PRESEK

List za mlade matematike, fizike, astronome in računalnikarje

ISSN 0351-6652
Letnik **25** (1997/1998)
Številka 3
Strani 130–136

Ivan Vidav:

KAKO UGOTOVIMO, DA JE NARAVNO ŠTEVILO SESTAVLJENO, PREDEN GA RAZSTAVIMO?

Ključne besede: matematika, teorija števil, naravna števila, praštevila, sestavljena števila.

Elektronska verzija: http://www.presek.si/25/1335-Vidav.pdf

KAKO UGOTOVIMO, DA JE NARAVNO ŠTEVILO SESTAVLJENO, PREDEN GA RAZSTAVIMO?

Uvod.
Pred nekaj leti sta Richard Crandall in Christopher Doenias (ZDA) z računalniki dognala, da je dvaindvajseti člen Fermatovega zaporedja F_{22} sestavljeno število. Do istega rezultata sta skoraj istočasno toda z drugačnim računalniškim programom prišla tudi Vilmar Trevisan in João Carvalho v Braziliji. Ne prvima ne drugima pa ni uspelo najti nobenega faktorja.

Fermatovo zaporedje se glasi

$$F_n = 2^{2^n} + 1 . \tag{1}$$

Členi F_n z indeksom n izredno hitro naraščajo. Tako se F_{22} izraža v desetiškem sestavu s številko, ki ima nad milijon števk, in je torej nepredstavljivo veliko. Je največje naravno število, o katerem vemo, da je sestavljeno, ne poznamo pa (še) nobenega njegovega faktorja.

Fermat je domneval, da sestoji zaporedje (1) iz samih praštevil. Za prve štiri člene to res velja: $F_1 = 5$, $F_2 = 17$, $F_3 = 257$ in $F_4 = 65\,537$. Toda že Euler je odkril, da je $F_5 = 2^{32}+1$ sestavljeno število, deljivo je namreč s 641. Pozneje so ugotovili, da so sestavljena števila tudi mnogi drugi členi, npr. $F_6, F_7, F_8, F_9, F_{10}$ itd., praštevila pa niso našli med njimi nobenega več. Zanimivo je, da sta Morehead in Western dognala na začetku tega stoletja, da sta F_7 in F_8 sestavljeni števili, čeprav nista dobila nobenega faktorja. Na prafaktorje so ju razstavili skoraj 70 let pozneje, ko so izdelali boljše metode za razstavljanje in so se pojavili sodobni računalniki. Števili F_9 in F_{10}, prvo ima v desetiškem sestavu 155 in drugo 309 števk, pa so razstavili na prafaktorje šele pred nekaj leti.

Kakor vemo iz aritmetike, je vsako naravno število bodisi praštevilo bodisi sestavljeno in, če je sestavljeno, se da razstaviti v bistvu na en sam način v produkt praštevil. Obstajajo metode, s katerimi moremo vsako dano število razstaviti na prafaktorje. Najpreprostejši postopek je s poskušanjem: Število N delimo z zaporednimi naravnimi števili 2, 3 itd. do največjega celega števila, ki ne presega $\sqrt{N}$. Če ni z nobenim deljivo, je N praštevilo, če pa je s katerim izmed navedenih števil deljivo, je najmanjše med njimi (to je prvi delitelj, ki nanj pri tem postopku naletimo), prafaktor p. N razstavimo v produkt $N = p \cdot N_1$ in na drugem faktorju N_1 ponovimo postopek. Metoda s poskušanjem nas sicer privede vselej do cilja, toda je izredno počasna. Veliko truda potrebujemo, da z njo razstavimo nekoliko večje število. Če bi pa hoteli po tej metodi z računalnikom,

ki opravi milijon deljenj na sekundo, razstaviti petdesetmestno število, bi potrebovali v najneugodnejšem primeru tudi nekaj bilijonov let.

Na dejstvu, da ne znamo razstaviti velikih števil v razumnem času na prafaktorje in to niti s sodobnimi računalniki ne, sloni metoda tajnopisa z javnim ključem, ki so jo razvili Rivest, Shamir in Aldeman (metoda RSA). Javni ključ je produkt dveh orjaških praštevil. Tajnopis pa lahko razvozla samo tisti, ki pozna oba faktorja (glej članek M. Vencelj: Šifriranje z javnim ključem, Presek 22, str. 354–357). Avtorji so pred dvajsetimi leti objavili v časopisu Scientific American število s 129 mesti in pozvali bralce, naj kdo izmed njih poskuša razstaviti to število v produkt. Razcep se je posrečil šele leta 1994. Med tem časom so namreč razvili nove metode za razstavljanje, ki so seveda hitrejše od metode z zaporednim deljenjem. Z njimi je zdaj mogoče razstaviti števila, ki imajo, zapisana v desetiškem sestavu, nekaj nad sto števk. Med drugim se je posrečilo razstaviti F_9 in F_{10}.

Kako lahko vemo o kakšnem naravnem številu, da je sestavljeno, preden smo ga razstavili? Včasih je to mogoče ugotoviti pri številih, ki se odlikujejo z določenimi lastnostmi, oziroma imajo posebno obliko. Namen tega članka je, da si ogledamo nekaj takih primerov.

1. Vzemimo število 1 000 001. Pišemo ga lahko v obliki

$$1\,000\,001 = 100^3 + 1^3\,,$$

se pravi kot vsoto dveh kubov. Iz elementarne algebre pa vemo, da se da vsota dveh kubov razstaviti

$$a^3 + b^3 = (a+b)(a^2 - ab + b^2)\,.$$

Če postavimo $a = 100$ in $b = 1$ dobimo razcep $1\,000\,001 = 101 \cdot 9901$. Oba faktorja na desni sta praštevili.

Tudi vsota dveh petih, sedmih in splošno dveh poljubnih potenc z enakima lihima eksponentoma se da razstaviti. Tako je npr. $100\,001 = 10^5 + 1^5 = 11 \cdot 9091$. V vseh teh primerih vemo, da je število sestavljeno, preden smo ga razstavili, pa tudi faktorja takoj najdemo.

2. Če je naravno število vsota dveh kvadratov, ni vselej sestavljeno. Včasih je praštevilo, kot kaže zgled $41 = 4^2 + 5^2$, včasih sestavljeno: $50 = 1^2 + 7^2 = 2 \cdot 5^2$. Pri tem velja:

Če je kakšno naravno število izrazljivo na dva različna načina kot vsota dveh kvadratov, je sestavljeno.

Na primer 65 je enako $1^2 + 8^2$ in $4^2 + 7^2$. Število 65 je produkt prafaktorjev 5 in 13, $65 = 5 \cdot 13$.

Dokažimo zdaj našo trditev! Denimo, da smo naravno število N na dva različna načina zapisali kot vsoto dveh kvadratov

$$N = A^2 + B^2 \qquad \text{in} \qquad N = C^2 + D^2 \,. \tag{2}$$

Tu so A, B, C, D znana naravna števila in je par A, B različen od para C, D. Pri dokazovanju se bomo omejili na primer, ko je N lih (če je sod, ima faktor 2 in je sestavljeno število). Ugotovili bomo, da je N produkt dveh takih faktorjev U in V, torej $N = UV$, ki sta oba izrazljiva z vsoto dveh kvadratov. Privzemimo, da je to res, in postavimo

$$U = a^2 + b^2 \qquad \text{in} \qquad V = c^2 + d^2 \,. \tag{3}$$

a, b, c, d so cela števila, ki jih za zdaj še ne poznamo. Kako bi jih izračunali?

Preprosta verifikacija pokaže, da veljata identiteti

$$UV = (a^2 + b^2)(c^2 + d^2) = (ac + bd)^2 + (ad - bc)^2 \tag{4}$$

in

$$UV = (a^2 + b^2)(c^2 + d^2) = (ac - bd)^2 + (ad + bc)^2 \tag{4*}$$

Ker je $UV = N$, vidimo, da sta enačbi (2) izpolnjeni, če postavimo

$$\begin{aligned} ac + bd &= A \,, \qquad & ad - bc &= B \,, \\ ac - bd &= C \qquad & ad + bc &= D \,. \end{aligned} \tag{5}$$

Poskušajmo iz tega sistema izračunati a, b, c in d. S seštevanjem in odštevanjem dobimo produkte

$$ac = \frac{1}{2}(A + C) \,, \quad ad = \frac{1}{2}(B + D) \,, \quad bd = \frac{1}{2}(A - C) \,, \quad bc = \frac{1}{2}(D - B) \,. \tag{6}$$

Ker je N lih, pove prva enačba (2), da je eno izmed števil A in B liho in eno sodo. Isto pove druga enačba (2) o paru C, D. Naj bosta npr. A in C soda ter B in D liha. Potem so vse desne strani v (6) cela števila. Ker so tudi a, b, c, d cela števila, vidimo iz prvih dveh enačb, da je a skupni delitelj števil $\frac{1}{2}(A + C)$ in $\frac{1}{2}(B + D)$. Vzemimo za a kar največji skupni delitelj teh dveh števil. Izračunamo ga lahko z Evklidovim algoritmom. Tako dobimo a in nato iz prvih dveh enačb (6) še c in d:

$$c = (A + C)/2a \qquad \text{in} \qquad d = (B + D)/2a \,.$$

Ker je a največji skupni delitelj produktov ac in ad, sta si c in d tuja. Potem izračunamo b iz tretje ali četrte enačbe. Obe nam dasta isto vrednost: Iz enačb (2) namreč izhaja, da je $A^2 - C^2 = D^2 - B^2$ in zato $(A - C)a/(B + D) = (D - B)a/(A + C)$. Da je tudi b celo število, ugotovimo takole: b je kvocient celih števil $(A - C)a$ in $B + D$. Torej je racionalen in ga lahko zapišemo v obliki okrajšanega ulomka $b = r/s$, kjer sta r in s celi števili brez skupnega faktorja in je $s > 0$. Ker sta produkta $bd = rd/s$ in $bc = rc/s$ celi števili, to namreč povesta zadnji enačbi (6), sta števca rd in rc v ulomkih na desni deljiva z s. Toda r je tuj proti s in sta potemtakem c in d deljiva z s. Ker sta si tudi d in c tuja, pa mora biti imenovalec $s = 1$ in $b = r$ celo število.

Pri tako določenih a, b, c, d veljajo enačbe (6). Če produkte (6) vstavimo v (5), vidimo, da so tudi te enačbe izpolnjene. Ker je $U = a^2 + b^2$ in $V = c^2 + d^2$, pove identiteta (4), da je $UV = A^2 + B^2 = N$. Par A, B je različen od para C, D in so zato desne strani v (6) različne od nič. To pa pomeni, da so tudi a, b, c, d različni od nič in, ker so cela števila, je $U > 1$ ter $V > 1$; razcep $N = UV$ je pravi. S tem smo dokazali trditev, da je N sestavljeno število, našli faktorja U in V, hkrati pa smo U in V izrazili z vsoto dveh kvadratov.

Ker lahko pišemo

$$F_n = \left(2^{2^{n-1}}\right)^2 + 1^2 ,$$

je vsako Fermatovo število vsota dveh kvadratov. Če bi se nam posrečilo zapisati F_n še kako drugače kot vsoto dveh kvadratov, bi vedeli, da je sestavljeno število, in tudi razstaviti bi ga znali v produkt dveh faktorjev. Za zgled vzemimo

$$F_5 = (2^{16})^2 + 1^2 = 65\,536^2 + 1 ,$$

ki ga lahko pišemo tudi v obliki

$$F_5 = 62\,264^2 + 20\,449^2 . \tag{7}$$

Zdaj imamo

$$A = 65\,536 , \quad B = 1 , \quad C = 62\,264 , \quad D = 20\,449 .$$

Enačbe (6) se tu glasijo

$$ac = 63\,900, \quad ad = 10\,225, \quad bd = 1636, \quad bc = 10\,224 . \tag{8}$$

Najprej poiščemo z Evklidovim algoritmom največji skupni delitelj števil 63 900 in 10 225 in dobimo, da je 25. Največji skupni delitelj je enak a, torej $a = 25$. Enačbe (8) zdaj dajo $c = 2\,556$, $d = 409$, $b = 4$. Potemtakem je $U = 25^2 + 4^2 = 641$ in $V = 2556^2 + 409^2 = 6\,700\,417$, torej $F_5 = 641 \cdot 6\,700\,417$. Oba faktorja sta praštevili.

Seveda bo kdo vprašal, kako smo našli izrazitev (7)? Odgovor se glasi: s poskušanjem. Vendar je treba priznati, da je s tem poskušanjem kar precej dela. Ker je tu faktor 641 razmeroma majhen, najdemo razcep veliko hitreje, če delimo F_5 z zaporednimi naravnimi števili.

3. Obstajajo tudi metode, s katerimi včasih ugotovimo, da je dano število sestavljeno, ne povejo pa te metode, kako priti do kakšnega faktorja. Mali Fermatov izrek iz teorije števil nam na primer da tale kriterij:

Naj bo N dano naravno število. Izberimo poljubno celo število a. Če razlika $a^N - a$ ni deljiva z N, je N sestavljeno število.

Dokaz najde bralec v knjigi: J. Grasselli, Osnove teorije števil, 1975, na strani 74.

Pripomba. Ta kriterij ne pove nič v primeru, kadar je razlika $a^N - a$ deljiva z N: tedaj je lahko N praštevilo ali sestavljeno število.

Test napravimo tako, da si najprej izberemo a, npr. $a = 2$ ali $a = 3$, in potem izračunamo $a^N - a$. Ker je N po navadi veliko število, se na prvi pogled zdi, da je ta metoda ugotavljanja praštevilskosti počasnejša od metode s poskušanjem, saj bi opravili deljenje z vsemi števili do $\sqrt{N}$ verjetno prej, kakor pa izračunali potenco a^N, ki je pri velikem N orjaško število. Vendar ta videz vara. Potenco a^N izračunamo razmeroma hitro z zaporednimi kvadriranji in si tako prihranimo veliko dela. In ker gre pri testu le za vprašanje deljivosti razlike $a^N - a$ z N, se lahko pri računanju omejimo na števila manjša od N.

Oglejmo si posebni primer, ko je N oblike $2^m + 1$, kjer je eksponent m sod (če je lih in > 1, je število N deljivo s 3 in sestavljeno). Pri Fermatovih številih je $m = 2^n$. Sestavimo zaporedje naravnih števil

$$o_0,\ o_1,\ o_2,\ o_3, \ldots \tag{9}$$

takole: Naj bo $o_0 = 3$. Če smo člen o_k že našli, ga kvadriramo in kvadrat o_k^2 delimo z N. Ostanek pri tej delitvi je naslednji člen o_{k+1}. (Denimo, da je $N > 9$. Potem je $o_1 = o_0^2 = 9$, ker dobimo ostanek 9, če delimo 9 s številom večjim od 9. Podobno je $o_2 = 81$, če je $N > 81$.) Zaporedje (9) lahko priredimo vsakemu naravnemu številu $N > 3$. Ker so členi $o_1, o_2, \ldots$ ostanki pri deljenju z N, so vsi manjši od N.

Iz zgoraj navedenega testa pri $a = 3$ izpeljemo z uporabo recipročnostnega zakona iz teorije števil tale pogoj za praštevilskost:

Število $N = 2^m + 1$ je praštevilo natanko takrat, kadar je člen o_{m-1} pripadajočega zaporedja (9) enak $N-1$, torej $o_{m-1} = N - 1 = 2^m$.

Zgledi.

1. Vzemimo najprej $m = 4$, torej $N = 2^4 + 1 = 17 = F_2$. Poiskati je treba člen o_3 zaporedja (9). Tu je $o_1 = 9$, $o_2 = 13$ in $o_3 = 16 = N - 1$. Res je $N = 17$ praštevilo.

2. Pri $m = 6$ potrebujemo člen o_5. Zdaj je $o_1 = 9$, $o_2 = 16$, $o_3 = 61$, $o_4 = 16$ in $o_5 = 61 \neq 64 = 2^6$. Število $N = 2^6 + 1 = 65$ ni praštevilo, $65 = 5 \cdot 13$.

Pripomba. Ni težko ugotoviti, da je $2^m + 1$ praštevilo kvečjemu tedaj, kadar je m potenca od 2, se pravi $m = 2^n$.

3. Pri Fermatovih številih F_n je eksponent $m = 2^n$, ki z n hitro narašča. Zato se hitro veča število členov zaporedja (9), ki jih je treba izračunati pri tem testu, še hitreje pa raste F_n. Za število F_5 je $m = 2^5 = 32$ in moramo izračunati člen o_{31}, če želimo ugotoviti, da F_5 ni praštevilo (faktorja nam test ne da). Z računanjem je precej dela in spet pridemo hitreje do faktorja 641 z zaporednim deljenjem.

Oglejmo si F_{22}. To število ima, zapisano v desetiškem sestavu, kakor smo že povedali, nad milijon števk. Ker je tu $m = 2^{22} = 4\,194\,304$, moramo izračunati 4 194 303 člene zaporedja (9). Pri določanju ostankov je treba deliti števila z nad milijon mesti. Dela je vsekakor ogromno. Vendar so ga sodobni računalniki zmogli. Potrebovali so okoli 10^{16} osnovnih operacij. Test je pokazal, da je F_{22} sestavljeno število, seveda pa ni dal nobenega faktorja. Razstaviti F_{22} na prafaktorje je težja naloga, ki terja neprimerno večji obseg računanja. (Z zaporednim deljenjem ne pridemo nikamor, saj je pri tako velikem številu, kakor je F_{22}, velika verjetnost, da ima tudi najmanjši prafaktor nad tisoč mest.) Morda se bo razcep posrečil, ko bodo odkrili še boljše metode za razstavljanje in izdelali še hitrejše računalnike.

Naloge.

1. Najmanjše naravno število, ki je izrazljivo na dva načina kot vsota dveh četrtih potenc, je 635 318 657. Je namreč

$$635\,318\,657 = 133^4 + 134^4 = 59^4 + 158^4\,.$$

Razstavi to število na prafaktorje!

2. Z žepnim računalnikom razstavi F_6 na dva faktorja, če veš, da je

$$F_6 = 4\,046\,803\,256^2 + 1\,438\,793\,759^2 .$$

3. Naj bo N sodo število, ki se da na dva različna načina zapisati kot vsota dveh kvadratov: $N = A^2 + B^2$ in $N = C^2 + D^2$. Dokaži, da so v tem primeru bodisi vsa števila A, B, C, D soda bodisi vsa liha in da sta faktorja U in V pripadajoče razcepitve večja od 2.

Ivan Vidav

Literatura

Richard E. Crandall: The Challenge of Large Numbers. Scientific American, Vol. 276, Febr. 1997, str. 58 – 62.

Akademika prof. dr. Ivana Vidava, znanstvenika in vzgojitelja številnih rodov slovenskih matematikov, poznajo Presekovi bralci predvsem kot avtorja zanimivih matematičnih člankov. V kratkem bo naš spoštovani sodelavec praznoval okrogli življenjski jubilej.

Za praznik mu iskreno voščimo!