**Algorytmy sprawdzające, czy dana liczba jest prawdopodobnie pierwsza.**

1. Test Millera-Rabina

Probabilistyczny test, w którym prawdopodobieństwo błędnego stwierdzenia złożoności lub pierwszości liczby zależy od ilości wykonanych iteracji pętli algorytmu. Prawdopodobieństwo to wynosi (1/4)2. Schemat wykonania dla liczby nieparzystej n i k prób, wygląda następująco:

Wylicz s - maksymalną potęgę dwójki dzielącą n-1.  
Podstaw d = n/2s  
powtórz k razy:  
 wylosuj a takie, że 1<a<n  
 sprawdź czy ad mod n różne od 1  
 jeżeli tak to sprawdz czy ad\*2rmod n rozne od n-1 dla wszystkich r, takich że: 0≤r≤s-1  
 jeżeli tak to to przerwij test - liczba nie jest pierwsza  
jeżeli nie przerwano testu dla żadnej z prób to liczba prawdopodobnie jest pierwsza

Algorytm ten można bardzo łatwo rozproszyć. Każda iteracja jest zdarzeniem niezależnym i rozłącznym względem innych iteracji. Wobec tego w dowolny sposób można je rozdzielać pomiędzy dowolną ilość klastrów obliczeniowych. Najtrudniejszą częścią tego algorytmu jest wyliczenie wyrażenia ad\*2rmod n, można w tym miejscu skorzystać z algorytmu szybkiego potęgowania modularnego.

Opis algorytmu:

<http://www.algorytm.org/algorytmy-arytmetyczne/test-pierwszosci-test-millera-rabina.html>

<http://edu.i-lo.tarnow.pl/inf/alg/001_search/0019.php>

<http://pl.wikipedia.org/wiki/Test_Millera-Rabina>

1. Test pierwszości Fermata (wykorzystujący Małe TW Fermata)

Test pierwszości Fermata jest testem probabilistycznym opartym na Małym TW Fermata. Jest to jeden z prostszych testów stwierdzających z dużym prawdopodobieństwem czy liczba jest pierwsza. Jego schemat dla liczby nieparzystej p i k prób wygląda następująco:

powtórz k razy:  
 wylosuj a takie, że 1<a<p  
 sprawdź czy ap-1 mod p = 1  
 jeżeli nie to przerwij test - liczba nie jest pierwsza  
jeżeli równość była spełniona dla wszystkich prób, liczba prawdopodobnie jest pierwsza

Podobnie jak test Millera-Rabina, test Fermata można bardzo łatwo rozpraszać. Każde powtórzenie algorytmu można rozwiązywać niezależnie od innych powtórzeń. Główną wadą tego algorytmu jest to, że daje pozytywny wynik nie tylko dla liczb pierwszych, ale również dla liczb Carmichela, które są złożone. W praktyce nie jest to jednak duży problem, ponieważ liczby Carmichela są dużo rzadsze od liczb pierwszych (mniej więcej jedna na milion liczb pierwszych).

Opis algorytmu:

<http://www.algorytm.org/algorytmy-arytmetyczne/test-pierwszosci-test-fermata.html>

<http://edu.i-lo.tarnow.pl/inf/alg/001_search/0018.php>

[http://pl.wikipedia.org/wiki/Test\_pierwszo%C5%9Bci\_Fermata](http://pl.wikipedia.org/wiki/Test_pierwszości_Fermata)

1. Chiński Test pierwszości

(…)

1. Test Solovaya-Strassena

(…)