PRESEK
List za mlade matematike, fizike, astronome in računalnikarje

ISSN 0351-6652
Letnik **30** (2002/2003)
Številka 3
Strani 155, X

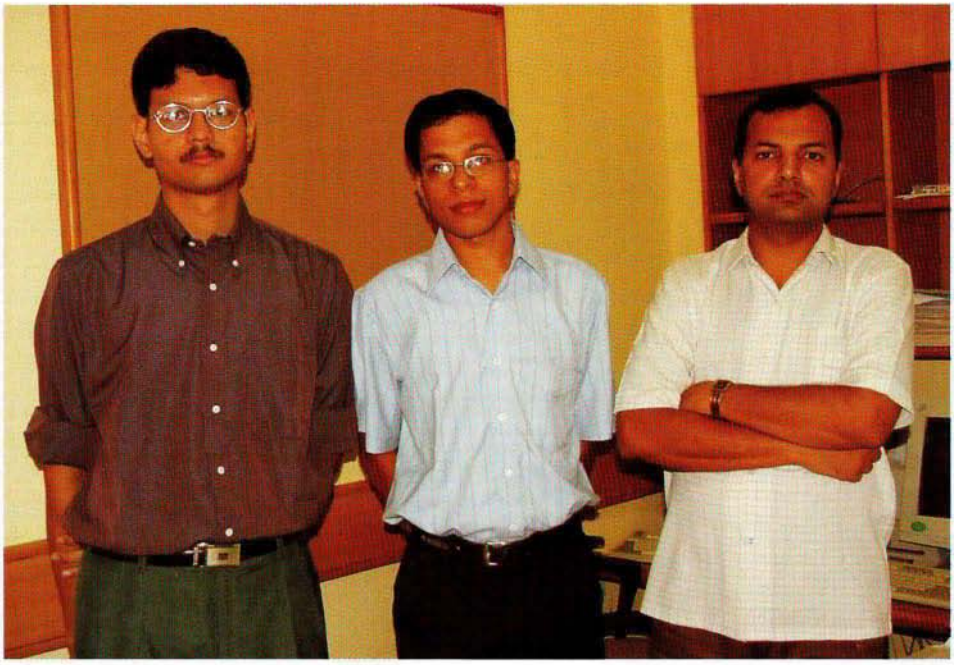
Marko Petkovšek:

REŠITEV PROBLEMA PRAŠTEVIL

Ključne besede: teorija števil, računalništvo, praštevila.

Elektronska verzija: http://www.presek.si/30/1519-Petkovsek.pdf

Nadaljevanje s str. 155.



Profesor Manindra Agraval (skrajno desno) in njegova podiplomska študenta Nitin Saksena in Niradž Kajal.

Računski postopek treh indijskih znanstvenikov bomo morda opisali kdaj drugič. Za zdaj povejmo le, da čas, ki ga novi postopek v najslabšem primeru potrebuje za preskus praštevilskosti števila n, zanesljivo ni večji od $C \ln^{12} n$, kjer je C neka konstanta. Avtorji domnevajo, da potrebni čas v resnici ni večji od $C \ln^6 n$. Za ilustracijo vzemimo, da njihova domneva drži in da je vrednost konstante C enaka času, ki ga naš računalnik potrebuje za eno deljenje. Potem bo za preskus praštevilskosti števila $n = 10^{100} + 267$ porabil približno 149 sekund oziroma dve minuti in pol. No, toliko bomo pa že počakali!

Novi postopek ima velik teoretičen pomen. V praksi pa se bodo za reševanje problema praštevil še vedno uporabljali verjetnostni algoritmi, ki so neprimerno hitrejši, kar dosežejo z žrtvovanjem absolutne pravilnosti odgovora. Verjetnostni algoritmi se namreč lahko včasih zmotijo in kakšno število razglasijo za praštevilo, čeprav je v resnici sestavljeno. Ker pa je verjetnost napake izredno majhna (veliko manjša od verjetnosti glavnega dobitka na loteriji), so ti algoritmi za potrebe kriptografije zaenkrat povsem ustrezni.

Marko Petkovšek

REŠITEV PROBLEMA PRAŠTEVIL

V začetku avgusta 2002 je časopis *New York Times* objavil novico, ki je vznemirila matematike in računalnikarje po vsem svetu. Indijski znanstveniki Manindra Agraval, Niradž Kajal in Nitin Saksena so namreč odkrili učinkovit računski postopek za reševanje naslednjega problema.

Problem praštevil. *Dano je naravno število n. Ali je n praštevilo?*

Seveda znajo ta preprosti problem rešiti že osnovnošolci.

1. METODA. *Število n po vrsti delimo z $2, 3, \ldots, n-1$. Če se deljenje nikoli ne izide, je n praštevilo, sicer je sestavljeno število.*

Zakaj torej takšno vznemirjenje? V kriptografiji, ki se ukvarja s šifriranjem sporočil, potrebujemo zelo velika praštevila, takšna s sto ali več desetiškimi mesti. Tipičen problem je npr. ugotoviti, ali je število $n = 10^{100} + 267$ praštevilo. Koliko časa bomo potrebovali s prvo metodo?

Recimo, da je naš računalnik zelo hiter in opravi 10^{12} deljenj na sekundo. Na odgovor bomo torej v najslabšem primeru (če je število n zares praštevilo in je treba opraviti vsa deljenja) čakali približno 10^{88} sekund oziroma 3.17×10^{80} let. Hmm ... Ali ne bi šlo hitreje? Bi. Če je število n produkt dveh faktorjev, je vsaj eden od njiju manjši ali enak $\sqrt{n}$. Torej zadošča n deliti s števili, ki ne presegajo $\sqrt{n}$. Poleg tega je dovolj deliti le s praštevili.

2. METODA. *Število n po vrsti delimo s praštevili od 2 do p, kjer je p največje praštevilo, ki ne presega $\sqrt{n}$. Če se deljenje nikoli ne izide, je n praštevilo, sicer je sestavljeno število.*

Pri oceni časovne zahtevnosti druge metode upoštevajmo le čas, potreben za deljenja, saj lahko tabelo praštevil do $\sqrt{n}$ pripravimo vnaprej. Vedeti moramo torej, koliko je praštevil, ki ne presegajo $\sqrt{n}$. Po znamenitem Gaussovem izreku o praštevilih je praštevil do N približno $N/\ln N$, kjer ln označuje naravni logaritem. Torej bo po drugi metodi treba opraviti približno $\sqrt{n}/\ln\sqrt{n} \approx 8.69 \times 10^{47}$ deljenj, kar bo trajalo 8.69×10^{35} sekund oziroma 2.75×10^{28} let. Tudi z drugo metodo ne bomo dočakali rezultata ($10^{100} + 267$ je namreč v resnici praštevilo).

Nadaljevanje na III. strani ovitka.