S1	Seniorska grupa

Predavanja subotom
Zagreb, sezona 2019./2020.

Kongruencije i sustavi ostataka

Krunoslav Ivanović

5. listopada 2019.

Mladi nadareni matematičari "Marin Getaldić"

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

Uvod

Već u ranim razredima osnovne škole naučimo što su prosti brojevi, ali izuzev faktorizacije složenih brojeva u njih, nikad se ne upoznamo pobliže s njihovim svojstvima. Upravo zbog toga što imaju samo 2 djeljitelja, sebe samog i jedinicu, postoje razni teoremi koji vrijede isključivo za proste brojeve. Jedan od njih je i Mali Fermatov teorem, ali prije nego što do njega dođemo, moramo prvo definirati neke pojmove.

1 Kongruencije

Promotrimo sljedeće skupove $\{1, 8, 15, 22, \ldots\}, \{2, 9, 16, 23, \ldots\}, \ldots, \{7, 14, 21, 28, \ldots\}$. Uočimo da se svaki od prirodnih brojeva nalazi u točno jednom od tih skupova, odnosno, kažemo da ti skupovi čine particiju skupa $\mathbb{N}$. Ono što je posebno kod tih skupova jest to što svaka dva člana u nekom od skupova daju isti ostatak pri dijeljenju sa sedam, odnosno, ako odaberemo neke brojeve a i b iz jednog od skupova, imamo $7 \mid a - b$[1].
Kao što smo napravili particiju skupa $\mathbb{N}$ ovisno o ostatku pri dijeljenju sa sedam, tako možemo napraviti i za bilo koji prirodni broj n. Pri tome uvodimo novu oznaku, $\equiv$, gdje vrijedi

$$a \equiv b \pmod{n} \iff n \mid a - b.$$

U pravilu, oznaka kongruencije ništa ništa drugo doli ljepši način da zapišemo da neka dva broja a i b daju isti ostatak pri dijeljenju s n.

Definicija 1.1 (Kongruencija)
Neka su n, a i b prirodni brojevi. Kažemo da je a kongruentno b modulo n (zapisujemo $a \equiv b \pmod{n}$) ako i samo ako n dijeli $a - b$ (zapisujemo $n \mid a - b$)

Unatoč tome što se trenutno čini redundatno uopće definirati neki novi simbol samo da bi istaknuli da dva broja daju isti ostatak pri dijeljenju s trećim, kongruencije imaju neka lijepa svojstva s kojima možemo raditi. Vrijede sljedeće stvari:

- Ako je $a \equiv b \pmod{n}$ i $c \equiv d \pmod{n}$, vrijedi $a \pm c \equiv b \pm d \pmod{n}$.
- Ako je $a \equiv b \pmod{n}$ i $c \equiv d \pmod{n}$, vrijedi $ac \equiv bd \pmod{n}$.
- Ako je $ac \equiv bc \pmod{n}$ i $\gcd(c, n) = 1$, vrijedi $a \equiv b \pmod{n}$.

Ono što trenutno ostaje nedorečeno jest dijeljenje kongruencija, no na to ćemo se vratiti kasnije. Uočimo da će nam od posebnog interesa biti promatranje kongruencija modulo neki prost broj, upravo zbog činjenice da ima samo 2 djeljitelja te je zbog toga skoro pa svaki broj relativno prost s njim.

2 Sustavi ostataka

Već u ranim razredima osnovne škole naučimo kako podijeliti dva broja. Ono što također naučimo da neki brojevi, nakon dijeljenja, daju ostatak i da je taj ostatak nužno manji od samog broja s kojim smo dijelili. U duhu tog, definirati ćemo dva skupa koji imaju veze s ostacima.

[1] čitamo 7 dijeli $a - b$

Definicija 2.1 (Potpuni sustav ostataka)

Skup $\mathcal{S}_\text{P}$ ćemo nazivati potpuni sustav ostataka modulo n ako se u njemu pojavljuju svi ostaci pri dijeljenju s n, odnosno, $\mathcal{S}_\text{P} = \{0, 1, 2, 3 \ldots, n-1\}$.

Kao što smo vidjeli u svojstvima kongruencija, ponekad je važno da neki ostatak bude relativno prost s modulom. Upravo zbog toga ćemo definirati i reducirani skup ostataka.

Definicija 2.2 (Reducirani sustav ostataka)

Skup $\mathcal{S}_\text{R}$ ćemo nazivati reduciranim sustav ostataka modulo n ako se u njemu pojavljuju svi ostaci pri dijeljenju s n koji su relativno prosti s n, odnosno, formalije zapisano, $\mathcal{S}_\text{R} = \{x \mid 0 \leq x < n, \gcd(x, n) = 1\}$.

U posebnom slučaju kada je n prost, $\mathcal{S}_\text{P} = \{0, 1, 2, \ldots, p-1\}$, a $\mathcal{S}_\text{R} = \{1, 2, 3 \ldots, p-1\}$. Sustavi ostataka su zanimljivi za promatrati zbog sljedećeg svojstva.

Teorem 2.3 (Invarijantnost sustava ostataka pod zbrajanjem)

Neka je a neki prirodan broj koji nije djeljv s n i neka je $a_i = i + a \pmod{n}, \forall i \in \{0, 1, 2, \ldots, n-1\}$. Tada je skup $\mathcal{A} = \{a_0, a_1, \ldots, a_{n-1}\}$ potpuni sustav ostataka modulo n.

Dokaz. Pretpostavimo da postoje neki a_i i a_j takvi da je $a_i \equiv a_j \pmod{n}$. Onda iz definicije vrijedi $a + i \equiv a + j \pmod{n}$, odnosno, $i \equiv j \pmod{n}$, što je besmisleno, odnosno, početna pretpostavka je pogrešna. Kako postoji točno n brojeva koji svi daju različite ostatke, nužno je da je skup $\mathcal{A}$ potpun sustav ostataka. □

Osim što je sustav ostataka invarijantan pod zbrajanjem, invarijantan je i pod množenjem.

Teorem 2.4 (Invarijantnost sustava ostataka pod množenjem)

Neka je p neki prost broj i neka je a prirodan broj koji nije djeljiv s p. Definiramo $a_i = i \cdot a \pmod{p}, \forall i \in \{0, 1, 2, \ldots, p-1\}$. Tada je skup $\mathcal{A} = \{a_0, a_1, \ldots a_{p-1}\}$ potpuni sustav ostataka modulo p.

Dokaz. Pretpostavimo da postoje neki a_i i a_j takvi da je $a_i \equiv a_j \pmod{p}$. Onda iz definicije vrijedi $a \cdot i \equiv a \cdot j \pmod{p}$, odnosno, $i \equiv j \pmod{p}$, što je besmisleno, odnosno, početna pretpostavka je pogrešna. Kako postoji točno p brojeva koji svi daju različite ostatke, nužno je da je skup $\mathcal{A}$ potpun sustav ostataka. □

Kao što vidimo, potpun sustav ostataka možemo "transformirati" s množenjem i zbrajanjem te ovisno s čime množimo i zbrajamo, on još uvijek ostaje potpun sustav ostataka. Sljedeće vrijedi za reducirani skup ostataka.

Teorem 2.5 (Invarijantnost reduciranog sustava ostataka pod množenjem)

Neka je $\mathcal{S}_\text{R} = \{a_0, a_1, \ldots, a_k\}$ reducirani sustav ostataka modulo n, i neka je a neki broj relativno prost s n. Onda je skup $\mathcal{A} = \{a \cdot a_0, a \cdot a_1, \ldots, a \cdot a_k\}$ reducirani sustav ostataka modulo n gledajući svaki od elemenata skupa modulo n.

Dokaz. Dokaz se provodi analogno kao i dokaz za potpuni sustav ostataka pa ga je nepotrebno pisati u potpunosti. □

2.1 Dijeljenje kongruencija

Prethodno u predavanju spomenuli smo da dijeljenje kongruencija trenutačno nećemo definirati, no došlo je vrijeme i za to. Prvenstveno ćemo definirati "dijelenje" za proste module čisto zbog "lakše" argumentacije, no ista argumentacija radi za složene module i brojeve relativno proste s tim modulom.
Umjesto da klasično definiramo dijeljenje, za svaki broj a, definirati ćemo a^{-1}(možemo pisati i $\frac{1}{a}$) koji će označavati multiplikativni inverz od a, odnosno, vrijediti će $a \cdot a^{-1} \equiv 1 \pmod{p}$.

Za početak, uočimo da će svaki broj (izuzev nule) nužno imati svoj multiplikativni inverz. Naime, uzmemo li potpuni sustav ostataka modulo p te svaki od članova pomnožimo s a, opet dobivamo potpuni sustav ostataka. Kako je $1 \in \mathcal{S}_{\mathrm{P}}$, znamo da postoji neki i takav da je $i \cdot a \equiv 1 \pmod{p}$. Također, uočimo da je za a, takav i jedinstven, odnosno, kada bi vrijedilo da je $a \cdot i \equiv 1 \equiv j \cdot a \pmod{p}$, imali bi i $i \equiv j \pmod{p}$ što je besmisleno.
Dakle, pokazali smo da svaki broj a ima svoj jedinstven multiplikativni inverz modulo p. Također, ako je b multiplikativni inverz od a, tada je i a multiplikativni inverz od b, odnosno, $(a^{-1})^{-1} = a$.

Definicija 2.6 (Dijeljenje s kongruencijama)
Dijelenje u kongruencijama definiramo kao množenje s multiplikativnim inverzom.

Zapravo je potpuno jednako kao i dijeljenje u cijelim brojevima, samo nije u potpunosti jasno da će svaki broj imati svoj multiplikativni inverz, odnosno, da će dijeljenje biti "dobro" definirano.

3 Mali Frematov teorem

Nakon što smo definirali kongruencije i sustave ostataka te promotrili što s njima možemo raditi, vrijeme je da dokažemo centralni teorem i ideju našeg predavanja, a to je mali Frematov teorem.

Teorem 3.1 (Mali Frematov teorem)
Neka je p prost broj. Onda za svaki prirodan broj a relativno prost s p vrijedi

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

Dokaz. Neka je $X = 1 \cdot 2 \cdot \ldots \cdot (p-1)$ i neka je a relativno prost s p. Promotrimo $\mathcal{S}_{\mathrm{R}}$ i $\mathcal{A} = \{a, 2a, \ldots, (p-1)a\}$. Znamo da je i $\mathcal{A}$ reducirani sustav ostataka nakon reduciranja članova modulo p pa znamo da je

$$1 \cdot 2 \cdot \ldots \cdot (p-1) \equiv a \cdot 2a \cdot \ldots \cdot (p-1)a \pmod{p},$$

odnosno,

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

odakle slijedi $a^{p-1} \equiv 1 \pmod{p}$. □
Ekvivalentna tvrdnja, teoremu, bez uvjeta da je a relativno prost s p je $a^p \equiv a \pmod{p}$. Iako se čini malo apstraktan, mali Frematov teorem može pomoći u brojnim zadacima, na primjer,

Primjer 3.1. Odredite ostatak pri dijeljenju broja 4^{2019} s 7.

Rješenje 3.1. Jasno je da nećemo moći direktno izračunati 4^{2019} pa dijeliti sa 7. Upravo u ovakvim zadacima pomaže mali Frematov teorem. Znamo da je $4^6 \equiv 1 \pmod{7}$ pa je

$$4^{2019} = (4^6)^{336} \cdot 4^3 \equiv 4^3 \equiv 1 \pmod{7}.$$

Izuzev u ovakvim zadacima, mali Frematov teorem može pomoći i u "apstraktnijim" problemima, recimo

Primjer 3.2. Ako su p i q različiti prosti brojevi, pokaži da je $p^{q-1} + q^{p-1} - 1$ djeljivo s pq.

Rješenje 3.2. Dokazati ćemo da $p \mid p^{q-1} + q^{p-1} - 1$, a dokaz za q će biti analogan. Za početak, uočimo da očito vrijedi $p \mid p^{q-1}$. Također, vrijedi $q^{p-1} \equiv 1 \pmod{p}$, odnosno, $p \mid q^{p-1} - 1$. Promatrajući ove dvije tvrdnje zajedno, imamo $p \mid p^{q-1} + q^{p-1} - 1$ što smo trebali i dokazati.

4 Eulerov teorem

Kao što smo za većinu stvari do sada imali "generalan" slučaj i slučaj kada je modul prost broj, tako i mali Frematov teorem ima generalizaciju. Prije nego što iskažemo teorem, potrebno je definirati novu funkciju.

Definicija 4.1 (Eulerova fi funkcija)
Eulerova fi funkcija (označavamo $\varphi(n)$) označava broj brojeva relativno prostih s n.

Za funkciju vrijede brojne stvari, no one nadilaze potrebu predavanja pa ih ovdje nećemo navoditi. Ono što hoćemo navesti jest Eulerov teorem, koji kaže

Teorem 4.2 (Eulerov teorem)
Neka je n prirodan broj i neka je a broj relativno prost s n. Onda je

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

Dokaz teorema nećemo ovdje navoditi jer je jako sličan dokazu malog Fermatovog teorema. Uočimo da je mali Fermatov teorem poseban slučaj Eulerovog teorema kada je n prost.

Pozor!
Stvari za zapamtiti:

- Mali Fermatov i Eulerov teorem
- kongruencije i dozvoljene operacije s njima
- skupovi koji se ne mijenjaju nakon što obavimo neku operaciju nad njima su korisni

5 Zadaci

Zadaci su subjektivno poredani po težini, težina varira od jednostavnih do lakših olimpijskih zadataka, a koriste se isključivo koncepti prikazani u prethodnom tekstu.

1. Nađite ostatak pri dijeljenju broja $3^{100} + 5^{100}$ brojem 7.
2. Dokažite kriterije djeljivosti sa $3, 9$ i 11. Ako ne znate neki od njih, pokušajte zaključiti.
3. Odredi sve proste brojeve p takve da $p \mid 2019^{p^{2019}} + 2$.
4. Dokažite da za svaki prost broj p postoji beskonačno mnogo brojeva oblika $2^n - n, n \in \mathbb{N}$ djeljivih s p.
5. Ako prost broj p dijeli $a^p - 1$ za neki $a \in \mathbb{N}$, pokaži da onda i p^2 dijeli $a^p - 1$.
6. Dokaži Wilsonov teorem, odnosno, dokaži da je za prost p,
$$(p-1)! \equiv -1 \pmod{p}.$$
7. Nađi sve prirodne brojeve relativno proste sa svim članovima beskonačnog niza
$$a_n = 2^n + 3^n + 6^n - 1, \ n \geq 1.$$
8. Neka je n prirodan broj i neka su $a_1, a_2, a_3, \ldots, a_k$ $(k \geq 2)$ različiti prirodni brojeve iz skupa $\{1, 2, \ldots, n\}$ takvi da n dijeli $a_i(a_{i+1} - 1)$ za $i = 1, 2, \ldots, k-1$. Dokaži da n ne dijeli $a_k(a_1 - 1)$.
9. Neka je $p > 2$ prost broj takav da $3 \mid p - 2$. Neka je
$$S = \{y^2 - x^3 - 1 \mid 0 \leq x, y \leq p - 1 \cap x, y \in \mathbb{Z}\}.$$
Pokaži da je maksimalno p elemenata skupa S djeljivo s p.