



Djeljivost: modularna aritmetika

Okvirna razina: HJMO / SŠ A var. županijsko

1. Kongruencije

Promotrimo sljedeće skupove

$$\{1, 5, 9, 13, \dots\}, \{2, 6, 10, 14, \dots\}, \{3, 7, 11, 15, \dots\}, \{4, 8, 12, 16, \dots\}.$$

Vidimo da se svaki od prirodnih brojeva nalazi u točno jednom od tih skupova. Ono što te skupove čini posebnima jest to što svaka dva člana u nekom od skupova daju isti ostatak pri dijeljenju brojem 4, odnosno, ako odaberemo neke brojeve a i b iz jednog od skupova, imamo $4 \mid a - b$.

Prilikom rješavanja zadataka možemo promatrati što se događa s ostacima promatranih brojeva prilikom izvođenja operacija nad njima, odnosno mijenjaju li se ostaci usklađeno s brojevima prilikom tih operacija. Odgovor je da, i zbog toga ima smisla govoriti o *modularnoj aritmetici*, aritmetici ostataka.

Definicija 1

Neka su $a, b \in \mathbb{Z}$, te $n \in \mathbb{N}$. Kažemo da je broj a kongruentan broju b modulo n ako vrijedi $n \mid a - b$. Pišemo $a \equiv b \pmod{n}$.

Napomena

Primijetimo da kongruencije po nekom modulu n grupiraju brojeve upravo prema ostatku pri dijeljenju s n . Odnosno, ako a i b daju isti ostatak, onda je $a - b$ djeljivo s n . Također, prema ovoj definiciji, dozvoljavamo i negativne predstavnike iste klase. Primjerice, možemo napisati $7 \equiv 3 \pmod{4}$, ali isto tako vrijedi i $7 \equiv -1 \pmod{4}$ jer je $7 - (-1) = 8$ djeljivo s 4.

Jedna od posljedica definicije kongruencija je, primjerice, tvrdnja

$$a \equiv a + kn \pmod{n}, \quad \text{za sve } a, k \in \mathbb{Z}, n \in \mathbb{N}.$$

Možemo ju dokazati: neka je r ostatak pri dijeljenju a s n , tj. $a \equiv r \pmod{n}$. Tada možemo zapisati $a = qn + r$ za neki $q \in \mathbb{Z}$, $0 \leq r < n$. Tada za proizvoljni $k \in \mathbb{Z}$ vrijedi $a + kn = qn + r + kn = (q + k)n + r$. Kako je $r < n$, r je ostatak pri dijeljenju $a + kn$ s n , odnosno vrijedi tvrdnja.

Kongruencije nam pomažu da lakše (kraće, preglednije) zapišemo neke tvrdnje o ostacima. Uz to, modularni zapis omogućava i računske operacije - možemo zbrajati, oduzimati, množiti, a u određenim uvjetima i dijeliti. Navodimo neka svojstva modularnog računa koja se mogu dokazati kad ih „prevedemo” u terminologiju kvocijenata i ostataka.

Propozicija 2: Svojstva kongruencija

$$\begin{aligned} a \equiv b \pmod{n}, c \equiv d \pmod{n} &\implies a + c \equiv b + d \pmod{n}, & a, b, c, d \in \mathbb{Z}, n \in \mathbb{N}, \\ a \equiv b \pmod{n}, c \equiv d \pmod{n} &\implies ac \equiv bd \pmod{n}, & a, b, c, d \in \mathbb{Z}, n \in \mathbb{N}, \\ a \equiv b \pmod{n} &\implies a^k \equiv b^k \pmod{n}, & a, b \in \mathbb{Z}, n \in \mathbb{N}, k \in \mathbb{N}_0 \\ ac \equiv bc \pmod{n} \text{ i } \text{nzd}(c, n) = 1 &\implies a \equiv b \pmod{n}, & a, b, c \in \mathbb{Z}, n \in \mathbb{N}. \end{aligned}$$

⚠ Oprez

U gornjoj propoziciji $\text{nzd}(c, n)$ označava najveći zajednički djelitelj. Ako za neka dva broja vrijedi $\text{nzd}(x, y) = 1$ to znači da su oni relativno prosti.

Važno je naglasiti da je ta pretpostavka ključna da bismo mogli pokratiti s c . Pogledajmo kao primjer

$$12 \equiv 2 \pmod{10},$$

što znamo da vrijedi. Kako je $12 = 2 \cdot 6$ i $2 = 2 \cdot 1$, kad bismo pokratili gornji izraz s 2, dobili bismo $6 \equiv 1 \pmod{10}$, što očito ne vrijedi. Naravno, radi se o tome da je $\text{nzd}(2, 10) = 2$, stoga ne možemo iskoristiti gornju implikaciju.

Primjer 1

Odredimo koje ostatke pri dijeljenju s 3 daju kvadrati prirodnih brojeva.

Ova tvrdnja može se dokazati i bez kongruencija, ali pogledajmo kako nam modularni zapis pomaže skratiti postupak. Promotrimo tri slučaja, ovisno o tome koji ostatak prirodan broj n daje pri dijeljenju s 3.

- $n \equiv 0 \pmod{3}$. Zaključujemo $n^2 \equiv 0^2 \equiv 0 \pmod{3}$.
- $n \equiv 1 \pmod{3}$. Zaključujemo $n^2 \equiv 1^2 \equiv 1 \pmod{3}$.
- $n \equiv 2 \pmod{3}$. Zaključujemo $n^2 \equiv 2^2 \equiv 1 \pmod{3}$.

Dakle, kvadrati prirodnih brojeva uvijek daju ostatak 0 ili 1.

Napomena

U cjelini „Djeljivost - ostaci” pokazano je da kvadrati cijelih pri dijeljenju s 4 također daju samo ostatke 0 ili 1. Pokušaj istu tvrdnju dokazati koristeći kongruencije, kao u gornjem primjeru.

Jesi li se kad pitao koji dan u tjednu je bio određen datum? Jasno je da se u srži odgovora kriju ostaci pri dijeljenju sa 7, pa tome možemo pristupiti kao u sljedećem primjeru.

Primjer 2

U godini N , tristoti dan je utorak. U godini $N + 1$, dvjestoti dan je također utorak. Koji dan u tjednu je bio na stoti dan godine $N - 1$?

Postoji ili $200 + 65 = 265$ ili $200 + 66 = 266$ dana između prva dva datuma, ovisno o tome je li godina prijestupna godina ili ne. Budući da je

$$265 \equiv 6 \pmod{7} \quad \text{i} \quad 266 \equiv 0 \pmod{7},$$

opisana situacija je moguća samo ako je godina N prijestupna. Iz toga nužno slijedi da $N - 1$ nije prijestupna, tj. da ima 365 dana. Dakle, postoji

$$265 + 300 = 565$$

dana između zadanih dana u godinama $N - 1$ i N .

Budući da je

$$565 \equiv 5 \pmod{7}$$

i budući da oduzimamo dane, ostaje nam 5 dana prije utorka, a to je četvrtak.

Pogledajmo primjere gdje baratamo računom kao da se radi o običnoj aritmetici.

Primjer 3

a) Pronaći ćemo sve cijele brojeve x za koje vrijedi $2x + 3 \equiv 4 \pmod{7}$. Prvo imamo

$$2x \equiv 4 - 3 = 1 \pmod{7}.$$

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 sa 2 iz čega slijedi $x \equiv 4 \pmod{7}$.

b) Nađimo prirodne brojeve koji zadovoljavaju jednadžbu

$$x^2 + 4x + 1 = 4y^2.$$

Zapišimo jednadžbu kao

$$x^2 + 1 = 4y^2 - 4x$$

te ju promotrimo modulo 4:

$$x^2 + 1 \equiv 0 \pmod{4}$$

$$x^2 \equiv -1 \pmod{4}$$

$$x^2 \equiv 3 \pmod{4}.$$

No to je nemoguće jer smo pokazali da kvadrat broja daje ostatak 0 ili 1 pri dijeljenju sa četiri. Dakle, nema prirodnih brojeva koji zadovoljavaju jednadžbu.

U gornjem primjeru iskoristili smo da za broj 2 postoji broj (4) takav da vrijedi $2 \cdot 4 \equiv 1 \pmod{7}$. Dosad smo već uočili da je „namještanje” na ostatak 1 česta ideja kod rješavanja zadataka, ali nema garancije da je to uvijek moguće. Preduvjet za to je da imamo brojeve koji su relativno prosti.

Definicija 3

Modularni inverz broja $a \in \mathbb{Z}$ modulo n je cijeli broj x takav da vrijedi $a \cdot x \equiv 1 \pmod{n}$.

Propozicija 4

Modularni inverz postoji ako i samo ako su a i n međusobno relativno prosti, tj. $\text{nzd}(a, n) = 1$.

Računom s kongruencijama možemo lako doći do zaključaka o ostacima većih i složenih brojeva.

Primjer 4

Želimo odrediti zadnju znamenku broja 3^{33} . Drugim riječima, želimo odrediti koji je ostatak tog broja pri dijeljenju s 10.

Promotrimo prvih nekoliko potencija broja 3 i njihove ostatke:

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

Naslućujemo da se ostaci ponavljaju te da ovise o eksponentu i njegovom ostatku pri dijeljenju s 4. Umjesto pogađanja ili dokazivanja općenite tvrdnje, možemo iskoristiti $33 = 4 \cdot 8 + 1$ uz tvrdnje iz gornje propozicije, pa modularnim računom sad imamo

$$\begin{aligned} 3^4 &\equiv 1 \pmod{10}, \\ 3^{32} &= (3^4)^8 \equiv 1^8 = 1 \pmod{10}, \\ 3^{33} &= 3^{32} \cdot 3 \equiv 1 \cdot 3 = 3 \pmod{10}. \end{aligned}$$

Dakle, zadnja znamenka danog broja je 3.

Već u gornjem primjeru vidi se da nam je često važno doći do ostatka 1 - između ostalog, ako postoji, on omogućava da uočimo „periodičnost” tj. ponavljanje ostataka.

Zadaci za samostalnu vježbu

1. a) Pokaži da 4 ne dijeli $n^2 + 2n - 1$ za sve prirodne brojeve n .
b) Pokaži da 7 dijeli $2^{n+2} + 3^{2n+1}$ za sve prirodne brojeve n .
2. Koje su posljednje dvije znamenke broja 17^{2026} ?
3. Odredi posljednju znamenku broja 7^{100} .
4. Neka su a, b, c prirodni brojevi takvi da $6 \mid a + b + c$. Dokaži da $6 \mid a^3 + b^3 + c^3$.
5. Dokaži $13 \mid 2^{12n+9} - 5^{4n+1}$.
6. Ako je zbroj kvadrata triju prostih brojeva a, b, c prost broj, dokaži da je barem jedan od brojeva a, b, c jednak 3.
7. Pronađi sve proste brojeve p i q takve da $p^2 - 2q^2 = 1$.
8. Dani su jedinstveni prirodni brojevi $a_2, a_3, a_4, a_5, a_6, a_7$ takvi da
$$\frac{5}{7} = \frac{a_2}{2!} + \frac{a_3}{3!} + \frac{a_4}{4!} + \frac{a_5}{5!} + \frac{a_6}{6!} + \frac{a_7}{7!},$$
gdje $0 \leq a_i < i$ za $i = 2, 3, 4, 5, 6, 7$. Koliko je $a_2 + a_3 + a_4 + a_5 + a_6 + a_7$?
9. Pronađi cjelobrojne vrijednosti x između -10 i 15 takve da je
$$P = 3x^3 + 7x^2$$
kvadrat cijelog broja.
10. Je li moguće poredati brojeve $1^1, 2^2, \dots, 2026^{2026}$ jedan za drugim tako da broj dobiven spajanjem znamenaka bude kvadrat nekog prirodnog broja? Na primjer, broj dobiven spajanjem $\overline{3^3 1^1 2^2}$ je 2714.
11. Dokaži da je umnožak zadnje znamenke broja 2^n i sume njegovih znamenaka osim zadnje djeljiv brojem 3.
12. Nađi sve prirodne brojeve n takve da je broj $n^n - 3$ djeljiv s 10.
13. Dokaži da ne postoje prirodni brojevi m i n takvi da je $3^m + 3^n + 1$ kvadrat prirodnog broja.
14. Postoji li prirodan broj n takav da je $8^n + 47$ prost broj?
15. Odredi sve pozitivne cijele brojeve a, b, c i prost broj p takve da vrijedi
$$73p^2 + 6 = 9a^2 + 17b^2 + 17c^2.$$

Upute za zadatke za samostalnu vježbu

1. U a) dijelu promatraj ostatke pri dijeljenju n sa 4, a u b) dijelu ostatke sa 7.
2. Promatraj ostatke pri dijeljenju sa 100. Za koju potenciju se dobije ostatak 1?
3. Uoči da se ostatak pri dijeljenju 7^n ponavlja s periodom 4 pa poveži to s eksponentom.
4. Promatraj djeljivost s 2 i 3.
5. Uoči $2^3 = 8 \equiv -5 \pmod{13}$.
6. Iskoristi ono što znamo o ostacima pri dijeljenju kvadrata s 3.
7. Za sve proste brojeve $p > 3$ vrijedi $p \equiv 1 \pmod{6}$ ili $p \equiv -1 \pmod{6}$. Prvo se uvjeri da je to istina, potom prouči ta dva slučaja.
8. Pomnoži sa $7!$ i promatraj ostatke modulo 7.
9. Zaključi da je $3x + 7$ kvadrat prirodnog broja i promatraj ostatke pri dijeljenju s 3.
10. Gledamo dekadski zapis: za bilo koji takav raspored možemo pronaći nenegativne cijele brojeve $x_1, x_2, \dots, x_{2026}$ takve da je dobiveni broj jednak
$$1^1 \cdot 10^{x_1} + 2^2 \cdot 10^{x_2} + \dots + 2026^{2026} \cdot 10^{x_{2026}}.$$
Na primjer, za raspored $\overline{3^3 1^1 2^2} = 2714$, vrijedi $2714 = 3^3 \cdot 10^2 + 1^1 \cdot 10^1 + 2^2 \cdot 10^0$. Gledaj i djeljivost s 3.
11. Iskoristi da suma znamenki broja m daje isti ostatak pri dijeljenju s 3 kao i broj m .
12. Promatraj n modulo 10. Očito mora biti $n^n \equiv 3 \pmod{10}$. Provjeri slučajeve.
13. Promatraj ostatke pri dijeljenju s 8.
14. Odgovor je ne. Ako nađemo neki k tako da bude $8^n + 47 \equiv 0 \pmod{k}$ tj. da je izraz djeljiv s k , preostaje provjeriti je li izraz veći od k . Dakle, ideja je da nađemo više različitih modula k za koje će, pod određenim uvjetima, vrijediti prethodna relacija. Ako nađemo takve module za svaki mogući oblik broja n , gotovi smo. Idi redom po modulima koje smo prolazili (npr. 3, 4, 5, 7, 9, 11, 13, ...) i vidi što možeš zaključiti o n u tim slučajevima.
15. Uočimo da je $73 = 72 + 1$, $9 = 8 + 1$ te $17 = 16 + 1$, pa gledamo modulo 8.

Rješenja zadataka za samostalnu vježbu

1. a) Ključna stvar je odabrati pravi modul. Ovdje nas zadatak navodi na ostatke pri dijeljenju s 4:

1) $n \equiv 0 \pmod{4}$: slijedi $n^2 + 2n - 1 \equiv 0 + 0 - 1 = -1 \pmod{4}$.

2) $n \equiv 1 \pmod{4}$: slijedi $n^2 + 2n - 1 \equiv 1^2 + 2 - 1 = 2 \pmod{4}$.

3) $n \equiv 2 \pmod{4}$: slijedi $n^2 + 2n - 1 \equiv 2^2 + 4 - 1 = 3 \pmod{4}$.

4) $n \equiv 3 \pmod{4}$: slijedi $n^2 + 2n - 1 \equiv 3^2 + 6 - 1 = 2 \pmod{4}$.

Vidimo da u svakom slučaju ostatak nije 0.

- b) Primijetimo da i 2 i 9 daju ostatak 2 pri dijeljenju s 7. Koristeći modularnu aritmetiku imamo

$$2^{n+2} + 3^{2n+1} = 4 \cdot 2^n + 3 \cdot 9^n \equiv (-3) \cdot 2^n + 3 \cdot 2^n \equiv 0 \pmod{7},$$

pa je izraz djeljiv sa 7.

2. Tražimo $17^{2026} \pmod{100}$.

$$17^2 \equiv 89 \pmod{100}$$

$$17^4 \equiv 21 \pmod{100}$$

$$17^8 \equiv 41 \pmod{100}$$

$$17^{10} \equiv 41 \cdot 89 \equiv 49 \pmod{100}$$

$$17^{20} \equiv 49^2 \equiv 1 \pmod{100}$$

Pa je

$$17^{2026} \equiv 17^{2020} \cdot 17^6 \equiv (17^{20})^{101} \cdot 17^4 \cdot 17^2 \equiv 1 \cdot 89 \cdot 21 \equiv 69 \pmod{100}.$$

Dakle, zadnje dvije znamenke su 69.

3. Promotrimo prvih nekoliko potencija broja 7:

$$7, 49, 343, 2401, 16807, \dots$$

Primijetimo da se zadnje znamenke potencija broja 7 ponavljaju s periodom 4. Odredimo prvo ostatak pri dijeljenju 7^{100} s 4.

$$7^{100} = (7^2)^{50} \equiv 1^{50} = 1 \pmod{4}.$$

Dakle, možemo zapisati $7^{100} = 4k + 1$ za neki $k \in \mathbb{N}$. Prema tome,

$$7^{7^{100}} = (7^4)^k \cdot 7 \equiv 1^k \cdot 7 = 7 \pmod{10}.$$

Zadnja znamenka traženog broja je 7.

4. Uočimo prvo da za svaki cijeli broj vrijedi $x^3 \equiv x \pmod{2}$ i $x^3 \equiv x \pmod{3}$. Prva tvrdnja je očita jer se (ne)parnost ne mijenja, a druga tvrdnja je očita za ostatke 0 i 1, dok za 2 vrijedi $2^3 = 8 \equiv 2 \pmod{3}$.

Sad zaključujemo

$$a^3 + b^3 + c^3 \equiv a + b + c \equiv 0 \pmod{2}, \quad a^3 + b^3 + c^3 \equiv a + b + c \equiv 0 \pmod{3}.$$

Kako je traženi broj djeljiv s 2 i 3, zaključujemo da mora biti djeljiv i s 6.

5. Nije baš očito kako bismo trebali prikazati dane brojeve. Jedna mogućnost je „namještanje” do multiplikativnog inverza brojeva 2 i 5, što možeš pokušati sam.

Ovdje ćemo uočiti $2^3 = 8 \equiv -5 \pmod{13}$ pa vrijedi

$$2^{12n+9} = 2^{3(4n+3)} \equiv 8^{4n+3} \equiv (-5)^{4n+3} \equiv -5^{4n+3} \pmod{13}.$$

Sad možemo izračunati

$$2^{12n+9} - 5^{4n+1} \equiv -5^{4n+3} - 5^{4n+1} = -5^{4n+1}(25 + 1) \equiv 0 \pmod{13}.$$

6. Pretpostavimo suprotno, da postoje takvi prosti brojevi a, b i c od kojih niti jedan nije jednak 3. Tada za svakog od njih vrijedi $a^2 \equiv b^2 \equiv c^2 \equiv 1 \pmod{3}$.

Međutim, tada je

$$a^2 + b^2 + c^2 \equiv 3 \equiv 0 \pmod{3}.$$

Ovo je moguće samo ako je $a^2 + b^2 + c^2 = 3$, što pak nije moguće jer iz $a, b, c \geq 2$ slijedi $a^2 + b^2 + c^2 \geq 12$.

Prema tome, pretpostavka je pogrešna i kontradikcijom možemo zaključiti da je barem jedan od brojeva jednak 3.

7. Pretpostavimo prvo da su $p, q > 3$. Može se pokazati da za sve proste $p > 3$ vrijedi $p \equiv 1$ ili $-1 \pmod{6}$. Ova tvrdnja dokazuje se isto kao analogne tvrdnje za module 2 i 3, što možeš jednako i dokazati (sam). Prema tome, za $p > 3$ vrijedi da je $p^2 \equiv 1 \pmod{6}$.

Isto tako za $q > 3$ vrijedi $q^2 \equiv 1 \pmod{6}$.

Slijedi da je $p^2 - 2q^2 \equiv 1 - 2 \equiv -1 \equiv 5 \pmod{6}$. Desna strana jednadžbe je kongruentna 1 $\pmod{6}$ stoga jednadžba nema rješenja za $p, q > 3$.

Pretpostavimo sad da je od brojeva p, q jednak 2 ili 3. Ako je $p = 2$, dobivamo da je $2q^2 = 4 - 1 = 3$ što nema rješenja u cijelim brojevima. Slično za $q = 3$ dobivamo da je $p^2 = 1 + 18 = 19$, što isto nema rješenja u cijelim brojevima.

Ako je $p = 3$, imamo $2q^2 = 9 - 1 = 8$, odnosno $q = 2$. U preostalom slučaju $q = 2$ dobivamo isto rješenje kao jedinu mogućnost.

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

8. Prvo pomnožimo sa 7!:

$$5 \cdot 6! = a_2(7 \cdot 6 \cdot 5 \cdot 4 \cdot 3) + a_3(7 \cdot 6 \cdot 5 \cdot 4) + a_4(7 \cdot 6 \cdot 5) + a_5(7 \cdot 6) + a_6 \cdot 7 + a_7.$$

Budući da vrijedi $0 \leq a_i < i$ za svaki i , i svi članovi zdesna su višekratnici broja 7, promotrimo jednadžbu modulo 7:

$$\begin{aligned} a_7 &\equiv 5 \cdot 6! \pmod{7} \\ &\equiv 5 \cdot 720 \pmod{7} \\ &\equiv 5 \cdot 6 \pmod{7} \\ &\equiv 2 \pmod{7}. \end{aligned}$$

Budući da je $0 \leq a_7 < 7$, imamo $a_7 = 2$ i

$$5 \cdot 6! - 2 = a_2(7 \cdot 6 \cdot 5 \cdot 4 \cdot 3) + a_3(7 \cdot 6 \cdot 5 \cdot 4) + a_4(7 \cdot 6 \cdot 5) + a_5(7 \cdot 6) + a_6 \cdot 7.$$

Sada gledamo ovu jednadžbu modulo 6:

$$7a_6 \equiv -2 \equiv 28 \pmod{6}$$

$$a_6 \equiv 4 \pmod{6} \Rightarrow a_6 = 4.$$

Nastavljamo tako da sljedeću jednadžbu gledamo modulo 5:

$$5 \cdot 6! - 2 - 4 \cdot 7 = a_2(7 \cdot 6 \cdot 5 \cdot 4 \cdot 3) + a_3(7 \cdot 6 \cdot 5 \cdot 4) + a_4(7 \cdot 6 \cdot 5) + a_5(7 \cdot 6),$$

što nam odmah daje $a_5 = 0$.

Dobivamo

$$5 \cdot 6! - 2 - 4 \cdot 7 = a_2(7 \cdot 6 \cdot 5 \cdot 4 \cdot 3) + a_3(7 \cdot 6 \cdot 5 \cdot 4) + a_4(7 \cdot 6 \cdot 5),$$

pa dijeljenjem sa $7 \cdot 6 \cdot 5$ dobijamo

$$17 = 12a_2 + 4a_3 + a_4.$$

Mogli bismo nastaviti uzimati modulo 4 i 3, ali već je iz ove jednadžbe primjetno $a_4 = a_3 = a_2 = 1$.

Zaključujemo

$$a_2 + a_3 + a_4 + a_5 + a_6 + a_7 = 1 + 1 + 1 + 0 + 4 + 2 = 9.$$

9. Budući da je

$$P = 3x^3 + 7x^2 = x^2(3x + 7) = N^2,$$

ili je $x = 0$ ili je $3x + 7$ kvadrat broja. Neka je

$$3x + 7 = K^2.$$

Tada

$$K^2 \equiv 3x + 7 \equiv 7 \equiv 1 \pmod{3}.$$

Ako je broj K oblika $3k$, onda $K^2 \not\equiv 1 \pmod{3}$, ali ako je K oblika $3k+1$ ili $3k+2$, onda vrijedi $K^2 \equiv 1 \pmod{3}$.

Za $k = 0$ imamo $K = 1, 2$ pa je $x = -2, -1$. Za $k = 1$ imamo $K = 4, 5$ pa je $x = 3, 6$. Za $k = 2$ imamo $K = 7, 8$ pa je $x = 14, 19$.

Dakle, traženi skup je

$$\{-2, -1, 0, 3, 6, 14\}.$$

10. Za bilo koji takav raspored možemo pronaći nenegativne cijele brojeve $x_1, x_2, \dots, x_{2026}$ takve da je dobiveni broj jednak

$$1^1 \cdot 10^{x_1} + 2^2 \cdot 10^{x_2} + \dots + 2026^{2026} \cdot 10^{x_{2026}}.$$

Na primjer, za raspored $\overline{3^3 1^1 2^2} = 2714$, 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

$$1^1 \cdot 10^{x_1} + 2^2 \cdot 10^{x_2} + \dots + 2026^{2026} \cdot 10^{x_{2026}} \equiv 1^1 + 2^2 + \dots + 2026^{2026} \pmod{3}.$$

Lako se provjeri da vrijede sljedeće tvrdnje:

- 1) ako je $a \equiv 0 \pmod{3}$, onda $a^a \equiv 0 \pmod{3}$,
- 2) ako je $a \equiv 1 \pmod{3}$, onda $a^a \equiv 1 \pmod{3}$,
- 3) ako je $a \equiv 2 \pmod{3}$ i a paran, onda $a^a \equiv 1 \pmod{3}$,
- 4) ako je $a \equiv 2 \pmod{3}$ i a neparan, onda $a^a \equiv 2 \pmod{3}$.

Koristeći gore navedene tvrdnje vidimo da je izraz

$$1^1 + 2^2 + 3^3 + 4^4 + 5^5 + 6^6 \equiv 2 \pmod{3}.$$

Analogno, $7^7 + \dots + 12^{12} \equiv 0 \pmod{3}$ i dalje za grupe od po 6 pribrojnika, pa vrijedi i $1^1 + 2^2 + \dots + 2022^{2022} \equiv 2 \pmod{3}$. Kako je $2026 = 337 \cdot 6 + 4$, vidimo da je izraz

$$1^1 + 2^2 + \dots + 2026^{2026}$$

kongruentan izrazu $337 \cdot 2 + 2023^{2023} + 2024^{2024} + 2025^{2025} + 2026^{2026} \equiv 2 + 1 + 1 + 0 + 1 = 2 \pmod{3}$.

Međutim, znamo da kvadrat cijelog broja ne može dati ostatak 2 pri dijeljenju s 3. Stoga zaključujemo da nije moguće posložiti brojeve $1^1, 2^2, \dots, 2026^{2026}$ jedan za drugim tako da dobiveni broj bude kvadrat nekog prirodnog broja.

- 11.** Označimo sumu svih znamenki (uključujući zadnju) broja m s $S(m)$. Znamo da vrijedi $S(m) \equiv m \pmod{3}$ za sve m , pa posebno i za 2^n .

Neka je a zadnja znamenka broja 2^n . Sada imamo:

$$a(S(2^n) - a) \equiv a(2^n - a) \pmod{3}.$$

Uočimo da, za parni n , $2^n \equiv 1 \pmod{3}$, dok za neparne n vrijedi $2^n \equiv 2 \pmod{3}$.

Također možemo uočiti (dokaži sam) da se zadnje znamenke broja 2^n periodično ponavljaju: 2, 4, 8, 6, 2, ...

Gledamo slučajeve ovisno o kongruenciji od n po modulu 4:

- 1) $n \equiv 0 \pmod{4} \Rightarrow a = 6$ i $2^n \equiv 1 \pmod{3}$. U oba slučaja dobivamo $a(2^n - a) \equiv 0 \pmod{3}$.
- 2) $n \equiv 1 \pmod{4} \Rightarrow a = 2$ i $2^n \equiv 2 \pmod{3}$, pa $a(2^n - a) \equiv 2(2 - 2) \equiv 0 \pmod{3}$.
- 3) $n \equiv 2 \pmod{4} \Rightarrow a = 4$ i $2^n \equiv 1 \pmod{3}$, pa $a(2^n - a) \equiv 4(1 - 4) \equiv 0 \pmod{3}$.
- 4) $n \equiv 3 \pmod{4} \Rightarrow a = 8$ i $2^n \equiv 2 \pmod{3}$, pa $a(2^n - a) \equiv 8(2 - 8) \equiv 0 \pmod{3}$.

- 12.** Tražimo sve brojeve takve da $n^n \equiv 3 \pmod{10}$. Također znamo da, ako je a zadnja znamenka broja n , vrijedi $n^n \equiv a^n \pmod{10}$. Prema tome, dovoljno je promatrati zadnje znamenke broja n i njihove potencije.

Prvo uočimo, ako je n paran tada je n^n paran pa ostatak ne može biti 3. Za neparne brojeve promotrimo slučajeve:

- 1) $n \equiv 1 \pmod{10} \Rightarrow n^n \equiv 1 \not\equiv 3 \pmod{10}$.

2) $n \equiv 3 \pmod{10}$: Ostaci koje 3^k daje pri dijeljenju s 10 su periodični i iznose redom 3, 9, 7, 1, 3, ... Ostatak 3 daju one potencije gdje je eksponent oblika $4l + 1$.

Dakle, n mora davati ostatak 3 pri dijeljenju s 10 te 1 pri dijeljenju s 4. To zadovoljavaju svi brojevi oblika $n = 20m + 13$.

3) $n \equiv 5 \pmod{10} \Rightarrow n^n \equiv 5 \not\equiv 3 \pmod{10}$.

4) $n \equiv 7 \pmod{10}$: Ostaci koje 7^k daje pri dijeljenju s 10 su periodični i iznose redom 7, 9, 3, 1, 7, ... Ostatak 3 daju one potencije gdje je eksponent oblika $4l + 3$.

Dakle, n mora davati ostatak 7 pri dijeljenju s 10 te 3 pri dijeljenju s 4. To zadovoljavaju svi brojevi oblika $n = 20m + 7$.

5) $n \equiv 9 \pmod{10}$: Potencije 9^k završavaju na 1 ili 9, dakle ne mogu dati ostatak 3.

Dakle, sva rješenja su brojevi oblika $n = 20m + 7$ i $20m + 13$ za $m \in \mathbb{N}_0$.

13. Pretpostavimo da postoji k takav da je $3^m + 3^n + 1 = k^2$. Uočimo prvo da je lijeva strana neparna, pa k mora biti neparan broj.

Broj k može davati ostatke 1, 3, 5 ili 7 pri dijeljenju s 8. U svim slučajevima vrijedi

$$k^2 \equiv 1 \pmod{8}.$$

S druge strane, $3^l \equiv 3 \pmod{8}$ za neparne l i $3^l \equiv 1 \pmod{8}$ za parne l .

Sada promotrimo $3^m + 3^n = k^2 - 1$. Desna strana je djeljiva s 8, međutim lijeva strana može davati samo ostatke 2, 4 ili 6 pri dijeljenju s 8. Dakle, $3^m + 3^n + 1$ ne može biti kvadrat prirodnog broja.

14. Označimo $m = 8^n + 47$. U ovom zadatku potrebno je promatrati slučajeve prema tome koji ostatak n daje pri dijeljenju s 4. Pokazat ćemo da u svakom slučaju broj m ne može biti prost.

1) n paran, tj. $n = 2k$. Tada je $m = 64^k + 47 \equiv 1 + 2 \equiv 0 \pmod{3}$. Dakle, m je djeljiv s 3 i $m > 3$ pa m ne može biti prost.

2) $n \equiv 1 \pmod{4}$, tj. $n = 4k + 1$. Tada je $m = 8 \cdot (8^k)^4 + 47 \equiv 3 + 2 \equiv 0 \pmod{5}$. Opet, m je djeljiv s 5 i $m > 5$ pa ne može biti prost.

3) $n \equiv 3 \pmod{4}$, tj. $n = 4k + 3$. Tada je $m = 8 \cdot 64^{2k+1} + 47 \equiv 8 \cdot (-1) + 8 \equiv 0 \pmod{13}$. Sada je m djeljiv s 13 i $m > 13$ pa ne može biti prost.

15. Primijetimo prvo da je jednadžba simetrična u b i c , odnosno ne bi se promijenila kad bismo zamijenili mjesta b i c . Zato možemo bez smanjenja općenitosti pretpostaviti $b \geq c$.

Pretpostavimo prvo $p \geq 3$. Tada p mora biti neparan. Iskoristimo da kvadrati neparnih brojeva uvijek daju ostatak 1 pri dijeljenju s 8:

$$73p^2 + 6 \equiv 79 \equiv 7 \pmod{8}.$$

Slijedi $9a^2 + 17b^2 + 17c^2 \equiv a^2 + b^2 + c^2 \equiv 7 \pmod{8}$.

Međutim, za svaki cijeli broj vrijedi da njegov kvadrat daje ostatak 0, 1 ili 4 pri dijeljenju s 8, pa je nemoguće dobiti ostatak 7 u gornjem zbroju.

Dakle, zaključujemo da mora vrijediti $p = 2$. Sada jednačba postaje

$$9a^2 + 17(b^2 + c^2) = 298,$$

odnosno $17(b^2 + c^2) = 298 - 9a^2$. Kako je $a^2 \geq 1$, imamo $17(b^2 + c^2) \leq 289 = 17^2$, pa zaključujemo $b^2 + c^2 \leq 17$. To je moguće samo ako je

$$(b, c) \in \{(1, 1), (2, 1), (2, 2), (3, 1), (3, 2), (4, 1)\}.$$

Provjerom vidimo da samo za rješenje $(4, 1)$ dobijemo da je a cijeli broj. Prema tome, dana jednačba ima dva rješenja:

$$(a, b, c, p) \in \{(1, 1, 4, 2), (1, 4, 1, 2)\}.$$