Co udowodnił Manindra Agrawal?

Jerzy BROWKIN

1. Liczbę naturalną n nazywamy **pierwszą**, jeżeli ma dokładnie dwa dzielniki: 1 i n. Liczbę naturalną n nazywamy **złożoną**, jeżeli ma co najmniej trzy dzielniki, tzn. oprócz dzielników 1 i n ma jeszcze dzielnik d, gdzie $1 < d < n$. Wtedy również liczba naturalna n/d jest dzielnikem liczby n. Gdyby obie liczby d i n/d były większe od $\sqrt{n}$, to mielibyśmy $n = d \cdot n/d > \sqrt{n} \cdot \sqrt{n} = n$, co daje sprzeczność. Zatem każda liczba złożona n ma dzielnik większy od 1 i nie przekraczający $\sqrt{n}$.

Jeżeli więc chcemy zbadać, czy liczba naturalna n jest pierwsza czy złożona, to wystarczy dzielić ją przez wszystkie liczby naturalne d, gdzie $1 < d \leqslant \sqrt{n}$. Jeżeli choć w jednym przypadku dzielenie da się wykonać bez reszty, to znajdziemy dzielnik liczby n różny od 1 i od n, a zatem n jest liczbą złożoną. W przeciwnym razie n jest liczbą pierwszą.

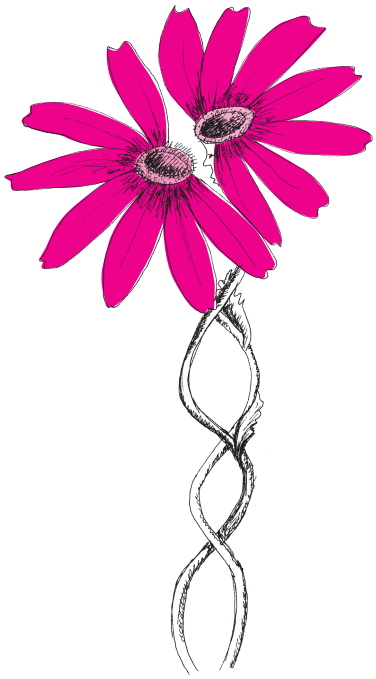
Ten algorytm badania pierwszości liczby naturalnej n jest zbyt pracochłonny, wymaga bowiem wykonania około $\sqrt{n}$ operacji elementarnych (dzieleń). Od dawna poszukiwano algorytmów, które wymagałyby wykonania znacznie mniejszej liczby operacji. Historia tych poszukiwań jest długa, lecz nie będziemy jej tu omawiać. W każdym razie żaden ze znalezionych algorytmów nie działał istotnie szybciej niż omówiony wyżej algorytm polegający na dzieleniu n przez wszystkie liczby naturalne nieprzekraczające $\sqrt{n}$.

Przełom nastąpił dopiero w roku 2002, gdy Manindra Agrawal i jego uczniowie – Neeraj Kayal i Nitin Saxena – z Politechniki w Kanpur (Indie) podali algorytm dla zbadania, czy dana liczba naturalna jest pierwsza czy złożona, wymagający wykonania znacznie mniejszej liczby operacji. Algorytm ten jest tak prosty, że przytoczymy go niżej. Dużo bardziej skomplikowane jest uzasadnienie, że jest on poprawny.

2. Algorytm AKS badania, czy liczba n jest pierwsza, czy złożona.

Krok 1. Badamy, czy istnieją takie liczby naturalne $r \geqslant 2$ i $s \geqslant 2$, że $n = r^s$. Jeżeli TAK, to liczba n jest złożona, jeżeli NIE, to przechodzimy do następnego kroku.

Komentarz. Gdyby $n = r^s$, gdzie $r \geqslant 2$, to $n \geqslant 2^s$. Stąd $s \leqslant \log n / \log 2$. Wystarczy więc zbadać, czy liczba $r = \sqrt[s]{n}$ jest całkowita dla $2 \leqslant s \leqslant \log n / \log 2$. Mamy więc do zbadania $C_1 \log n$ liczb, gdzie C_1 jest pewną stałą.



Krok 2. Bierzemy liczbę $r = 2$ i badamy, czy r dzieli n. Jeżeli TAK, to n jest liczbą złożoną, gdy r jest mniejsze od n, i jest liczbą pierwszą, gdy $r = n$. Jeżeli NIE, to badamy, czy

1) liczba $r - 1$ ma „duży" dzielnik pierwszy q, tzn. spełniający nierówność $q > 4\sqrt{r} \log n$.

2) liczba $n^{(r-1)/q} - 1$ jest podzielna przez r.

Jeżeli 1) lub 2) nie zachodzi, to jako r bierzemy następną liczbę pierwszą i postępujemy analogicznie.

Komentarz. Wiadomo, że istnieje taka stała C_2, że dla pewnej liczby pierwszej $r < C_2(\log n)^6$ zachodzi 1) i 2).

W kroku 2 badamy więc co najwyżej $C_2(\log n)^6$ liczb r i albo jedna z nich dzieli n (wtedy liczba n jest złożona), albo znajdziemy liczbę pierwszą r spełniającą 1) i 2).

Krok 3. Mamy liczbę pierwszą r spełniającą warunki 1) i 2). Dla każdego a, gdzie $1 \leqslant a \leqslant 2\sqrt{r} \log n$, dzielimy wielomian

$$(X - a)^n - X^n - a \text{ przez } X^r - 1.$$

Jeżeli za każdym razem reszta z tego dzielenia jest wielomianem o wszystkich współczynnikach podzielnych przez n, to liczba n jest pierwsza. W przeciwnym razie jest ona złożona.

Komentarz. Jak wiemy, $r \leqslant C_2(\log n)^6$, zatem liczba wielomianów rozpatrywanych w kroku 3 nie przekracza $2\sqrt{r} \log n \leqslant 2\sqrt{C_2}(\log n)^4 = C_3(\log n)^4$, gdzie C_3 jest pewną stałą.

Wobec tego w całym algorytmie liczba operacji elementarnych wykonanych na liczbach lub wielomianach nie przekracza

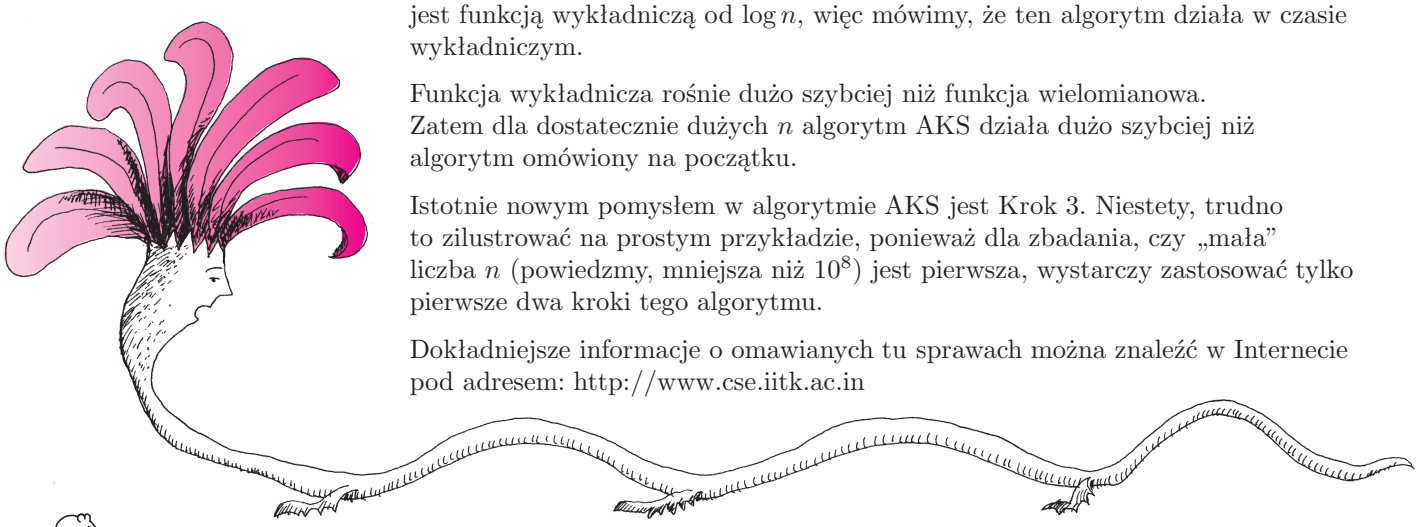
$$C_1 \log n + C_2(\log n)^6 + C_3(\log n)^4.$$

To wyrażenie jest pewnym wielomianem od $\log n$, mówimy więc, że algorytm AKS działa w czasie wielomianowym.

Algorytm omówiony na początku wymagał wykonania $\sqrt{n}$ operacji. Ponieważ

$$\sqrt{n} = n^{1/2} = 2^{(\log n)/(2\log 2)} = \left(2^{1/(2\log 2)}\right)^{\log n}$$

jest funkcją wykładniczą od $\log n$, więc mówimy, że ten algorytm działa w czasie wykładniczym.



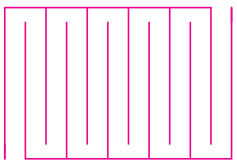
Funkcja wykładnicza rośnie dużo szybciej niż funkcja wielomianowa. Zatem dla dostatecznie dużych n algorytm AKS działa dużo szybciej niż algorytm omówiony na początku.

Istotnie nowym pomysłem w algorytmie AKS jest Krok 3. Niestety, trudno to zilustrować na prostym przykładzie, ponieważ dla zbadania, czy „mała" liczba n (powiedzmy, mniejsza niż 10^8) jest pierwsza, wystarczy zastosować tylko pierwsze dwa kroki tego algorytmu.

Dokładniejsze informacje o omawianych tu sprawach można znaleźć w Internecie pod adresem: http://www.cse.iitk.ac.in

Zadania

Redaguje Ewa CZUCHRY



F 597. Wykonano kondensator złożony z dwóch układów płaszczyzn przewodzących (rysunek obok). Zaniedbując efekty brzegowe, znaleźć pojemność tego kondensatora. Odległość między płaszczyznami jednego układu jest jednakowa i równa $2d$, a liczba płaszczyzn wynosi $2n$.
Rozwiązanie na str. 5

F 598. Jedną płaszczyznę nienaładowanego kondensatora o pojemności C uziemiono, a drugą połączono długim cienkim przewodem ze znajdującą się w dużej odległości przewodzącą kulą o promieniu r i ładunku q_0. Jaki ładunek zostanie na kuli?
Rozwiązanie na str. 7

Redaguje Mikołaj ROTKIEWICZ

W poniższych grach uczestniczy dwoje zawodników: Alicja i Bartek. Gracze wykonują posunięcia na przemian. Grę zaczyna Alicja. Przegrywa ten, kto nie może wykonać ruchu zgodnego z regułami gry.

M 1027. Na stole leży n cukierków. W każdym ruchu gracz musi zjeść mniej niż połowę pozostałych na stole cukierków, ale co najmniej jeden. Na przykład, dla $n = 3$ w pierwszym ruchu Alicja musi zjeść 1 cukierek, po czym Bartek nie ma ruchu. Wyznaczyć $n \in \mathbb{N}$, dla których Alicja ma strategię wygrywającą.
Rozwiązanie na str. 5

M 1028. Na stole leżą dwie grupy złożone odpowiednio z m i n żetonów $(m, n \geqslant 1)$. W pojedynczym ruchu gracz wybiera grupę, a żetony wybranej grupy wyrzuca do kosza. Drugą grupę dzieli na dwie nowe grupy (po co najmniej jednym żetonie). Dla jakich (m, n) Bartek ma strategię wygrywającą?
Rozwiązanie na str. 6

M 1029. Na początku na tablicy napisana jest liczba naturalna $n \geqslant 2$. Posunięcie gracza polega na zastąpieniu napisanej na tablicy liczby k liczbą $k - d$, gdzie d jest dzielnikiem k oraz $1 \leqslant d < k$. Wyznaczyć n, przy których Alicja ma strategię wygrywającą.
Rozwiązanie na str. 16