MLADI NADARENI MATEMATIČARI
Marin Getaldić

Prosti brojevi

20.12.2015.

Uvod

Definicija 1. *Kažemo da je prirodan broj p* ***prost broj*** *ako ima točno dva (različita) djelitelja (konkretno, to su 1 i p). U suprotnom kažemo da je broj složen.*

Važnost prostih brojeva očituje se u idućem teoremu:

Teorem 1 (Fundamentalni teorem aritmetike)**.** *Svaki prirodan broj n ima jedinstvenu faktorizaciju na proste faktore.*
Formalno: postoje prosti brojevi $p_1, p_2, ..., p_k$ i prikladni eksponenti $\alpha_1, \alpha_2, ..., \alpha_k$ t.d. vrijedi:

$$n = p_1^{\alpha_1} p_2^{\alpha_2} ... p_k^{\alpha_k}$$

Dakle, svaki se broj može razložiti na produkt potencija prostih brojeva. To je primarni razlog zašto se mnoge jednadžbe u cijelim brojevima mogu razriješiti promatranjem djeljivosti s prostim brojevima, i zašto su baš prosti brojevi centralna tema proučavanja u teoriji brojeva.

Iako se teorem čini očit, i dugo vremena se u povijesti matematike smatrao takvim, ipak nije potpuno trivijalan. Dokaz da takva faktorizacija postoji jest poprilično lagan (pokušajte dokazati). Malo veći problem je u pokazivanju jedinstvenosti. U tu svrhu možemo koristiti iduću tvrdnju:

Teorem 2 (Euklidova lema)**.** *Neka je p prost broj i neka $p|ab$. Tada $p|a$ ili $p|b$.*

Pomoću ovog svojstva lako se pokaže jedinstvenost u FTA. Ali i obratno, ovo svojstvo se lako pokaže iz jedinstvene faktorizacije. Vidimo, dakle, da je svojstvo iskazano u Euklidovoj lemi vrlo bitno za proste brojeve.

Počnimo zadatke s najstarijim rezultatom o prostim brojevima:

Primjer 1 (Euklidov teorem)**.** *Skup prostih brojeva je beskonačan.*

Pretpostavimo suprotno: da je skup prostih brojeva konačan. Neka su, dakle, $p_1, p_2, ..., p_n$ "svi" prosti brojevi. Promotrimo sljedeći broj:

$$p_1 p_2 ... p_n + 1$$

Taj broj ne može biti djeljiv niti s jednim od p_i. No, kao i svaki prirodan broj, mora imati faktorizaciju na proste brojeve, a kako ih je po pretpostavci samo konačno, neki od p_i morao bi se pojaviti u faktorizaciji. Tada bi broj ipak bio djeljiv s tim p_i, što je nemoguće. Prema tome, naša početna pretpostavka bila je kriva i zaključujemo – skup prostih brojeva je beskonačan skup.

Primjer 2. *Postoji li proizvoljno velik skup uzastopnih složenih brojeva, tj. drugim riječima, može li "udaljenost" između susjednih prostih brojeva biti proizvoljno velika?*

Odgovor: Da! Promotrimo brojeve $n! + 2, n! + 3, n! + 4, ..., n! + n$. Svaki od njih je složen (uvjerite se). Sve skupa ih je $n - 1$, ali n je proizvoljan, dakle "rupe" između prostih brojeva mogu biti proizvoljno velike!

Zadatci i rješenja

Zadatak 1.
Nađite sve prirodne brojeve n takve da su $3n-4$, $4n-5$ i $5n-3$ prosti brojevi.

Rješenje.
Jedan način je razlikovati je li broj n paran ili neparan – pokušajte.

Nešto elegantnije, možemo primijetiti da je suma tih brojeva jednaka $12n-12$, što je paran broj. Ali ako su ono sve prosti brojevi onda bi suma trebala biti neparna – jedina mogućnost je da je neki od brojeva paran. Kako je jedini paran prost broj upravo 2, zaključujemo da je neki od danih brojeva jednak 2. Direktno provjerimo $3n-4=2$, $4n-5=2$ i $5n-3=2$ te nađemo da je $n=2$.

Zadatak 2.
Ako su $8p-1$ i p prosti brojevi, pokažite da je $8p+1$ složen.

Zadatak 3.
Odredite sve parove prostih brojeva p i q koji zadovoljavaju $p^2-2q^2=1$.

Zadatak 4.
Dokažite sljedeće tvrdnje o prostim brojevima.

(a) Ako je $p \geq 5$, p je nužno oblika $6k+1$ ili $6k-1$.

(b) Ako je $p \geq 3$, p je nužno oblika $4k+1$ ili $4k+3$.

(c) Ako je $p \geq 7$, p je nužno oblika $10k+1$ ili $10k+3$ ili $10k+7$ ili $10k+9$.

Pokušajte poopćiti tvrdnje prethodnih zadataka (primijetimo da se uvjeti mogu sročiti jednostavno kao "svi osim prvih nekoliko prostih brojeva").

Zadatak 5.
Neka je $p>5$ prost broj. Dokažite da $p-4$ nije četvrta potencija nekog prirodnog broja (dakle, $p-4 \neq n^4$ za bilo koji n).

Zadatak 6.
Ako je $p>5$ prost broj, dokažite da $360|p^4-5p^2+4$.

Zadatak 7.
Ako su p i q prosti brojevi veći od 3, dokažite da $24|p^2-q^2$.

Zadatak 8.
Za koje proste brojeve p je i 2^p+p^2 prost broj?

Zadatak 9.
Neka su p i q prosti brojevi. Riješite jednadžbu

$$p+q=(p-q)^3.$$

Dva zadatka za opću kulturu:

Zadatak 10.
Neka je 2^n-1 prost broj. Pokažite da je tada n nužno prost broj.
Prosti brojevi oblika 2^p-1, gdje je p prost, nazivaju se *Mersenneovi prosti brojevi.*
Fun fact: Može se pokazati da su u korespondenciji s parnim savršenim brojevima (Euklid-Euler teorem).
Fun fact 2: Za Mersenneove proste brojeve imamo najbolje metode utvrđivanja "prostosti", te su najveći prosti brojevi koje smo do danas izračunali tog oblika. Trenutačno najveći poznati prost broj je $2^{57885161}-1$.

Zadatak 11.
Neka je $2^n + 1$ prost broj. Dokažite da je tada n potencija broja dva.
Definiramo Fermatove brojeve $F_n = 2^{2^n} + 1$. Prosti brojevi tog oblika nazivaju se *Fermatovi prosti brojevi.*
Fun fact: Može se pokazati (teško) da se pravilni n-terokut može konstruirati ako (i samo ako) je n umnožak potencije broja dva i Fermatovih prostih brojeva (na prvu potenciju). Dakle n-ovi za koje je n-terokut konstruktibilan (šestarom i ravnalom) su

$$n = 3,\ 4,\ 5,\ 6,\ 8,\ 10,\ 12,\ 15,\ 16,\ 17,\ 20,\ 24,\ 30,\ 32,\ ...$$

Napomena Slijede teži zadatci – rješenja možete potražiti u literaturi s kraja ovog predavanja.

Zadatak 12.
Dokažite da prostih brojeva oblika $4k + 3$ ima beskonačno.

Rješenje.
Hint: Pretpostavite suprotno i promotrite broj $4p_1p_2\cdots p_n - 1$.

Zadatak 13.
(Malo teži zadatak) Riješite u prirodnim brojevima jednadžbu

$$x^{x+y} = y^{y-x}.$$

Zadatak 14.
Dokažite da broj koji se sastoji od točno 2^n znamenki sadrži barem n različitih prostih faktora.

Zadatak 15.
Ako je a neparan prirodni broj, pokažite da su $a^{2^n} + 2^{2^n}$ i $a^{2^m} + 2^{2^m}$ relativno prosti za sve različite prirodne brojeve m, n. Primijetite da ste tako dobili beskonačan niz međusobno relativno prostih brojeva. Zaključite da postoji beskonačno prostih brojeva.

Rješenja zadataka

Rješenje zadatka 2. Primijetimo da su $8p-1$, $8p$ i $8p+1$ tri uzastopna broja. Ako p nije 3, onda niti prvi niti drugi od tih brojeva nije djeljiv s 3. To znači da 3 dijeli $8p+1$, pa je stoga složen. Provjerimo još samo slučaj $p=3$. Tada je $8p+1=25$, pa je i tada broj složen.

Rješenje zadatka 3. Prebacimo na drugu stranu: $p^2-1=2q^2$ i faktoriziramo: $(p-1)(p+1)=2q^2$. Ako je p neparan (kao što većina i jest), s lijeve se strane pojavljuje broj djeljiv s 4 (ustvari barem s 8). Dakle, 4 dijeli $2q^2$, što znači da q ima faktor 2. Kako je q prost, slijedi da je $q=2$. Tada je $p=3$. Dakle, jedino rješenje s neparnim p je $(p,q)=(3,2)$. Preostaje primijetiti da je $p=2$ nemoguće.

Rješenje zadatka 4. Sve tvrdnje baziraju se na idućoj intuitivnoj tvrdnji:

Teorem 3 (Teorem o dijeljenju s ostatkom)**.** *Za svaki cijeli broj a i prirodan b postoje q i r tako da je $a=bq+r$, $0\leqslant r<b$.*

Što to znači za naš zadatak? Uzmimo npr. da gledamo dijeljenje s 6. Po teoremu, svaki se broj može zapisati u obliku $6k+r$, gdje je $r\in\{0,1,2,3,4,5\}$.
Ako je broj oblika $6k$, jasno je da je djeljiv s 6, pa nije prost.
Ako je oblika $6k+2=2(3k+1)$, nije prost (osim za k=0, što je 2).
Ako je oblika $6k+3=3(2k+1)$, nije prost (osim za k=0, što je 3).
Ako je oblika $6k+4=2(3k+2)$, nije prost.
Dakle, jedine preostale mogućnosti su $6k+1$ i $6k+5$.
Ostali zadaci analogno. Što se tiče općenite tvrdnje, primijetite da je skup $\{1,5\}$ upravo skup brojeva relativno prostih s 6. Isto u drugim zadacima.

Rješenje zadatka 5. Kad bi vrijedilo $p-4=n^4$, tada bi bilo

$$p=n^4+4=n^4+4n^2+4-4n^2=(n^2+2-2n)(n^2+2+2n)=((n+1)^2+1)((n-1)^2+1)$$

Vidimo da za $n\neq 1,-1$ imamo netrivijalne faktore, a za ove n dobije se samo $p=5$, što je prema zadatku isključeno.

Rješenje zadatka 6. Faktoriziramo:

$$p^4-5p^2+4=(p^2-1)(p^2-4)=(p-2)(p-1)(p+1)(p+2)$$

Želimo dokazati djeljivost s $360=2^3 3^2 5$. Dovoljno je pogledati posebno za svaki prost broj u faktorizaciji.
Promotrimo prvo djeljivost s $2^3=8$. p je prost broj veći od 5, dakle neparan. To znači da su $p-1$ i $p+1$ dva susjedna parna broja. Poznato je da je umnožak dva susjedna parna broja djeljiv s 8. (Ako vam nije poznato – dokažite $n^2\equiv 1 \pmod 8$ ako je n neparan.
Kako dokazati djeljivost s 9? S obzirom da p nije djeljiv s 3, vrijedi $p\equiv\pm1$, dakle $p^2\equiv 1\equiv 4$ i imamo dva faktora djeljiva s 3.
Napokon, za djeljivost s 5 prisjetimo se da među 5 uzastopnih cijelih brojeva mora postojati neki djeljiv s 5. Kako p nije djeljiv s 5, neki od $p-2$, $p-1$, $p+1$, $p+2$ jest.

Rješenje zadatka 7. Dovoljno je pokazati $p^2\equiv 1 \pmod{24}$. Naravno, isto će vrijediti i za q. Kako je $24=3\cdot 8$, treba provjeriti zasebno za 3 i 8. No, to se vidi vrlo lako.

Rješenje zadatka 8. Zadatak se može riješiti promatranjem mod 3. No, možemo i bez kongruencija uz malo algebre. Promotrimo prvo neparne p.

$$2^p + p^2 = 2^p + 1 + p^2 - 1 = (2+1)(1 - 2 + 2^2 + ... + 2^{p-1}) + (p-1)(p+1) = 3k + (p-1)(p+1).$$

Neka je $p > 3$. Kako p nije 3, a neki od $p-1$, p, $p+1$ djeljiv je s 3, vidimo da je dani broj djeljiv s 3. Dakle, jedine mogućnosti su $p = 2, 3$. Lako se provjeri da dobijemo prost broj samo za $p = 3$ i to je broj 17.

Rješenje zadatka 9. Primijetimo prvo da p, q moraju biti različiti. Promotrimo danu jednadžbu $\pmod{p+q}$. Kad promatramo po tom modulu, zamišljamo kao da je $p = -q$.

$$0 \equiv p + q \equiv (p-q)^3 \equiv 8p^3 \pmod{p+q}.$$

Dakle, $p+q$ dijeli $8p^3$. No, ne može dijeliti p^3 (Zašto?), pa mora biti $p+q|8$. Malo razmatrajući slučajeve, vidimo da su naši brojevi ili oba 2, ili 3 i 5. Uvrštavajući u jednadžbu, vidimo da je ustvari samo $(p,q) = (5,3)$ rješenje.

Popis literature za složenije zadatke

1 104 *number theory problems*, Titu Andreescu, Dorin Andrica, Zuming Feng

2 *Putnam and Beyond*, Razvan Gelca, Titu Andreescu

12. zadatak je primjer 1.20. u [1].
13. zadatak je iz [2], 735. zadatak.
14. zadatak: Introductory problem 36 u [1].
15. zadatak: primjer 1.22. u [1].