T12	Teža grupa

Predavanja subotom
sezona 2020./2021.

Prosti brojevi

Maja Drmač

20. veljače 2021.

Mladi nadareni matematičari
"Marin Getaldić"

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

Uvod

Današnje predavanje je namijenjeno vježbanju zadataka koji se rješavaju koristeći svojstva prostih brojeva. Prisjetimo se nekih osnovnih teorema i definicija.

Neka su a i $b \in N$. Tada je *mjera* od a i b najveći zajednički djelitelj od a i b. Označava se kao $M(a,b)$ ili $\gcd(a,b)$. Vrijedi

$$M(a,1)=1,\ M(a,a)=a,\ M(a,0)=a,\ M(a,b)=M(b,a).$$

Brojeve a i b nazivamo *relativno prostima* ako $\gcd(a,b)=1$.

Prirodan broj nazivamo prostim ako ima točno dva djelitelja: samog sebe i 1. *1 nije prost broj!*
Euklidova lema: ako je p prost, $p|ab \Rightarrow p|a$ ili $p|b$.

Osnovni teorem aritmetike: svaki prirodni broj veći od 1 može se prikazati kao umnožak potencija prostih brojeva i to jedinstveno do na poredak faktora, tj. $n = p_1^{\alpha_1}p_2^{\alpha_2}...p_r^{\alpha_r}$ gdje su $p_1,...,p_r$ međusobno različiti prosti brojevi.

Eulerova ϕ funkcija: funkcija $\mathbb{N}\to\mathbb{N}$ gdje $\phi(n)$ predstavlja broj brojeva manjih od n koji su relativno prosti s n. Korisno svojstvo ove funkcije je da za m i n relativno proste vrijedi $\phi(mn)=\phi(m)\phi(n)$. Za proste brojeve vrijedi $\phi(p)=p-1$. Eksplicitna formula za broj $n=p_1^{k_1}p_2^{k_2}...p_r^{k_r}$ je

$$\phi(n)=n(1-\frac{1}{p_1})(1-\frac{1}{p_2})...(1-\frac{1}{p_r}).$$

Eulerov teorem: za a i m relativno proste vrijedi

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

Mali Fermatov teorem: ako je p prost broj tada za svaki a vrijedi

$$a^p\equiv a \pmod p.$$

Specijalno, ako je $\gcd(a,p)=1$ vrijedi

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

Wilsonov teorem: ako je p prost broj tada je $(p-1)!\equiv -1 \pmod p$.

Bertrandov postulat: za svaki $n>1$ postoji prost broj p takav da je $n<p<2n$.

Lakši zadaci

1. Ako je zbroj kvadrata tri prosta broja isto prost, dokaži da je barem jedan od brojeva jednak 3.
2. Odredi sve prirodne brojeve n za koje su među brojevima n, 4^n+1 i n^2+2 barem dva prosta broja.
3. Dokaži da za cijele brojeve x,y i prosti broj p vrijedi $(x+y)^p\equiv x^p+y^p \pmod p$.
4. Neka je p prost broj. Odredi sve parove cijelih brojeva (a,b) za koje vrijedi $p(a-2)=a(b-1)$.

Umjereni zadaci

5. Neka su p i q različiti neparni prosti brojevi. Dokaži da broj $(pq+1)^4 - 1$ ima barem četiri različita prosta djelitelja.

6. Dani su prosti broj p i prirodni broj $n \geq p-1$. Ako je broj $np+1$ kvadrat nekog prirodnog broja, dokaži da je $n+1$ zbroj kvadrata nekih p, ne nužno različitih, prirodnih brojeva.

7. a) Nađi sve proste brojeve p takve da $p \mid 2^p - 1$.
   b) Koliko ima prirodnih brojeva $m \leq 1000$ za koje postoji prirodan $n \leq 1000$ takav da $m \mid 2^n - 1$?

8. Nađi sve proste brojeve p, q za koje je $p^{2q} + q^{2p}$ isto prost.

9. Nađi sve proste brojeve p i q takve da je $p^{q-1} + q^{p-1}$ kvadrat prirodnog broja.

Teži zadaci

10. Neka je $n \in \mathbb{N}$ takav da je
$$\sum_{i=1}^{23} \frac{1}{i} = \frac{n}{23!}.$$
Odredi $n \pmod{13}$.

11. Dva prosta broja p, q $(p > q)$ zadovoljavaju $p^q + 9q^6 = k^2$ gdje je k prirodan broj. Odredi $p+q$.

12. a) Dokaži da broj oblika n^2+1 nema prost faktor oblika $4k+3$, $k \in \mathbb{N}_0$.
   b) Dokaži da broj $4mn - m - n$ nije potpun kvadrat ni za koje $m, n \in \mathbb{N}$.

13. Neka su p i q prosti brojevi takvi da je $p = 2q+1$. Dokaži da je broj $(q!)^2 + (-1)^q$ djeljiv s p.

14. Nađi sve prirodne brojeve m, n takve da je $n! = m^4$.

Hintovi

1. Kvadrati modulo 3.
2. Modulo 2, 3, 5.
3. Binomna ekspanzija - što vrijedi za $\binom{p}{k}$ za $k = 1, 2, ..., p-1$?
4. $a \mid p(a-2) \Longrightarrow$?
5. Razlika kvadrata/faktorizacija. Svojstva $M(a, b)$.
6. Faktorizacija, rastavljanje na slučajeve.
7. a) Mali Fermatov teorem. b) Eulerov teorem.
8. Parnost i Mali Fermatov teorem.
9. Rastavljanje na slučajeve po parnosti.
10. Wilsonov teorem.
11. Faktorizacija, rastavljanje na slučajeve.
12. a) Mali Fermatov teorem. b) Pokušaj svesti na a) dio.
13. Wilsonov teorem.
14. Bertrandov postulat.

Rješenja

1. Županijsko 2009. SŠ A - 2. razred, 4. zadatak
2. Općinsko 2021. SŠ A - 1. razred, 7. zadatak
3. Po binomnom poučku je $(x+y)^p = \sum_{k=0}^{p} \binom{p}{k} x^{p-k}y^k = x^p + \sum_{k=1}^{p-1} \binom{p}{k} x^{p-k}y^k + y^p$. Za $k = 1, 2, ..., p-1$, $\binom{p}{k} = \frac{p!}{(p-k)!k!}$ je djeljivo s p: $(p-k)$ i k su manji od p pa ni $(p-k)!$ ni $k!$ nije djeljivo s p, a kako je $p!$ djeljivo s p, slijedi da je $\frac{p!}{(p-k)!k!}$ djeljivo s p. Sada vrijedi da je

   $$(x+y)^p = \sum_{k=0}^{p} \binom{p}{k} x^{p-k}y^k \equiv x^p + 0 + 0 + ... + 0 + y^p \equiv x^p + y^p \pmod{p},$$

   što je i trebalo dokazati.
4. Županijsko 2017. SŠ A - 2. razred, 1. zadatak
5. Općinsko 2010. SŠ A - 1. razred, 8. zadatak
6. Državno 2018. SŠ A - 1. razred, 3. zadatak
7. a) Očito $p = 2$ nije rješenje pa neka je $p > 2$. Uvjet zadatka možemo napisati kao $2^p \equiv 1 \pmod{p}$. Ali iz malog Fermatovog teorema slijedi $2^p \equiv 2 \pmod{p}$, kontradikcija. Ne postoji takav prost broj.
   b) Očito je da za svaki n je $2^n - 1$ neparno pa m ne može biti paran. Neka je m onda neparan broj, dakle $\gcd(m, 2) = 1$. Uočimo da je uvjet zadatka pronalaženje broja n takvog da $2^n \equiv 1 \pmod{m}$. Prisjetimo li se Eulerovog teorema, vidimo da za $n = \phi(m)$ vrijedi uvjet zadatka, a kako je $\phi(m) < m$ onda je sigurno uvijek $n \leq 1000$. Znači da za svaki neparni broj manji ili jednak 1000 postoji takav broj n, a neparnih brojeva manjih ili jednakih 1000 ima 500.
8. Neka je $p^{2q} + q^{2p} = r$ gdje je r prost broj. Uvrštavanjem vidimo da $p = q = 2$ nije rješenje i da je $r > 4$. Pretpostavimo da su i p i q neparni: tada je $p^{2q} + q^{2p}$ parno, odnosno r je paran, prost broj veći od 4 - kontradikcija. Znači da je ili p ili q paran, ali s obzirom da su oba broja prosta i znamo da $p = q = 2$ nije rješenje, točno jedan od ta dva broja je jednak 2. Bez smanjenja općenitosti, neka je $p = 2$. Početna jednadžba onda postaje

   $$2^{2q} + q^4 = r \Rightarrow 4^q + q^4 = r.$$

   Nadalje, promotrimo ovaj izraz modulo 5. Kako je $4 \equiv -1 \pmod{5}$, 4^q daje ostatak 1 ili -1 pri dijeljenju s 5, ovisno o parnosti broja q. Kako smo zaključili da je q neparan, znači da 4^q daje ostatak -1 pri dijeljenju s 5. S druge strane, q^4 daje ostatak 1 ili 0 pri dijeljenju s 5 zbog Malog Fermatovog teorema. Sada razlikujemo dva slučaja:

   1. slučaj: q^4 je dijeljiv s 5. Kako je q prost broj, a q^4 je djeljivo s 5 ako i samo ako je q dijeljiv s 5, jedina mogućnost je $q = 5$. Preostaje provjeriti je li $4^5 + 5^4 = 1649$ prost broj. Kako je $1649 = 17 \cdot 97$, ovaj slučaj nema rješenja.

   2. slučaj: q^4 daje ostatak 1 pri dijeljenju s 5. Kako 4^q daje ostatak -1 pri dijeljenju s 5, $4^q + q^4 \equiv -1 + 1 \equiv 0 \pmod{5}$, odnosno r je dijeljiv s 5. S obzirom da je r prost broj, $r = 5$ je jedina mogućnost. Međutim, jednadžba $4^q + q^4 = 5$ nema rješenje u prostim brojevima jer $q = 1$ nije prost broj.

   Zaključujemo da ne postoje prosti brojevi p, q, r takvi da je $p^{2q} + q^{2p} = r$.
9. Državno 2018. SŠ A - 2. razred, 4. zadatak
10. ARML 2002.
11. Rješenje na školjci.
12. Iznad 6. zadatka i 6. zadatak
13. Art of Problem Solving
14. Rješenje je poopćenje ovog zadatka.