Test pierwszości Solovaya-Strassena.

Projekt z przedmiotu PTKB.

Michał Aniserowicz

1 Opis zadania

Celem projektu jest zaimplementowanie probabilistycznego testu pierwszości Solovaya-Strassena.

2 Teoria

Probabilistyczny test pierwszości Solovaya-Strassena został opracowany przez Roberta M. Solovaya i Volkera Strassena. Określa on, czy dana liczba jest liczbą złożoną czy prawdopodobnie pierwszą.

Podstawową wykorzystywaną przez niego własnością jest wykazany przez Eulera fakt, że dla każdej liczby pierwszej p i dowolnej liczby naturalnej a, zachodzi:

$a^{(p-1)/2} \equiv \left(\frac{a}{p}\right) \pmod{p}$,

gdzie $\left(\frac{a}{p}\right)$ jest symbolem Legendre'a.

2.1 Symbol Legendre'a

Symbol Legendre'a to funkcja $\left(\frac{a}{p}\right)$ zdefiniowana następująco:

$$\left(\frac{a}{p}\right) = \begin{cases} 0 & \text{, jeśli } a \equiv 0 \pmod{p} \\ 1 & \text{, jeśli istnieje takie } b\text{, że } b^2 = a \mod p \\ -1 & \text{, jeśli nie istnieje żadne } b \text{ takie że } b^2 = a \mod p \end{cases},$$

gdzie p jest liczbą pierwszą większą od 2.

W teście Solovaya-Strassena użyto uogólnienia symbolu Legendre'a - symbolu Jacobiego.

2.2 Symbol Jacobiego

Symbol Jacobiego jest uogólnieniem symbolu Legendre'a na liczby nieparzyste (niekoniecznie pierwsze). Jeśli rozkład liczby n na czynniki pierwsze to:

$p_1^{c_1} p_2^{c_2} \cdots p_k^{c_k}$,

to symbol Jacobiego jest równy przez symbol Legendre'a:

$\left(\frac{a}{n}\right) = \left(\frac{a}{p_1}\right)^{c_1} \left(\frac{a}{p_2}\right)^{c_2} \cdots \left(\frac{a}{p_k}\right)^{c_k}$.

Można zauważyć, że jeśli n jest pierwsze, symbol Jacobiego jest równy symbolowi Legendre'a.

2.3 Algorytm

Sprawdzenie, czy dana liczba naturalna n jest pierwsza, odbywa się poprzez sprawdzenie, czy dla różnych wartości liczby naturalnej a $(1 < a < n)$ spełniona jest kongruencja:

$\left(\frac{a}{n}\right) \equiv a^{(n-1)/2} \pmod{n}$.

Jeśli dla którejkolwiek wartości a powyższa kongruencja nie jest spełniona, to liczba p jest liczbą złożoną - wartość symbolu Jacobiego dla pary liczb (n, a) nie jest równa wartości symbolu Legendre'a dla tej pary (patrz Sekcja 2.2).

Kroki algorytmu są następujące:

1. Pobierz parametry wejściowe: n i k.
2. Powtórz k razy:
   (a) Wybierz losowo a $(1 < a < n)$;
   (b) Oblicz $x \leftarrow \left(\frac{a}{n}\right)$;
   (c) Jeśli $x = 0$ lub $x \neq a^{(n-1)/2} \pmod{n}$, zwróć: `złożona`.
3. Zwróć: `prawdopodobnie pierwsza`.

Prawdopodobieństwo zwrócenia błędnego wyniku (tzn. zwrócenia `prawdopodobnie pierwsza` dla liczby złożonej) wynosi 2^{-k}.

3 Implementacja

Aplikację implementującą test Solovaya-Strassena napisano w języku C# (platforma .NET). Kod źródłowy programu wraz komentarzami zawiera Załącznik A.

Aplikacja została podzielona na następujące moduły:

- `SolovayStrassen.Logic` - implementuje algorytm. Zawiera klasy: `SolovayStrassenAlgorithm` i `JacobiAlgorithm`.
- `SolovayStrassen.Logic.Tests` - zawiera testy jednostkowe algorytmu (klasy: `PrimeNumberTests` i `ComplexNumberTests`).
- `SolovayStrassen.Console` - punkt wejścia programu. Pobiera parametry wiersza poleceń (n i k) i wywołuje algorytm.

Załącznik B zawiera pliki binarne programu i przykładowy skrypt uruchamiający. Przykładowa komenda uruchamiająca program:

```
SolovayStrassen 274876858367 1000
```

4 Testowanie

Aplikację przetestowano przy pomocy automatycznych testów jednostkowych. Duże liczby pierwsze zaczerpnięto z: *http://en.wikipedia.org/wiki/List_of_prime_numbers*.

Wszystkie testy potwierdzają poprawność działania algorytmu.

Załączniki

A Katalog *source/* - kod źródłowy aplikacji.

B Katalog *app/* - pliki binarne aplikacji wraz z przykładowym skryptem uruchamiającym.