Kombinatorni dokazi
malog Fermatova i Wilsonova teorema

Borka Jadrijević i Fani Rožić, Split

Možda najpoznatije tvrdnje koje govore o svojstvima prostih brojeva su mali Fermatov teorem i Wilsonov teorem. **Wilsonov teorem** kaže da je, u slučaju kada je p prost, ostatak pri dijeljenju $(p-1)!$ s p jednak -1. Ili, zapisano koristeći kongruencije $(p-1)! \equiv -1 \pmod{p}$. **Mali Fermatov teorem** govori o prostim potencijama cijelih brojeva. Naime, on tvrdi: ako je p prost, tada n^p i n imaju isti ostatak pri dijeljenju s p za svaki cijeli broj n, tj. $n^p \equiv n \pmod{p}$.

Gornje tvrdnje imaju veliku teorijsku, ali i praktičnu primjenu. Primjerice, mali Fermatov teorem koristi se kao osnova za neke testove prostosti, a upravo brzi algoritmi za testiranje prostosti imaju važnu primjenu u kriptografiji – matematičkoj disciplini koja se bavi zaštitom tajnosti podataka.

Mali Fermatov teorem uobličio je Pierre de Fermat u jednom pismu 1640. godine, ali dokaz nije dao. Prvi objavljeni dokaz ovog teorema dao je Euler 1736. godine. Međutim, izgleda da je Leibniz imao dokaz još 1689. god., ali ga nije objavio.

Arapski matematičar, Ibn al-Haytham (965.–1040.) znan kao Alhazen, rješavajući razne probleme s kongruencijama koristio je svojstvo prostih brojeva koje mi danas nazivamo Wilsonov teorem. Sam teorem pripisuje se Sir Johnu Wilsonu, studentu Edwarda Waringa. Teorem je Waring objavio 1770. godine, premda ga ni on, ni Wilson nisu znali dokazati. Prvi poznati dokaz Wilsonova teorema dao je Lagrange 1771. godine. Leibniz je izgleda znao i za ovu tvrdnju još 1683. godine ali, slično kao i dokaz malog Fermatova teorema, nije ju objavio.

Danas postoje desetci raznovrsnih dokaza spomenutih teorema, ali su možda najatraktivniji dokazi, koji traže najmanje matematičke pozadine, upravo kombinatorni dokazi koje ćemo ovdje prezentirati. Osnova tih dokaza je prebrojavanje konačnog skupa objekata na dva različita načina.

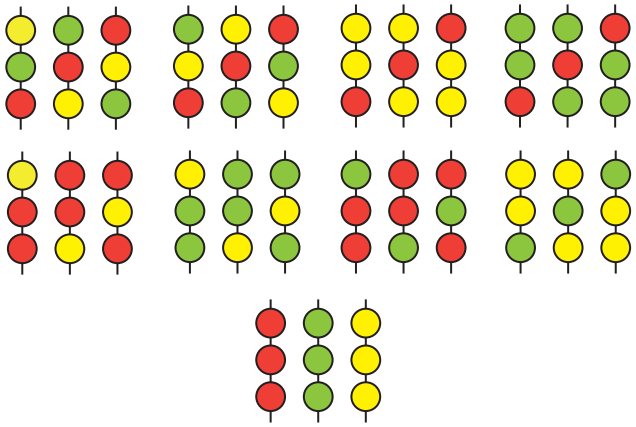
Dokaz malog Fermatova teorema prebrojavanjem narukvica

U iskazu malog Fermatova teorema, zbog prirode dokaza, pretpostavit ćemo da je n prirodan broj. Kada dokažemo da tvrdnja vrijedi za svaki prirodan broj n, vrlo lako se vidi da tvrdnja vrijedi i za svaki cijeli broj n.

Teorem 1. (mali Fermatov teorem) *Neka je p prost broj i n prirodan broj, tada $p \mid (n^p - n)$.*

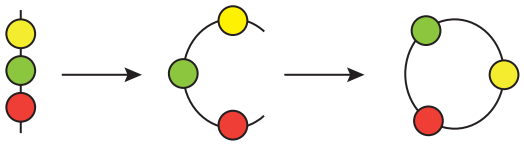
Očito, tvrdnja vrijedi za $n = 1$, pa promatrajmo slučaj $n \geq 2$. Pretpostavimo da želimo formira-

ti nizove s p obojanih perlica i da imamo dovoljno perlica tako da možemo neograničeno koristiti svaku od mogućih n boja. Pitamo se, koliko različitih nizova možemo dobiti? Koristeći jedan od osnovnih principa prebrojavanja tzv. *produktno pravilo*, zaključujemo da je to n^p jer za svaku perlicu imamo na raspolaganju n boja, a niz nam se sastoji od p perlica. Slika 1. ilustrira slučaj kada je $n = 3$ i $p = 3$.



Slika 1.

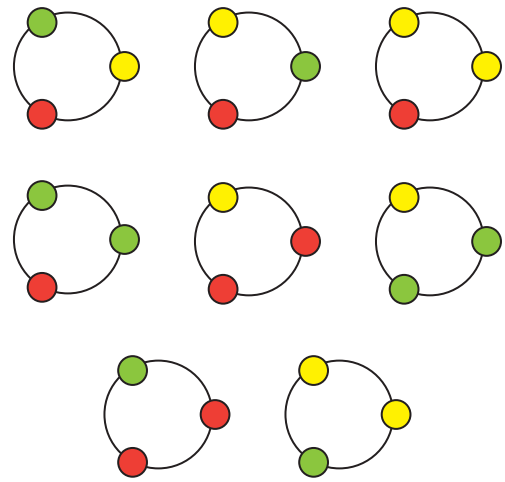
Od n^p dobivenih nizova, točno njih n ima sve perlice u istoj boji (na slici 1 to su nizovi u zadnjoj grupi). Stavimo te nizove na stranu, a od svakog od preostalih $n^p - n$ raznobojnih nizova napravimo narukvicu na način koji je ilustriran na slici 2, tj. spojimo njihove krajeve kako bismo dobili isto toliko narukvica.



Slika 2.

Uzmimo sada neki niz perlica i perlicu s vrha tog niza prebacimo na dno, a ostale perlice pomaknimo za jedno mjesto gore. Ovim pomakom perlica dobili smo novi niz perlica, a da pritom nismo promijenili izgled narukvice.

Za slučaj $n = 3$ i $p = 3$, imamo $n^p - n = 24$ različita raznobojna niza. Ove nizove možemo podijeliti u 8 grupa po 3 niza tako da su u svakoj grupi nizovi dobiveni jedan iz drugog koristeći jedan ili više ovakvih pomaka perlica (vidjeti prvih 8 grupa na slici 1). Svakoj od ovih 8 grupa odgovara točno jedna narukvica (slika 3).



Slika 3.

Pogledajmo općenito. Želimo $n^p - n$ različitih raznobojnih nizova perlica podijeliti u grupe tako da svakom nizu u danoj grupi odgovara ista narukvica. Pitamo se koliko nizova perlica ima u svakoj grupi? Neka je k najmanji broj opisanih pomaka koje možemo primijeniti na niz od p perlica dok ne dobijemo početni raspored boja. Naravno da je $k > 1$ jer smo jednobojne nizove stavili na stranu. Uočimo da ćemo nakon $2k$ pomaka ponovno dobiti početni raspored boja. Isto tako i nakon $3k$ pomaka, $4k$ pomaka, itd. Po Euklidovoj lemi o dijeljenju, postoje jedinstveni nenegativni cijeli brojevi h i r takvi da je

$$p = hk + r, \qquad 0 \leq r < k.$$

Budući da dobivamo isti raspored boja nakon hk pomaka te također nakon p pomaka (zato što se nakon p pomaka sve perlice nalaze u prvobitnom položaju), potrebno je točno r pomaka nakon hk-tog pomaka da bismo dobili početni raspored

boja. Kako je $r < k$, a k je najmanji broj potrebnih pomaka da bismo dobili početni raspored boja, vidimo da r mora biti jednak 0. Dakle, $p = hk$, što povlači $k = p$ jer je $k > 1$ i p je prost. Stoga, postoji točno p različitih nizova perlica koji daju istu narukvicu. U skladu s tim $n^p - n$ nizova razdvajamo u grupe od po p nizova, tako da svaki niz iz te grupe daje istu narukvicu i tako da različitim grupama odgovaraju različite narukvice. Prema tome, broj različitih narukvica N pomnožen s p daje ukupan broj različitih raznobojnih nizova, tj. $pN = n^p - n$, a to znači da

$$p \mid (n^p - n),$$

što je tvrdnja malog Fermatova teorema.

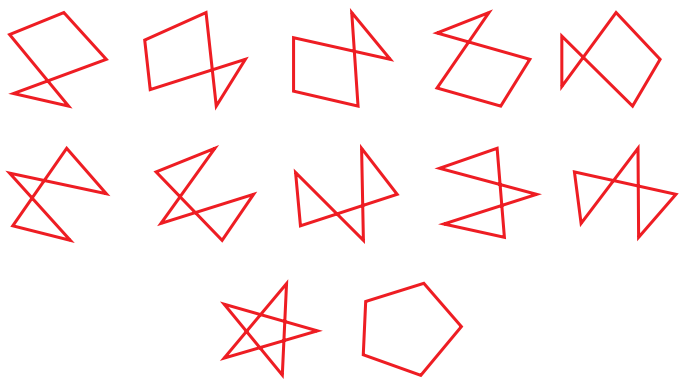
Kako smo pokazali da tvrdnja vrijedi za sve prirodne brojeve n i budući da je za $n = 0$ očito zadovoljena, preostaje nam dokazati da vrijedi i za sve negativne cijele brojeve. Uočimo prvo da su svi prosti brojevi p, osim $p = 2$, neparni te da se svaki negativni cijeli broj može zapisati u obliku $-n$, gdje je n neki prirodan broj. Ako je p neparan prost broj, onda je $(-n)^p - (-n) = -(n^p - n)$ pa tvrdnja vrijedi i za negativne cijele brojeve jer znamo da $p \mid (n^p - n)$ ako je n prirodan broj. Za $p = 2$ tvrdnja također vrijedi jer 2 dijeli $(-n)^2 - (-n) = n(n+1)$ jer je jedan od uzastopnih brojeva n i $n+1$ paran.

Dokaz Wilsonova teorema prebrojavanjem zvjezdastih mnogokuta

Dokaz Wilsonova teorema koji ćemo sada dati, pojavio se oko 1930. godine u jednom ruskom časopisu, a bio je potpisan s A. B. (Moskva). Autor je taj dokaz predstavio kao geometrijski, premda bi se, prema današnjim kriterijima, on ubrajao u kombinatorne dokaze.

Teorem 2. (Wilsonov teorem) *Ako je p prost broj, tada $p \mid ((p-1)! + 1)$.*

Ako je $p = 2$, tvrdnja je očita. Stoga, pretpostavimo da je p neparan prost broj. Promotrimo p točaka na kružnici koje su raspoređene tako da je dijele na p lukova jednake duljine. Koliko mnogokuta možemo dobiti spajanjem ovih točaka, pri čemu je križanje stranica također dopušteno? Ovako dobivene mnogokute nazivamo zvjezdastim p-mnogokutima jer su njihovi vrhovi zapravo vrhovi pravilnog (konveksnog) mnogokuta s p stranica. Prema produktnom pravilu, mogli bismo pomisliti kako imamo $p!$ različitih zvjezdastih p-mnogokuta jer se prvi vrh može odabrati na p načina, drugi vrh na $p-1$ načina i tako dalje. Međutim, uočimo da svaki zvjezdasti p-mnogokut možemo opisati na $2p$ različitih načina i to polazeći od bilo kojeg od njegovih p vrhova odabirući jednu ili drugu stranicu iz tog vrha kao početnu stranicu. Stoga stvarno imamo $p!/2p$ različitih zvjezdastih p-mnogokuta. Pojasnimo to za slučaj $p = 5$. Slika 4 prikazuje svih 12 zvjezdastih peterokuta.



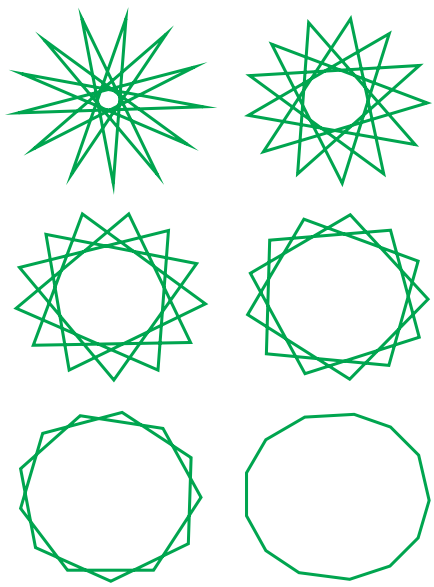
Slika 4.

Ako vrhove zvjezdastih peterokuta na slici 4 označimo redom (u pozitivnom smjeru) počevši od najdesnijeg s $1, 2, \ldots, 5$, tada svaki peterokut možemo opisati na $2p = 10$ načina, tj. s 10 različitih uređenih petorki. Primjerice, prvi peterokut u prvom redu na slici 4 možemo opisati petorkama

$$\begin{array}{ccccc} 12354 & 23541 & 35412 & 45321 & 53214 \\ 14532 & 21453 & 32145 & 41235 & 54123 \end{array}.$$

Ovdje npr. 35412 znači da smo krenuli od vrha 3 i odabrali stranicu koja taj vrh spaja s vrhom 5. Preostala tri člana petorke jedinstveno su određena odabranim peterokutom.

Od $p!/2p$ različitih zvjezdastih p-mnogokuta, točno njih $(p-1)/2$ ostaje neizmijenjeno rotacijom za kut od $2\pi/p$ radijana. Ovakvi p-mnogokuti nazivaju se pravilni zvjezdasti p-mnogokuti jer su to "zvijezde", kod kojih svaki od p vrhova ima isti pripadni kut $(2k+1)\pi/p$, gdje je $0 \leq k < (p-1)/2$. Dakle, u slučaju $p = 5$, imamo dva takva pravilna peterokuta, a prikazani su na slici 4 u trećem redu. U slučaju $p = 13$, imamo točno 6 pravilnih zvjezdastih trinaesterokuta (slika 5).



Slika 5.

Odvojimo pravilne zvjezdaste p-mnogokute, a preostalih $p!/2p-(p-1)/2$ nepravilnih p-mnogokuta razvrstajmo u skupove tako da se članovi svakog od tih skupova mogu dobiti od jednog člana koristeći uzastopnu rotaciju za kut od $2\pi/p$. Pitamo se koliko svaki od tih skupova ima elemenata? U slučaju $p = 5$, imamo dva takva skupa po 5 različitih peterokuta (to su peterokuti u prvom, odnosno drugom redu na slici 4). Općenito, svaki od tih skupova ima p elemenata. Kako bismo pokazali da se u svakom skupu zaista nalazi p elemenata, koristimo istu metodu kao i kod dokaza malog Fermatova teorema gdje smo pokazali da svakoj narukvici pripada p različitih nizova po p perlica. Ovdje, jedna rotacija p-mnogokuta za kut od $2\pi/p$ radijana odgovara jednom pomaku perlica u nizu. Stoga je ukupan broj ovih skupova

$$\frac{\frac{p!}{2p} - \frac{p-1}{2}}{p} = \frac{(p-1)! - p + 1}{2p}.$$

Ovo povlači da $p \mid ((p-1)! - p + 1)$ što vrijedi ako i samo ako

$$p \mid ((p-1)! + 1)$$

a to je upravo tvrdnja Wilsonova teorema.

Vrijede li obrati Wilsonova i malog Fermatova teorema i zašto je to važno?

Kao što smo već rekli, kriptografija je matematička disciplina koja se bavi zaštitom tajnosti podataka. Ona ima dugu i zanimljivu, a ponekad i tajnovitu prošlost. Danas, kad društvo ovisi o informacijama u elektroničkom obliku, uz problem zaštite tajnosti podataka javljaju se i još neki dodatni problemi kao što su: zaštita od neovlaštene promjene podataka, zaštita od lažnog predstavljanja, itd. Te probleme rješava tzv. *kriptografija javnog ključa*. U konstrukciji većine kriptosustava s javnim ključem kreće se od jednog ili više velikih prostih brojeva. Dakle, važno pitanje je kako za dani prirodan broj odrediti je li prost ili je složen. Za to koristimo tzv. *testove prostosti*. To su kriteriji koje broj p mora zadovoljiti da bi bio prost. Razlikujemo testove koji dokazuju prostost i vjerojatnosne testove prostosti. Kod testova za dokazivanje prostosti imamo sljedeće: ako p ne zadovolji neki od zadanih kriterija, onda je sigurno složen, a ako ih sve zadovolji, onda je sigurno prost. S druge strane, kod vjerojatnosnih testova prostosti imamo: ako p ne zadovolji neki od zadanih kriterija, onda je sigurno složen, a ako ih sve zadovolji, onda je "vjerojatno prost", što znači da je vrlo velika vjerojatnost da je p prost. Važno je napomenuti da se u praksi koriste vjerojatnosni testovi jer su puno brži od svih poznatih metoda za dokazivanje prostosti.

Budući da Wilsonov i mali Fermatov teorem govore o nekim svojstvima prostih brojeva, pogledajmo možemo li ih iskoristiti za testiranje prostosti. Prvo moramo utvrditi vrijede li njihovi obrati.

Lako se pokaže da za sve složene prirodne brojeve $m > 4$ vrijedi $m \mid (m-1)!$, što povlači $m \nmid ((m-1)!+1)$. Kako je to očito i za $m = 4$, onda za sve složene prirodne brojeve m imamo $m \nmid ((m-1)!+1)$. Ovo znači da ako za prirodan broj p veći od 1 vrijedi $p \mid ((p-1)!+1)$, onda možemo zaključiti da je p prost. Prema tome, vrijedi i jači oblik Wilsonova teorema:

Teorem 3. (Wilsonov teorem) *Neka je p prirodan broj veći od 1. Tada je p prost ako i samo ako $p \mid ((p-1)!+1)$.*

Dakle, Wilsonov teorem u potpunosti karakterizira proste brojeve. Drugim riječima to je test za dokazivanje prostosti, odnosno on nam daje kriterij kako utvrditi je li neki prirodan broj prost ili je složen. Međutim, ovaj je lijepi rezultat uglavnom od teoretske važnosti jer se $(p-1)!$ "sporo" računa za velike brojeve p, a time i provjerava je li $p \mid ((p-1)!+1)$.

S druge strane, lako je vidjeti da obrat malog Fermatova teorema općenito ne vrijedi. Primjerice, broj $341 = 11 \cdot 31$ je složen i vrijedi

$$341 \mid \left(2^{341} - 2\right).$$

Ovo nam govori da postoje i složeni brojevi p koji zadovoljavaju svojstvo

$$p \mid (n^p - n)$$

za neki (pa čak i za svaki) prirodan broj n. Očito, ovo svojstvo je važno svojstvo prostih brojeva, ali ne karakterizira proste brojeve. Međutim, postoje vrlo efikasne metode za provjeru ovog svojstva, pa se ono koristi kao osnova za neke vjerojatnosne testove prostosti.

Kažemo da je složen broj m *pseudoprost u bazi* b (kraće: m je $psp(b)$) ako

$$m \mid (b^m - b). \qquad (1)$$

Očito je broj 341 pseudoprost u bazi 2, tj. 341 je $psp(2)$. Postojanje pseudoprostih brojeva nam pokazuje da testiranje samo s jednom bazom nije dovoljno da bismo zaključili da je broj prost. Zato možemo pokušati kombinirati više baza. Primjerice, broj 341 nije $psp(3)$ jer

$$341 \nmid \left(3^{341} - 3\right). \qquad (2)$$

Iz (2) slijedi da 341 nije prost, pa možemo reći da je baza $b = 3$ *svjedok složenosti* broja 341. Mogli bismo zaključiti: ako broj m zadovoljava svojstvo (1) za "dovoljan" broj baza b, onda je vjerojatno prost. No, primjerice, broj $561 = 3 \cdot 11 \cdot 17$ je pseudoprost u svakoj bazi b. Takvi se brojevi nazivaju *Carmichaelovi brojevi*. Postojanje Carmichaelovih brojeva pokazuje važan nedostatak testiranja prostosti na osnovi malog Fermatova teorema. No, malim modificiranjem testa taj se nedostatak može ukloniti. Ta modifikacija osnova je za tzv. *Miller-Rabinov test prostosti*. Ako m prođe taj test za k baza b, onda je vjerojatnost da je m složen $\leq \frac{1}{4^k}$. Npr. za $k = 20$ je vjerojatnost da je m složen manja od 10^{-12}. Tako dobiveni "vjerojatno prosti brojevi" nazivaju se još i *industrijski prosti brojevi*.

LITERATURA

1/ G. E. Andrews: *Number theory*, Dover publications, 1994.

2/ A. Bogomolny: *Geometric Proof of Wilson's Theorem*, Learn to enjoy, `http://www.cut-the-knot.org/blue/GeometricWilson.shtml`.

3/ R. D. Carmichael: *The Theory of Numbers*, New York: John Wiley & Sons, Inc., 1914.

4/ L. E. Dickson: *History of the Theory of Numbers*, Volume 1. Chelsea Publishing Company, New York, 1952.

5/ A. Dujella, M. Maretić: *Kriptografija*, Element, Zagreb, 2007.

6/ S. W. Golomb: *Combinatorial Proof of Fermat's "Little" Theorem*, Amer. Math. Monthly, Vol. 63, No. 10, (1956), p. 718.

7/ D. Veljan: *Kombinatorna i diskretna matematika*, Algoritam, Zagreb, 2001.

8/ *Proofs of Fermat's little theorem*, Wikipedia, the Free Encyclopedia, `http://en.wikipedia.org/wiki/Proofs of Fermat's little theorem`.