MetaMath tečaj 2025.

7. tjedan

Mali Fermatov i Eulerov teorem

Dario Vuksan

10.11.2025.

Uvod i primjeri

Za ovu temu potrebno je osnovno predznanje o modularnoj aritmetici, tj. kongruencijama. Ako se nikad nisi susreo/la s tim nazivom, preporučam da pogledaš ovo predavanje da se upoznaš s kongruencijama, pročitaš svojstva i proučiš nekoliko primjera jednostavnih zadataka.

Na početku ćemo kratkom intuitivnom opservacijom napraviti uvod u mali Fermatov teorem i pokazati njegovu primjenu na nekoliko malih primjera. Zatim ćemo uvesti pojam Eulerove funkcije i na kraju Eulerov teorem koji je ustvari generalizacija malog Fermatovog teorema.

Napomena: Zapis $a \equiv b \pmod{n}$, koji uključuje znak $\equiv$ i zagrade oko mod, podrazumijeva kongruenciju modulo n i takva se relacija razlikuje od jednakosti. Pored toga, zapis $a \bmod b$ predstavlja binarnu operaciju čiji je rezultat ostatak pri dijeljenju a brojem b, odnosno jedinstveni nenegativni cijeli broj r $(0 \leq r < b)$ za koji vrijedi $r \equiv a \pmod{b}$. Čitatelji upoznati s programiranjem prepoznat će $a \bmod b$ kao operaciju koja je u mnogim programskim jezicima definirana znakom %. Broj n kojim radimo modulo operacije u literaturi se naziva *modulus*, stoga ću ga tako nazivati i u ovom predavanju.

Zašto uopće promatrati potencije? Kada potenciramo cijele brojeve modulo n, postoji konačno mnogo mogućih rezultata, načelno zato što postoji konačno mnogo ostataka modulo n, oni su od 0 do $n-1$. To znači da kad višestruko množiš istim brojem a, niz ostataka će se eventualno ponavljati, tj. napravit će *ciklus*. Na primjer, modulo 7:

$3^0 \equiv 1$
$3^1 \equiv 3$
$3^2 \equiv 9 \equiv 2$
$3^3 \equiv 2 \cdot 3 \equiv 6$
$3^4 \equiv 6 \cdot 3 \equiv 18 \equiv 4$
$3^5 \equiv 4 \cdot 3 \equiv 12 \equiv 5$
$3^6 \equiv 5 \cdot 3 \equiv 15 \equiv 1$

Ostatci se ciklički vraćaju na 1 na šestoj potenciji. Ovo nije slučajnost: kada je modulus p prost broj ($p = 7$ u našem primjeru), a broj kojeg množimo relativno prost s njim, nikada nećemo pogoditi nulu, jer ne možemo množenjem dva broja relativno prosta s p dobiti broj koji je djeljiv s p. U igri su samo ostatci $1, 2, \ldots, p-1$ - ima ih točno $p-1$, a ponavljano množenje istim brojem (kao što je u primjeru prikazano s 3) samo se "prebacujemo" s jednog od njih na drugi. Nakon $p-1$ množenja je očekivano da će ciklus tada završiti, a 1 će se pojaviti na kraju upravo zato što je i $a^0 \equiv 1$. Ovo je srž malog Fermatovog teorema. Međutim, to ne znači da se jedinica nužno neće pojaviti i ranije. Na primjer, u potencijama broja 2 modulo 7 ostatci će biti redom $2, 4, 1, 2, 4, 1$. Jedino što je važno je da je na šestom $(6 = 7-1)$ mjestu jedinica, a u slučaju da postoje manji ciklusi, kao što je ovdje $2, 4, 1$, njihova duljina uvijek će biti djelitelj duljine cijelog ciklusa, logično, jer se cijeli ciklus sastoji od nekog broja manjih ciklusa.

Teorem 1 *(Mali Fermatov teorem)*

Neka je a cijeli broj, a p prost broj. Ako su a i p relativno prosti, tj. $\gcd(a, p) = 1$, onda je $a^{p-1} \equiv 1 \pmod{p}$.

Ideja dokaza

U dokazu je ključna činjenica da skupovi brojeva $\{1, 2, 3, \ldots, p-1\}$ i $\{a, 2a, 3a, \ldots, (p-1)a\}$ imaju iste ostatke modulo p

Dokaz

Promotrimo prvih $p-1$ višekratnika broja a: $a, 2a, 3a, \ldots, (p-1)a$. Pokažimo prvo da su svi oni različiti modulo p. Naime, pretpostavimo da su neka dva ista: $ia \equiv ja \pmod{p}$ za neke i, j $(1 \leq i, j \leq p-1)$. Ta kongruencija ekvivalentna je $a\,(i-j) \equiv 0 \pmod{p}$. Budući da je $\gcd(a, p) = 1$, jedino je moguće da p dijeli $i-j$, odnosno $i-j = kp$ za neki k. Ali, i i j nalaze se između 1 i $p-1$, zato $i-j$ ne može biti nijedan višekratnik broja p osim nule, stoga je $i = j$. Dobili smo da $p-1$ brojeva $a, 2a, 3a, \ldots, (p-1)a$ daje različite ostatke modulo p, a dodatno nijedan od tih ostataka nije nula, zaključimo da su ti ostatci upravo $1, 2, 3, \ldots, p-1$ u nekom poretku.
Sada možemo zapisati ovu kongruenciju:

$$a \cdot 2a \cdot 3a \cdot \ldots \cdot (p-1)a \equiv 1 \cdot 2 \cdot 3 \cdot \ldots \cdot (p-1) \pmod{p}$$

$$a^{p-1}(p-1)! \equiv (p-1)! \pmod{p}$$

Vrijedi $\gcd(p, (p-1)!) = 1$, dakle, možemo "skratiti" $(p-1)!$ s obje strane kongruencije, pa konačno imamo

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

Propozicija 1

Za prost broj p i bilo koji cijeli broj a, uključujući i višekratnike od p, vrijedi $a^p \equiv a \pmod{p}$

Oprez

Ne vrijedi obrat malog Fermatovog teorema! Ako su a i n relativno prosti takvi da je $a^{n-1} \equiv 1 \pmod{n}$, iz toga ne slijedi da je n prost broj. Na primjer, uzmimo $a = 7$ i $n = 25$. Vrijedi $\gcd(7, 25) = 1$ i $7^{24} \equiv 1 \pmod{25}$ (ovo zahtijeva malo računanja), ali $25 = 5 \cdot 5$ je složen broj.

Korolar *(Fun fact)*

S druge strane, ako imamo broj x koji ne znamo je li prost ili složen, te odaberemo neki a njemu relativno prost, računanjem a^{x-1} modulo x, ako rezultat nije 1, zaključili smo da x nije prost broj iako ne znamo ništa o njegovim faktorima! Ovo se naziva *test prostosti* i specifično ovaj je u praksi vrlo slab, neki brojevi (npr. 1729) daju 1 za sve kandidate a.

Primjer 1

Izračunaj 3^{33} modulo 7. (Odredi ostatak pri dijeljenju broja 3^{33} sa 7.)

Rješenje

Budući da je 7 prost broj i $\gcd(3, 7) = 1$, mali Fermatov teorem govori $3^6 \equiv 1 \pmod{7}$. Eksponent 33 možemo zapisati kao $5 \cdot 6 + 3$ pa imamo:

$$3^{33} = 3^{5 \cdot 6 + 3} = 3^{5 \cdot 6} \cdot 3^3 = \left(3^6\right)^5 \cdot 3^3 \equiv 1^5 \cdot 3^3 \equiv 27 \equiv 6 \pmod{7}$$

Primjer 2

Odredi sve proste brojeve p takve da je $29^p + 1$ djeljiv s p.

Ideja rješenja

Iskoristimo mali Fermatov teorem za $a = 29$

Rješenje

Tvrdnja zadatka zapisana kao kongruencija glasi $29^p + 1 \equiv 0 \pmod{p}$.
Prema malom Fermatovom teoremu imamo $29^p \equiv 29 \pmod{p}$.
Kombiniranjem te dvije kongruencije dobivamo $30 \equiv 0 \pmod{p}$ iz čega slijedi da je p djelitelj broja 30.

Provjerom potvrdimo da brojevi $p = 2, 3, 5$ doista zadovoljavaju traženu tvrdnju.

Vratimo se na diskusiju s početka predavanja. Analizirali smo što se događa kad računamo potencije modulo neki prosti broj. Što ako modulus n nije prost? Tada će, jasno, biti manje od $n-1$ brojeva u skupu ostataka. Promatrat ćemo samo potencije brojeva koji su relativno prosti s n. Pogledajmo potencije broja 2 modulo 9:
$2^1 \equiv 2$
$2^2 \equiv 4$
$2^3 \equiv 8$
$2^4 \equiv 16 \equiv 7$
$2^5 \equiv 14 \equiv 5$
$2^6 \equiv 10 \equiv 1$
i to je kraj ciklusa, odavde će se ostaci samo ponavljati.

Za složene brojeve n, broj različitih ostataka dok ne dođemo do kraja ciklusa je općenito jednak vrijednosti $\varphi(n)$ (vidi dolje za definiciju Eulerove funkcije). Iz potpunog skupa ostataka $1, 2, \ldots, n-1$ jednostavno smo, osim nule, izbacili sve one koji nisu relativno prosti s n. Ako počnemo od nekog broja koji je relativno prost s n, i množimo ga relativno prostim brojem, logički se može zaključiti da nikada nećemo dotaknuti broj koji nije relativno prost s n. Sve koji nisu relativno prosti smo maknuli iz skupa $\{1, 2, 3, \ldots, n-1\}$ i preostalo nam je $\varphi(n)$ brojeva.

Definicija *(Eulerova funkcija)*

Eulerova funkcija je funkcija $\varphi(n)$ (čita se *fi* od n) koja svakom prirodnom broju $n > 1$ pridružuje broj relativno prostih brojeva s n koji su manji od n. Posebno je definirano $\varphi(1) = 1$.

Na primjer: $\varphi(12) = 4$, od brojeva $1, 2, 3, 4, 5, 6, 7, 8, 9, 10$ i 11, samo su $1, 5, 7$ i 11 relativno prosti s 12.

Lema 1 *(Korisna svojstva Eulerove funkcije)*

$\varphi(p) = p - 1$ za prosti broj p

$\varphi(m) \cdot \varphi(n) = \varphi(mn)$ za relativno proste $m, n \in \mathbb{N}$

$\varphi(p^k) = p^k - p^{k-1}$

$\sum_{d|n} \varphi(d) = n$ (za sve djelitelje d_i broja n vrijedi $\varphi(d_1) + \varphi(d_2) + \ldots + \varphi(d_k) = n$)

Korolar

Ako je rastav broja n na proste faktore $p_1^{\alpha_1} p_2^{\alpha_2} \dots p_m^{\alpha_m}$, tada je

$$\varphi(n) = n\left(1 - \frac{1}{p_1}\right)\left(1 - \frac{1}{p_2}\right)\dots\left(1 - \frac{1}{p_m}\right)$$

Ovaj korolar može se dokazati i kombinatornim prebrojavanjem, npr. ako je $S = \{1, 2, \dots, n\}$ i za svaki prosti djelitelj p_i od n definiramo $A_i = \{x \in S : p_i | x\}$, tada je $\varphi(n) = |S| - |A_1 \cup A_2 \cup \dots \cup A_k|$

Primjer 3

Odredi $\varphi(300)$

Rješenje

Faktoriziramo $300 = 2^2 \cdot 3 \cdot 5^2$. Izračunamo

$$\varphi(300) = 300\left(1 - \frac{1}{2}\right)\left(1 - \frac{1}{3}\right)\left(1 - \frac{1}{5}\right) = 300 \cdot \frac{1}{2} \cdot \frac{2}{3} \cdot \frac{4}{5} = 80$$

Teorem 2 *(Eulerov teorem)*

Ako su a i n relativno prosti brojevi, tada vrijedi $a^{\varphi(n)} \equiv 1 \pmod{n}$

Ideja dokaza

Analogija s malim Fermatovim teoremom, samo što promatramo reducirani skup ostataka $\{1, 2, 3, \dots, n-1\}$

Dokaz

Neka su $r_1, r_2, \dots, r_{\varphi(n)}$ svi brojevi manji od n i relativno prosti s n. Primjerice, za $n = 12$, to su $1, 5, 7, 11$.

Kao i u dokazu malog Fermata, množenje svakog broja nekim brojem a ($\gcd(a, n) = 1$) modulo n samo će permutirati te brojeve, tj. tvrdimo da su brojevi

$$ar_1, ar_2, \dots, ar_{\varphi(n)}$$

također svi različiti modulo n i svaki je relativno prost s n.

Dokaz da su različiti: ako je $ar_i \equiv ar_j \pmod{n}$, tada je $a(r_i - r_j) \equiv 0 \pmod{n}$. Budući da je $\gcd(a, n) = 1$, slijedi $r_i \equiv r_j \pmod{n}$, pa $i = j$.

Dokaz da su relativno prosti: vrijedi $\gcd(a, n) = 1$ i $\gcd(r_i, n) = 1$, stoga je sigurno i $\gcd(ar_i, n) = 1$, jer nije moguće da množenjem dva broja relativno prosta s n dobijemo umnožak koji nije relativno prost s n.

Dakle, skup $\{ar_1, ar_2, \dots, ar_{\varphi(n)}\}$ je isti skup kao i $\{r_1, r_2, \dots, r_{\varphi(n)}\}$ kada elemente promatramo modulo n.

Nastavljamo kao i u dokazu MFT:

$$(ar_1) \cdot (ar_2) \cdot \dots \cdot (ar_{\varphi(n)}) \equiv r_1 \cdot r_2 \cdot \dots \cdot r_{\varphi(n)} \pmod{n}$$

Lijeva strana je $a^{\varphi(n)} \cdot \left(r_1 \cdot r_2 \cdot \dots \cdot r_{\varphi(n)}\right)$, a kako su svi r_i relativno prosti s n, tako je i njihov umnožak, pa ga možemo skratiti s obje strane da dobijemo

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

što je trebalo dokazati.

Za pojednostavljivanje velikih potencija korisna je sljedeća lema čiji je dokaz ostavljen tebi kao zadatak.

Lema 2

Za relativno proste a i n vrijedi $a^b \equiv a^{b \bmod \varphi(n)} \pmod{n}$

Primjer 4

Dokaži da $51 \mid 10^{32n+9} - 7$ za svaki prirodni n.

Rješenje

Moramo pokazati da je $10^{32n+9} \equiv 7 \pmod{51}$.

Imamo $\varphi(51) = 32$ i $\gcd(10, 51) = 1$ pa je po Eulerovom teoremu $10^{32} \equiv 1 \pmod{51}$, a potenciranjem te kongruencije slijedi $10^{32n} \equiv 1 \pmod{51} \iff 10^{32n+9} \equiv 10^9 \pmod{51}$.

Preostaje pokazati da je $10^9 \equiv 7 \pmod{51}$. Počevši od $10^2 = 100 \equiv -2 \iff 10^8 \equiv 16 \pmod{51}$, stoga je $10^9 \equiv 160 = 3 \cdot 51 + 7 \equiv 7 \pmod{51}$.

Primjer 5

Odredi zadnje dvije znamenke broja $3^{3^{3^3}}$.

Ideja rješenja

Koristimo Lemu 2.

Rješenje

Zadnje dvije znamenke znači odredimo kongruenciju modulo 100.

$3^{3^{3^3}} \equiv 3^{\left(3^{3^3} \bmod \varphi(100)\right)} \pmod{100}$

Imamo $\varphi(100) = 40$ i sada nas zanima $3^{3^3} \equiv ? \pmod{40}$

Imamo $\varphi(40) = 16$ pa je $3^{3^3} \equiv 3^{3^3 \bmod 16} \equiv 3^{11} \equiv 27 \pmod{40}$ - to lagano izračunamo koristeći činjenicu da je $3^4 = 81 \equiv 1 \pmod{40}$. Dobili smo da je $3^{3^3} \equiv 27 \pmod{40}$ i vraćanjem u prvu kongruenciju slijedi:

$3^{3^{3^3}} \equiv 3^{\left(3^{3^3} \bmod \varphi(100)\right)} \equiv 3^{27} \pmod{100}$

Računanje 3^{27} modulo 100 je jednostavno, ali dugačko, zato ćemo ga izostaviti u ovom rješenju. Tražene dvije znamenke su 87.

Evo nešto što će biti korisno u nekim zadacima:

Propozicija 2

Neka su m i n relativno prosti brojevi i a, b takvi da vrijedi:

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

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

Tada vrijedi $a \equiv b \pmod{mn}$. Dokaz je intuitivan: m i n oba dijele $a - b$, a relativno su prosti, pa slijedi $mn \mid a - b$.

Sretno u rješavanju!

Lagani lanac

Zadatak 1

Izračunaj 128^{131} modulo 17.

Ideja rješenja

Primijenimo Lemu 2

Rješenje

$128^{131} \equiv 128^{131 \bmod \varphi(17)} \equiv 128^3 \pmod{17}$

Dodatno je $128 \equiv 9 \pmod{17}$ pa je $128^3 \equiv 9^3 \pmod{17}$.

Odavde jednostavno izračunamo rješenje 15.

Zadatak 2

Odredi posljednje dvije znamenke broja $7^{7^{100}}$.

Ideja rješenja

Primijenimo Lemu 2

Rješenje

Prema Lemi 2: $7^{7^{100}} \equiv 7^{7^{100} \bmod \varphi(100)} \pmod{100}$

Treba odrediti $7^{100} \pmod{40}$:

$$7^{100} \equiv 7^{100 \bmod \varphi(40)} \equiv 7^{100 \bmod 16} \equiv 7^4 \equiv \left(7^2\right)^2 \equiv 9^2 \equiv 1 \pmod{40}$$

Konačno je $7^{7^{100}} \equiv 7^1 \pmod{100}$. Posljednje dvije znamenke su 07.

Zadatak 3

Odredi $2^{20} + 3^{30} + 4^{40} + \ldots + 9^{90} \pmod{7}$.

Ideja rješenja

MFT ili Lema 2.

Rješenje

$7^{70} \equiv 0 \pmod{7}$. Za ostale primjenimo lemu:

$$2^{20}+3^{30}+4^{40}+\ldots+9^{90} \equiv 2^2+3^0+4^4+5^2+6^0+0+8^2+9^0 \equiv 4+1+4+4+1+0+1+1 \equiv 2 \pmod{7}$$

Zadatak 4

Pretpostavimo da $14 \mid a_1 + a_2 + \ldots + a_{2025}$. Dokaži da tada $14 \mid a_1^7 + a_2^7 + \ldots + a_{2025}^7$.

Ideja rješenja

Promotrimo jedan član. Kada je broj djeljiv s 14?

Rješenje

Broj je djeljiv s 14 ako je istovremeno djeljiv i s 2 i s 14. Očito je da je $a_i \equiv a_i^7 \pmod 2$ jer su iste parnosti, a po malom Fermatovom teoremu vrijedi $a_i^7 \equiv a \pmod 7$. Kombiniranjem te dvije kongruencije koristeći tvrdnju iz Propozicije 2 zaključimo:

$$a_i^7 \equiv a \pmod{14}$$

odnosno svaki broj daje isti ostatak pri dijeljenju s 14 kao i njegova sedma potencija. Odavde slijedi tvrdnja zadatka.

Zadatak 5

Dokaži lemu: za relativno proste a i n vrijedi $a^b \equiv a^{b \bmod \varphi(n)} \pmod n$

Ideja rješenja

Zapis kongruencije kao jednakosti (teorem o dijeljenju s ostatkom)

Rješenje

Označimo $b \bmod \varphi(n) = r$. Zapisano preko kongruencije glasi $b \equiv r \pmod{\varphi(n)}$, a preko jednakosti $b = k \cdot \varphi(n) + r$ za neki k.

Uvrštavanjem slijedi $a^b = a^{k\cdot\varphi(n)+r} = a^{k\cdot\varphi(n)} \cdot a^r = \left(a^{\varphi(n)}\right)^k \cdot a^r \equiv 1^k \cdot a^r \equiv a^r \pmod n$

Umjereni lanac

Zadatak 1

Odredi sve proste brojeve p takve da $p^2 \mid 5^{p^2}+1$.

Ideja rješenja

Koristit ćemo mali Fermatov teorem da smanjimo eksponent.

Rješenje

Prema MFT-u vrijedi $5^p \equiv 5 \pmod{p}$ (bez obzira na to je li $\gcd(p,5)=1$). Primijetimo da $p^2 \mid 5^{p^2}+1 \Longrightarrow p \mid 5^{p^2}+1$, tj. zapisano pomoću kongruencija:

$$5^{p^2}+1 \equiv 0 \pmod{p^2} \Longrightarrow 5^{p^2}+1 \equiv 0 \pmod{p}$$

Vrijedi $5^{p^2} = (5^p)^p$ pa primjenom ranije spomenutog MFT-a dobijemo

$$5^{p^2}+1 \equiv (5^p)^p+1 \equiv 5^p+1 \equiv 5+1 \equiv 0 \pmod{p}$$

odakle postoje dvije mogućnosti: $p=2$ i $p=3$. Provjera:

$p=2 \to 5^{2^2}+1 \equiv 1^4+1 \equiv 2 \pmod{4}$

$p=3 \to 5^{3^2}+1 \equiv \left(5^3\right)^3+1 \equiv 8^3+1 \equiv 0 \pmod{9}$

Jedini p s traženim svojstvom je 3.

Zadatak 2

Odredi

$$3!^{4!^{5!^{6!}}} \pmod{11}$$

Ideja rješenja

Primjena Leme 2 s oprezom na relativnu prostost

Rješenje

Na početku odmah primijenimo lemu jer je $\gcd(3!,11)=1$:

$$3!^{4!^{5!^{6!}}} \equiv 6^{4!^{5!^{6!}} \bmod 10} \pmod{11}$$

Da bismo odredili $4!^{5!^{6!}} \pmod{10}$, ne možemo primijeniti Eulerov teorem niti lemu zato što $4!$ i 10 nisu relativno prosti. Ipak, $4!=24$ i možemo lako uočiti da parne potencije broja 24 završavaju znamenkom 6, a neparne znamenkom 4. Očito je ovdje eksponent $5!^{6!}$ paran broj, stoga zaključimo $4!^{5!^{6!}} \equiv 6 \pmod{10}$. Konačno

$$3!^{4!^{5!^{6!}}} \equiv 6^6 \equiv \left(6^2\right)^3 \equiv 3^3 \equiv 5 \pmod{11}$$

Zadatak 3

Neka su p i q različiti prosti brojevi. Dokaži da vrijedi

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

Ideja rješenja

Propozicija 2, dokažemo posebno za $\pmod p$ i posebno za $\pmod q$

Rješenje

Po malom Fermatovom teoremu vrijedi

$$p^{q-1} \equiv 1 \pmod q \iff q \mid p^{q-1} - 1$$

Možemo slobodno dodati višekratnike broja q, zbroj će i dalje biti djeljiv s q: $q \mid p^{q-1} + q^{p-1} - 1$. Analogno $p \mid q^{p-1} + p^{q-1} - 1$. Zbog činjenice da su p i q relativno prosti, slijedi tvrdnja zadatka.

Zadatak 4

Dokaži da ne postoji $n > 1$ takav da $n \mid 2^n - 1$

Ideja rješenja

TODO

Rješenje

Očito n ne može biti paran broj jer paran broj ne može biti djelitelj neparnog broja. Dakle $\gcd(2, n) = 1$.

Ako je n prost broj, prema MFT-u vrijedi $2^n \equiv 2 \pmod n$, a tvrdnja zadatka je $2^n \equiv 1 \pmod n$. Kombiniranjem te dvije kongruencije slijedi $2 \equiv 1 \pmod n$ što je ekvivalentno $n \mid 1$, kontradikcija.

U drugom slučaju neka je $p \geq 3$ najmanji prosti djelitelj broja n i $k = \frac{n}{p}$. Vrijedi $2^n \equiv 1 \pmod p$ i $2^{p-1} \equiv 1 \pmod p$. Postoji ciklus ostataka duljine $p - 1$ i ciklus ostataka duljine n, s tim da je $p - 1 < n$. Mali Fermatov teorem nam govori da za svaki eventualni ciklus ostataka duljine $\leq n$, njegova duljina mora biti djelitelj broja n, kao što je razmotreno u uvodu (načelno zato što nekoliko tih kraćih ciklusa čine cijeli ciklus duljine n). Postoji ciklus duljine $p-1$ pa je $p-1 \mid n$. Međutim, $p \mid n$, što znači da dva broja p i $p-1$ koji su različite parnosti oba dijele n, a zaključili smo da n nema parnih djelitelja, došli smo do kontradikcije.

Dakle, ne postoji takav n.

Izazovni lanac

Zadatak 1

Dokaži da $221 \mid n^{n^{n^n}} - n^{n^n}$ za svaki $n \geq 3$.

Ideja rješenja

$221 = 13 \cdot 17$. Dokažemo posebno za $\pmod{13}$ i $\pmod{17}$

Rješenje

Prilagođeno prema ovom zadatku, na poveznici je navedeno i rješenje koje implicitno koristi Lemu 2.

Zadatak 2

Odredi sve prirodne brojeve n za koje je $\varphi(n) = \frac{n}{2}$

Ideja rješenja

Koristi formulu za Eulerovu funkciju, malo ju transformiraj i promatraj parnost.

Rješenje

$$\varphi(n) = n\left(1 - \frac{1}{p_1}\right)\ldots\left(1 - \frac{1}{p_m}\right) = \frac{n}{2}$$

Želimo postići $\left(1 - \frac{1}{p_1}\right)\ldots\left(1 - \frac{1}{p_m}\right) = \frac{1}{2}$. Ako je $p_1 = 2$, tada je to ujedno jedini prosti faktor, jer bi dodavanjem novih umnožak na lijevoj strani postao manji od $\frac{1}{2}$. Odavde je $n = 2^k$.

U slučaju da ne uzmemo 2 kao prosti faktor, svi p_i su neparni. Svaki faktor $1 - \frac{1}{p_i} = \frac{p_i - 1}{p_i}$ imat će paran brojnik i neparan nazivnik:

$$\frac{(p_1 - 1)(p_2 - 1)\ldots(p_m - 1)}{p_1 p_2 p_3 \ldots p_m} = \frac{1}{2} \iff 2(p_1 - 1)(p_2 - 1)\ldots(p_m - 1) = p_1 p_2 p_3 \ldots p_m$$

Desna strana je neparan broj, a lijeva paran - kontradikcija. Uočite da smo mogli direktno dokazati da je 2 jedini mogući prosti faktor, jer umnožak na desnoj strani najviše može biti djeljiv s 2, nikako s 4, a zbog toga svaki $(p_i - 1)$ na lijevoj strani mora biti neparan.

Alternativno rješenje (izvor):

Samo neparni brojevi u skupu $\{1, 2, ..., 2^k\}$ su relativno prosti s 2^k, a oni čine polovicu brojeva u tom skupu, stoga je $\varphi(2^k) = \frac{2^k}{2} = 2^{k-1}$.

Pretpostavimo da je $n = 2^k b$ za neparan $b > 1$. Zbog multiplikativnosti Eulerove funkcije i $\gcd(2^k, b) = 1$, vrijedi:

$$\varphi(n) = \varphi(2^k b) = \varphi(2^k)\varphi(b) = 2^{k-1}\varphi(b)$$

gdje smo u zadnjoj jednakosti iskoristili činjenicu da je $\varphi(n) = \frac{n}{2}$ za $n = 2^k$. Mi želimo:

$$\varphi(n) = \frac{n}{2} = \frac{2^k b}{2} = 2^{k-1} b$$

pa iz dvije jednakosti slijedi $\varphi(b) = b$ što je moguće samo za $b = 1$, kontradikcija.

Zadatak 3 *(RSA kriptografija)*

Zadani su prirodni brojevi m, n i e uz uvjet $m < n$ i $n = pq$ je umnožak dva prosta broja. Broj d je inverz broja e modulo $\varphi(n)$, tj. vrijedi $ed \equiv 1 \pmod{\varphi(n)}$. Neka je $c \equiv m^e \pmod{n}$. Dokaži da je $m \equiv c^d \pmod{n}$.

Ideja rješenja

Uvrstimo c i vidimo gdje će nas to dovesti

Rješenje

Imamo $c^d \equiv (m^e)^d \equiv m^{ed} \pmod{n}$. Želimo dokazati $m^{ed} \equiv m \pmod{n}$.
Izraz $ed \equiv 1 \pmod{\varphi(n)}$ možemo zapisati kao $ed = k \cdot \varphi(n) + 1$ za neki $k \in \mathbb{N}$ i uvrstiti ga u m^{ed} pa je

$$m^{ed} = m^{k\cdot\varphi(n)+1} = m^{k\cdot\varphi(n)} \cdot m = \left(m^{\varphi(n)}\right)^k \cdot m$$

Odavde, ako je $\gcd(m, n) = 1$, prvi faktor u gornjem izrazu kongruentan je $1 \pmod{n}$ prema Eulerovom teoremu, pa je dokaz izravno gotov:

$$c^d \equiv m^{ed} \equiv \left(m^{\varphi(n)}\right)^k \cdot m \equiv 1^k \cdot m \equiv m \pmod{n}$$

U drugom slučaju, neka je $\gcd(m, n) = p$. To možemo napraviti bez smanjenja općenitosti jer je n umnožak dva prosta faktora pa je svejedno koji je p, a koji q. Osim toga, $\gcd(m, n) \neq n$ jer je $m < n$ pa je nemoguće da je n faktor od m.
Ako je m djeljiv brojem p, svaki njegov višekratnik također je djeljiv brojem p i vrijedi $m^{ed} \equiv m \pmod{p}$. S druge strane, sigurno je $\gcd(m, q) = 1$ (u suprotnom bi q bio djelitelj broja m, a kako je p isto djelitelj m, m bi bio djeljiv i njihovim umnoškom, odnosno n, što je kontradikcija uvjetu $m < n$), pa je prema Eulerovom teoremu $m^{\varphi(q)} = m^{q-1} \equiv 1 \pmod{q}$, iz čega slijedi

$$m^{ed} = m^{\varphi(n)\cdot k} \cdot m = \left(m^{q-1}\right)^{(p-1)\cdot k} \cdot m \equiv 1^{(p-1)\cdot k} \cdot m \equiv m \pmod{q}$$

U drugoj jednakosti uvrstili smo $\varphi(n) = \varphi(pq) = \varphi(p) \cdot \varphi(q) = (p-1)(q-1)$.

Konačno, iz dvije relacije $m^{ed} \equiv m \pmod{p}$ i $m^{ed} \equiv m \pmod{q}$ vrijedi $m^{ed} \equiv m \pmod{pq = n}$. (koristeći svojstvo na kraju uvoda i korišteno više puta u prijašnjim rješenjima)