Rozkład liczb na czynniki.

3 grudnia 2013

Rozkład Fermata
Chcemy rozłożyć liczbę q na czynniki przy pomocy algorytmu Fermata. Algorytm przebiaga następująco:

1. Przedstawiamy liczbę q jako $a = 2^k * n$
2. Obliczamy x = $\lfloor \sqrt{n} \rfloor$ (gdzie $\lfloor . \rfloor$ to część całkowita liczby np. $\lfloor 1.6 \rfloor = 1$). Jeżeli $\sqrt{n} = \lfloor \sqrt{n} \rfloor$ (jest liczbą całkowitą) to n ma dzielnik x z krotnością 2 ($n = x^2$). Jeżeli tak nie jest to $x = x + 1$ i przechodzimy do następnego kroku.
3. Dopóki $x < (n+1)/2$ wykonujemy następujące kroki:
   (a) Obliczamy $y^2 = x^2 - n$
   (b) Jeżeli $y^2 > 0$ i $\left\lfloor \sqrt{y^2} \right\rfloor = \sqrt{y^2}$ to liczba n ma podzielniki równe $y + x, x - y$
   (c) Jeżeli nie to $x = x + 1$

Część pierwsza zadania polega na napisaniu programu, którego wynikiem jest lista pierwszych podzielników danej liczby q z ich krotnościami, np dla q=78 wynikiem będzie lista [2,3,13] z krotnościami [1,1,1] bo $78 = 2^1 3^1 13^1$.

Test Lucasa: n- nieparzysta liczba naturalna, b liczba całkowita $2 \leqslant b \leqslant n-1$, $n-1 = p_1^{e_1} * ... p_n^{e_n}$, gdzie p_n są liczbami pierwszymi. Jeżeli dla każdego p_n zachodzą relacje:

1. $b^{n-1} \equiv 1 (mod\ n)$
2. $b^{\frac{n-1}{p_n}} \not\equiv 1 (mod\ n)$

to n jest liczbą pierwszą (ponownie skuteczność testu zależy od wyboru liczby b).

Zadanie: korzystając z progarmu rozkładającego liczby na czynniki pierwsze należy zaimplementować podane testy na perwszość liczb.