



Uvod

Neka su $a, b \in \mathbb{Z}$, $n \in \mathbb{N}$. Kažemo da je broj a **kongruentan** broju b **modulo** n ako vrijedi $n \mid a - b$ (čitaj: n dijeli razliku a i b). To pišemo kao $a \equiv b \pmod{n}$. Na primjer:

- $7 \equiv 1 \pmod{2}$
- $9 \equiv 4 \equiv -1 \pmod{5}$
- $15 \equiv \pm 3 \pmod{6}$

Možemo zaključiti: a je kongruentan b modulo n **ako i samo ako** a i b daju isti ostatak pri dijeljenju sa n .

Osnovna svojstva kongruencija slijede direktno iz svojstava djeljivosti. Za $a, b, c, d \in \mathbb{Z}$ i $n \in \mathbb{N}$ vrijedi sljedeće:

- $a \equiv a \pmod{n}$
- $a \equiv b \pmod{n} \Rightarrow b \equiv a \pmod{n}$
- $a \equiv b \pmod{n}$ i $b \equiv c \pmod{n} \Rightarrow a \equiv c \pmod{n}$
- $a \equiv b \pmod{n}$ i $c \equiv d \pmod{n} \Rightarrow a \pm c \equiv b \pm d \pmod{n}$
- $a \equiv b \pmod{n}$ i $c \equiv d \pmod{n} \Rightarrow ac \equiv bd \pmod{n}$
- $a \equiv b \pmod{n} \Rightarrow a^k \equiv b^k \pmod{n}$ za $k \in \mathbb{N}$
- $ac \equiv bc \pmod{n}$ i $\gcd(c, n) = 1 \Rightarrow a \equiv b \pmod{n}$; općenitije, $ac \equiv bc \pmod{n} \Rightarrow a \equiv b \pmod{\frac{n}{\gcd(n, c)}}$

Zagrijavanje

Ovi zadaci služe za dokazivanje nekih osnovnih tvrdnji koje se koriste u zadacima. Ako ste ih već vidjeli, slobodno preskočite.

1. Dokaži da kvadrat cijelog broja daje ostatak 0 ili 1 pri dijeljenju s 3/pri dijeljenju s 4.
2. Dokaži da za $b \in \mathbb{N}$ i $k \in \mathbb{N}$, $b^k \equiv 1$ ili $-1 \pmod{b+1}$.
3. Dokaži da je svaki prost broj veći od 3 oblika $6k+1$ ili $6k-1$, $k \in \mathbb{N}$.
4. Dokaži da kub cijelog broja daje ostatak 0, 1 ili 6 pri dijeljenju sa 7.

Lakši zadaci

5. Za koje $x \in \mathbb{Z}$ vrijedi $2x + 3 \equiv 4 \pmod{7}$?
6. Pokaži da 4 ne dijeli $n^2 + 2n - 1$ za sve prirodne brojeve n .
7. Dokažite da niti jedan član niza $a_n = 4^n + \frac{5 + (-1)^n}{2}$ nije kvadrat prirodnog broja.
8. Nađi sve proste brojeve p za koje su $2p+1$ i $4p+1$ isto prosti.

9. Neka su a, b, c prirodni brojevi takvi da $6 \mid a + b + c$. Dokaži da $6 \mid a^3 + b^3 + c^3$.
10. Odredi posljednjih 2019 znamenki broja $2^{2019} \cdot 5^{2018} \cdot 9^{2017}$.
11. Nađi sve $x, y \in \mathbb{Z}$ takve da je $15x^2 - 7y^2 = 1$.
12. Dokaži da $13 \mid 2^{12n+9} - 5^{4n+1}$ za $n \in \mathbb{N}$.
13. Nađi sve prirodne brojeve n i m takve da je $n^2 - 7m^2 = 28$.

Teži zadaci

14. Nađi sve $n \in \mathbb{Z}$ za koje postoje cijeli brojevi a i b takvi da je $n = \frac{2a^3 - 5b^3 - 1}{7}$.
15. Nađi sve proste brojeve p, q, r takve da je $p^{2q} + q^{2p} = r$.
16. Dokaži da ne postoje prirodni brojevi m i n takvi da je $3^m + 3^n + 1$ kvadrat prirodnog broja.
17. Nađi sve proste brojeve p i q takve da je $p^2 - 2q^2 = 1$.
18. Nađi sve prirodne brojeve n takve da je $n^n - 3$ djeljivo s 10.
19. Ako su za $n \in \mathbb{N}$ $2n + 1$ i $3n + 1$ kvadrati prirodnih brojeva, dokaži da je n djeljiv s 40.
20. Neka je $x = 1 + 2^2 + 3^3 + \dots + 1983^{1983}$. Dokaži da x nije oblika m^k za $m, k \in \mathbb{N}$ i $k \geq 3$.

Hintovi

1. $a \equiv b \pmod{n} \Rightarrow a^k \equiv b^k \pmod{n}$ za $k \in \mathbb{N}$
2. $(b+1) \mid b - (-1) \Rightarrow b \equiv? \pmod{b+1}$
3. Može li neki prost broj biti oblika $6k+2$? A $6k+3$ ili $6k+4$?
4. $a \equiv b \pmod{n} \Rightarrow a^k \equiv b^k \pmod{n}$ za $k \in \mathbb{N}$
5. $\gcd(2, 7) = 1$ pa probajte dobiti na desnoj strani nešto djeljivo s 2.
6. Što ako je n paran, a što ako je neparan? Rastavi na slučajeve.
7. $\frac{5+(-1)^n}{2}$ ima dvije moguće vrijednosti. Prisjetite se tvrdnje 1. zadatka.
8. Modulo 3.
9. Je li $x \equiv x^3 \pmod{2}$ za svaki $x \in \mathbb{Z}$? A $x \equiv x^3 \pmod{3}$?
10. $2^{2019} \cdot 5^{2018} \cdot 9^{2017} = 2 \cdot 9^{2017} \cdot 10^{2018}$. Prisjetite se tvrdnje 2. zadatka.
11. Modulo 3. Prisjetite se 1. zadatka.
12. $2^{12n+9} = 2^{3(4n+3)} = (2^3)^{4n+3}$.
13. $7 \mid 28$ i $7 \mid 7m^2 \dots$
14. Zadatak je ekvivalentan s $7n+1 = 2a^3 - 5b^3$. Što onda zaključujemo o $2a^3 - 5b^3$?
15. Promatrajte parnost brojeva p, q, r .
16. Modulo 8.
17. 3. zadatak
18. Ovisno o $n \pmod{10}$, koje su moguće vrijednosti $n^n \pmod{10}$?
19. Djeljivost s 40 $\iff$ djeljivost s 5 i 8. Koji su kvadratni ostatci modulo 5 i 8?
20. $n^n \pmod{4}$ i $\pmod{8}$

Rješenja

1. Svaki prirodan broj n može davati ostatak 0, 1 ili 2 pri dijeljenju s 3, odnosno zapisano pomoću kongruencija: $n \equiv 0, 1$ ili $2 \pmod{3}$. Znamo da $a \equiv b \pmod{c} \Rightarrow a^k \equiv b^k \pmod{c}$ za svaki $k \in \mathbb{N}$ pa je $n^2 \equiv 0^2, 1^2$ ili $2^2 \pmod{3}$, odnosno $n^2 \equiv 0, 1$ ili $4 \pmod{3}$. Međutim, kako je $4 \equiv 1 \pmod{3}$, onda je $n^2 \equiv 0$ ili $1 \pmod{3}$. Na identičan način dobivamo da je $n^2 \equiv 0, 1, 4$ ili $9 \pmod{4}$, a kako je $4 \equiv 0 \pmod{4}$ i $9 \equiv 1 \pmod{4}$, znači da je $n^2 \equiv 0$ ili $1 \pmod{4}$, što smo i trebali pokazati.
2. Kako je $b \equiv -1 \pmod{b+1}$, slijedi $b^k \equiv (-1)^k \pmod{b+1}$. $(-1)^k$ može poprimiti samo vrijednosti 1 ili -1 , ovisno o parnosti broja k .

3. [Rješenje s math.stackexchange.com](#)

4. Identičan postupak kao i u prvom zadatku.
5. $2x + 3 \equiv 4 \pmod{7} \Rightarrow 2x \equiv 1 \equiv 8 \pmod{7} \Rightarrow x \equiv 4 \pmod{7}$, a zadnji korak smijemo napraviti jer su 2 i 7 relativno prosti.
6. Ako je n paran $n^2 + 2n - 1$ je neparan pa nije djeljiv s 4.
Ako je n neparan, tada je $n \equiv -1, 1 \pmod{4}$, pa je $n^2 + 2n - 1 \equiv (-1)^2 + 2 \cdot (-1) - 1 \equiv -2 \pmod{4}$ ili $n^2 + 2n - 1 \equiv 1^2 + 2 \cdot 1 - 1 \equiv 2 \pmod{4}$, u oba slučaja opet nije djeljivo s 4.

7.

$$a_n = \begin{cases} 4^n + 3 & \text{za } n \equiv 0 \pmod{2}; \\ 4^n + 2 & \text{za } n \equiv 1 \pmod{2}. \end{cases}$$

Budući da su jedini kvadratni ostaci modulo 4 jednaki 1 ili 0, zaključujemo da se u nizu ne nalazi niti jedan potpun kvadrat.

8. Ako je $p \equiv 1 \pmod{3}$, $2p + 1 \equiv 2 + 1 \equiv 3 \equiv 0 \pmod{3}$, odnosno $2p + 1$ je složen broj. Ako je $p \equiv 2 \pmod{3}$, $4p + 1 \equiv 8 + 1 \equiv 9 \equiv 0 \pmod{3}$, odnosno $4p + 1$ je složen broj. Preostaje nam samo slučaj $p \equiv 0 \pmod{3}$, a s obzirom da je p prost broj, $p = 3$ je jedina mogućnost. $2p + 1$ je tada 7, a $4p + 1$ je 13 i to su oboje prosti brojevi pa je $p = 3$ jedino rješenje.
9. Uočavanje $x^3 \equiv x \pmod{2}$ i $x^3 \equiv x \pmod{3} \Rightarrow x^3 \equiv x \pmod{6}$, $\forall x \in \mathbb{N}$, iz čega slijedi tvrdnja zadatka.
10. [Općinsko 2019. - 3. razred, 3. zadatak](#)
11. Promatramo jednadžbu modulo 3. $15x^2 \equiv 0 \pmod{3}$, $1 \equiv 1 \pmod{3}$ pa je $7y^2 \equiv 0 - 1 \equiv -1 \equiv 2 \pmod{3}$. Kako je $7 \equiv 1 \pmod{3}$, slijedi $y^2 \equiv 2 \pmod{3}$ što je nemoguće. Dakle, jednadžba nema rješenja u cijelim brojevima.
12. $2^{12n+9} = 2^{3(4n+3)} = 8^{4n+3} \equiv (-5)^{4n+3} \equiv -(5)^{4n+3} \pmod{13}$.
 $2^{12n+9} - 5^{4n+1} \equiv -(5)^{4n+3} - 5^{4n+1} \equiv -(5)^{4n+1}(25 + 1) \equiv 0 \pmod{13}$.
13. $7 \mid 7m^2$ i $7 \mid 28$ pa $7 \mid n^2 \Rightarrow 7 \mid n$. Neka je $n = 7k, k \in \mathbb{N}$. Dijeljenjem početne jednadžbe sa 7 dobivamo $7k^2 - m^2 = 4$. Kako je $7k^2 \equiv 7 \pmod{7}$, zaključujemo $m^2 \equiv 7 - 4 = 3 \pmod{7}$. Međutim, kvadratni ostaci $\pmod{7}$ su 1, 2, 4 pa ova jednadžba nema rješenja u prirodnim brojevima.
14. Ovaj izraz se može preoblikovati u $7n + 1 = 2a^3 - 5b^3$, odnosno $2a^3 - 5b^3 \equiv 1 \pmod{7}$. Nadalje, $2a^3 - 5b^3 \equiv 2a^3 - 5b^3 + 7b^3 \pmod{7} \Rightarrow 2a^3 - 5b^3 \equiv 2a^3 + 2b^3 \pmod{7} \Rightarrow 2(a^3 + b^3) \equiv 1 \pmod{7}$. Kako je $x^3 \equiv 0, 1$ ili $-1 \pmod{7}$ za svaki $x \in \mathbb{Z}$, slijedi $2(a^3 + b^3) \equiv 0, 2, 3, 4$ ili $5 \pmod{7}$, odnosno $2(a^3 + b^3)$ ne može biti 1 $\pmod{7}$. Zaključujemo da ne postoji n iz zadatka.
15. Uvrštavanjem vidimo da $p = q = 2$ nije rješenje i da je $r > 4$. Pretpostavimo da su i p i q neparni: tada je $p^{2q} + q^{2p}$ parno, odnosno r je paran, prost broj veći od 4 - kontradikcija. Znači da je ili p ili q paran, ali s obzirom da su oba broja prosta i znamo da $p = q = 2$ nije rješenje, točno jedan od ta dva broja je jednak 2. Bez smanjenja općenitosti, neka je $p = 2$ jer je jednadžba simetrična po pitanju p i q (ako je (p, q) rješenje onda je i (q, p)). Početna jednadžba onda postaje

$$2^{2q} + q^4 = r \Rightarrow 4^q + q^4 = r.$$

Nadalje, promotrimo ovaj izraz modulo 5. Kako je $4 \equiv -1 \pmod{5}$, 4^q daje ostatak 1 ili -1 pri dijeljenju s 5, ovisno o parnosti broja q (-1 ako je q neparan, a 1 ako je q paran). Kako smo zaključili da je q neparan, znači da 4^q daje ostatak -1 pri dijeljenju s 5. S druge strane, q^4 daje ostatak 1 ili 0 pri dijeljenju s 5, jer je $1^4 \equiv 2^4 \equiv 3^4 \equiv 4^4 \equiv 1 \pmod{5}$. Sada razlikujemo dva slučaja:

1. *slučaj*: q^4 je djeljiv s 5. Kako je q prost broj, a q^4 je djeljivo s 5 ako i samo ako je q djeljiv s 5, jedina mogućnost je $q = 5$. Preostaje provjeriti je li $4^5 + 5^4 = 1649$ prost broj. Kako je $1649 = 17 \cdot 97$, ovaj slučaj nema rješenja.

2. *slučaj*: q^4 daje ostatak 1 pri dijeljenju s 5. Kako 4^q daje ostatak -1 pri dijeljenju s 5, $4^q + q^4 \equiv -1 + 1 \equiv 0 \pmod{5}$, odnosno r je djeljiv s 5. S obzirom da je r prost broj, $r = 5$ je jedina mogućnost. Međutim, jednačba $4^q + q^4 = 5$ nema rješenje u prostim brojevima jer $q = 1$ nije prost broj.

Zaključujemo da ne postoje prosti brojevi p, q, r takvi da je $p^{2q} + q^{2p} = r$.

16. Državno 2014. - 2. razred 3. zadatak

17. Za sve $p, q > 3$, $p \equiv 1$ ili $-1 \pmod{6}$ pa je $p^2 \equiv 1 \pmod{6}$, isto tako je $q^2 \equiv 1 \pmod{6}$ pa je $p^2 - 2q^2 \equiv 1 - 2 \equiv -1 \equiv 5 \pmod{6}$, a kako je desna strana jednačbe $1 \pmod{6}$, jednačba nema rješenja za $p, q > 3$. Preostaje provjeriti $q = 2, 3$ i $p = 2, 3$. Za $q = 2$ je $p^2 = 1 + 8 = 9 \Rightarrow p = 3$, a za $q = 3$ i $p = 2$ nema rješenja (za $p = 3$ dobivamo već nađeno rješenje $q = 2$). Dakle, jedino rješenje je $(p, q) = (3, 2)$.

18. Općinsko 2016. - 3. razred 7. zadatak

19. $2n + 1$ je neparan kvadrat pa je $2n + 1 \equiv 1 \pmod{4}$, odnosno n je paran broj. Iz tog slijedi da je $3n + 1$ isto neparan kvadrat pa je $3n + 1 \equiv 1 \pmod{8}$, odnosno n je djeljiv s 8.

Preostaje još dokazati da je n djeljiv s 5. Uočimo da su kvadrati cijelih brojeva kongruentni 0, 1 ili 4 $\pmod{5}$, te pretpostavimo da n nije djeljiv s 5. Tada postoje 4 mogućnosti:

$$n \equiv 1 \pmod{5} \Rightarrow 2n + 1 \equiv 3 \pmod{5} \text{ (nije kvadrat)}$$

$$n \equiv 2 \pmod{5} \Rightarrow 3n + 1 \equiv 7 \equiv 2 \pmod{5} \text{ (nije kvadrat)}$$

$$n \equiv 3 \pmod{5} \Rightarrow 2n + 1 \equiv 7 \equiv 2 \pmod{5} \text{ (nije kvadrat)}$$

$$n \equiv 4 \pmod{5} \Rightarrow 3n + 1 \equiv 13 \equiv 3 \pmod{5} \text{ (nije kvadrat)}$$

Zaključujemo da je n djeljiv s 5 pa je n djeljiv s $5 \cdot 8 = 40$.

20. Promatrajmo $x \pmod{4}$. Primjetimo da $(4k + 1)^{4k+1} \equiv 1^{4k+1} \equiv 1 \pmod{4}$, $(2k)^{2k} \equiv 0 \pmod{4}$ i $(4k + 3)^{4k+3} \equiv (-1)^{4k+3} \equiv -1 \pmod{4}$ pa je $1 + 2^2 + 3^3 + \dots + 1983^{1983} \equiv 1 + 0 + (-1) + 0 + 1 + \dots + (-1) \equiv 0 \pmod{4}$, odnosno $4 \mid x$.

Pretpostavimo da je $x = m^k$ za $k \geq 3$. Ako $4 \mid m^k$, zbog donje granice na k nužno i $8 \mid m^k$ (preciznije, minimalno $2^k \mid m^k$). Za sve parne brojeve $n > 2$, $n^n \equiv 0 \pmod{8}$ (jer se faktor 2 pojavljuje barem 3 puta). Za $n = 2k + 1$, $n^n = n^{2k+1} = (n^k)^2 \cdot n$, a kako kvadrati neparnih brojeva daju ostatak 1 pri dijeljenju s 8, slijedi $n^n \equiv 1^2 \cdot n \equiv n \pmod{8}$). Zato je

$$x = 1 + 2^2 + 3^3 + \dots + 1983^{1983} \equiv 1 + 2^2 + 3 + 0 + 5 + \dots + 1981 + 0 + 1983 \equiv 4 + (1 + 3 + 5 + \dots + 1983) \equiv 4 + 992^2 \equiv 4 \pmod{8}$$

odnosno x nije djeljiv s 8, što je kontradikcija s našom pretpostavkom. Dakle, x nije oblika m^k za $m, k \in \mathbb{N}$ i $k \geq 3$.