J15 Juniorska grupa
Predavanja subotom
Zagreb

Kongruencije

Marko Žagar

5.3.2022.

Mladi nadareni matematičari "Marin Getaldić"

mnm.hr | Mladi nadareni matematičari "Marin Getaldić" | matematicari.mnm

Uvod

Teorija kongruencija ili modularna aritmetika stvorio je poznati njemački matematičar Carl Friedrich Gauss. Objavio ju je u djelu Disquisitiones Arithmeticae 1801. godine.

Najbolji primjer ovog moćnog alata je mjerenje vremena u takovanu aritmetiku modulu 24, djeleći dan na 24 sata nakon čega brojanje vremena kreće iz ponova.

Definicija 1

Neka je n prirodan broj, te neka su a i b cijeli brojevi. Ako n dijeli razliku a b, tada kažemo da je a kongruentan b modulo n, ili da su a i b kongruentni modulo n, te pišemo $a \equiv b \pmod{n}$.

Primjer 1. $17 \equiv 5 \pmod{12}$
$5 \equiv 5 \pmod{12}$
$24 \equiv 0 \pmod{12}$
$6 \equiv 34 \pmod{40}$.

Teorem 2

Neka su $a, b \in \mathbb{Z}$ i $n \in \mathbb{N}$. Vrijedi $a \equiv b \pmod{n}$ ako i samo ako a i b daju isti ostatak pri dijeljenju s n.

Teorem 3

Vrijede sljedeća svojstva kongruencija:

1. $a \equiv a \pmod{n}$ za sve cijele brojeve a i sve prirodne brojeve n
2. ako je $a \equiv b \pmod{n}$ onda je i $b \equiv a \pmod{n}$
3. ako je $a \equiv b \pmod{n}$ i $b \equiv c \pmod{n}$ onda je $a \equiv c \pmod{n}$
4. ako je $a \equiv b \pmod{n}$ i $c \equiv d \pmod{n}$ onda je $a + c \equiv b + d \pmod{n}$
5. ako je $a \equiv b \pmod{n}$ i $c \equiv d \pmod{n}$ onda je $ac \equiv bd \pmod{n}$
6. ako je $a \equiv b \pmod{n}$ i $k \in \mathbb{N}$ onda je $a^k \equiv b^k \pmod{n}$
7. ako je $ac \equiv bc \pmod{n}$ i $\mathrm{M}(c, n) = 1$ onda je $a \equiv b \pmod{n}$;
   općenito vrijedi ako je $ac \equiv bc \pmod{n}$ onda je $a \equiv b \pmod{\frac{n}{\mathrm{M}(n,c)}}$

Primjer 2. Dokažite da kvadrat cijelog broja može biti kongruentan isključivo 0 ili 1 mod 3.

Rješenje.
Promotrimo 3 slučaja.

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 i zaključujemo da vrijedi i tvrdnja zadatka. ◁

Lakši zadaci

1. Dokažite da kvadrat cijelog broja može biti kongruentan isključivo 0 ili 1 mod 4.

2. Koja je posljednja znamenka broja 3^{33}?

3. Dokažite da za svaki $a \in \mathbb{N}$ i svaki $n \in \mathbb{N}$ vrijedi:

$$a^n \equiv 1 \pmod{a+1} \text{ ili } a^n \equiv -1 \pmod{a+1}$$

4. Dokažite da je svaki prost broj veći od 3 oblika $6k+1$ ili $6k-1$, $k \in \mathbb{N}$.

Umjereni zadaci

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

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

7. Dokažite da 7 dijeli $2^{n+2} + 3^{2n+1}$ za sve prirodne brojeve n.

8. Ako je zbroj kvadrata triju prostih brojeva a, b, c prost broj, dokažite da je barem jedan od brojeva a, b, c jednak 3.

Teži zadaci

9. Odredite sve prirodne brojeve m i n za koje je $6^m + 2^n + 2$ potpun kvadrat.

10. Dokažite da postoji prirodan broj koji započinje znamenkama 1938472638628, a djeljiv je brojem 2022.

Više zadataka možete pronaći na www.skoljka.org.

Hintovi

1. Primijenite ideju kao u *primjeru 2.*

2. Primijetite kako se nakon nekog vremena zadnje znamenke, odnosno ostaci pri dijeljenju s 10 počinju ponavljati.

3. Primijetite kako je $b \equiv -1 \pmod{b+1}$.

4. Može li prost broj biti oblika $6k$, $6k+2$, $6k+3$ ili $6k+4$?

5. Promatrajte slučajeve ovisno o ostatku pri dijeljenju broja n sa 3.

6. Zapišite brojeve kao $k-1$, k, $k+1$.

7. Preoblikujte izraz tako da je u potencijama samo n te koristite svojstva kongruencija kod potencija.

8. Pretpostavi suprotno i isprobaj djeljivost s 3.

9. Primijetite da je zadani broj paran, što znači da je djeliv i sa 4 (s obzirom da je potpun kvadrat).

10. Postoji li takav broj koji se sastoji od nekoliko ponavljanja zadanog niza te znamenaka 0?

Rješenja

1. Slično kao u *primjeru 2.* pogledajmo 4 slučaja:

1. slučaj $n \equiv 0 \pmod 4$
$\implies n^2 \equiv 0^2 = 0 \pmod 4$

2. slučaj $n \equiv 1 \pmod 4$
$\implies n^2 \equiv 1^2 = 1 \pmod 4$

3. slučaj $n \equiv 2 \pmod 4$
$\implies n^2 \equiv 2^2 \equiv 0 \pmod 4$

4. slučaj $n \equiv 3 \pmod 4$
$\implies n^2 \equiv 3^3 \equiv 1 \pmod 4$

2. Primijetimo kako vrijedi:

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

Zato zaključujemo da je $3^{33} \equiv 3 \cdot (3^4)^8 \equiv 3 \cdot 1 = 3 \pmod{10}$ pa je zadnja znamenka danog broja 3.

3. Kako $a+1 \mid a+1 \iff a-(-1) \mid a+1$, zaključujemo da je $a \equiv -1 \pmod{a+1}$.
Sada, množenjem navedenog izraza n puta dobivamo $a^n \equiv (-1)^n$, odakle slijedi tvrdnja zadatka.

4. Promotrimo preostale ostatke prirodnog broja $n > 3$ pri dijeljenju sa 6.
$n \equiv 0 \pmod 6$
No, tada je n djeljiv s 2, a kako je veći od 2, zaključujemo da nije prost.
$n \equiv 2 \pmod 6$
Analogno, tada je n djeljiv s 2, a kako je veći od 2, zaključujemo da nije prost.
$n \equiv 3 \pmod 6$
Tada je n djeljiv s 3, a kako je veći od 3, zaključujemo da nije prost.
$n \equiv 4 \pmod 6$
No, kao i u ranijim slučajevima, tada je n djeljiv s 2, a kako je veći od 2, zaključujemo da nije prost.
Preostaje zaključiti kako su jedine preostale mogućnosti za prosti broj brojevi oblika $6k+1$ i $6k-1$.

5. Županijsko natjecanje 2014., SŠ A-2.1.

6. Želimo odrediti $(k-1)^3 + k^3 + (k+1)^3 \pmod 9$.

$$\begin{aligned} (k-1)^3 + k^3 + (k+1)^3 &= k^3 - 3k^2 + 3k - 1 + k^3 + k^3 + 3k^2 + 3k + 1 \\ &= 3k(k^2+2) \end{aligned}$$

Vidimo da je željeni izraz djeljiv s 3, dakle ostaje provjeriti $k(k^2+2) \pmod 3$.
To provjeravamo za sve tri mogućnosti:

$$\begin{aligned} k \equiv 0 \pmod 3 &\implies k(k^2+2) \equiv 0 \pmod 3 \\ k \equiv 1 \pmod 3 &\implies k(k^2+2) \equiv 1 \cdot (1+2) \equiv 0 \pmod 3 \\ k \equiv 2 \pmod 3 &\implies k(k^2+2) \equiv 2 \cdot (2+2) \equiv 0 \pmod 3 \end{aligned}$$

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

8. Županijsko natjecanje 2009., SŠ A-2.4.

9. Državno natjecanje 2009., SŠ-A 3.1.

10. Označimo sa t niz znamenaka 1938472638628 (za rješenje je potpuno nebitno o kojem je nizu znamenaka riječ).
Promotrimo brojeve: $\overline{t}, \overline{tt}, ..., \overline{tt..t}$ pri čemu zadnji od brojeva ima 2023 puta niz znamenaka t.
Po Dirichletovom principu, među tim brojevima postoje barem 2 s istim ostatkom pri dijeljenju sa 2022. Njihova je razlika djeljiva brojem 2022, a kako započinje nizom znamenaka t zadovoljava uvjete zadatka.