Testy liczb pierwszych

19 listopada 2013

Do przeprawadzenia testu, czy dana liczba jest pierwsza będzie potrzebny sposób a^k modulo n: Załóżmy, że chcemy obliczyć 3^{13} mod 10, przedstawiamy wykładnik 13 w postaci binarnej: 1101 czyli 3^{13} mod 10 = $(3^{1*8}3^{1*4}3^{0*2} * 3^{1*1})$ mod 10 = 3^{1*8} mod 10 3^{1*4} mod 10 3^{0*2} mod 10 3^{1*1} mod 10. Liczymy teraz odpowiednio $3^1 mod 10 = 3$, 3^2 mod 10 = $(3^1)^2$ mod 10 = 9 itp, zbieramy wyniki reszt z dzielenia w listę [1,1,9,3] i mnożymy przez niezerowe elementy binarnej postaci wykładnika 1101 dostając, że 3^{13} mod 10 = 1*1*1*1*1*3 = 3. Podsumowując by efektywnie policzyć a^k modulo n potrzebujemy: binarnego przedstawienia wykładnika k oraz reszt z dzielenia kolejnych kwadratów a mod n (proszę zwrócić uwagę, że ponieważ działamy modulo n to w celu obliczenia a^{z+2} mod n wystarczy wziąć wynik a^z mod n, podnieść go do kwadratu i policzyć resztę modn np. 3^4 mod 10 = 1^2 mod 10 = 1, zamiast liczenia 81*81 mod 10 = 6561 mod 10=1). Mając tą pomocniczą procedurę możemy przejść do omawiania testu Millera-Rabina. Korzystamy z twierdzenia Fermata

$$a^p \equiv a \; mod \; p \tag{1}$$

gdzie a jest liczbą całkowitą a p dodatnią liczbą pierwszą. Chcemy zbadań czy liczba nieparzysta n jest pierwsza.

1. Wybieramy pewną liczbę b z zakresu $0 < b < n - 1$.
2. Przedstawiamy n-1=2^k*q
3. Obliczamy b^q mod n, b^{2q} mod n, .. $b^{2^k q}$ mod n. Jeżeli
   - albo pierwsza reszta wynosi 1 (mod n)
   - albo któraś z następnych reszt wynosi n-1 ≡ -1 mod n

   to liczba n jest może być liczbą pierwszą. Jeżeli nie to jest liczbą złożoną.

Korzystając z twierdzenia, które mówi o tym, że liczba n jest liczbą silnie pseudopierwszą dla co najwyżej $\frac{1}{4}$ podstaw $0 < b < n$, by mieć pradopodobieństwo $P(x) = 1 - \frac{1}{4^x}$ tego że nasza liczba jest liczbą pierwszą należy wybrać x różnych podstaw b. Zadanie: napisać program kóry dla zadanej liczby sprawdzi (z zadanym prawdopodobieństwem) czy jest ona liczbą pierwszą.

Test Lucasa-Lehmera. Do zaimplementowania testu potrzebna jest definicja liczb Mersenne'a $M(x) = 2^x - 1$ oraz ciąg rekurencyjny określony wzorem $s_0 = 4, s_{k+1} = s_k^2 - 2$. Twierdzenie mówi, że jeżeli liczba p jest pierwsa, to liczba M(p) jest pierwsza wtedy i tylko wtedy gdy $s_{p-2} \equiv 0 (mod M(p))$

Test Lucasa: n- nieparzysta liczba naturalna, b liczba całkowita $2 \leqslant b \leqslant n - 1$. Jeżeli dla każdego pierwszego podzielnika liczby n-1 zachodzą relacje:

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

to n jest liczbą pierwszą

Zadanie: należy zaimplementować podane testy na perwszość liczb.