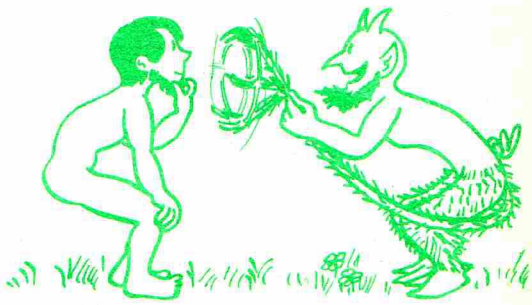
W tej tak zwięzłej historii pierwszych piętnastu lat teorii kwantowej uderzają pewne dziwne fakty. Przede wszystkim, wśród owych przełomowych prac prawie nie ma takich, które by były całkowicie poprawne. W każdym razie, nawet jeśli wniosek jest słuszny, to droga, która do niego doprowadziła, jest co najmniej w pewnym stopniu błędna. I nic w tym dziwnego. Odgadując nową teorię fizycy starają się przecież oprzeć na tym, co jest już znane, a więc na teorii, która w przyszłości ma zostać odrzucona. Z góry zaś trudno przewidzieć, który jej element przetrwa rewolucję. Po drugie, poszczególne odkrycia niesłychanie się ze sobą zazębiają. Chciałoby się powiedzieć, że gdy nadchodzi właściwy czas, to nowa teoria narasta lawinowo: mała grudka śniegu popchnięta w grudniu 1900 roku przez Plancka urosła do potężnej lawiny, w której grzmocie nadal żyjemy. Po trzecie, w odkryciach niezwykłą rolę odgrywa element przypadku. Gdyby na przykład prawo Coulomba miało inną postać niż ma, wzór klasyczny i kwantowy na rozpraszanie w polu tej siły różniłyby się i Rutherford na podstawie znajomości wzoru klasycznego może by nie wydedukował istnienia jądra atomowego. Takich „gdyby" w historii kwantów było więcej. Po czwarte, nowa teoria nie powstała ot tak, „z głowy". Konieczne były coraz to nowe doświadczenia i ścisła współpraca teoretyków i eksperymentatorów. Po piąte wreszcie — czego nie miałem okazji zademonstrować w tym artykule, ale do czego może warto będzie kiedyś powrócić — fizycy w poszukiwaniu nowej teorii po trosze „nawracają się" na filozofię, dziedzinę, którą często w dniach powodzenia nieco sobie lekceważą. Co jest jednak także dość charakterystyczne, filozofia, która poszczególnym fizykom służy jako latarnia morska kierująca ich do właściwego portu, bardzo często okazuje się nie tą, która ostatecznie pozwala na najgłębsze zrozumienie nowych odkryć, i która potem, przynajmniej przejściowo, triumfuje. Choć więc nauka, i to szczególnie taka jak fizyka, ma swoją logikę, to trudno to powiedzieć o jej historii.

Gdy jedziemy samochodem przez most, nie zastanawiamy się, czy wytrzyma. Inżynier to sprawdził.
Gdy inżynier oblicza wytrzymałość mostu, nie zastanawia się, czy wytrzymałość betonu jest taka, jak mu podano. W laboratorium to sprawdzono.
Gdy laborant oblicza wytrzymałość materiału, nie zastanawia się, czy podane mu wzory teoretyczne są prawdziwe. Sprawdzono je w pracowni naukowej.
Gdy naukowiec wyprowadza wzory wytrzymałości materiałów, nie zastanawia się, czy matematyka, której używa do tego celu, jest bezbłędna. Matematycy to sprawdzili.
Gdy matematyk wyprowadza wzory na podstawie aksjomatów teorii, nie pyta „czy naprawdę w przyrodzie dzieje się tak, jak każe matematyka?"
A więc skąd wiemy, że most wytrzyma?



Probabilistyczne algorytmy sprawdzania, czy dana liczba naturalna jest pierwsza

Dr hab. Antoni KRECZMAR

Zadanie polegające na sprawdzaniu, czy dana liczba naturalna nieparzysta n jest liczbą pierwszą, ma swoją długą historię. Zadanie na pozór proste, jednak ze względu na konieczność wykonania długich obliczeń staje się rachunkowo niewykonalne. Oczywiście, jeśli n jest małe, można próbować po kolei wszystkie liczby nieparzyste mniejsze od n i sprawdzać, czy są wśród nich ewentualne dzielniki n. Już w czasach poprzedzających wynalezienie komputera, matematycy widzieli nieskuteczność takiej metody dla dużych liczb. Karol Gauss podaje w swoim dziele „*Disquisitiones Arithmeticae*" kilka interesujących algorytmów działających znacznie szybciej od tego najprostszego, korzystającego bezpośrednio z definicji liczby pierwszej. Jednakże nawet obecnie, przy istniejących niesłychanie szybkich komputerach, nie znamy dostatecznie szybkiego algorytmu rozwiązującego to zadanie. Wyjaśnijmy zatem na przykładzie tego zadania, co to znaczy, że algorytm jest dostatecznie szybki. Jeżeli liczba n ma długość przedstawienia binarnego b, tzn. b jest rzędu $\log_2(n)$, to wszystkie znane algorytmy działają w czasie proporcjonalnym do $n^c = 2^{cb}$ ze stałą $c > 1/4$. Takie algorytmy nazywamy wykładniczymi, albowiem czas ich działania rośnie jak a^k, $a > 1$, gdzie k jest rozmiarem danych (w naszym przypadku $k = b$).

Zwrot „czas działania jest równy 2^{25}" znaczy, że obliczenia wymagają 2^{25} operacji elementarnych. Faktyczny czas działania (np. w sekundach) zależy od sprawności konkretnej maszyny.

Jeżeli taki algorytm zastosujemy dla $b = 100$, tzn. dla liczby n rzędu 2^{100}, to czas jego działania będzie rzędu co najmniej 2^{25}. I może to, że ta liczba jest rzędu około 34 milionów, nie jest takie niepokojące, jak to, że dla $b = 200$ mamy już rząd 2^{50}, czyli, że czas wzrósł kwadratowo.
Dla liczb naturalnych n rzędu 2^{200}, nawet na najszybszym komputerze wykonanie takiego algorytmu jest niemożliwe. Zakładając na przykład, że komputer wykonuje 2^{20} (ponad 1 milion) operacji na sekundę, musiałby on liczyć 2^{30} sekund, czyli więcej niż 2^{18} godzin, czyli więcej niż 2^{13} dni, czyli więcej niż 2^8 miesięcy, czyli więcej niż 2^4 (czyli 16) lat. Algorytmy, których czas działania jest wielomianowy, tzn. rzędu $p(k)$ dla pewnego wielomianu $p(x)$, działają szybciej niż algorytmy wykładnicze, dla dostatecznie dużych k. W szczególności poszukuje się algorytmów liniowych, tzn. takich, których czas działania jest rzędu k. Są one w sensie czasu działania optymalne, albowiem szybciej niż rozmiar danych algorytm nie może działać, gdyż co najmniej tyle czasu zajmuje „przeczytanie" danych przez algorytm.
Ponieważ nie znamy algorytmu wielomianowego sprawdzającego, czy dana liczba naturalna nieparzysta n jest liczbą pierwszą, najpierw R. Solovay i V. Strassen, a następnie M. Rabin skonstruowali algorytmy rozwiązujące to zadanie w sposób niepełny, ale, jak zaraz zobaczymy, w pewnym sensie całkiem zadowalający.
Rozważmy liczbę naturalną nieparzystą n. Algorytm Solovaya i Strassena jest następujący. Losujemy liczbę m ze zbioru $\{1, 2, \ldots, n-1\}$. Obliczamy NWD(n, m) (największy wspólny dzielnik liczb n i m). Jeżeli NWD $(n, m) \neq 1$, znaczy to, że n nie jest liczbą pierwszą. Jeżeli NWD$(n, m) = 1$, to obliczamy wówczas wartość symbolu Jacobiego $\left(\frac{m}{n}\right)$ oraz resztę z dzielenia $m^{(n-1)/2}$ przez n, przyjmując, że jest ona z przedziału $[-1, n-2]$. Oznaczmy $x_{n,m} = \left(\frac{m}{n}\right)$, $y_{n,m} = m^{(n-1)/2} \bmod n$. Jeżeli $x_{n,m} = y_{n,m}$, to przyjmujemy, że n jest liczbą pierwszą, w przeciwnym przypadku przyjmujemy, że jest liczbą złożoną. Solovay i Strassen dowodzą, że jeżeli n jest liczbą pierwszą, to algorytm zawsze odpowie pozytywnie, natomiast gdy n jest liczbą złożoną, to algorytm odpowie pozytywnie (tzn. da błędną odpowiedź) z prawdopodobieństwem $\leqslant 1/2$. Dokładniej, wykazują oni, że dla liczb złożonych n zbiór $\{m$: NWD$(m, n) = 1$ i $1 \leqslant m \leqslant n-1$ $x_{n,m} = y_{n,m}\}$ ma liczebność co najwyżej $(n-1)/2$. Można wykazać, że dla danego n, $b = \log_2(n)$, wykonanie takiej próby zużywa czasu co najwyżej rzędu b. Zatem koszt jednej próby jest liniowy względem rozmiaru zadania. Wykonując t takich prób, w czasie rzędu tb, otrzymamy dla liczby złożonej wynik pozytywny z prawdopodobieństwem $\leqslant \frac{1}{2^t}$. Wykonując na przykład 60 takich prób, otrzymamy w czasie rzędu $60b$ odpowiedź pozytywną z prawdopodobieństwem błędu 2^{-60} — czyli średnio 1 błąd na 10^{18} testów. Takie prawdopodobieństwo błędu jest znacznie mniejsze niż prawdopodobieństwo „pękłamania" komputera.
Podobne rozumowanie doprowadziło M. Rabina do skonstruowania algorytmu probabilistycznego, który po wykonaniu t prób daje odpowiedź pozytywną z błędem nie przekraczającym $\frac{1}{2^{2t}}$, również w czasie rzędu tb. Algorytm Rabina został zaprogramowany i uruchomiony na komputerze. Wykonano najpierw test na liczbach postaci $n = 2^p - 1$, gdzie p jest pierwsza, $500 \geqslant p$. Takie liczby przez wiele lat były przedmiotem rywalizacji firm komputerowych reklamujących swój sprzęt. Znalezienie kolejnej największej liczby pierwszej tej postaci budziło podziw przede wszystkim ze względu na doskonałość sprzętu, na którym takie obliczenia wykonywano. Przecież komputer musiał liczyć niezwykle szybko i bezawaryjnie przez wiele godzin.
Algorytm Rabina w czasie 10 minut sprawdził wszystkie takie liczby i wykrył bez błędu wszystkie liczby pierwsze. Jako ciekawostkę podamy jeszcze, że algorytm został zastosowany do znalezienia dużych liczb pierwszych bliźniaczych, tzn. postaci p, $p+2$, obie pierwsze. Po pół godzinie liczenia algorytm wskazał, że dwie liczby, $338(p_1 \cdot p_2 \cdot p_3 \cdot p_4 \cdot \ldots \cdot p_{299}) + 821$ oraz większa od niej o 2, są liczbami bliźniaczymi, ale po następnych 5 godzinach liczenia algorytm nie znalazł już większej takiej pary.
Na zakończenie podamy jeszcze, w jaki sposób można wykonywać algorytm Solovaya i Strassena. Największy wspólny dzielnik NWD(n, m) można znaleźć stosując algorytm Euklidesa. Resztę z dzielenia $m^{(n-1)/2}$ przez n obliczamy korzystając z rozwinięcia dwójkowego liczby $(n-1)/2$, a następnie podnosząc m do potęgi 1, 2, 4, 8 itd., mnożąc jednocześnie tak te potęgi, aby otrzymać $m(n-1)/2$ (wszystkie kroki zawsze modulo n). Mnożymy zatem te potęgi, gdzie w rozwiązaniu dwójkowym $(n-1)/2$ występuje 1. Wreszcie wartość symbolu Jacobiego można obliczyć stosując wzór rekurencyjny:

$$\left(\frac{m}{n}\right) = \begin{cases} 1 & \text{jeżeli } m = 1 \\ \left(\frac{k}{n}\right) \cdot (-1)^{(n^2-1)/8} & \text{jeżeli } m = 2k \\ \left(\frac{n}{m}\right) \cdot (-1)^{(m-1)(n-1)/4} & \text{w pozostałych przypadkach.} \end{cases}$$

Zwracamy uwagę, że (jest to napisane kilka wierszy niżej) największy wspólny dzielnik obliczamy za pomocą algorytmu Euklidesa. Nie musimy zatem znać rozkładu liczb m i n na czynniki.

Największą znaną liczbą pierwszą jest w tej chwili $2^{21701} - 1$.

Aby określić symbol Jacobiego, przypomnijmy najpierw, że gdy dwie liczby całkowite a i b dają z dzielenia przez m tę samą resztę, to nazywamy je przystającymi modulo m i piszemy $a \equiv b \pmod m$. Zależność tego typu nazywamy kongruencją.
Niech p będzie liczbą pierwszą, różną od 2, zaś a — liczbą niepodzielną przez p. Symbol Legendre'a $\left(\frac{a}{p}\right)$ określamy jako równy $+1$ lub -1 w zależności od tego, czy istnieje liczba x taka, że $x^2 \equiv a \pmod p$, czy nie. Na przykład $\left(\frac{3}{11}\right) = +1$, bo $5^2 = 25 \equiv 3 \pmod{11}$, $\left(\frac{2}{5}\right) = -1$, bo nie ma liczby x, której kwadrat kończyłby się na 2 lub 7.
Jeżeli teraz m jest dowolną liczbą nieparzystą i $m = p_1 \ldots p_s$, gdzie p_i są liczbami pierwszymi i NWD$(a, m) = 1$, to symbol Jacobiego $\left(\frac{a}{m}\right)$ określamy jako iloczyn symboli Legendre'a: $\left(\frac{a}{m}\right) = \left(\frac{a}{p_1}\right) \cdot \ldots \cdot \left(\frac{a}{p_s}\right)$.
W końcowej części artykułu podany jest wzór rekurencyjny służący do obliczania $\left(\frac{a}{m}\right)$.
Symbole Legendre'a i Jacobiego znajdują zastosowania w teorii liczb, ale wprowadzone zostały w związku z badaniami w dziedzinie tzw. całek eliptycznych. Jedną z takich całek jest $\int \sqrt{1 - a^2 \sin^2 x}\,dx$, pojawiająca się np. przy obliczaniu długości łuku elipsy.