J6	Juniorska grupa

Predavanja subotom
Zagreb, sezona 2023./24.

Kongruencije

Mislav Plavac

25.11.2023.

Mladi nadareni matematičari
"Marin Getaldić"

1. Uvod

Promotrimo sljedeće skupove $\{1, 5, 9, 13, \ldots\}, \{2, 6, 10, 14, \ldots\}, \ldots, \{4, 8, 12, 16, \ldots\}$. 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 $4 \mid a - b$.
Zanima nas što se događa s ostatcima promatranih brojeva prilikom vršenja operacija nad njima, odnosno mijenjaju li se ostatci usklađeno s brojevima prilikom tih operacija? Odgovor je da, i zbog toga ima smisla govoriti o **modularnoj aritmetici**.

Definicija 1.1: Kongruencija dva cijela broja

Neka su $a, b \in \mathbb{Z}$, $n \in \mathbb{N}$. Kažemo da je broj a **kongruentan** broju b **modulo** n ako vrijedi $n \mid a - b$. Tada pišemo

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

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

Napomena 1.2

Također za $n \in \mathbb{N}$ možemo reći da su $a, b \in \mathbb{Z}$ kongruenti modulo n ako postoji $k \in \mathbb{Z}$ takav da je $a = kn + b$.

npr. $23 \equiv 7 \pmod{4}$, jer 23 i 7 oboje daju ostatak 3 pri dijeljenju sa 4. Zbog toga postoji k takav da $23 = 4k + 7$. Konkretno, vrijedi $23 = 4 \cdot 4 + 7$.

- $13 \equiv 3 \pmod{10}$ jer $10 \mid 13 - 3$
- $-2 \equiv 4 \pmod{6}$ jer $6 \mid (-2) - 4$

Propozicija 1.3: Svojstva kongruencija

Neka su $a, b, c, d \in \mathbb{Z}$ i $n, k \in \mathbb{N}$ tada

- $a \equiv a \pm kn \pmod{n}$
- $a \equiv b \pmod{n},\ c \equiv d \pmod{n} \implies a \pm c \equiv b \pm d \pmod{n}$
- $a \equiv b \pmod{n},\ c \equiv d \pmod{n} \implies ac \equiv bd \pmod{n}$
- $a \equiv b \pmod{n} \implies a^k \equiv b^k \pmod{n}$

- $ac \equiv bc \pmod{n}$ i $\gcd(c,n) = 1 \implies a \equiv b \pmod{n}$

Primjer 1. Odredite zadnju znamenku broja 3^{17}.

Rješenje 1. Raspišimo prvih par potencija.

$$3^1 = 3,\ 3^2 = 9,\ 3^3 = 27,\ 3^4 = 81,\ 3^5 = 243$$

Vidimo da se nakon 4 ponavlja znamenka, a kako je $17 = 4 \cdot 4 + 1$ jedino nam je bitan ovaj 1 jer se svakih 4 zadnja znamenka vraća na 3. Dakle, zadnja znamekna je 3.
Formalnije, vidimo da je $3^4 \equiv 1 \pmod{10}$ pa imamo

$$3^{17} \equiv 3 \cdot 3^{16} \equiv 3 \cdot (3^4)^4 \equiv 3 \cdot 1 \equiv 3 \pmod{10}$$

□

Ovo nam je možda pomoglo ovdje, ali nije uvijek tako jednostavno, primjerice za zadnje 3 znamenke broja 17^{2567} bismo dobili da se ponavlja tek za 17^{100}, ako mi ne vjerujete probajte sami raspisati kasnije. Za to će nam koristiti jedna posebna funkcija.

2. Eulerova funkcija i Eulerov teorem

Definicija 2.1

Eulerova funkcija $\phi(n)$ je broj brojeva iz skupa $\{1, 2, ..., n\}$ koji su **relativno prosti** s n.

Napomena 2.2

Za $a, b \in \mathbb{N}$ kažemo da su relativno prosti ako im je najveći zajednički djelitelj 1, tj. $\gcd(a,b) = 1$. Broj 1 je relativno prost sa svim prirodnim brojevima.

Primjer 2. Odredite $\phi(10)$

Rješenje 2. Promatrajmo skup $\{1,2,3,4,5,6,7,8,9,10\}$ i vidimo da su $1, 3, 7, 9$ relativno prosti s 10 pa je $\phi(10) = 4$. □

Ovo ne bude ni korisno ni efikasno za veće brojeve, primjerice $\phi(720) = 192$, ali zato postoji bolji način i par svojstava funkcije koja nam pomažu to izračunati.

Propozicija 2.3: Svojstva Eulerove funkcije

- Ako imamo rastav broja n na proste faktore $n = p_1^{\alpha_1} \cdot p_2^{\alpha_2} \cdot ... \cdot p_l^{\alpha_l}$, vrijedi:

$$\phi(n) = n \cdot (1 - \frac{1}{p_1}) \cdot ... \cdot (1 - \frac{1}{p_l})$$

- ϕ je multiplikativna, tj. vrijedi:

$$\phi(nm) = \phi(n)\phi(m) \text{ za } \gcd(m,n) = 1$$

- Ako je p prost broj, $\phi(p) = p - 1$.

Primjer 3. Izračunajte $\phi(720)$.

Rješenje 3. Kako je $720 = 2^4 \cdot 3^2 \cdot 5$ tada po formuli imamo

$$\phi(720) = 720 \cdot \left(1 - \frac{1}{2}\right)\left(1 - \frac{1}{3}\right)\left(1 - \frac{1}{5}\right) = 192$$

□

Teorem 2.4: Eulerov teorem

Neka su $a, n \in \mathbb{N}$ relativno prosti brojevi. Tada vrijedi:

$$a^{\phi(n)} \equiv 1 \pmod{n}$$

Direktna posljedica ovog teorema i svojstva eulerove funkcije je Mali Fermatov teorem.

Korolar 2.5: Mali Fermatov teorem

Neka je $a \in \mathbb{N}$ i neka je p prost broj takav da a nije djeljiv s p. Tada vrijedi:

$$a^{p-1} \equiv 1 \pmod{p}$$

Također, jedna korisna lema

Lema 2.6

Neka su $a, b \in \mathbb{N}$. Ako su a, n realtivno prosti, tj. $\gcd(a, n) = 1$ tada vrijedi:

$$a^b \equiv a^{b \pmod{\phi(n)}} \bmod n$$

Primjer 4. Odredite zadnju znamenku broja 7^{7^7}.
Napomena. $7^{7^7} = 7^{(7^7)} \neq (7^7)^7$

Rješenje 4. Tražimo:

$$7^{7^7} \bmod 10$$

$$7^{7^7} \equiv 7^x \bmod 10$$

Gdje je $x = (7^7 \bmod 4)$ odnosno $x = 3$

$$7^{7^7} \equiv 7^3 \equiv 3 \bmod 10$$

□

Primjer 5. Odredite zadnju znamenku broja 3^{17} koristeći Mali Fermatov teorem.

⚠ Oprez 1

Bitno je provjeriti uvjet da su brojevi relativno prosti. Primjerice ne postoji $k \in \mathbb{Z}$ takav da je $2^k \equiv 1 \pmod{10}$.

3. Kongruencije u diofantskim jednadžbama

Primjer 6. Odredite sve $x, y \in \mathbb{N}$ takve da vrijedi

$$x^2 + 10y = 1234567$$

Primjer 7. Oredite sve $x, y \in \mathbb{N}$ takve da vrijedi

$$x^2 - y^2 = 2014$$

Definicija 3.1

Za $b \in \mathbb{N}$ kažemo da je modularni inverz od $a \in \mathbb{N}$ modulo n ako je $ab \equiv 1 \pmod{n}$.

Propozicija 3.2

Ako postoji, modularni inverz je jedinstven modulo n.
Ako je p prost, svaki broj u skupu $\{1, 2, \ldots, p-2, p-1\}$ ima modularni inverz.

Zbog toga možemo pisati a^{-1} kao modularni inverz.

Primjer 8. Dokaži da jednadžba $19x^3 - 84y^2 = 1984$ nema rješenja u cijelim brojevima.

Rješenje 5. Reduciramo li jednadžbu $\pmod 7$ dobivamo:

$$\begin{aligned} 5x^3 &\equiv 3 \pmod 7 \quad / \cdot 3 \\ 15x^3 &\equiv 9 \pmod 7 \\ x^3 &\equiv 2 \pmod 7 \end{aligned}$$

što je nemoguće, dakle jednadžba nema rješenja. □

Lakši zadaci

1. Dokaži da kvadrat cijelog broja daje ostatak 0 ili 1 pri dijeljenju s 3/pri dijeljenju s 4.

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

3. Odredite ostatak pri djeljenju broja $3^{100}+5^{100}$ sa 7.

4. Nađite ostatak pri djeljenju broja $(7^{2014})^{2015}+(3^{2014})^{2015}$ s 11.

5. Neka je n prirodan broj, a $S(n)$ suma njegovim znamenki. Dokažite da vrijedi $n \equiv S(n) \pmod 3$.

6. Odredite posljednju znamenku broja $7^{7^{100}}$.

7. Nađite sve prirodne brojeve m, n koji zadovoljavaju jednadžbu

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

8. Ako su p i q različiti prosti brojevi, dokažite da je broj

$$p^{q-1}+q^{p-1}-1$$

djeljiv s pq.

9. Neka je $n \in \mathbb{N}$ takav da je $n+2$ prost. Pokažite da $n+2$ tada dijeli $n \cdot 2^n + 1$.

Zadaci

10. Oredite sve parove prostih brojeva (p,q) takve da je

$$p^q \cdot q^p + 1$$

također prosti broj.

11. Odredi zbroj:

$$\left\lfloor \frac{2^0}{3} \right\rfloor + \left\lfloor \frac{2^1}{3} \right\rfloor + \left\lfloor \frac{2^2}{3} \right\rfloor + ... + \left\lfloor \frac{2^{1000}}{3} \right\rfloor$$

Napomena. $\lfloor x \rfloor$ je najveći cijeli broj koji je manji od x, npr. $\lfloor 3.14 \rfloor = 3$, $\lfloor -2.718 \rfloor = -3$

12. Je li moguće posložiti brojeve $1^1, 2^2, ..., 2008^{2008}$ 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.)

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

14. Nađi sve proste brojeve p i q takve da je

$$p^2 - 2q^2 = 1$$

15. Nađi sve prirodne brojeve n takve da je $n^n - 3$ djeljivo s 10.

16. Odredi sve parove (a, b) prirodnih brojeva za koje vrijedi

$$a^b - b^a + 2^a = 17a^4 - 2b^2 + 52$$

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

18. Odredi sve pozitivne cijele brojeve a, b, c i prost broj p takve da vrijedi

$$73p^2 + 6 = 9a^2 + 17b^2 + 17c^2$$

4. Hintovi

Lakši zadaci

1. Svaki prirodan broj zapiši u ovisnosti od dijeljenju s 3 tj. 4.
2. Može li neki prost broj biti oblika $6k+2$? A $6k+3$ ili $6k+4$?
3. Pronađi potenciju koja je kongruentna 1 modulo 7.
4. Pronađi potenciju koja je kongruentna 1 modulo 11.
5. Zapiši broj pomoću sume umnoška znamenki i potencija broja 10.
6. Promatraj ostatak pri dijelju brojem 10, Eulerova funkcija.
7. Promatrajte ostatke pri dijeljenju brojem 3.
8. Mali Fermatov teorem.
9. Mali Fermatov teorem.

Zadaci

10. Promatrajte parnost izraza. Raspišite "male" slučajeve.
11. $2^{2n} \equiv 1 \pmod 3, 2^{2n-1} \equiv 2 \pmod 3$.
12. Za bilo koji takav raspored možemo pronaći nenegativne cijele brojeve $x_1, x_2, ..., x_{2008}$ takve da je dobiveni broj jednak $1^1 \cdot 10^{x_1} + 2^2 \cdot 10^{x_2} + ... + 2008^{2008} \cdot 10^{x_{2008}}$. Na primjer, za raspored $\overline{3^3 1^1 2^2} = 2714$, vrijedi $2714 = 3^3 \cdot 10^2 + 1^1 \cdot 10^1 + 2^2 \cdot 10^0$.
13. Promatrajte $\pmod 8$.
14. Promatrajte $p \pmod 6$.
15. Ovisno o $n \pmod{10}$, koje su moguće vrijednosti $n^n \pmod{10}$?
16. Raspišite par malih slučajeva, promatrajte parnosti.
17. Raspišite par malih slučajeva.
18. Što ako je p neparan?

5. Rješenja

Lakši zadaci

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. Ovo je ekvivalentno tvrdnji da 2 i 3 ne dijele p pa p ne može biti oblika $6k + 2$, $6k + 3$ ni $6k + 4$.

3. Zadatak 2.

4. Primjetimo da je potencija u oba slučaja $2014 \cdot 2015$, kako je $\phi(11) = 10$ imat ćemo

$$7^{2014 \cdot 2015} \equiv 7^{2014 \cdot 2015 \pmod{10}} \equiv 7^0 = 1$$

istim postupkom dobijemo da je $7^{2014 \cdot 2015} \equiv 1$ pa je ostatak pri dijeljennju $1 + 1 = 2$.

5. $n = \overline{a_k a_{k-1} a_{k-2} \ldots a_1 a_0} = 10^k \cdot a_k + 10^{k-1} \cdot a_{k-1} + \ldots + 10^1 \cdot a_1 + 10^0 \cdot a_0 \equiv a_k + a_{k-1} + \ldots + a_1 + a_0 \equiv S(n) \pmod 3$.

6. Tražimo zadnju zanemnku pa gledamo modulo 10. Kako je $\phi(10) = 4$ imamo tada

$$7^{100} \equiv (8 - 1)^{100} \equiv (-1)^{100} \equiv 1 \pmod 4$$

Tada imamo

$$7^{7^{100}} \equiv 7^1 \equiv 7 \pmod{10}$$

7. Zadatak 5.

8. Ako je djeljiv s pq mora biti djeljiv i s p i s q. Promatrajmo izraz modulo p. Znamo da je $p^{q-1} \equiv 0 \pmod p$ te kako su p, q različiti prosti brojevi pa su relativno prosti prema Fermatovom malom teoremu imamo $q^{p-1} \equiv 1 \pmod p$. Dakle,

$$p^{q-1} + q^{p-1} - 1 \equiv 0 + 1 - 1 \equiv 0 \pmod p$$

Analogno za q. Kako je djeljivo i s q i s p te kako su oni međusobno različiti dokazali smo da je izraz djeljiv s pq.

9.

$$n2^n + 1 \equiv (-2) \cdot 2^n + 1 \equiv -2^{n+1} + 1 \equiv -1 + 1 \equiv 0 \pmod{n+2}$$

gdje smo koristili da je $n + 2$ relativno prost s 2 pa po malom Fermatovom teoremu vrijedi $2^{n+1} \equiv 1 \pmod{n+2}$.

Zadaci

10. Ako su p, q oba neparni onda je cijeli izraz paran i > 4 pa ne može biti prosti broj. Neka je nadalje, bez smanjenja općenitosti, $p = 2$. Sada imamo izraz

$$2^q \cdot q^2 + 1$$

Za $q = 2$ dobivamo rješenje 17, a za $q = 3$ dobivamo rješenje 73. Neka je nadalje $q > 3$. Pokažimo da je tada izraz uvjek djeljiv s 3. Kako je q prosti i veći od 3 sigurno je relativno prost s 3 pa po Fermatovom malom teoremu imamo $q^2 \equiv 1 \pmod 3$. Sada imamo

$$2^q \cdot q^2 + 1 \equiv (-1)^q \cdot 1 + 1 \equiv -1 + 1 \equiv 0 \pmod 3$$

pa za $q > 3$ nemamo rješenja. Jedina rješenja su $(2, 2), (2, 3), (3, 2)$.

11. Example 2.3.4.

12. Za bilo koji takav raspored možemo pronaći nenegativne cijele brojeve $x_1, x_2, ..., x_{2008}$ takve da je dobiveni broj jednak $1^1 \cdot 10^{x_1} + 2^2 \cdot 10^{x_2} + ... + 2008^{2008} \cdot 10^{x_{2008}}$. 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 $1^1 \cdot 10^{x_1} + 2^2 \cdot 10^{x_2} + ... + 2008^{2008} \cdot 10^{x_{2008}} \equiv 1^1 + 2^2 + ... + 2008^{2008} \pmod 3$.

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 gore navedene tvrdnje vidimo da izraz $1^1 + 2^2 + 3^3 + 4^4 + 5^5 + 6^6 + 7^7 \equiv 0 \pmod 3$. Analogno $8^8 + ... + 14^{14} \equiv 0 \pmod 3$ pa vrijedi i $1^1 + 2^2 + ... + 2002^{2002} \equiv 0 \pmod 3$. Sada vidimo da je izraz $1^1 + 2^2 + ... + 2008^{2008} \equiv 2003^{2003} + 2004^{2004} + 2005^{2005} + 2006^{2006} + 2007^{2007} \equiv 2 \pmod 3$. Međutim, po primjeru 1.2., kvadrat cijelog broja ne može dati ostatak 2 pri dijeljenju s 3. Stoga zaključujemo da nije moguće posložiti brojeve $1^1, 2^2, ..., 2008^{2008}$ jedan za drugim tako da dobiveni broj bude kvadrat nekog prirodnog broja.

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

14. 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 $p^2 - 2q^2 \equiv 1 - 2 = -1 \equiv 5 \pmod 6$, a kako je desna strana jednadžbe 1 (mod 6), jednadžba 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 $(p, q) = (3, 2)$.

15. Općinsko 2016. - 3. razred, 7. zadatak

16. Školsko 2021. - 3. razred, 7. zadatak

17. JBMO shortlist 2020. NT 1.

18. JBMO shortlist 2020. NT 2.