

Test pierwszości Solovaya-Strassena.

Projekt z przedmiotu PTKB.

Michał Aniserowicz, Jakub Turek

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:

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

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 Kroki algorytmu

3 Implementacja

- Język programowania: c#, platforma .NET.

4 Testowanie