Pokroky matematiky, fyziky a astronomie

Carl Pomerance

Vyprávění o dvou sítech

Pokroky matematiky, fyziky a astronomie, Vol. 43 (1998), No. 1, 9--29

Persistent URL: http://dml.cz/dmlcz/138468

[3] P. MÁLEK: *Historie a současnost homeopatie.* Vesmír *69* (1990), 69–72.
[4] J. HEŘT a kol.: *Homeopatie, clusterová medicína, anthroposofická medicína. Medicína pro třetí tisíciletí?* Nakladatelství Lidové noviny, Praha 1997.
[5] J. PLÁŠEK, J. ZVÁROVÁ: *Je homeopatické léčení účinnější než placebo?* Čas. lék. čes. *135* (1996), 575–579..
[6] E. DAVENAS, F. BEAUVAIS, J. AMARA, M. OVERBAUM, B. ROBINZON, A. MIADONNA, A. TEDESCHI, B. POMERANZ, P. FORTNER, P. BELON, J. SAINTE-LAUDY, B. POITEVIN, J. BENVENISTE: *Human basophil degranulation triggered by very dilute antiserum against IgE.* Nature *333* (1988), 816–818.
[7] J. MADDOX, J. RANDI, W. W. STEWART: *„High-dilution" experiments a delusion.* Nature *334* (1988), 287–290.
[8] J. MADDOX: *Waves caused by extreme dilution.* Nature *335* (1988), 760–763.
[9] P. MÁLEK: *Benvenistova aféra.* Vesmír *68* (1989), 395–397.
[10] W. BIENERT: *Slovník katolické dogmatiky.* MCM, Olomouc 1994.
[11] JAN PAVEL II.: *Projev k Papežské akademii věd 29. 10. 1990.* Universum 5/92 (1992), 1–4.
[12] J. HUTH: *Krize „Krize objektivity".* Čs. čas. fyz. *44* (1994), 379–382.
[13] W. WELSH: *Naše postmoderní moderna.* Zvon, Praha 1994.
[14] J. NOVOTNÝ: *Co je postmodernismus?* Čs. čas. fyz. *44* (1994), 373–375.
[15] H. J. STÖRIG: *Malé dějiny filosofie.* Zvon, Praha 1992.

Vyprávění o dvou sítech

Carl Pomerance

Tento článek je věnován památce Paula Erdőse, mého přítele a učitele.

Teď přišla ta nejlepší doba pro hrátky s faktorizací, tj. s rozkladem velkých čísel na prvočinitele. V roce 1970 bylo stěží možné rozložit „obtížná" dvaceticiferná čísla. V roce 1980, v době rozkvětu Brillhartova–Morrisonova faktorizačního algoritmu, *metody řetězových zlomků* (continued fraction factoring algorithm), se rozklad padesáticiferných čísel stával běžnou věcí. V roce 1990 můj vlastní algoritmus *kvadratického síta* (quadratic sieve factoring algorithm) umožnil zdvojnásobit délku čísel, jež mohla být rozložena, rekordní mělo 116 cifer.

CARL POMERANCE je profesorem matematiky na University of Georgia, Athens, USA, e-mail: carl@ada.math.uga.edu

A tale of two sieves. Notices Amer. Math. Soc. *43* (1996), 1473–1485.

Přeložili JAN CHLEBOUN, MICHAL KŘÍŽEK a KAREL SEGETH za podpory grantu 201/97/0217 GA ČR. Originál článku je přístupný na adrese http://www.ams.org/publications/notices/199612/pomerance.html

Do roku 1994 bylo kvadratickým sítem rozloženo slavné, nepokořené 129ciferné číslo ze souboru RSA[1]), které, podle odhadu Martina Gardnera v časopise Scientific American z roku 1976, mělo vzdorovat 40×10^{15} let (ačkoliv jiné tehdejší odhady byly skromnější). Ale kvadratické síto dnes už není mistrem. Tím se stalo Pollardovo *síto číselného tělesa* (number field sieve), když na jaře 1996 úspěšně rozložilo 130ciferné číslo ze sbírky RSA, a to za 15 % času, který by na to bylo bývalo potřebovalo síto kvadratické.

V tomto článku se stručně seznámíme s uvedenými faktorizačními algoritmy — dvěma síty — a též s některými z mnoha lidí, kteří je pomohli vyvinout.

V polovině tohoto století se početní záležitosti zdály být nemoderní. Ve většině odborných knih byl problém rozkladu velkých čísel z velké části opomíjen, protože byl považován za triviální. Koneckonců *v principu* byl řešitelný, tak o čem ještě mluvit? Jen málo výzkumníků ignorovalo názory té doby a pokračovalo v pokusech najít rychlé metody faktorizace. Pro tuto hrstku badatelů to byl základní problém, jeden z těch, které by neměly být odloženy stranou.

Ale časy se mění. Během posledních několika desetiletí jsme viděli příchod dostupných a rychlých počítačů a také vzestup kryptografických systémů, jejichž bezpečnost je založena na předpokládané neschopnosti rychle faktorizovat (a na jiných poznatcích z teorie čísel). Faktorizací se dnes zabývá mnoho lidí. Uznávají ji nejen jako měřítko bezpečnosti kryptografických systémů, ale i pro počítání samotné. Sdružení ACM (Association for Computing Machinery) věnovalo v roce 1984 pamětní desku ústavu IEEE (Institute for Electrical and Electronics Engineers) u příležitosti jeho stého výročí. Na ní byl vyryt rozklad čísla $2^{251} - 1$ na prvočinitele, v onom roce totiž byl pomocí kvadratického síta dokončen. Prezident ACM k tomu poznamenal:

„Před třemi sty lety francouzský matematik Mersenne považoval $2^{251} - 1$ za složené, to jest rozložitelné číslo. Před zhruba sto lety bylo dokázáno, že toto číslo opravdu složené je, avšak ještě před dvaceti lety byla výpočetní náročnost jeho rozkladu považována za nepřekonatelnou. Opravdu, při použití obvyklých počítačů a tradičních vyhledávacích algoritmů byl potřebný čas odhadován na asi 10^{20} let. Letos v únoru bylo v Sandia Laboratories toto číslo rozloženo na počítači Cray během 32 hodin. To je světový rekord. V počítání jsme urazili dlouhou cestu, a abychom připomněli příspěvek IEEE k tomuto oboru, nechali jsme těch pět činitelů Mersennova složeného čísla vyrýt na desku. Happy Birthday, IEEE."

Rozkládání velkých čísel je zvláštní odvětví matematiky a velmi připomíná experimentální vědy, kde příroda má poslední a rozhodující slovo. Jestliže nějaký algoritmus rozkládající číslo n po chvíli práce skončí výrokem „d je dělitel n", pak toto tvrzení může být snadno ověřeno, tj. poslední a rozhodující slovo patří celým číslům. Lze se tak docela pěkně obejít bez důkazu, že metoda obecně funguje. Ale stejně jako v experimentálních vědách, i tady může být pro porozumění a pokrok cenná jak

[1]) *Poznámka překladatelů:* Počáteční písmena příjmení tří autorů, kteří navrhli metodu šifrování pomocí veřejného klíče založenou na obtížnosti rozkladu velkých čísel na prvočinitele (R. L. Rivest, A. Shamir, L. M. Adleman: *A method for obtaining digital signatures and public-key cryptosystems*, Comm. ACM *21* (1978), 120–126).

rigorózní, tak heuristická analýza. A ovšem, stejně jako v experimentálních vědách, i zde se občas objeví napětí mezi teoretiky a praktiky. Někdo se domnívá, že teoretické studium faktorizace je darmožrout (neboli, jak to jednou barvitě vyjádřil Hendrik Lenstra parafrází Siegela, „čuník v rozáriu"), který se těší nezasloužené pozornosti díky tomu, že algoritmy suše označuje nálepkami „polynomiální", „exponenciální", „náhodný" atd., avšak nic nebo jen málo nabízí těm dříčům, kteří opravdu počítají. V tomto názoru je zrnko pravdy, nicméně jak uvidíme, teorie sehrála významnou roli při vývoji obou sít, o nichž budeme hovořit.

Soutěžní úloha

Začněme od začátku, přinejmenším od toho mého. Když přednáším o faktorizaci, často opakuji starou příhodu, která se mi stala na střední škole. Účastnil jsem se matematické soutěže a jedna z úloh byla rozložit během pěti minut číslo 8051. Nebylo nám zakázáno používat kapesní kalkulačky, ty tenkrát, okolo roku 1960, kdy se to stalo, vůbec neexistovaly! Nu, v aritmetice jsem byl docela dobrý a věděl jsem, že v časovém limitu mohu zkoušet dělit čísly až do odmocniny z 8051 (což je zhruba 90). Ale během každého testu, zejména soutěžního, se mnoho studentů pokouší vcítit do mysli osoby, která ho připravila. Jistě by nám nezadali problém, jehož jediný rozumný způsob řešení by spočíval v horečném zkoušení možných dělitelů. K cíli musí vést i jiná, obratná cesta. Tak jsem strávil několik minut jejím hledáním, zatímco ve mně vzrůstalo znepokojení, že ztrácím příliš mnoho času. Pak jsem opožděně začal s pokusným dělením, jenže čas jsem už skutečně promarnil a úlohu jsem nevyřešil.

Najdete ten důvtipný způsob řešení? Chcete-li o něm chvíli přemýšlet, odložte čtení dalšího odstavce.

Fermat a Kraitchik

Celý trik je založen na rozepsání 8051 jako $8100 - 49$, což je $90^2 - 7^2$, takže k rozložení čísla 8051 můžeme využít znalosti algebry, přesněji faktorizace rozdílu čtverců. Výsledek je 83×97.

Vede tento postup vždy k cíli? Platí, že každé liché složené číslo může být rozloženo jako rozdíl kvadrátů: stačí užít rovnost $ab = \left(\frac{1}{2}(a+b)\right)^2 - \left(\frac{1}{2}(a-b)\right)^2$. Snaha vyjádřit číslo jako rozdíl dvojice čtverců, to je vlastně Fermatova faktorizační metoda. Podobně jako pokusné dělení, které je někdy velmi snadné (když existuje malý dělitel), také metoda rozdílu čtverců zná jednoduché případy. Například najít příslušné kvadráty je snadné, jestliže $n = ab$, kde hodnoty a a b jsou velmi blízké $\sqrt{n}$, jak je tomu v případě $n = 8051$. Avšak v nejhorších případech může být metoda rozdílu čtverců daleko horší než pokusné dělení. I z jiného hlediska je horší. Při pokusném dělení se velmi mnoho čísel ocitne v kategorii snadných případů, většina čísel totiž má malého dělitele. Jenže jen malá část čísel má dělitele blízkého jejich odmocnině, takže metoda rozdílu čtverců pracuje efektivně jen s malou částí možných vstupů. (Ačkoli pokusné dělení umožňuje

začít faktorizaci pro většinu vstupů, úplný rozklad je obvykle daleko obtížnější. Většina čísel mu odolává, i když použijeme kombinaci pokusného dělení a metody rozdílu čtverců.)

Ve dvacátých letech tohoto století přišel Maurice Kraitchik[2]) se zajímavým zlepšením Fermatovy techniky rozdílu čtverců, a právě toto vylepšení je základem většiny moderních faktorizačních algoritmů. (Myšlenka sama má kořeny v pracích Gaussových a Seelhoffových, avšak Kraitchik ji rozvinul a představil nové generaci v novém století. O raném údobí faktorizace naleznete více v [23].) Místo aby zkoušel hledat celá čísla u a v, pro něž $u^2 - v^2 = n$, Kraitchik si uvědomil, že by stačilo najít u a v taková, aby $u^2 - v^2$ bylo rovno *násobku* n, tj. $u^2 \equiv v^2 \bmod n$. Tato kongruence může mít nezajímavá řešení, když $u \equiv \pm v \bmod n$, ale též řešení zajímavá, jestliže $u \not\equiv \pm v \bmod n$. Je-li n liché a dělitelné aspoň dvěma odlišnými prvočísly, pak přinejmenším polovina všech řešení rovnice $u^2 \equiv v^2 \bmod n$ je zajímavého druhu, pokud součin uv je nesoudělný s n. A pro zajímavé řešení u, v platí, že největší společný dělitel $u - v$ a n, označený $(u - v, n)$, musí být netriviálním dělitelem n. Opravdu, n dělí $u^2 - v^2 = (u - v)(u + v)$, ale nedělí žádného z činitelů. Tudíž n musí být nějak rozděleno mezi $u - v$ a $u + v$.

Na okraj poznamenejme, že nalezení největšího společného dělitele (a, b) dvou zadaných čísel a a b je velmi snadný úkol. Jestliže $0 < a \leqq b$ a a dělí b, pak $(a, b) = a$. Jestliže a nedělí b, potom zůstává zbytek r a $(a, b) = (a, r)$. Tato hezká myšlenka záměny rozsáhlejšího problému za menší je přes dva tisíce let stará a pochází od Euklida. Je to rychlý postup, nalezení největšího společného dělitele čísel a a b trvá počítači zhruba tak dlouho jako jejich vzájemné vynásobení.

Podívejme se, jak by Kraitchik mohl rozložit $n = 2041$. První čtverec větší než n je $46^2 = 2116$. Vezměme posloupnost čísel $Q(x) = x^2 - n$, kde $x = 46, 47, \ldots$ Dostaneme

$$75,\ 168,\ 263,\ 360,\ 459,\ 560,\ \ldots$$

Protože se dosud neobjevily žádné kvadráty, Fermat by pokračoval v hledání. Ale Kraitchik nabízí něco jiného. Pokouší se najít několik takových čísel x, aby platilo, že součin odpovídajících hodnot $Q(x)$ je čtverec. Pak totiž z rovností $Q(x_1) \cdots Q(x_k) = v^2$ a $x_1 \cdots x_k = u$ plyne

$$u^2 = x_1^2 \cdots x_k^2 \equiv (x_1^2 - n) \cdots (x_k^2 - n) = Q(x_1) \cdots Q(x_k) = v^2 \bmod n,$$

což znamená, že jsme našli řešení problému $u^2 \equiv v^2 \bmod n$. Jak však najít množinu $x_1, \ldots, x_k$? Kraitchik si povšiml, že některá z čísel $Q(x)$ se rozkládají *velmi* snadno:

$$75 = 3 \cdot 5^2, \quad 168 = 2^3 \cdot 3 \cdot 7, \quad 360 = 2^3 \cdot 3^2 \cdot 5, \quad 560 = 2^4 \cdot 5 \cdot 7.$$

Na základě předchozích rozkladů tak může říci, že součin těchto čtyř čísel je $2^{10} \cdot 3^4 \cdot 5^4 \cdot 7^2$, čtverec! Získal $u^2 \equiv v^2 \bmod n$, kde

$$u = 46 \cdot 47 \cdot 49 \cdot 51 \equiv 311 \bmod 2041,$$
$$v = 2^5 \cdot 3^2 \cdot 5^2 \cdot 7 \equiv 1416 \bmod 2041.$$

[2]) *Poznámka překladatelů:* Přesnější by bylo psát Kraïtchik.

Nyní je téměř hotov, neboť $311 \not\equiv \pm 1416 \bmod 2041$. Aby určil největšího společného dělitele $(1416 - 311, 2041)$, použije Euklidova algoritmu a dospěje k číslu 13, čili $2041 = 13 \cdot 157$.

Řetězové zlomky

Podstatou Kraitchikovy metody je zkoušet „hrát si" s posloupností $x^2 - n$, kde x nabývá celočíselných hodnot blízkých $\sqrt{n}$, a hledat podposloupnost, jejíž součin je čtverec. Jestliže odmocnina tohoto čtverce je rovna ν a součin odpovídajících hodnot x je roven u, pak $u^2 \equiv \nu^2 \bmod n$ a můžeme doufat, že tato kongruence je „zajímavá", konkrétně, že $u \not\equiv \pm\nu \bmod n$. V roce 1931 navrhli D. H. Lehmer a R. E. Powers nahradit Kraitchikovu funkci $Q(x) = x^2 - n$ funkcí jinou, odvozenou z rozvoje $\sqrt{n}$ do řetězového zlomku.

Je-li a_i/b_i i-tý řetězový zlomek konvergující k $\sqrt{n}$, označme $Q_i = a_i^2 - b_i^2 n$. Potom $Q_i \equiv a_i^2 \bmod n$. Místo čísel $Q(x)$ tedy můžeme zkoumat hodnoty Q_i, protože v obou případech jsou kongruentní modulo n se známými kvadráty. Ačkoli řetězové zlomky mohou při výpočtech působit potíže, případ kvadratických iracionalit[3]) je docela příjemný. Existuje jednoduchý iterační postup (viz [16]) známý už Gaussovi a možná ještě dříve, jímž lze vypočítat vše, co je zapotřebí, tj. posloupnost celých čísel Q_i a reziduí $a_i \bmod n$.

Ale proč komplikovat dokonale jednoduchý kvadratický polynom něčím tak exotickým, jako jsou řetězové zlomky? Důvodem je nerovnost $|Q_i| < 2\sqrt{n}$. Čísla Q_i jsou v absolutní hodnotě menší než $Q(x)$. (Když se x vzdaluje od $\sqrt{n}$, čísla $Q(x)$ rostou přibližně lineárně se směrnicí $2\sqrt{n}$.) Chce-li si někdo „hrát" s čísly, aby mezi nimi našel ta, jejichž součin je čtverec, je pravděpodobně jednodušší pracovat s čísly menšími než s většími. Takže Lehmerovy a Powersovy řetězové zlomky jsou zjevně výhodnější než Kraitchikův kvadratický mnohočlen.

Jak si „hrát" s čísly

Je jistě zvláštní, když algoritmus obsahuje instrukci požadující, abyste si hráli s nějakými čísly a našli jejich podmnožinu se součinem rovným čtverci. Vzpomínám si na kreslený vtip, kde u tabule popsané tajemnými matematickými symboly stojí dva vědci v bílých pláštích a jeden z nich ukazuje na obzvlášť zapeklitou část a říká tomu druhému, že právě v tomhle místě nastává zázrak. Je to zázrak, že jsme v Kraitchikově posloupnosti byli schopni najít čísla 75, 168, 360 a 560 se součinem rovným čtverci? Proč bychom měli očekávat, že takovou podposloupnost najdeme, a jestliže existuje, jak ji můžeme najít efektivně?

Systematickou strategii hledání takové podposloupnosti dané posloupnosti, aby její součin byl čtverec, objevili John Brillhart a Michael Morrison. Je překvapující, že

[3]) *Poznámka překladatelů:* Jsou to čísla tvaru $a + b\sqrt{c}$ (quadratic irrationals).

v jádře jde pouze o lineární algebru (viz [16]). Ke každému přirozenému číslu m existuje „vektor exponentů“ $\nu(m)$ definovaný prostřednictvím rozkladu čísla m. Nechť p_i značí i-té prvočíslo a nechť $m = \prod p_i^{\nu_i}$. (Násobí se přes všechna prvočísla, ale jen konečný počet exponentů ν_i je nenulových.) Pak $\nu(m)$ je vektor $(\nu_1, \nu_2, \ldots)$. Například vynecháme-li nekonečnou posloupnost nul, která následuje za čtvrtou složkou, dostaneme

$$\begin{aligned}\nu(75) &= (0,1,2,0),\\ \nu(168) &= (3,1,0,1),\\ \nu(360) &= (3,2,1,0),\\ \nu(560) &= (4,0,1,1).\end{aligned}$$

Pro naše účely poskytují vektory exponentů *příliš mnoho* informací. Zajímají nás pouze čtverce, a protože kladné celé číslo m je čtvercem právě tehdy, když každá složka $\nu(m)$ je sudá, můžeme exponenty redukovat modulo 2. Jelikož ν převádí násobení na sčítání, hledáme čísla, pro něž platí, že součet jejich vektorů exponentů je roven nule modulo 2. Po redukci uvedených vektorů modulo 2 dostaneme vektory

$$\begin{aligned}\nu(75) &\equiv (0,1,0,0) \bmod 2,\\ \nu(168) &\equiv (1,1,0,1) \bmod 2,\\ \nu(360) &\equiv (1,0,1,0) \bmod 2,\\ \nu(560) &\equiv (0,0,1,1) \bmod 2.\end{aligned}$$

Všimněte si, že jejich součet je roven nulovému vektoru![4]) Tudíž součin čísel 75, 168, 360 a 560 je čtverec.

Aby tento postup byl systematický, Brillhart a Morrison navrhují zvolit nějaké číslo B a zabývat se pouze těmi čísly v posloupnosti, která lze úplně rozložit na mocniny prvních B prvočísel. Ve výše uvedeném příkladu je $B = 4$. Jakmile získáme $B + 1$ takových čísel, máme $B + 1$ vektorů v B-dimenzionálním vektorovém prostoru $\mathbb{F}_2^B$. Je jasné, že musí být lineárně závislé. Co však znamená pojem lineární závislosti nad tělesem $\mathbb{F}_2$? Jelikož jeho jedinými skaláry jsou 0 a 1, relace pro lineární závislost prostě odpovídá částečnému součtu, který se rovná nulovému vektoru. A z lineární algebry známe mnoho algoritmů, jež nám umožňují najít tuto závislost.

Poznamenejme, že jsme měli trochu štěstí, protože jsme našli závislost mezi pouhými čtyřmi vektory a nepotřebovali jsme jich pět, což by v nejhorším případě mohlo nastat.

Brillhart a Morrison nazývají prvočísla $p_1, p_2, \ldots, p_B$ „rozkladovou bází“. (Přesněji, vyřazují ta prvočísla p_j, pro něž n není kongruentní se čtvercem, protože taková prvočísla nikdy nemohou dělit číslo Q_i v metodě řetězových zlomků ani číslo $Q(x)$ v Kraitchikově algoritmu.) Jaké velké B by mělo být zvoleno? Bude-li malé, pak není nutné shromáždit mnoho čísel, abychom mohli skončit. Ale jestliže bude příliš malé, pak pravděpodobnost, že v posloupnosti najdeme nějaké číslo s úplným rozkladem

[4]) *Poznámka překladatelů:* Roven modulo 2.

na prvních B prvočísel, je tak nepatrná, že bude těžké najít aspoň jedno takové číslo. Někde tedy leží uspokojivý kompromis. Pro rozklad čísla 2041 Kraitchikovou metodou se jako vhodně zvolené ukázalo být $B = 4$.

Některá z pomocných čísel mohou být záporná. Jak budeme zacházet s jejich vektory exponentů? Zřejmě nemůžeme ignorovat znaménko, protože kvadráty nejsou záporné. Do každého vektoru však můžeme zavést zvláštní složku, která pro kladná čísla nabývá hodnoty 0 a pro záporná hodnoty 1. (To je jako kdybychom do rozkladové báze zahrnuli i „prvočíslo" -1.) Připustit záporná pomocná čísla tedy znamená pouze zvýšit dimenzi problému o jedničku.

Například opět vezměme číslo 2041 a pokusme se ho rozložit pomocí Kraitchikova polynomu, nyní však připusťme i záporné hodnoty. Pro $Q(x) = x^2 - 2041$ a rozkladovou bázi 2, 3 a 5 dostáváme

$$\begin{aligned} Q(43) &= -192 = -2^6 \cdot 3 \leftrightarrow (1,0,1,0) \\ Q(44) &= -105 \\ Q(45) &= -16 = -2^4 \leftrightarrow (1,0,0,0) \\ Q(46) &= 75 = 3 \cdot 5^2 \leftrightarrow (0,0,1,0), \end{aligned}$$

kde první složky odpovídají exponentu u čísla -1. Při použití záporných čísel a menší rozkladové báze 2, 3 a 5 jsme měli náramné štěstí, protože již ty tři dosud získané vektory jsou lineárně závislé. To vede na kongruenci $(43 \cdot 45 \cdot 46)^2 \equiv (-192)(-16)(75) \bmod 2041$ neboli $1247^2 \equiv 480^2 \bmod 2041$. Opět získáme 13 jako dělitele 2041, neboť $(1247 - 480, 2041) = 13$.

Je možné říci, že poslední krok — nalezení největšího společného dělitele — vždy vede k netriviálnímu rozkladu? Ne, není. Čtenář si může vyzkoušet ještě jiný soubor kvadrátů majících vztah k číslu 2041. Tentokrát ho tvoří $Q(x)$ pro $x = 41$, 45 a 49 a vzniká kongruence $601^2 \equiv 1440^2 \bmod 2041$. Řečeno naší dřívější terminologií, tato kongruence je nezajímavá, protože $601 \equiv -1440 \bmod 2041$. A abychom měli jistotu, největší společný dělitel $(601 - 1440, 2041)$ je zcela triviální, totiž 1.

Hladká čísla a podněty z teorie složitosti

S příchodem kódování RSA pomocí veřejného klíče koncem sedmdesátých let začalo být zvlášť důležité zkusit odhadnout, jak obtížnou záležitostí rozklad čísel vlastně je. Nejenže bychom měli vědět, co je dnes možné, ale také bychom rádi předpověděli, co by asi vyžadoval rozklad těch čísel, která jsou za hranicí dnešních možností. Zkušenost říká, že počítače stejné cenové třídy zdvojnásobují svou rychlost a kapacitu každých 18 až 24 měsíců. Vyjděme z tohoto předpokladu a neočekávejme žádné nové faktorizační algoritmy. Co bude technicky možné za deset let?

K hledání odpovědí na tento typ otázek se hodí teorie složitosti. Jak ale analyzovat faktorizaci založenou na Kraitchikově polynomu nebo Lehmerově–Powersově řetězovém zlomku? Cestu navrhl Richard Schroeppel ve své nepublikované korespondenci z pozdních sedmdesátých let. V podstatě začal tím, že čísla Q_i z metody řetězových

zlomků nebo čísla $Q(x)$ z Kraitchikovy metody považoval za „náhodná". Jestliže dostáváte proud zcela náhodných čísel shora omezených nějakým X, jak dlouhou byste měli očekávat dobu, kterou vám zabere nalezení podposloupnosti, jejíž součin je roven čtverci?

Pokud číslo nemá prvočinitele větší než Y, nazveme je Y-hladké. (Číslo, které je rozložitelné nad prvočísly až do hodnoty p_B, je p_B-hladké.) Jaká je pravděpodobnost, že náhodně zvolené přirozené číslo menší nebo rovné X je Y-hladké? Odpověď zní[5]) $\Psi(X,Y)/[X] \approx \Psi(X,Y)/X$, kde $\Psi(X,Y)$ je počet Y-hladkých čísel v intervalu $\langle 1, X\rangle$. Očekávaný počet náhodných čísel, která musí být vyšetřena, abychom nalezli právě jedno číslo Y-hladké, je tedy roven převrácené hodnotě této pravděpodobnosti, tj. $X/\Psi(X,Y)$. My ovšem musíme najít zhruba $\pi(Y)$ takových Y-hladkých čísel, $\pi(Y)$ značí počet prvočísel menších nebo rovných Y. Tudíž očekávaný počet náhodných čísel, která musíme zkoumat, je přibližně $\pi(Y)X/\Psi(X,Y)$. A kolik to asi dá práce ověřit, zda je číslo Y-hladké? Jestliže k tomu použijeme metodu pokusného dělení, je to okolo $\pi(Y)$ kroků. Takže očekávaný počet všech kroků je $\pi(Y)^2X/\Psi(X,Y)$.

Vybrat Y jako funkci X tak, aby se minimalizovala hodnota $\pi(Y)^2X/\Psi(X,Y)$, je záležitostí analytické teorie čísel. Koncem sedmdesátých let však ještě neexistovaly nástroje pro přesné provedení takového odhadu.

Změna přišla až v roce 1983 v článku [4], jehož předběžné verze však byly k dispozici už několik let předtím. Tak jaké je to minimum? Má hodnotu zhruba $\exp(2\sqrt{\log X \log\log X})$ a nastane tehdy, když je Y přibližně rovno $\exp(\frac{1}{2}\sqrt{\log X \log\log X})$. Ale co vůbec jsou „$X$" a „$Y$"?[6]) Číslo X je odhad pro typické pomocné číslo, které algoritmus produkuje. V metodě řetězových zlomků lze za X vzít $2\sqrt{n}$. U Kraitchikova polynomu je X maličko větší: $n^{1/2+\varepsilon}$. A číslo Y je odhad pro p_B, největší číslo v rozkladové bázi.

Rozklad čísla n, ať už Lehmerovou–Powersovou metodou řetězových zlomků nebo Kraitchikovým polynomem, by tedy měl vyžadovat okolo $\exp(\sqrt{2\log n \log\log n})$ kroků. To není matematická věta, nýbrž dohad. Tato domněnka se opírá o již uvedenou heuristickou argumentaci, v níž se předpokládá, že pomocná čísla generovaná řetězovým zlomkem $\sqrt{n}$ nebo Kraitchikovým kvadratickým polynomem jsou „náhodná" vzhledem k vlastnosti Y-hladkosti. To nebylo dokázáno. Navíc ani množství Y-hladkých pomocných čísel nemusí stačit k rozkladu n, protože pokaždé, když užíváme lineární závislost nad $\mathbb{F}_2$, abychom sestavili kongruentní kvadráty, můžeme mít velkou smůlu a ulovit jen nezajímavá řešení, která nám při rozkladu nepomohou. Za opětovného předpokladu náhodnosti ovšem neočekáváme neobvykle dlouhé šňůry smůly, což znovu podporuje naši domněnku.

Jak už bylo zmíněno, takovými úvahami o složitosti se prvně zabýval Richard Schroeppel v nepublikované práci z konce sedmdesátých let. (Předpokládal výsledek, který jsme již uvedli podle [4], ačkoli tehdy to nebyla ani věta a vlastně ani domněnka.)

---

[5]) *Poznámka překladatelů:* Symbolem $[X]$ je označena celá část reálného čísla X.

[6]) Věru, to je otázka, která vyvádí z míry mnoho studentů elementární algebry, nemluvě o filozofech matematiky.

Vyzbrojen nástroji pro studium složitosti přišel tehdy s novým postupem, který se stal známým jako *lineární síto*. Byl to předchůdce a též inspirátor kvadratického síta.

Teorie složitosti vede k lepšímu algoritmu, kvadratickému sítu

Předchozí nástin složitosti ukazuje místo, kde bychom mohli dosáhnout určitého zlepšení. Jde o čas, který potřebujeme k rozpoznání těch pomocných čísel, která se plně rozkládají na prvočísla do hodnoty $Y = p_B$, tj. k určení Y-hladkých čísel. V úvaze jsme předpokládali, že to vyžaduje asi $\pi(Y)$ kroků, kde $\pi(Y)$ je počet prvočísel menších nebo rovných Y. Pravděpodobnost, že číslo je Y-hladké, je při zavedeném značení rovna $\Psi(X,Y)/[X]$. Jak byste mohli očekávat a jak se to potvrzuje v praxi, jestliže je Y rozumně velké a X je značně velké, tato pravděpodobnost je velmi, velmi malá. Takže pomocná čísla přicházejí jedno za druhým a my musíme každému z nich věnovat celou dobu, jen abychom téměř vždy zjistili, že není Y-hladké a že ho tedy vyřadíme.

Začátkem roku 1981 mne napadlo, že k rychlému rozpoznání hladkých hodnot Kraitchikova kvadratického dvojčlenu $Q(x) = x^2 - n$ by se dalo použít něco podobného Eratosthenovu sítu. Eratosthenovo síto je známý prostředek pro nalezení všech prvočísel v nějakém počátečním intervalu přirozených čísel. Zakroužkujeme první prvočíslo 2, a pak přeškrtneme každé druhé číslo, tedy 4, 6, 8 atd. Další neoznačené číslo je 3. Zakroužkujeme ho a přeškrtneme každé třetí číslo. A tak dále. Poté co dosáhneme odmocniny z horní meze celého síta, můžeme skončit s prosíváním a v intervalu zakroužkovat všechna zbývající neoznačená čísla. Zakroužkovaná čísla jsou prvočísla, vyškrtnutá čísla jsou složená.

Všimněme si, že Eratosthenovo síto umí více než jen najít prvočísla. Některá vyškrtnutá čísla jsou přeškrtnuta několikrát. Například 30 je přeškrtnuto třikrát, stejně jako 42, protože tato čísla mají tři prvočinitele. Můžeme tedy zběžným pohledem najít čísla, která jsou mnohokrát přeškrtnuta, a tak rychle objevit čísla, která mají hodně prvočinitelů. A je jasné, že mít hodně prvočinitelů souvisí s tím, že jsou všechny malé.

Ale můžeme udělat více než jen pozorovat souvislosti. Pokud místo škrtání dělíme příslušným prvočíslem, čísla jako 30 a 42 se do konce prosívání transformují na 1, neboť jsou úplně rozložena na prvočísla, která síto užívá. Řekněme, že místo prosívání vzhledem k prvočíslům až do velikosti odmocniny z horní meze síta prosíváme pouze vzhledem k prvočíslům do hodnoty Y a že čísla místo přeškrtávání dělíme prvočíslem. Každé číslo, které je na konci prosívání rovno 1, je Y-hladké. Ale ne každé Y-hladké číslo uvázne v tomto sítě. Například 60 se po vydělení svými prvočiniteli změní na 2. Problém tkví ve vyšších mocninách prvočísel menších nebo rovných Y. To můžeme napravit tím, že prvočíslem dělíme opakovaně, tj. dělíme i mocninami prvočísla. Pak výsledné jedničky přesně odpovídají Y-hladkým číslům v daném intervalu.

Čas, který se na to spotřebuje, je neuvěřitelně krátký ve srovnání se zjišťováním Y-hladkosti pokusným dělením každého kandidáta. Je-li délka intervalu N, pak počet kroků je jen asi $N \log\log Y$, což je průměrně okolo $\log\log Y$ kroků na kandidáta.

V počátečním intervalu tedy umíme rychle rozeznat Y-hladká čísla. Ale můžeme tuto myšlenku použít i k rozpoznání Y-hladkých hodnot kvadratického dvojčlenu

$Q(x) = x^2 - n$? Síto je založeno na tom, že pro každé číslo m jsou násobky m pravidelně rozloženy v celém vyšetřovaném souboru. Vezměme tedy například prvočíslo p a ptejme se, pro které hodnoty x je $Q(x)$ dělitelné p. To není těžký problém. Jestliže n (rozkládané číslo) je modulo p rovno nenulovému čtverci, pak existují dvě reziduální třídy a a b modulo p takové, že $Q(x) \equiv 0 \bmod p$ právě tehdy, když $x \equiv a \bmod p$ nebo $x \equiv b \bmod p$. Jestliže n není modulo p rovno čtverci, pak $Q(x)$ není dělitelné p a žádné další výpočty s p už nemusíme dělat.

Tudíž jde v podstatě o stejnou myšlenku, a Y-hladké hodnoty $Q(x)$ tedy můžeme najít za cenu přibližně $\log\log Y$ kroků vynaložených na jednoho kandidáta.

Co nám přinesla úvaha o složitosti? Náročnost rozkladu čísla n je nyní $\exp(\sqrt{\log n \log\log n})$, z exponentu zmizel činitel $\sqrt{2}$. Je to velký úspěch? Nepochybně ano. Nižší složitost a další příjemné vlastnosti této metody umožnily dvojnásobné zvětšení délky čísel, která mohou být rozložena (ve srovnání s dříve vyloženou metodou řetězových zlomků). A tak se z úvah o složitosti a bez numerických experimentů zrodila metoda kvadratického síta.

Implementace a vylepšení

Měl jsem velké štěstí, že se ukázalo, že kvadratické síto je algoritmus schopný soutěže. Častěji se totiž stává, že když někdo vymýšlí algoritmy pouze na základě složitostních úvah a myšlenkových experimentů, výsledek je příliš neohrabaný na to, aby mohl konkurovat ostatním metodám. Navíc i když je základní myšlenka zdravá, stále ještě mohou existovat významná zlepšení vyčkávající, až je objeví lidé, kteří algoritmus testují. To se přihodilo i kvadratickému sítu.

Prvním člověkem, který vyzkoušel metodu kvadratického síta na velkém čísle, byl Joseph Gerver (viz [9]). Chopil se této úlohy jako příležitosti naučit se programovat a úspěšně rozložil 47ciferné číslo převzaté z Cunninghamova projektu. Tento projekt, který začátkem dvacátého století zahájili podplukovník Allan J. Cunningham a H. J. Woodall, spočívá ve faktorizaci čísel $b^n \pm 1$ pro b menší nebo rovné 12 (které není mocninou) a n jdoucí k velkým hodnotám (viz [3]). Gerverovo číslo bylo jedním z dělitelů čísla $3^{225} - 1$.

Ve skutečnosti však bylo těžké někoho přesvědčit, aby kvadratické síto vyzkoušel. Mnozí z pracovníků na Cunninghamově projektu se zdáli být spokojeni s metodou řetězových zlomků a mysleli si, že větší hodnoty Kraitchikova polynomu $Q(x)$ ve srovnání s čísly Q_i z metody řetězových zlomků znamenají příliš velké znevýhodnění pro nezralou metodu kvadratického síta. Ale na konferenci ve Winnipegu na podzim roku 1982 jsem přesvědčil Guse Simmonse a Tonyho Warnocka ze Sandia Laboratories, aby síto vyzkoušeli na počítači Cray.

Úkol naprogramovat kvadratické síto byl v Sandia Laboratories přidělen Jimovi Davisovi a Dianě Holdridgeové. Ti jej nejen úspěšně zvládli, nýbrž rychle začali lámat rekordy. Davis našel důležité zlepšení, které zmírnilo zmíněnou nevýhodu. Objevil způsob, jak přejít k jiným kvadratickým polynomům poté, co hodnoty toho prvního, $Q(x) = x^2 - n$, nepříjemně vzrostly. Ačkoli tato myšlenka odhad složitosti podstatně

nezměnila, její zásluhou se metoda stala daleko praktičtější. Úspěch těchto pracovníků se nejen objevil na obálce časopisu Mathematical Intelligencer (obálka třetího čísla šestého ročníku z roku 1984 ukazuje počítač Cray a rozklad čísla se 71 cifrou), ale dokonce i časopis Time mu věnoval krátký článek doplněný Simmonsovou fotografií.

Je ironií, že krátce předtím, než se tato skupina pustila do práce, jiný tým v Sandia Laboratories navrhl a vyrobil integrovaný obvod RSA pro šifrování pomocí veřejného klíče, jehož bezpečnost byla založena na naší neschopnosti rozkládat čísla se stovkou cifer. To už teď nebylo dost bezpečné a obvod musel být sešrotován.

Zhruba v té době a nezávisle na Davisovi přišel Peter Montgomery s jiným, trochu lepším způsobem změny polynomů, a my jsme začali používat spíše jeho než Davisovu metodu.

Jedna velká výhoda kvadratického síta proti metodě řetězových zlomků spočívá v tom, že u kvadratického síta je obzvlášť jednoduché rozdělit úlohu rozkladu mezi mnoho počítačů. Například při použití více polynomů může každý počítač dostat svou vlastní množinu kvadratických polynomů k prosívání. Největších úspěchů s kvadratickým sítem zpočátku dosahovaly superpočítače jako Cray MPX v Sandia Laboratories. Avšak s rozšířením levných pracovních stanic a osobních počítačů a díky přirozenému způsobu, jakým může být metoda kvadratického síta rozdělena na menší úlohy, přešly rekordy na ty, kdo organizovali skupinové útoky na cílová čísla.

Robert Silverman byl první, kdo rozložil číslo pomocí mnoha počítačů. Red Alford a já jsme později použili více než sto velmi primitivních, do sítě nezapojených osobních počítačů, abychom rozložili pár stociferných čísel (viz [2]). Ale nevytvořili jsme žádný rekord, protože zatímco jsme se postupně vyzbrojovali technikou, Arjen Lenstra a Mark Manasse [12] udělali rozhodující krok v rozdělení úlohy. Kvadratické síto nabídli v Internetu a žádali lidi z celého světa o počítačový čas. Tímto společným úsilím se v roce 1994 konečně podařilo rozložit 129ciferné číslo ze souboru RSA. Tento projekt vedený Derekem Atkinsem, Michaelem Graffem, Paulem Leylandem a Lenstrou trval osm měsíců reálného času a vyžadoval přes 10^{17} elementárních kroků.

Kvadratické síto je velmi jednoduchý algoritmus, což je jedna z jeho silných stránek. Vzhledem k jeho jednoduchosti by se mohlo zdát, že by bylo možné navrhnout speciální počítač určený výhradně k rozkladu velkých čísel. Jeff Smith a Sam Wagstaff z University of Georgia sestavili speciální procesor pro metodu řetězových zlomků. Byl přezdíván „georgijský louskáček" a dosáhl jistých úspěchů, ale zastínilo ho kvadratické síto na konvenčních počítačích. Smith, Randy a já (viz [21]) jsme si mysleli, že bychom mohli zkonstruovat speciální procesor pro kvadratické síto. „Quasimodo" (Quadratic Sieve Motor) byl sestaven, ale nikdy správně nefungoval. Vzhledem k exponenciálnímu šíření levných a vysoce kvalitních počítačů ztratil později takový přístup praktický smysl.

Počátky prosívání pomocí číselného tělesa

V roce 1988 rozeslal John Pollard několika lidem dopis, v němž nastínil myšlenku svého postupu při rozkládání jistých velkých čísel pomocí algebraického číselného

tělesa. Inspiroval se přitom diskrétním logaritmickým algoritmem Dona Coppersmitha, Andrewa Odlyzka a Richarda Schroeppela [6]. Jeho původní myšlenka se netýkala všech velkých složených čísel, ale jen určitých „hezky" složených čísel, která kromě toho, že jsou blízká mocninám, oplývají i dalšími přednostmi. Pollard ilustroval svou myšlenku na rozkladu čísla $2^{2^7}+1$, což je sedmé Fermatovo číslo. Je zajímavé, že téměř o dvacet let dříve bylo toto číslo prvním velkým úspěchem faktorizační metody řetězových zlomků.

Musím přiznat, že jsem nejprve nebyl příliš nadšen Pollardovou metodou, protože se mi jevila použitelná jen pro málo čísel. Někteří lidé ji však vzali vážně. Jedním z nich byl i Hendrik Lenstra. Vylepšil některé detaily algoritmu a se svým bratrem Arjenem a s Markem Manassem použili tuto metodu k rozkladu několika velkých čísel z Cunninghamova projektu. Po několika úspěších (z nichž nejpozoruhodnější byl rozklad 138ciferného čísla) a poté, co Brian LaMacchia a Andrew Odlyzko učinili několik postřehů, když se zabývali velkými řídkými maticemi, které v metodě vystupují, zaměřili bratři Lenstrové a Manasse svůj pohled na skutečně náročný cíl: $2^{2^9}+1$, deváté Fermatovo číslo.[7]) Jeho rozklad byl zjevně nad síly kvadratického síta. Vlastní metoda eliptických křivek Hendrika Lenstry, kterou objevil začátkem roku 1985 a která je dobrá zejména pro rozklad čísel, jež mají relativně malý prvočinitel (řekněme jen kolem 30 cifer), zatím neumožňovala deváté Fermatovo číslo rozložit. Na jaře roku 1990 se bratřím Lenstrům a Manassovi podařilo získat prvočíselný rozklad čísla $2^{2^9}+1$. Tento senzační výkon oznamoval světu, že Pollardovo síto číselného tělesa uspělo.

Ale co obecná čísla? V létě 1989 jsem měl přednášet na shromáždění Canadian Number Theory Association ve Vancouveru. Měla to být přehledná přednáška o rozkládání čísel. Uvědomil jsem si, že by bylo dobré se zde zmínit o nové Pollardově metodě. Po cestě na shromáždění jsem v letadle provedl analýzu složitosti této metody, pokud by měla pracovat pro obecná čísla. Předpokládal jsem, že nenastane nesčíslné množství technických potíží a že metodu lze použít na obecná čísla. Byl jsem ohromen. Výpočetní složitost pro tento algoritmus, který vlastně zatím neexistoval, měla tvar $\exp(c(\log n)^{1/3}(\log\log n)^{2/3})$. Zásadní rozdíl ve srovnání se složitostí kvadratického síta byl ten, že nejdůležitější veličina v exponentu, mocnina $\log n$, měla exponent zmenšený z $1/2$ na $1/3$. Pokud zmenšení *konstanty* v exponentu mělo takový hluboký vliv při přechodu z metody řetězových zlomků ke kvadratickému sítu, pomysleme si, jaký důsledek může mít zmenšení *exponentu* v exponentu. Proto si tato metoda zasluhovala seriózní prozkoumání.

Nepřeji si vzbudit dojem, že jsem touto analýzou složitosti našel jednoduchou cestu, jak aplikovat síto číselného tělesa na obecné složené číslo. Od toho jsem byl daleko. Pouze jsem měl neurčité tušení povzbudivých možností do budoucna. O to, že tyto možnosti byly vůbec realizovány, se zasloužili především Joe Buhler a Hendrik Lenstra i další badatelé. O několik měsíců dříve Lenstra navíc udělal analýzu

[7]) Toto číslo bylo navrženo v původní Pollardově zprávě jakožto cíl, který stojí za námahu. Bylo známo, že je složené — ve skutečnosti byl znám jeden jeho sedmiciferný prvočinitel — ale zbývající činitel o 148 cifrách byl ještě složený a jeho činitele nebyly známy.

složitosti pro Pollardovu metodu použitou na speciální čísla a rovněž přišel k výrazu $\exp(c(\log n)^{1/3}(\log\log n)^{2/3})$. Moje vlastní analýza byla založena na některých optimistických algebraických předpokladech a na tvrzeních, která mohla platit pro obecná čísla díky jistým průměrovacím argumentům.

Startovním bodem Pollardovy metody pro rozklad n je začít s nerozložitelným monickým polynomem[8]) $f(x)$ definovaným nad celými čísly a s celým číslem m takovým, že $f(m) \equiv 0 \bmod n$. Polynom by měl mít „přiměřený" stupeň d v tom smyslu, že pokud má n mezi 100 a 200 ciframi, pak by d mělo být 5 nebo 6. Pro takové číslo, jako je deváté Fermatovo číslo $n = 2^{2^9} + 1$, je snadné objevit vhodný polynom. Poznamenejme, že $8n = 2^{515} + 8$. Nechť tedy $f(x) = x^5 + 8$ a nechť $m = 2^{103}$.

Jaký užitek může dát takový polynom? Nechť α je komplexní kořen $f(x)$ a uvažujme okruh $\mathbb{Z}[\alpha]$ sestávající ze všech polynomiálních výrazů v α s celočíselnými koeficienty. Protože $f(\alpha) = 0$ a $f(m) \equiv 0 \bmod n$, substitucí rezidua $m \bmod n$ místo každého α dostaneme přirozené zobrazení φ ze $\mathbb{Z}[\alpha]$ do $\mathbb{Z}/(n\mathbb{Z})$.[9]) Naše podmínky kladené na f, α a m zaručují, že φ je dobře definováno. A nejen to, φ je okruhový homomorfismus.

Předpokládejme nyní, že S je konečná množina dvojic $\langle a, b\rangle$ nesoudělných celých čísel se dvěma vlastnostmi. První vlastností je, že součin algebraických celých čísel $a - \alpha b$ přes všechny páry $\langle a, b\rangle$ z S je čtvercem v $\mathbb{Z}[\alpha]$, řekněme γ^2. Druhou vlastností S je to, že součin všech čísel $a - mb$ přes páry $\langle a, b\rangle$ z S je čtvercem v $\mathbb{Z}$, řekněme ν^2. Protože γ lze napsat jako polynomiální výraz v α, můžeme každý výskyt α zaměnit celým číslem m, čímž dospějeme k celému číslu u, pro něž $\varphi(\gamma) \equiv u \bmod n$. Pak

$$u^2 \equiv \varphi(\gamma)^2 = \varphi(\gamma^2) = \varphi\Big(\prod_{\langle a,b\rangle\in S}(a - \alpha b)\Big) = \prod_{\langle a,b\rangle\in S}\varphi(a - \alpha b) \equiv$$
$$\equiv \prod_{\langle a,b\rangle\in S}(a - mb) = \nu^2 \bmod n$$

a my už víme, co udělat s u a ν. Stejně jako Kraitchik před sedmdesáti lety budeme doufat, že dostaneme zajímavou kongruenci $u \not\equiv \pm\nu \bmod n$. A pokud tomu tak bude, vezmeme největší společný dělitel $(u - \nu, n)$, abychom dostali netriviální činitel z rozkladu čísla n.

Odkud se vezme množina S párů $\langle a, b\rangle$? Protože alespoň pro druhou vlastnost S se předpokládá, že součin čísel $a - mb$ je čtvercem, je zřejmé, že bychom mohli opět použít vektory exponentů a síto. Zde jsou dvě proměnné a a b místo jediné proměnné v $Q(x)$ u kvadratického síta. Pohlížíme na to jako na parametrizovaný systém lineárních polynomů. Můžeme pevně zvolit b a nechat a probíhat celý interval, pak uvažovat další hodnotu b a vše opakovat.

Ale S musí mít ještě druhou vlastnost: pro tytéž páry $\langle a, b\rangle$ je součin čísel tvaru $a - \alpha b$ čtvercem v $\mathbb{Z}[\alpha]$. Pollarda však napadlo, že kdybychom byli v té příznivé situaci, kdy $\mathbb{Z}[\alpha]$ je úplný okruh všech algebraických celých čísel v $\mathbb{Q}(\alpha)$, navíc je to okruh

[8]) *Poznámka překladatelů:* Polynom se nazývá monický, když koeficient u jeho nejvyšší mocniny je roven 1.

[9]) *Poznámka překladatelů:* Symbol $\mathbb{Z}/(n\mathbb{Z})$ označuje okruh celých čísel modulo n, tj. faktorový okruh okruhu $\mathbb{Z}$ podle ideálu $n\mathbb{Z}$ celočíselných násobků čísla n.

s jednoznačnými rozklady a známe bázi pro jednotky, pak bychom rovněž mohli snadno vytvářet vektory exponentů pro algebraická celá čísla $a - \alpha b$ a v podstatě opakovat celý algoritmus. Abychom zařídili, že obě vlastnosti S platí současně, stačilo by pouze uvažovat delší vektory exponentů, které mají souřadnice pro všechna malá prvočísla, pro znaménko čísla $a - \alpha b$, pro všechna „malá" prvočísla v $\mathbb{Z}[\alpha]$ a také pro každou jednotku z jednotkové báze.

Ale jak to uděláme pro obecné n? Jak ve skutečnosti dosáhneme prvního kroku, který spočívá v nalezení polynomu $f(x)$ a celého čísla m s vlastností $f(m) \equiv 0 \bmod n$? A pokud bychom je uměli nalézt, proč bychom měli očekávat, že $\mathbb{Z}[\alpha]$ má všechny pěkné vlastnosti pro to, aby Pollardův postup fungoval?

Síto číselného tělesa se vyvíjí

Naštěstí existuje velmi jednoduchý prostředek, jak začít, neboli jak najít $f(x)$ a m. Trik spočívá v tom, že se $f(x)$ hledá až *nakonec*. Nejprve se musíme rozhodnout, jaký stupeň d polynomu f zvolíme. Pak označíme m celou část čísla $n^{1/d}$. Nyní napíšeme n v soustavě o základu m tak, že $n = m^d + c_{d-1}m^{d-1} + \ldots + c_0$, kde čísla c_i splňují nerovnosti $0 \leqq c_i < m$. (Jestliže $n > (2d)^d$, pak počáteční „cifra" c_d je 1.) A už před námi stojí polynom $f(x) = x^d + c_{d-1}x^{d-1} + \ldots + c_0$. Máme tedy monický polynom $f(x)$. Je ale nerozložitelný (tj. ireducibilní)?

Existuje mnoho strategií pro rozklad primitivních polynomů definovaných v $\mathbb{Z}$ na nerozložitelné činitele. Známe například proslulý algoritmus s polynomiálním časem od Arjena Lenstry, Hendrika Lenstry a Lászla Lovásze pro rozklad primitivních polynomů nad $\mathbb{Z}$ (výpočetní čas je ohraničený pevnou mocninou součtu stupně a počtu cifer v koeficientech). Předpokládejme tedy, že nemáme štěstí a že předchozí postup vede na rozložitelný (tj. reducibilní) polynom $f(x)$, řekněme $f(x) = g(x)h(x)$. Pak $n = f(m) = g(m)h(m)$ a podle výsledku Johna Brillharta, Michaela Filaseta a Andrewa Odlyzka je tento rozklad n netriviální. Ale náš cíl je nalézt netriviální rozklad n, takže tahle situace vůbec není nešťastná! Jelikož téměř všechny polynomy jsou nerozložitelné, je více než pravděpodobné, že konstrukce nám umožní začít se sítem číselného tělesa a nebudeme muset okamžitě rozkládat n.

Zbýval ještě jeden hlavní problém. A to, jak překonat ten fakt, že není důvod očekávat, že by okruh $\mathbb{Z}[\alpha]$ vůbec měl nějakou pěknou vlastnost. V roce 1990 vyřešili Joe Buhler, Hendrik Lenstra a já zbývající obtíže a publikovali jsme v [11] popis *obecného síta číselného tělesa*, do nějž jsme vtělili velmi praktický nápad Lena Adlemana [1], který zjednodušil některé naše konstrukce.[10])

Zde je krátké shrnutí toho, co jsme udělali. Norma $N(a - \alpha b)$ čísla $a - \alpha b$ (nad $\mathbb{Q}$) se snadno předělá na $b^d f(a/b)$. To je homogenizovaný tvar f. Řekneme, že $a - \alpha b$ je Y-hladké, jestliže $N(a - \alpha b)$ je Y-hladké. Z toho, že norma je multiplikativní, vyplývá,

[10]) Ačkoli Adlemanův nápad nezměnil naše teoretické odhady složitosti pro výpočetní čas, jeho zjednodušení odstranila zbývající překážky tak, že metoda byla prakticky schopná konkurovat kvadratickému sítu. Je zajímavé, že sám Adleman (jakož i většina ostatních) považoval kolem roku 1990 obecné síto číselného tělesa za čistě spekulativní metodu.

že pokud součin různých algebraických celých čísel $a - \alpha b$ je čtvercem algebraického celého čísla, pak také odpovídající součin norem je čtvercem celého čísla. Poznamenejme též, že víme, jak nalézt množinu dvojic $\langle a, b\rangle$, pro něž součiny čísel $N(a - \alpha b)$ dávají čtverec. To lze udělat pomocí síta pro nalezení Y-hladkých hodnot normy $N(a - \alpha b)$, a ty pak zkombinovat pomocí algebry vektorů exponentů nad $\mathbb{F}_2$.

Máme tedy jen součin čísel $N(a - \alpha b)$ rovný čtverci, kdežto nutná podmínka pro to, aby součin čísel $a - \alpha b$ byl čtvercem, je velice vzdálená postačující podmínce. Hlavním důvodem je to, že norma zobrazuje rozmanité prvoideály na týž prvek v $\mathbb{Z}$, a tak norma může být snadno čtvercem, aniž by byl vzor (tj. argument) čtvercem. Například dva prvočinitele $2 + \mathrm{i}$ a $2 - \mathrm{i}$ prvního stupně v $\mathbb{Z}$ mají normu 5. Jejich součin je 5, což dává normu $25 = 5^2$, ale $(2 + \mathrm{i})(2 - \mathrm{i}) = 5$ neobsahuje čtverec. (Poznamenejme, že pokud pracujeme v okruhu všech algebraických celých čísel v $\mathbb{Q}(\alpha)$, pak všechny prvoideální činitele $a - \alpha b$ jsou pro nesoudělná celá čísla a a b stupně jedna; jejich normy jsou totiž prvočísla.) Pro každé prvočíslo p nechť R_p je množina řešení kongruence $f(x) \equiv 0 \bmod p$. Když narazíme na dvojici $\langle a, b\rangle$ s p, které dělí $N(a - \alpha b)$, pak některý prvoideál nad p dělí $a - \alpha b$. A můžeme říci který, protože a/b bude kongruentní modulo p s jedním prvkem množiny R_p, což bude sloužit k rozlišování různých prvoideálů nad p. Tak můžeme zařídit, aby naše exponenciální vektory měly $\#R_p$ souřadnic[11]) pro každé prvočíslo p, a tak se držet cesty rozkladu $a - \alpha b$ na prvoideály. Poznamenejme, že $\#R_p \leqq d$, což je stupeň $f(x)$.

Dostali jsme se tedy přes zásadní překážku, ale stále ještě existuje mnoho potíží. Předpokládá se, že pracujeme v okruhu $\mathbb{Z}[\alpha]$, což nemusí být okruh všech algebraických celých čísel. Ve skutečnosti tento okruh nemusí být dedekindovský okruh, takže ani nemusíme mít rozklad na prvoideály. I kdybychom měli rozklad na prvoideály, předchozí odstavec nás pouze ujišťuje, že hlavní ideál generovaný součinem algebraických celých čísel $a - \alpha b$ je čtvercem nějakého ideálu, ne však nutně čtvercem hlavního ideálu. A i kdyby byl čtvercem hlavního ideálu, kvůli jednotkám to nemusí být čtverec algebraického celého čísla. (Například ideál generovaný číslem -9 je čtvercem ideálu v $\mathbb{Z}$, ale -9 není čtvercem.) I kdyby součin čísel $a - \alpha b$ byl čtvercem algebraického celého čísla, jak můžeme vědět, že je to čtverec prvku ze $\mathbb{Z}[\alpha]$?

Poslední potíž se dá celkem snadno zvládnout, užijeme-li $f'(\alpha)^2$ jako násobitel,[12]) ale ostatní těžkosti se zdají obtížné. Len Adleman [1] však přišel s jednoduchou a geniální myšlenkou, jak jedním rázem překonat všechny těžkosti. Jde o to, že i když jsme postaveni před některé nehezké překážky, tvoří (modulo čtverce) $\mathbb{F}_2$-vektorový prostor dosti malé dimenze. Takže první nápad by mohl být ignorování problému. Ale ta dimenze zas není *tak* malá. Adleman navrhoval náhodně vybírat určité kvadratické charaktery a využívat jejich hodnoty v číslech $a - \alpha b$, aby se zvětšily vektory exponentů. (Jisté kvadratické charaktery byly náhodně, ale pevně zvoleny na počátku.) Takže upravujeme součin čísel $a - \alpha b$ tak, aby byl nejenom čtvercem až na „prostor překážek", ale aby s velkou pravděpodobností byl skutečným čtvercem.

[11]) *Poznámka překladatelů:* Symbol # označuje počet prvků množiny.

[12]) Platí věta, že pro monický nerozložitelný polynom nad $\mathbb{Z}$ s komplexním kořenem α a pro γ z okruhu algebraických celých čísel z $\mathbb{Q}(\alpha)$ je $f'(\alpha)\gamma$ v $\mathbb{Z}[\alpha]$. Je-li tedy γ^2 čtvercem v okruhu algebraických celých čísel z $\mathbb{Q}(\alpha)$, pak $f'(\alpha)^2\gamma^2$ je čtvercem v $\mathbb{Z}[\alpha]$.

Vezměme například předchozí problém s -9, což není čtverec. Ani když nejsme schopni nějak „vidět" problém znaménka čísla, které se nám ale jistě jeví jako čtverec, protože víme, že pro každé prvočíslo p je exponent u p v prvočíselném rozkladu -9 sudý, můžeme ještě problém odhalit. Zde uvádíme jak: Uvažujme kvadratický charakter a jeho hodnotu v -9, například Lagrangeův symbol $(-9/p)$, který je roven 1, je-li -9 čtvercem modulo p, a je roven -1, není-li -9 čtvercem modulo p. Vyzkoušejme to, řekněme, pro $p = 7$. Je snadné vypočítat tento symbol a zjistit, že je roven -1. Tedy -9 není čtvercem modulo 7, a tak nemůže být čtvercem v $\mathbb{Z}$. I když -9 je čtvercem modulo nějaké prvočíslo p, nezaručuje to, že je čtvercem v $\mathbb{Z}$. Kdybychom například zkoušeli 5 místo 7, pak by -9 stále vypadalo jako čtverec. Adlemanova myšlenka spočívá ve vyčíslení hladkých hodnot čísel $a - \alpha b$ pro zvolené kvadratické charaktery a v použití prostředků lineární algebry pro vytvoření prvku se *dvěma* vlastnostmi: jeho (nezvětšený) vektor exponentů má všechny složky sudé a jeho hodnota je pro každý charakter rovna 1. Toto algebraické celé číslo je s vysokou pravděpodobností (v heuristickém smyslu) čtvercem. Pokud to není čtverec, můžeme pokračovat tak, že použijeme lineární algebru nad $\mathbb{F}_2$ pro vytvoření dalšího kandidáta.

Kromě toho existují ještě další obtíže. Jednou z nich je „problém odmocniny". Jestliže máte prvočíselný rozklad různých celých čísel, jejichž součin je čtverec, můžete snadno nalézt odmocninu tohoto čtverce pomocí prvočíselného rozkladu. Avšak v $\mathbb{Z}[\alpha]$ se to nezdá tak samozřejmé. Nicméně existují nástroje i pro řešení tohoto problému, který však stále zůstává výpočetně zajímavým krokem algoritmu. Zvědavého čtenáře odkazujeme na [15].

Možná není jasné, proč je síto číselného tělesa dobrý algoritmus na rozkládání čísel. Klíčovou veličinou ve faktorizační metodě, jakou je kvadratické síto nebo síto číselného tělesa, je to, co jsem dříve nazýval X. Je to odhad velikosti pomocných čísel, jejichž kombinací hodláme dostat čtverec. Znalost X nám dává složitost — okolo $\exp(\sqrt{2 \log X \log\log X})$. V kvadratickém sítu je X přibližně rovno $n^{1/2+\varepsilon}$. Ale v sítu číselného tělesa můžeme vybrat polynom $f(x)$ a celé číslo m takovým způsobem, že součin $(a - mb)N(a - \alpha b)$ (činitelů, které chceme najít hladké) je ohraničený hodnotou X tvaru $\exp(c'(\log n)^{2/3}(\log\log n)^{1/3})$. Takto je počet cifer pomocných čísel, která prosíváme přes všechny hladké hodnoty, přibližně rovný počtu cifer čísla n *umocněnému* na $\frac{2}{3}$, kdežto u kvadratického síta mají pomocná čísla více než polovinu počtu cifer čísla n. Proto je při srovnávání síto číselného tělesa tak asymptoticky rychlé.

Už dříve jsem se zmínil, že heuristicky vzatý výpočetní čas síta číselného tělesa pro rozklad čísla n má tvar $\exp(c(\log n)^{1/3}(\log\log n)^{2/3})$, ale neuvedl jsem, co je c. Existují vlastně tři hodnoty c, které závisí na tom, kterou verzi síta číselného tělesa použijeme. „Speciální" síto číselného tělesa, jež je bližší Pollardově původní metodě a dobře přizpůsobené k rozkladu čísel jako $2^{2^9} + 1$, která jsou blízko vysokých mocnin, má $c = \left(\frac{32}{9}\right)^{1/3} \approx 1{,}526$. „Obecné" síto číselného tělesa je metoda, kterou jsem nastínil v tomto článku a která je použitelná na jakékoliv liché složené číslo, jež není mocninou. Ta má $c = \left(\frac{64}{9}\right)^{1/3} \approx 1{,}923$. Konečně Don Coppersmith [5] navrhl verzi obecného síta číselného tělesa, v níž se používá mnoho polynomů. Hodnota c pro tuto metodu je $\frac{1}{3}(92 + 26\sqrt{13})^{1/3} \approx 1{,}902$. Asymptoticky stojí jako šampión mezi metodami rozkladu pro nejhorší případy. Původně se zdálo, že Coppersmithův nápad je zcela neprak-

tický, ale v [8] se zvažuje, zda myšlenka použít několik polynomů může mít nějakou praktickou cenu.

Současná situace v rozkládání

V dubnu 1996 dokončil velký tým (viz [7]) rozklad dosud nepokořeného 130ciferného čísla ze souboru RSA. Použil obecný postup prosívání pomocí číselného tělesa, a tak byla hozena rukavice kvadratickému sítu, které se za rozklad největšího „obtížného" čísla těšilo věhlasu šampióna od roku 1983. Ačkoli byl skutečný čas zhruba stejný jako při rozkladu 129ciferného nesnadno rozložitelného čísla pomocí kvadratického síta o dva roky dříve, bylo odhadnuto, že nový rozklad si vyžádal jen okolo 15 % výpočetního času. Tento rozpor vznikl tím, že v projektu bylo použito méně počítačů a nastala i nějaká „doba nečinnosti", během níž se psal program pro finální stadium algoritmu.

TABULKA. **Prvních dvacet Fermatových čísel**

m	známý rozklad $F_m = 2^{2^m} + 1$
0	3
1	5
2	17
3	257
4	65537
5	$641 \cdot P_7$
6	$274177 \cdot P_{14}$
7	$59649589127497217 \cdot P_{22}$
8	$1238926361552897 \cdot P_{62}$
9	$2424833 \cdot 7455602825647884208337395736200454918783366342657 \cdot P_{99}$
10	$45592577 \cdot 6487031809 \cdot 4659775785220018543264560743076778192897 \cdot P_{252}$
11	$319489 \cdot 974849 \cdot 167988556341760475137 \cdot 3560841906445833920513 \cdot P_{564}$
12	$114689 \cdot 26017793 \cdot 63766529 \cdot 190274191361 \cdot 1256132134125569 \cdot C_{1187}$
13	$2710954639361 \cdot 2663848877152141313 \cdot 3603109844542291969 \cdot$ $\cdot 319546020820551643220672513 \cdot C_{2391}$
14	C_{4933}
15	$1214251009 \cdot 2327042503868417 \cdot C_{9840}$
16	$825753601 \cdot C_{19720}$
17	$31065037602817 \cdot C_{39444}$
18	$13631489 \cdot C_{78906}$
19	$70525124609 \cdot 646730219521 \cdot C_{157804}$

Symbol P_k v tabulce označuje prvočíslo o k dekadických cifrách, zatímco C_k označuje složené číslo o k dekadických cifrách, pro něž neznáme žádný netriviální rozklad.[13])

[13]) *Poznámka překladatelů:* Konkrétní tvar čísel P_k a C_k lze snadno dopočítat ze znalosti F_m a ostatních činitelů.

Historie rozkladu Fermatových čísel je jakýsi mikrokosmos historie faktorizace. Sám Fermat věděl, že F_0 až F_4 jsou prvočísla, a domníval se, že i všechna ostatní čísla v posloupnosti $2^{2^m}+1$ jsou prvočíselná. Euler však rozložil F_5. Není obtížné nalézt tento rozklad, pokud použijeme zesílené Fermatovo tvrzení,[14]) podle něhož každý prvočinitel p čísla F_m je tvaru $p \equiv 1 \bmod 2^{m+2}$, kde m je alespoň 2. Tedy všechny prvočinitele F_5 jsou tvaru $1 \bmod 128$ a první takové prvočíslo, které není menším Fermatovým číslem, je 641. Tato myšlenka byla použita k rozkladu F_6 (Landry, 1880) a k získání „malých" prvočinitelů více než 80 dalších Fermatových čísel, která nejsou obsažena v této tabulce.

Prvním úspěchem Brillhartovy–Morrisonovy faktorizační metody řetězových zlomků bylo Fermatovo číslo F_7. Brent a Pollard přizpůsobili[15]) Pollardovu metodu ϱ k rozkladu F_8. Jak jsme již připomněli v tomto článku, F_9 bylo rozloženo pomocí síta číselného tělesa. Fermatova čísla F_{10} a F_{11} rozložil Brent pomocí Lenstrovy metody eliptických křivek.

Víme, že čísla F_{14}, F_{20} a F_{22} jsou složená, ale zatím neznáme žádné prvočinitele těchto čísel. To, že jsou složená, bylo objeveno pomocí *Pepinova kritéria*: F_m je prvočíslo právě tehdy, když $3^{(F_m-1)/2} \equiv -1 \bmod F_m$. Nejmenší Fermatovo číslo, o němž nevíme, zda je prvočíslo či složené číslo, je F_{24}. Mnoho číselných teoretiků se domnívá, že každé Fermatovo číslo za F_4 je složené.

Fermatova čísla souvisejí se starým Euklidovým problémem: pro která n je možno zkonstruovat pravidelný n-úhelník pomocí pravítka a kružítka? Gauss dokázal, že pravidelný mnohoúhelník je konstruovatelný právě tehdy, když $n \geqq 3$ a největší lichý činitel obsažený v n je součinem vzájemně různých Fermatových prvočísel. Tato věta, kterou Gauss objevil ve svých 19 letech, jej provázela až do hrobu: na jeho pomníku je vyryt pravidelný sedmnáctiúhelník.[16])

Kde tedy leží hranice mezi efektivním použitím kvadratického síta a síta číselného tělesa? Odpověď na tuto otázku poněkud závisí na tom, s kým mluvíte. Jedna věc, se kterou každý souhlasí, je, že pro menší čísla — řekněme o méně než 100 cifrách — je lepší kvadratické síto a pro větší čísla — řekněme o více než 130 cifrách — je lepší síto číselného tělesa. Jeden z důvodů, proč na takovou otázku není snadná odpověď, je ten, že výsledek je vysoce závislý na jemnostech programování a na druhu použitých počítačů. Například jak bylo oznámeno v [7], výkon síta číselného tělesa je citlivý na velikost paměti počítače. Kvadratické síto je na to rovněž citlivé, ale ne v tak značné míře.

Je toho mnoho, co v tomto krátkém přehledu *nebylo* řečeno. Důležitým opomenutím je diskuse o algoritmu a složitosti části týkající se prostředků lineární algebry pro

[14]) *Poznámka překladatelů:* Tento výsledek dokázal až É. A. Lucas v roce 1878. Fermat pravděpodobně pouze věděl, že $p \equiv 1 \bmod 2^{m+1}$.

[15]) *Poznámka překladatelů:* Viz R. P. Brent, J. M. Pollard: *Factorization of the eight Fermat number.* Math. Comp. *36* (1981), 627–630.

[16]) *Poznámka překladatelů:* G. Greaves, který recenzoval tento článek pro Mathematical Reviews 97f:11100, tomu též věřil, dokud nenavštívil Gaussův pomník v Göttingen (viz také MR 93g:00006).

kvadratické síto a síto číselného tělesa. Na počátku jsme aplikovali Gaussovu eliminaci, tak jak ji Brillhart a Morrison použili pro metodu řetězových zlomků. Ale rozměr problému se zvětšoval. Pro rekordní rozklady nyní platí, že rozkladová báze velikosti zhruba milionu je standardem. Problém lineární algebry charakterizovaný maticemi typu milion krát milion zřejmě není maličkostí. O tom existuje zajímavá nová práce, jež obsahuje přizpůsobení iteračních metod pro řídké matice nad reálnými čísly na řídké matice nad $\mathbb{F}_2$ (viz [14]).

Různé variace základní myšlenky síta číselného tělesa ukazují jakýsi příslib. Můžeme zaměnit lineární výraz $a - mb$ použitý v sítu číselného tělesa za $b^k g(a/b)$, kde $g(x)$ je nad $\mathbb{Z}$ nerozložitelný polynom stupně k takový, že $g(m) \equiv 0 \bmod n$. To znamená, že používáme dva polynomy $f(x)$ a $g(x)$ se společným kořenem $m \bmod n$ (původní scénář nám radil brát $g(x) = x - m$). Předmětem soudobého výzkumu je přijít s dobrými strategiemi pro výběr polynomů. Jiná varianta běžného síta číselného tělesa spočívá v záměně polynomu $f(x)$ systémem polynomů podél přímek navrhovaných Coppersmithem. Popis síta číselného tělesa zahrnujícího obě tyto myšlenky je uveden v [8].

Diskrétní logaritmický problém (pro danou cyklickou grupu s generátorem g a prvek h grupy nalezněte celé číslo x tak, aby $g^x = h$) budí také velký zájem v kryptografii. Jak již bylo řečeno, Pollardova originální myšlenka prosívání pomocí číselného tělesa se zrodila mimo diskrétní logaritmický algoritmus. Prošli jsme celý kruh od doby, kdy Dan Gordon, Oliver Schirokauer a Len Adleman předložili obměny síta číselného tělesa, které můžeme použít k výpočtu diskrétních logaritmů v multiplikativní grupě konečných těles (viz nedávný přehled [22]).

Nic jsem neřekl o předmětu testování prvočísel. Je obecně mnohem jednodušší rozpoznat, že číslo je složené, než je rozložit. Když se rozhodneme na nějaké číslo použít komplikovanou a časově náročnou faktorizační metodu, z jiných testů již víme, že je to liché složené číslo a není mocninou.

Sotva skrovně jsem se zmínil o faktorizační metodě eliptických křivek pocházející od Hendrika Lenstry. Tento algoritmus je mnohem lepší než oba algoritmy kvadratického síta i síta číselného tělesa pro všechna čísla až na malou množinu složených, tzv. „obtížně rozložitelných" čísel, pro něž si vyhrazujeme metody prosívání.

Existuje též rigorózní stránka rozkládání, kdy se vědci pokoušejí pominout heuristiku a dokazují věty o rozkladových algoritmech. Dosud jsme byli mnohem úspěšnější při dokazování vět o pravděpodobnostních metodách než o metodách deterministických. Nezdá se, že bychom byli blízko důkazu, že různé praktické metody, jako kvadratické síto a síto číselného tělesa, skutečně pracují tak, jak se tvrdí. Naštěstí čísla, která se pokoušíme rozložit, nejsou informována o tom, že nemáme důkaz!

Pro další čtení doporučuji některé z již zmíněných publikací a též [10, 13, 17, 18, 19, 20]. Navíc píši s Richardem Crandallem knihu *Primes: A computational perspective*, která by měla vyjít v roce 1997.

Doufám, že jsem vám aspoň částečně přiblížil myšlenky a vzrušení provázející vývoj kvadratického síta a síta číselného tělesa. Tento vývoj měl štěstí na souhru mezi teoretickými odhady složitosti a dobrou programátorskou intuicí. Jedno bez druhého by nás nikdy nepřivedlo tam, kde jsme nyní.

Poděkování

Tento článek je založen na stejnojmenné přednášce, která byla součástí Pitcherova přednáškového cyklu na Lehigh University od 30. dubna do 2. května 1996. Velice oceňuji povzbuzení a přízeň organizátorů při psaní tohoto článku. Také děkuji redaktorům z Notices of the AMS, zejména Susaně Landauové, za jejich podporu. Jsem velmi vděčný i za kritické připomínky, jež mi sdělili Joe Buhler, Scott Contini, Richard Crandall, Bruce Dodson, Andrew Granville, Hendrik Lenstra, Kevin McCurley, Andrew Odlyzko, David Pomerance, Richard Schroeppel, John Selfridge a Hugh Williams.

Literatura

[1] L. M. ADLEMAN: *Factoring numbers using singular integers.* Proc. 23rd Annual ACM Sympos. Theory of Computing (STOC) 1991, 64–71.

[2] W. R. ALFORD, C. POMERANCE: *Implementing the self initializing quadratic sieve on a distributed network.* In: *Number Theoretic and Algebraic Methods in Computer Science*, Proc. Internat. Moscow Conf., June–July 1993 (A. J. van der Poorten, I. Shparlinski, H. G. Zimmer, eds.), World Scientific 1995, 163–174.

[3] J. BRILLHART, D. H. LEHMER, J. L. SELFRIDGE, B. TUCKERMAN, S. S. WAGSTAFF JR.: *Factorizations of* $b^n \pm 1$, $b = 2, 3, 5, 6, 7, 10, 11, 12$, *up to high powers,* second ed., vol. 22, Contemp. Math., Amer. Math. Soc., Providence, RI 1988.

[4] E. R. CANFIELD, P. ERDŐS, C. POMERANCE: *On a problem of Oppenheim concerning „Factorisatio Numerorum".* J. Number Theory *17* (1983), 1–28.

[5] D. COPPERSMITH: *Modifications to the number field sieve.* J. Cryptology *6* (1993), 169–180.

[6] D. COPPERSMITH, A. M. ODLYZKO, R. SCHROEPPEL: *Discrete logarithms in* $GF(p)$. Algorithmica *1* (1986), 1–15.

[7] J. COWIE, B. DODSON, R. MARIJE ELKENBRACHT-HUIZING, A. K. LENSTRA, P. L. MONTGOMERY, J. ZAYER: *A world wide number field sieve factoring record: On to* 512 *bits.* Advances in Cryptology – Asiacrypt '96, to appear.

[8] M. ELKENBRACHT-HUIZING: *A multiple polynomial general number field sieve.* In: *Algorithmic Number Theory*, Second Internat. Sympos., ANTS-II, to appear.

[9] J. GERVER: *Factoring large numbers with a quadratic sieve.* Math. Comp. *41* (1983), 287–294.

[10] A. K. LENSTRA: *Integer factoring.* Preprint.

[11] A. K. LENSTRA, H. W. LENSTRA JR. (eds.): *The development of the number field sieve.* Lecture Notes in Math., vol. 1554, Springer-Verlag, Berlin, Heidelberg 1993.

[12] A. K. LENSTRA, M. S. MANASSE: *Factoring by electronic mail.* In: *Advances in Cryptology – Eurocrypt '89* (J.-J. Quisquater, J. Vandewalle, eds.), Springer-Verlag, Berlin, Heidelberg 1990, 355–371.

[13] H. W. LENSTRA JR.: *Elliptic curves and number theoretic algorithms.* In: Proc. Internat. Congr. Math., Berkeley, CA, 1986, vol. 1 (A. M. Gleason, ed.), Amer. Math. Soc., Providence, RI 1987, 99–120.

[14] P. L. MONTGOMERY: *A block Lanczos algorithm for finding dependencies over* $GF(2)$. In: *Advances in Cryptology – Eurocrypt '95* (L. C. Guillou, J.-J. Quisquater, eds.), Springer-Verlag, Berlin, Heidelberg 1995, 106–120.

[15] P. L. MONTGOMERY: *Square roots of products of algebraic integers.* In: *Mathematics of Computation 1943-1993, Fifty Years of Computational Mathematics* (W. Gautschi, ed.), Proc. Sympos. Appl. Math., vol. *48*, Amer. Math. Soc., Providence, RI 1994, 567–571.

[16] M. A. MORRISON, J. BRILLHART: *A method of factorization and the factorization of* F_7. Math. Comp. *29* (1975), 183–205.
[17] A. M. ODLYZKO: *The future of integer factorization.* CryptoBytes (The technical newsletter of RSA Laboratories), *1* (1995) 2, 5–12.
[18] C. POMERANCE (ed.): *Cryptology and computational number theory.* Proc. Sympos. Appl. Math., vol. *42*, Amer. Math. Soc., Providence, RI 1990.
[19] C. POMERANCE: *The number field sieve.* In: *Mathematics of Computation 1943-1993, Fifty Years of Computational Mathematics* (W. Gautschi, ed.), Proc. Sympos. Appl. Math., vol. *48*, Amer. Math. Soc., Providence, RI 1994, 465–480.
[20] C. POMERANCE: *On the role of smooth numbers in number theoretic algorithms.* In: Proc. Internat. Congr. Math., Zurich, Switzerland, 1994, vol. 1 (S. D. Chatterji, ed.), Birkhauser-Verlag, Basel 1995, 411–422.
[21] C. POMERANCE, J. W. SMITH, R. TULER: *A pipeline architecture for factoring large integers with the quadratic sieve algorithm.* SIAM J. Comput. *17* (1988), 387–403.
[22] O. SCHIROKAUER, D. WEBER, T. DENNY: *Discrete logarithms: The effectiveness of the index calculus method.* Algorithmic Number Theory, Second Internat. Sympos., ANTS-II, to appear.
[23] H. C. WILLIAMS, J. O. SHALLIT: *Factoring integers before computers.* In: *Mathematics of Computation 1943–1993, Fifty Years of Computational Mathematics* (W. Gautschi, ed.), Proc. Sympos. Appl. Math. *48*, Amer. Math. Soc., Providence, RI 1994, 481–531.

Optická vlákna

Radomír Vacek, Praha

S rozvojem lidské společnosti došlo v posledním století k obrovskému rozvoji techniky, který s sebou přináší potřebu přenosu a zpracování stále většího množství informací. Nosnou elektromagnetickou vlnu sloužící jako přenosový prostředek je zapotřebí modulovat stále vyšší a vyšší rychlostí. Rychlost této modulace určuje významným způsobem kapacitu přenosového systému. S požadavky na vyšší kapacitu se postupně přešlo od využívání dlouhých, středních, krátkých, velmi krátkých a ultrakrátkých elektromagnetických vln do centimetrové, milimetrové a submilimetrové oblasti spektra. Jako nosné elektromagnetické vlny se během několika posledních desetiletí začaly využívat i infračervené záření a světlo.

Myšlenka využít světlo (obecněji optické záření) k přenosu informace není nikterak nová. Již ve středověku byl v klimaticky příznivých podmínkách Středomoří používán tzv. sluneční telegraf konstruovaný pomocí soustavy zrcadel a sloužící k předávání krátkých zpráv. V minulém století si otec klasického telefonu Bell nechal patentovat

Ing. RADOMÍR VACEK, CSc. (1953), katedra chemické fyziky a optiky, Matematicko-fyzikální fakulta Karlovy univerzity, Ke Karlovu 3, 121 16 Praha 2.