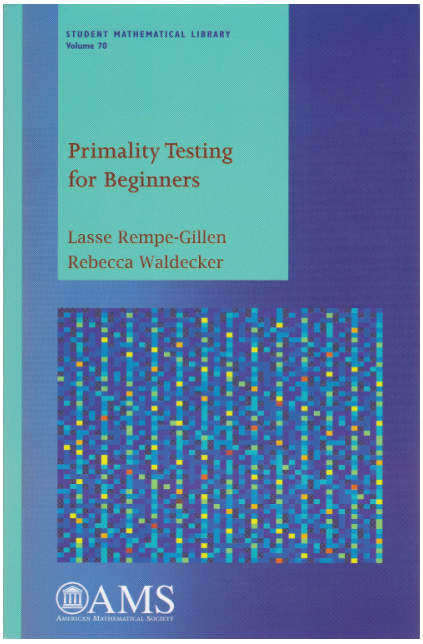
L. Rempe-Gillen, R. Waldecker, Primality testing for beginners, Student Mathematical Library Vol. 70, American Mathematical Society, 2014, 244 strani.



S praštevili se srečamo že zelo zgodaj. Učimo se, da lahko poljubno naravno število, različno od ena, zapišemo kot produkt potenc praštevil. Torej so praštevila osnovni gradnik naravnih števil, in po tej svoji lastnosti so tudi dobila ime. Pri iskanju prafaktorjev danega števila kaj hitro ugotovimo, da na vprašanje, ali je neko število praštevilo, ne znamo vedno enostavno odgovoriti. Problem poiskati algoritem, ki bi v polinomskem času glede na število znakov v zapisu danega števila (učinkovit algoritem) pri enakem številu vedno podal enak odgovor (deterministični algoritem), ali je število res praštevilo, je dolgo časa mučil matematike. Že v 70. letih so obstajali nedeterministični algoritmi, ki testirajo praštevilskost z visoko verjetnostjo pravilnega odgovora. Leta 2002 pa so Agrawal, Kayal in Saxena odkrili učinkovit in deterministični test praštevilskosti, ki je danes znan kot *AKS algoritem*. Najava rezultata je kmalu pritegnila veliko pozornosti, objava v prestižni reviji *Annals of Mathematics* pa je sledila dve leti kasneje. Osrednji namen knjige je predstaviti natanko tiste koncepte, ki so potrebni za razumevanje smisla in dokaza omenjenega rezultata, pri čemer se predpostavlja poznavanje le srednješolske matematike. Iz predgovora je mogoče razbrati, da je knjiga nastala po predavanjih avtorjev na nemški poletni akademiji za srednješolce leta 2005. Povod za izvedbo takih predavanj je bila izjemna dostopnost do tako pomembnega in lepega dosežka, kar je v matematiki prava redkost.

Knjiga je namenjena predvsem mladim matematikom in bolj amaterskim entuziastom z matematično žilico, ki želijo podrobneje spoznati paradigmo

in prakso modernega matematičnega raziskovanja, v katerem poleg dobrega poznavanja teorije igrajo (že pri samem oblikovanju hipotez, kot tudi pri njihovem testiranju in dokazovanju) nepogrešljivo vlogo tudi računalniki, algoritmi in eksperimentiranje, podobno eksperimentiranju v drugih znanostih. Toda to nikakor ne pomeni, da knjiga ni zanimiva tudi za bolj izkušene matematike.

Knjiga je napisana in oblikovana zelo pregledno, z algoritmi v okvirčkih, ter z definicijami in izreki na osenčenih poljih. V uvodu je poleg privlačnega opisa celotne vsebine pojasnjen tudi koncept matematičnega dokaza, razložen pa je tudi pomen definicij, lem in izrekov. Prav tako so opisani pogosti simboli in pojmi, ki so stavljeni krepko. Vsi algoritmi so zapisani v preprosti psevdokodi, kar olajša branje programiranja neveščemu bralcu. Knjiga je razdeljena na dva dela, *Osnove* in *AKS algoritem*. Sledita dodatka, namenjena odprtim problemom in rešitvam pomembnejših nalog, prav tako seznam literature in uporabljenih simbolov ter stvarno kazalo. Skoraj vsako poglavje se zaključi z navedbo in kratkim opisom dodatne literature. Večina podpoglavij na koncu vsebuje naloge, ki pomagajo pri utrjevanju in razumevanju snovi iz pripadajočega podpoglavja ter poudarjajo lastno aktivnost bralca (angl. learning by doing). Pogosto nalogam sledi še razdelek z dodatnimi napotitvami na ustrezno literaturo in zgodovinskimi pojasnili ter zahtevnejšimi nalogami.

Na kratko preglejmo vsebino knjige. Prvi del, *Osnove*, vsebuje štiri poglavja. Prvo obravnava osnovne lastnosti naravnih števil in praštevil. Spoznamo princip matematične indukcije, pojem deljivosti, osnovni izrek aritmetike, Evklidov algoritem in Eratostenovo rešeto. Že res, da je Eratostenovo rešeto deterministično algoritem za odločitveni problem PRAŠTEVILSKOST (angl. PRIMES), ki naj z da ali ne odgovori na vprašanje, ali je dano število n praštevilo. Toda ta algoritem je daleč od učinkovitega, saj je njegova časovna zahtevnost polinomska v n, ne pa tudi v $\log n$.

Drugo poglavje je namenjeno algoritmom in računski zahtevnosti. Že uvodne besede nakazujejo, da na preprosto vprašanje, kaj je algoritem, ni lahko najti dobrega odgovora. Za ponazoritev pojma algoritem avtorja posrečeno navedeta algoritma za peko palačink ter za pisanje kriminalnih uspešnic, nato pa v obliki algoritma zapišeta še znano Collatzovo funkcijo, ki sodo število n zamenja z $n/2$, liho število n pa s $3n + 1$. Mimogrede

je predstavljena še slavna in nedokazana Collatzova domneva, ki pravi, da se ta postopek vselej konča s številom 1. V nadaljevanju sta definirana in s kopico primerov ilustrirana razreda **P** in **NP**, poglavje pa se zaključi z definicijama nedeterminističnih algoritmov tipov Monte Carlo in Las Vegas, ki spadata v razred verjetnostnih algoritmov. Metoda Monte Carlo daje pravilne rezultate le z določeno verjetnostjo, metoda Las Vegas pa vselej daje pravilen rezultat, toda njen računski čas je lahko neomejen. Cilj knjige je dokaz trditve PRAŠTEVILSKOST $\in \mathbf{P}$.

Tretje poglavje je jedro knjige, saj tu spoznamo pojme in orodja iz teorije števil, na katerih temeljijo vsi moderni testi praštevilskosti. Najpomembnejša rezultata sta *mali Frematov izrek* $a^{p-1} \equiv 1 \pmod{p}$, ki velja za vsako celo število a tuje praštevilu p, in Eulerjeva posplošitev $a^{\varphi(n)} \equiv 1 \pmod{n}$ za $n \geq 2$, kjer je $D(a,n) = 1$, $\varphi(n)$ pa je število tistih elementov množice $\{1, \ldots, n-1\}$, ki so tuja številu n. S tem je povezan tudi *red števila a po modulu n* z oznako $\mathrm{ord}_a(n)$, ki je definiran kot najmanjši tak eksponent $k \in \mathbb{N}$, za katerega velja $a^k \equiv 1 \pmod{n}$. Izrek lahko uporabimo za naslednji *Frematov test*. Naključno izberimo a iz množice $\{1, \ldots, n-1\}$. Če je $D(a,n) \neq 1$, odgovorimo »n je sestavljeno število«. V nasprotnem izračunamo a^{n-1} po modulu n, za kar obstaja učinkovit algoritem. Če dobljeno število ni 1, ponovno odgovorimo »n je sestavljeno število«, v nasprotnem pa »n je morda praštevilo«. Mali Fermatov izrek zagotavlja, da v primeru praštevila n algoritem vrne rezultat »n je morda praštevilo«, toda to se lahko zgodi tudi za sestavljena števila n, npr. za $n = 15$ in $a = 11$. Taka števila n se imenujejo *psevdoprаštevila glede na osnovo a*. Izkaže se, da je število tistih osnov, za katera je n psevdopraštevilo, lahko $\varphi(n)$ ali pa največ $\varphi(n)/2$. Če bi vedno veljalo le slednje, bi bil Fermatov test učinkovit algoritem tipa Monte Carlo (**RP**) za odločitveni problem SESTAVLJENOST (ang. COMPOSITES). Žal pa obstajajo *Carmichaelova števila*, ki so psevdoprаštevila glede na vsako možno bazo. Prvo tako število je 561. Vseeno lahko Fermatov test popravimo do verjetnostnega algoritma. Gary L. Miller je leta 1976 dokazal posebno verzijo malega Fermatovega izreka, ki ga je štiri leta kasneje Michael O. Rabin uporabil pri konstrukciji *Miller-Rabinovega algoritma*, ki dokazuje pripadnost problema SESTAVLJENOST razredu **RP**. V knjigi je pravilnost delovanja algoritma dokazana v četrtem poglavju, kjer pred tem spoznamo še osnove kriptografije in RSA metode šifriranja, najpomembnej-

šega primera kriptografije z javnim ključem. Pri tej metodi odločilno vlogo igrajo javno znana števila, ki so produkt dveh velikih in naključno generiranih praštevil, skriti tudi uporabnikoma RSA šifriranja. Varnost metode temelji na principu, da je bistveno lažje ugotoviti, da je neko število sestavljeno, kot pa ga faktorizirati. Prvi del odlično opravi Miller-Rabinov algoritem, ki je popularen tudi zaradi svoje hitrosti. Čeprav sta računski zahtevnosti AKS in Miller-Rabinovega algoritma enaki, je njuna hitrost na konkretnih primerih težko primerljiva. Učinkovitost izbora naključnega praštevila zagotavlja šibka verzija praštevilskega izreka $x \ll \pi(x) \log x$, ki je v knjigi dokazana pred Miller-Rabinovim algoritmom. Do sedaj še nikomur ni uspelo najti učinkovitega algoritma, ki bi podal faktorizacijo poljubnega števila, in splošno prepričanje je, da tak algoritem ne obstaja. Bi se pa to z iznajdbo delujočega kvantnega računalnika spremenilo, saj taki kvantni algoritmi obstajajo.

Drugi del knjige ima tri poglavja in je namenjen AKS algoritmu. V prvem poglavju izvemo, da prava pot k determinističnemu testu praštevilskosti pelje preko polinomske različice malega Fermatovega izreka: *za praštevilo* p *velja* $(P(X))^p \equiv P(X^p) \pmod{p}$, *kjer je* $P(X)$ *celoštevilski polinom.* Osnovne lastnosti polinomske modularne aritmetike se obravnavajo že v zadnjih dveh podpoglavjih tretjega poglavja v prvem delu knjige. Toda take kongruence še niso dovolj, potrebno je študirati

$$(P(X))^n \equiv P(X^n) \pmod{n, Q},$$

kjer je tudi Q celoštevilski polinom. Ta zapis pomeni, da pri deljenju leve in desne strani s Q dobimo enak ostanek po modulu n. Posledica Fermatovega izreka je, da če za neka polinoma P in Q kongruenca ne velja, je n sestavljeno število. Obratno ni vedno res, kot kaže primer $(X-1)^{24} \equiv X^{24} - 1 \pmod{24, X^2-1}$, ki je bralcu prepuščen v samostojno reševanje. Vprašanje je, ali obstajata taki majhni množici polinomov P in Q, za katere veljavnost pripadajočih kongruenc implicira praštevilskosti števila n. Agrawal, Kayal in Saxena so dokazali, da takšni množici obstajata. Koraki njihovega algoritma so presenetljivo enostavni, toda preverba učinkovitosti delovanja je bistveno težja. V prvem koraku preverimo, ali je n popolna potenca, za kar obstaja učinkovit algoritem. Če je odgovor negativen, se v drugem koraku z r sprehodimo po naravnih številih na naslednji način. Najprej se

z Eratostenovim rešetom prepričamo, da je r praštevilo. Če velja $r < n$ in r deli n, odgovorimo »n ni praštevilo«. Če je $r \geq n$, odgovorimo »n je praštevilo«. Če ne velja nič od tega, izračunamo $\mathrm{ord}_r(n)$. Drugi korak ponavljamo, dokler ne dobimo enega od gornjih dveh odgovorov ali dokler ne velja $\mathrm{ord}_r(n) > (2\log_2 n)^2$. Če se zgodi slednje, začnemo z izvajanjem tretjega koraka, kjer preverjamo veljavnost kongruence

$$(X + a)^n \equiv X^n + a \pmod{n, X^r - 1}$$

za vsak $a \in \{1, \ldots, r\}$. Če katera od kongruenc ni izpolnjena, odgovorimo »n ni praštevilo«, sicer pa »n je praštevilo«. Seveda se porajata ključni vprašanji, ali pravilnost vseh kongruenc res zagotavlja praštevilskost števila n, in ali lahko vedno učinkovito poiščemo tak r, pri čemer mora njegova velikost naraščati kvečjemu polinomsko v $\log n$. Na prvo vprašanje odgovori osrednji izrek Agrawala, Kayala in Saxene, ki je dokazan v drugem poglavju. Zahtevane lastnosti števila r so dokazane v zadnjem poglavju knjige, kjer je pravilnost delovanja AKS algoritma pregledno dokazana po korakih. V zaključku sledijo še diskusije o hitrosti algoritma, nekaterih odvečnih omejitvah in nadaljnjem razvoju.

Knjigo, ki daje celovit pregled vsega, kar je potrebno za razumevanje AKS algoritma, zaokrožajo nekateri izreki in odprti problemi s področja teorije števil in reference za nadaljnji študij. Mnogi slavni odprti problemi iz teorije števil so navdihnili tudi popularne knjige, kot je npr. Doxiadisova *Uncle Petros and Goldbach's Conjecture*. Vsem, ki jih zanimajo praštevila in odprti problemi v zvezi z njimi ter odkrivanje zelo velikih praštevil, avtorja svetujeta ogled spletne strani *The Prime Pages*, dostopne na `https://primes.utm.edu/`.

Knjiga izpolnjuje uvodne obljube in ponuja številne priložnosti za njeno uporabo. Na gimnazijskem matematičnem krožku bi se jo lahko predelalo v enem letu, program bi bilo mogoče izvesti tudi v obliki delavnic in projektov na kakšnem od matematičnih taborov. Ker je vsebina knjige na stičišču elementarne in računske teorije števil, je vsebina zagotovo zanimiva za nadarjene dijake. Vsekakor imamo pred seboj odlično napisano strokovno matematično knjigo.

Jurij Kovič in Aleksander Simonič