Zaawansowane metody kryptografii i ochrony informacji (14L)

# Porównanie dwóch wybranych testów pierwszości (Solovaya-Strassena i Fermata)

## Prowadzący projekt:

## Mgr inż. Marcin Tunia

# Wprowadzenie

Zagadnienie badania liczb pierwszych od wielu lat znajduje się w centrum zainteresowań matematyków, ze względu na prostotę opisu podstawowych problemów i mocne skorelowanie tych tworów matematycznych ze światem codziennym. W wyniku rozwoju teorii liczb, odkryto szereg własności liczb pierwszych; cały czas jednak mnóstwo zagadnień pozostaje otwartych, jak na przykład problem faktoryzacji liczb całkowitych, problem wyznaczenia wzoru jawnego na liczby pierwsze czy problem znajdowania liczb pierwszych o zadanych właściwościach. Z drugiej strony, na skutek rozwoju kryptografii asymetrycznej w ubiegłym wieku, okazało się, że istnieje szereg zastosowań w kryptografii, w których liczby pierwsze mogą być użyte, aby zrealizować pewne usługi bezpieczeństwa jak poufność czy integralność danych.

Kluczowym problemem w stosowaniu liczb pierwszych, jest stwierdzenie, czy dana liczba jest pierwsza. Z matematycznego punktu widzenia problem jest dość prosty, ponieważ na mocy np. twierdzenia Wilsona [1] wystarczy sprawdzić, czy dana liczba *p* spełnia kongruencję

.

Ze względu na problem obliczania silni, jest to algorytm niepraktyczny dla dużych liczb – w obecnej chwili potrzebne są liczby pierwsze rzędu tysięcy bitów, dla których obliczenie tego typu wyrażeń jest problemem nierozwiązywalnym w sensownym czasie (rzędu kilku sekund) na typowym komputerze. Stąd potrzeba stosowania bardziej wyrafinowanych testów, aby poradzić sobie z ograniczeniami czasowymi (i często też pamięciowymi).

Testy pierwszości można w pierwszej kolejności podzielić na testy deterministyczne i testy niedeterministyczne. W niniejszej pracy skupiono się na tych ostatnich, ze względu na fakt ich powszechnego stosowania w praktyce – posiadają zwykle mniejszą złożoność asymptotyczną niż testy deterministyczne – np. sito Eratostenesa działa w czasie

,

Natomiast najszybszy (asymptotyczne, na chwilę obecną) test deterministyczny AKS działa w czasie

.

Dla porównania badane testy Fermata i Solovaya-Strassena mają złożoność czasową

,

Biorąc pod uwagę stałą, jaka kryje się pod notacją duże O, algorytmy niedeterministyczne są dużo szybsze dla „małych” liczb.

# Opis algorytmów

## Test Fermata

### Pseudokod

## Test Solovaya-Strassena

W poniższym algorytmie wykorzystywane są elementarne pojęcia z teorii liczb jak reszty kwadratowe oraz przystawanie modulo *p*. Poniżej będziemy używać symbolu Jacobiego, zdefiniowanego następująco:

Test opiera się na następującym twierdzeniu Eulera:

*Jeżeli liczba p jest liczbą pierwszą, oraz (a,p) = 1, to*

Gdy liczba *p* nie jest liczbą pierwszą, to liczbę *a*, dla której nie zachodzi powyższa kongruencja, nazywamy *świadkiem złożoności liczby p*. Można udowodnić, że dla liczby złożonej przynajmniej połowa liczb od niej mniejszych nie spełnia powyższej kongruencji. W związku z tym losując *k* razy liczbę *a*, prawdopodobieństwo niewykrycia złożoności badanej liczby jest równe, co najmniej:

,

Jest więc dowolnie bliskie 1, w zależności od ilości wykonanych testów.

### Pseudokod

# Zastosowania

Biorąc pod uwagę zastosowania czysto kryptograficzne (są one w głównym kręgu zainteresowań na tym przedmiocie), powyższe algorytmy mogą być wykorzystane w algorytmach i protokołach wymagających użycia liczb pierwszych (lub z dużym prawdopodobieństwem pierwszych). Do nich zaliczają się algorytmy i protokoły oparte na RSA czy algorytmie ElGamal – w klasycznym ujęciu tych algorytmów operacje wykonywane są z użyciem liczb, które są niemożliwe do rozłożenia na czynniki pierwsze – ze względu na relatywnie duże wartości tych czynników ( porównywalne z pierwiastkiem z danej liczby, aby wykluczyć użycie małych czynników pierwszych).

Ze względu na istnienie liczb Carmicheala, test Fermata nie jest szeroko wykorzystywany w praktyce – jest ich nieskończenie wiele, stąd też nie można testu poprawić, na przykład tablicując wszystkie takie liczby. Z drugiej strony jest to bardzo szybki test – wymaga podniesienia danej liczby do zadanej z góry potęgi, co można zrealizować w czasie wielomianowym od długości bitowej liczby, której pierwszość się bada.

Test Solovaya-Strassena jest prekursorem testu Millera-Rabina, który jest szeroko stosowany w systemach informatycznych – np. biblioteka standardowa języka Java używa testu Millera-Rabina do generowania liczb potencjalnie pierwszych w klasie BigInteger.

# Testy

# Instrukcja obsługi aplikacji

# Bibliografia

1. Dowód Twierdzenia Wilsona - http://en.wikipedia.org/wiki/Wilson%27s\_theorem