Algorytm rozkładu liczby pierwszej na sumę kwadratów

doc. dr Wojciech GUZICKI

(por. artykuł na str. 5)

Jeden z najszybszych algorytmów rozkładu liczby pierwszej postaci $4k+1$ na sumę kwadratów wygląda następująco:

krok I: znajdź taką liczbę $x < p$, że $x^2 \equiv -1 (\mathrm{mod}\, p)$,
krok II: zastosuj algorytm Euklidesa do p i x; pierwsze dwie reszty, mniejsze od $\sqrt{p}$, są liczbami a i b.

Krok II jest wykonywany bardzo szybko. Przypomnijmy, na czym polega algorytm Euklidesa. Mając dwie liczby r_0 i r_1 (zakładamy, że $r_0 \geq r_1$) wypisujemy ciąg reszt z kolejnych dzieleń:

$$\begin{aligned}
r_0 &= r_1 \cdot q_1 + r_2, & 0 \leq r_2 < r_1,\\
r_1 &= r_2 \cdot q_2 + r_3, & 0 \leq r_3 < r_2,\\
r_2 &= r_3 \cdot q_3 + r_4, & 0 \leq r_4 < r_3,\\
&\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\\
r_{n-2} &= r_{n-1} \cdot q_{n-1} + r_n, & 0 \leq r_n < r_{n-1},\\
r_{n-1} &= r_n \cdot q_n.
\end{aligned}$$

Postępowanie to kończymy, gdy kolejna reszta będzie równa 0 ($r_{n+1} = 0$). Twierdzenie Lamégo mówi, że liczba dzieleń nie przekroczy pięciokrotnej liczby cyfr liczby r_1. Dla liczb p i x, mających kilkadziesiąt cyfr, wykonamy zatem co najwyżej kilkaset dzieleń, co może być wykonane na dużym komputerze w bardzo krótkim czasie. Zauważmy, że liczba działań, które tu wykonujemy, nie jest już proporcjonalna do liczby p, lecz do liczby cyfr (czyli logarytmu dziesiętnego) liczby x (a więc i do liczby cyfr liczby p). Krok II algorytmu kończy się zresztą wcześniej. Można pokazać, że wypiszemy dokładnie połowę wszystkich reszt.

Trochę gorzej jest z krokiem I. Liczbę x znajdujemy w następujący sposób. Najpierw znajdujemy tzw. niereszte kwadratową modulo p, tzn. taką liczbę c, że kongruencja $x^2 \equiv c (\mathrm{mod}\, p)$ nie ma rozwiązania. Euler wykazał, że wtedy $c^{(p-1)/2} \equiv -1 (\mathrm{mod}\, p)$. Zatem $c^{2n} \equiv -1 (\mathrm{mod}\, p)$, a więc za x wystarczy wziąć liczbę c^n, a właściwie resztę z dzielenia tej liczby przez p.

Pojawiają się tu dwa problemy. Po pierwsze, jak obliczyć c^n? Wydaje się, że trzeba wykonać n mnożeń przez liczbę c. Okazuje się, że jednak nie. Wyobraźmy sobie dla przykładu, że mamy obliczyć liczbę c^{16}. W tym celu wykonamy tylko 4 mnożenia:

$$\begin{aligned}
&\text{mnożymy } c \cdot c \text{ otrzymując } c^2,\\
&\text{mnożymy } c^2 \cdot c^2 \text{ otrzymując } c^4,\\
&\text{mnożymy } c^4 \cdot c^4 \text{ otrzymując } c^8 \text{ i wreszcie}\\
&\text{mnożymy } c^8 \cdot c^8 \text{ otrzymując } c^{16}.
\end{aligned}$$

W podobny sposób można wykazać, że liczba mnożeń potrzebnych do wyznaczenia c^n jest proporcjonalna do logarytmu (przy podstawie 2) liczby n. Zauważamy przy tym, że nie interesuje nas dokładne wyznaczenie liczby c^n, ale jedynie reszty z dzielenia jej przez p. W kolejnych mnożeniach nie będziemy zatem mieli do czynienia z coraz większymi liczbami (przez co kolejne mnożenia trwałyby coraz dłużej), ale za każdym razem mnożymy liczby mniejsze od p i bierzemy resztę z dzielenia przez p. Ta część algorytmu będzie zatem trwała krótko, jej czas działania jest znów proporcjonalny do logarytmu liczby p.

A jak znaleźć niereszte kwadratową modulo p? Musimy wiedzieć, w jaki sposób sprawdzić, czy liczba c jest niereszta kwadratową oraz wiedzieć, gdzie ich szukać. Okazuje się, że dość łatwo jest sprawdzić, czy liczba c jest niereszta kwadratową. Pomocne jest tu tzw. prawo wzajemności dla reszt kwadratowych (po szczegóły odeślę Czytelnika do *Teorii liczb* W. Sierpińskiego). Jak jednak szukać tych niereszt? Okazuje się, że bardzo skuteczne jest szukanie ich „po kolei". Bierzemy kolejne liczby pierwsze (łatwo zauważyć, że to wystarczy) i sprawdzamy, która z nich jest niereszta. Ale jak długo będzie to trwało?

Łatwo dowodzi się, że istnieje $(p-1)/2$ niereszt kwadratowych modulo p, mniejszych od p. Ale nie wiemy, jak duża jest najmniejsza z nich. Taki algorytm może więc okazać się znów nieprzydatny, czas działania może znów być proporcjonalny do p. Jednak w praktyce bardzo szybko znajdujemy niereszte. Dla liczb p, mniejszych od 1 000 000 (pamiętając, że $p \equiv 1 (\mathrm{mod}\, 4)$), znajdujemy niereszte wśród liczb nie większych od 37.

Przypuszczamy, że zawsze dość szybko taką niereszte znajdziemy. Wnioskiem z (nie udowodnionej) Uogólnionej Hipotezy Riemanna jest oszacowanie: najmniejsza niereszta jest mniejsza od $2 \cdot (\log_2 p)^2$. Jest to jednak tylko przypuszczenie – za to skuteczne.

FIZYCZNE NOWINKI

Ewolucje w kosmosie, czyli jak wykorzystać grawitację

Grawitacja kojarzy się nam zwykle z czymś, co „przeszkadza" oderwać się od Ziemi, Księżyca, planet itp. Przecież sondy międzyplanetarne wyposażone są w silniki konieczne do pokonania przyciągania grawitacyjnego ciał niebieskich lub do zmiany orbity. Można jednak w tych celach wykorzystać właśnie grawitację. W styczniu 1990 r. Japończycy wystrzelili pierwszy pozaziemski sputnik, nazwany Hiten – od nazwy buddyjskiego anioła. Przez sprytne wykorzystanie przyciągania Słońca, Ziemi i Księżyca inżynierowie z Instytutu Naukowego Przestrzeni i Astronautyki mają nadzieję zmusić Hitena do wykonania serii skomplikowanych ewolucji wokół Ziemi i Księżyca bez użycia żadnych silników. Zresztą Hiten jest bardzo mały, jego masa wynosi zaledwie 182 kg (niewiele więcej niż japońskiego zapaśnika *sumo*) i nie ma odpowiednich ku temu silników.

Hiten został wyniesiony na orbitę Ziemi przez małą rakietę na paliwo stałe. W marcu 1990 r. przyciąganie grawitacyjne Księżyca „wyciągnęło" Hitena na orbitę z apogeum 750 tys. km (odległość Księżyca od Ziemi wynosi ok. 380 tys. km). Po prawie 4 miesiącach „leniwego" okrążania Ziemi Hiten przeszedł ponownie blisko Księżyca, co spowodowało zmniejszenie apogeum orbity do 560 tys. km. Teraz sonda zbliża się do Księżyca co miesiąc. Po trzech zbliżeniach, które nastąpiły 4 sierpnia, 7 września i 2 października 1990 r., Księżyc spowodował wyrzucenie sondy na odległość 1350 tys. km od Ziemi, aby na początku 1991 r. „złapać" go na orbitę bliższą Ziemi. Po serii kolejnych zbliżeń do Księżyca perigeum orbity zmaleje do 120 km (nie tysięcy!). Ma to nastąpić w połowie marca 1991 r. W czasie tego zbliżenia do Ziemi oddziaływanie z górnymi warstwami atmosfery ziemskiej powinno spowolnić Hitena na tyle, aby umieścić go w tzw. punkcie Lagrange'a, gdzie przyciąganie grawitacyjne Ziemi i Słońca równoważy się. Po krótkim pobycie w tym punkcie Hiten, za pomocą swoich miniaturowych silniczków, zostałby umieszczony na orbicie okołoksiężycowej.

Jak dotąd, Hiten spisuje się znakomicie. Jedynie mini-satelita wielkości piłki baseballowej, który odłączył się od Hitena w czasie pierwszego zbliżenia do Księżyca, „zniknął" naukowcom. Już po jego odłączeniu się stwierdzono, że układ telemetryczny mini-satelity nie działa prawidłowo i nie można śledzić go z Ziemi.

Ciekawe, jak zakończy się misja Hitena. Kierownik programu naukowego Hitena, K. T. Uesugi twierdzi, że hamowanie w atmosferze ziemskiej jest bardzo ryzykowne i może skończyć się fatalnie.

Jan KALINOWSKI

(wg *Nature* z 2 sierpnia 1990 r., str. 400)