2 \equiv 1 \pmod{3}.$$

3. slučaj:  $n \equiv 2 \pmod{3}$ . Zaključujemo

$$n^2 \equiv 2^2 \equiv 1 \pmod{3}.$$

Stoga tvrdnja zadatka vrijedi u sva tri slučaja.

**Primjer 3.** Za koje cijele brojeve  $x$  vrijedi

$$2x + 3 \equiv 4 \pmod{7}?$$

**Rješenje.**  $2x + 3 \equiv 4 \pmod{7}$ . Nakon što od obje strane kongruencije oduzmemo 3, dobivamo  $2x \equiv 1 \pmod{7}$ . Budući da taj izraz želimo podijeliti s 2, zapisat ćemo ga tako da se na desnoj strani nalazi paran broj, odnosno  $2x \equiv 1 \equiv 8 \pmod{7}$ . S obzirom na to da su 2 i 7 relativno prosti, kongruenciju smijemo podijeliti s 2 iz čega slijedi  $x \equiv 4 \pmod{7}$ .

**Primjer 4.** Koji parovi  $(m, n)$  prirodnih brojeva zadovoljavaju jednadžbu  $2^m - 3^n = 1$ ?

**Rješenje.** Vrijedi  $2^m = 3^n + 1$ . Kako je  $2 \equiv -1 \pmod{3}$  te  $1 \equiv 3^n + 1 = 2^m \equiv (-1)^m \pmod{3}$ ,  $m$  mora biti paran. Tada  $m$  možemo zapisati kao  $m = 2 \cdot m_1$ , za neki  $m_1 \in \mathbf{N}$ , a danu jednadžbu u obliku  $(2^{m_1} - 1)(2^{m_1} + 1) = 3^n$ . Sada slijedi da su i  $2^{m_1} - 1$  i  $2^{m_1} + 1$  potencije broja 3.  $2^{m_1} - 1$  i  $2^{m_1} + 1$  se razlikuju točno za 2, stoga je jedina mogućnost  $2^{m_1} - 1 = 1$  i  $2^{m_1} + 1 = 3$ , odnosno da je  $m_1 = 1$ . Zaključujemo da je jedino rješenje  $(m, n) = (2, 1)$ .

**Primjer 5.** Pronađite sve proste brojeve  $p$  i  $q$  takve da  $p^2 - 2q^2 = 1$ .

**Rješenje.** Prvo moramo uočiti da je za sve proste  $p, q > 3$ ,  $p \equiv 1$  ili  $-1 \pmod{6}$ . Razlikujemo sada dva slučaja.

1. *slučaj:* Za  $p > 3$  i  $q > 3$  slijedi da je  $p^2 \equiv 1 \pmod{6}$ . Isto tako je  $q^2 \equiv 1 \pmod{6}$  pa je  $p^2 - 2q^2 \equiv 1 - 2 = -1 \equiv 5 \pmod{6}$ . Desna strana jednadžbe je kongruentna  $1 \pmod{6}$ , stoga jednadžba nema rješenja za  $p, q > 3$ .

2. *slučaj:* Jedan od brojeva  $p, q$  je 2 ili 3. Ako je  $p = 2$ , dobivamo da je  $2q^2 = 4 - 1 = 3$  što nema rješenja u cijelim brojevima. Slično za  $p = 3$  dobivamo da je  $p^2 = 1 + 18 = 19$ , što isto nema rješenja u cijelim brojevima. U preostala dva slučaja rješavanjem kvadratne jednadžbe dobivamo isto rješenje,  $(p, q) = (3, 2)$ .

Dakle, jedino rješenje je  $(p, q) = (2, 3)$ .

**Primjer 6.** Dokažite da  $n^2 + 3n + 5$  nije djeljivo sa 121.

**Rješenje.** Pretpostavimo suprotno, odnosno da je  $n^2 + 3n + 5$  djeljivo sa 121. Tada je posebno taj broj djeljiv i s 11. Budući da je  $(n-4)^2 \equiv n^2 - 8n + 16 \equiv n^2 + 3n + 5 \equiv 0 \pmod{11}$ , slijedi da je  $(n-4)^2$  djeljivo s 11. Posebno,  $n-4$  je djeljivo s 11, odnosno  $n = 11k + 4$ , za neki cijeli broj  $k$ . Slijedi da je  $n^2 + 3n + 5 \equiv (11k+4)^2 + 3(11k+4) + 5 \equiv 121k^2 + 121k + 33 \equiv 33 \pmod{121}$ , što je u kontradikciji s pretpostavkom da je  $n^2 + 3n + 5$  djeljivo sa 121. Time smo dokazali tvrdnju zadatka.

**Primjer 7.** Neka je  $a$  prirodan broj veći od 1. Dokažite da je broj

$$n(2n+1)(3n+1) \cdots (an+1)$$

djeljiv sa svim prostim brojevima manjim od  $a$ , za svaki prirodan broj  $n$ .

*Županijsko natjecanje 2009., 4. raz., A varijanta*

**Rješenje.** Neka je  $p$  prost broj manji od  $a$ . Ako je  $n$  djeljiv s  $p$ , očito je promatrani umnožak djeljiv s  $n$ . Pretpostavimo da  $n$  nije djeljiv s  $p$ . Tada brojevi  $2n+1, 3n+1, \dots, (p+1)(n+1)$  daju redom ostatke  $r_1, r_2, r_p$  pri dijeljenju s  $p$ . Kada bi vrijedilo  $r_i = r_j$  za neki  $i, j \in \{1, 2, \dots, p\}, i \neq j$ , onda bi razlika

$$((i+1)n+1) - ((j+1)n+1) = (i-j)n$$

bila djeljiva s  $p$ . Međutim, kako po pretpostavci  $p$  ne dijeli  $n$ , broj  $i-j$  mora biti djeljiv s  $p$ , što je nemoguće jer je  $1 \leq |i-j| < p$ . Zaključujemo da su svi ostatci različiti. Kako imamo  $p$  različitih ostataka, skup  $\{r_1, r_2, \dots, r_p\}$  je potpun sustav ostataka modulo  $p$ , pa je jedan od ostataka jednak nuli. Stoga je i promatrani umnožak djeljiv s  $p$ .

**Primjer 8.** Je li moguće posložiti brojeve  $1^1, 2^2, \dots, 2008^{2008}$  jedan za drugim tako da broj dobiven spajanjem znamenaka bude kvadrat nekog prirodnog broja? (Na primjer, broj dobiven spajanjem  $3^3 1^1 2^2$  je 2714.)

**Rješenje.** Za bilo koji takav raspored možemo pronaći nenegativne cijele brojeve  $x_1, x_2, \dots, x_{2008}$  takve da je dobiveni broj jednak  $1^1 \cdot 10^{x_1} + 2^2 \cdot 10^{x_2} + \dots + 2008^{2008} \cdot 10^{x_{2008}}$ . Na primjer, za raspored  $3^3 1^1 2^2 = 2714$ , vrijedi  $2714 = 3^3 \cdot 10^2 + 1^1 \cdot 10^1 + 2^2 \cdot 10^0$ .

Kako je  $10 \equiv 1 \pmod{3}$  vrijedi  $1^1 \cdot 10^{x_1} + 2^2 \cdot 10^{x_2} + \dots + 2008^{2008} \cdot 10^{x_{2008}} \equiv 1^1 + 2^2 + \dots + 2008^{2008} \pmod{3}$ .

Lako se provjeri da vrijede sljedeće tvrdnje:

Ako je  $a \equiv 0 \pmod{3}$  onda  $a^a \equiv 0 \pmod{3}$ .

Ako je  $a \equiv 1 \pmod{3}$  onda  $a^a \equiv 1 \pmod{3}$ .

Ako je  $a \equiv 2 \pmod{3}$  i  $a$  paran onda  $a^a \equiv 1 \pmod{3}$ .

Ako je  $a \equiv 2 \pmod{3}$  i  $a$  neparan onda  $a^a \equiv 2 \pmod{3}$ .

Koristeći se gore navedenim tvrdnjama, vidimo da izraz  $1^1 + 2^2 + 3^3 + 4^4 + 5^5 + 6^6 + 7^7 \equiv 0 \pmod{3}$ . Analogno  $8^8 + \dots + 14^{14} \equiv 0 \pmod{3}$  pa vrijedi  $1^1 + 2^2 + \dots + 2008^{2008} \equiv 2003^{2003} + 2004^{2004} + 2005^{2005} + 2006^{2006} + 2007^{2007} \equiv 2 \pmod{3}$ . Međutim, po primjeru 2., kvadrat cijelog broja ne može dati ostatak 2 pri dijeljenju s 3. Stoga zaključujemo da nije moguće posložiti brojeve  $1^1, 2^2, \dots, 2008^{2008}$  jedan za drugim tako da je dobiveni broj kvadrat nekog prirodnog broja.

### Zadatci za vježbu

Slijedi izbor zadataka za vježbu koji se rješavaju uz pomoć kongruencija. Podsjećamo da su dobre taktike rješavanja: promatrati izraz u odnosu na ostatak modulo neki  $n$ , iskoristiti oblik broja u daljnjoj jednadžbi (npr. znamo li da je  $a$  oblika  $3k+1$ , onda u zadani izraz umjesto  $a$  uvrstiti  $3k+1$ ). Ne zaboravimo da je korisno preurediti kongruenciju koristeći se svojstvima kongruencija navedenih u uvodu, pri čemu posebno oprezni trebamo biti pri dijeljenju kongruencija. Navedeni zadatci su dobar temelj za rješavanje zadataka iz teorije brojeva bez naprednijih alata poput Eulerova teorema, malog Fermatova teorema ili kineskog teorema o ostatcima.

1. Odredite posljednjih 2019 znamenaka broja  $2^{2019} \cdot 5^{2018} \cdot 9^{2017}$ .

*Općinsko natjecanje 2019., 3. raz., A varijanta*

2. Pronađite sve proste brojeve  $p$  takve da su i  $2p+1$  i  $4p+1$  prosti brojevi.

*Rješenje: Jedini takav broj je 3. Promatrajte  $2p+1$  i  $4p+1$  u odnosu na ostatak koji  $p$  daje pri dijeljenju s 3.*

3. Dokažite da je zbroj kubova triju uzastopnih cijelih brojeva djeljiv s 9.

*Uputa: raspisati zbroj kubova i promatrati izraz modulo 9.*

4. Dokažite da je za svaki prirodan broj  $n$  broj  $n^{19} - n^7$  djeljiv s 30.

*Županijsko natjecanje 2008., 1. raz., A varijanta*

5. Neka je  $n$  prirodni broj i neka je  $S$  zbroj svih prirodnih brojeva od 1 do  $n$ . Dokažite da broj  $S$  ne može biti za 1 manji od višekratnika broja 3.

*Županijsko natjecanje 2014., 2. raz., A varijanta*

6. Dokažite da ne postoje prirodni brojevi  $m$  i  $n$  takvi da je  $3^m + 3^n + 1$  kvadrat prirodnog broja.

*Državno natjecanje 2014., 2. raz., A varijanta*

7. Pronađite sve prirodne brojeve  $n$  takve da je  $n^n - 3$  djeljivo s 10.

*Školsko natjecanje 2016., 3. raz., A varijanta*

8. Neka je  $n$  prirodan broj takav da je  $n+1$  djeljiv s 24.

a) Dokažite da  $n$  ima paran broj djelitelja.

b) Dokažite da je zbroj djelitelja broja  $n$  djeljiv s 24.

*Državno natjecanje 2007., 3. i 4. raz., A varijanta*

9. Postoji li prirodan broj  $n$  takav da je  $8^n + 47$  prost broj?

*JBMO Shortlist 2020.*

### LITERATURA

1/ Zadatci s natjecanja iz matematike, <http://www.antonija-horvatek.from.hr/natjecanja-iz-matematike>

2/ Predavanja udruge Mladi nadareni matematičari "Marin Getaldić", <https://mm.hr/online-predavanja>

3/ A. Engel (1998.): *Problem Solving Strategies*, Springer

4/ Art of Problem Solving, <https://artofproblemsolving.com/community>