Testy liczb pierwszych

11 listopada 2015

Procedura pomocnicza - potęgowanie modulo.
Standardowe obliczenie 3^{13} mod 10 wymaga wykonania 12 mnożeń i dzielenia. Ponieważ chodzi nam o dzielenie modulo możemy ograniczyć liczbę wykonanych działać. Potrzebna nam będzie binarna reprezentacja wykładnika. 13 w reprezentacji binarnej jest równe 1101 tzn.

$$3^{13}\text{mod}10 = (3^8 * 3^4 * 3^1)\text{mod}10. \tag{1}$$

Następnie obliczamy kolejno

$$3^1 \bmod 10 = 3 \tag{2}$$
$$3^2 \bmod 10 = (3^1)^2 \bmod 10 = 9\text{mod } 10 = 9 \tag{3}$$
$$3^4 \bmod 10 = (3^2)^2 \bmod 10 = 9^2\text{mod } 10 = 1 \tag{4}$$
$$3^8 \bmod 10 = (3^4)^2 \bmod 10 = 1^2\text{mod } 10 = 1 \tag{5}$$

Ponieważ $3^{13} = (3^8 * 3^4 * 3^1)$ to $3^{13}\text{mod}10 = 1 * 1 * 3 = 3$. Uwaga, potęgowanie należy zacząć wykonywać od najmniejszych wykładników. To znaczy, jeżeli chcemy policzyć 5^{41}mod 137 to wykonujemy następujące operacje:

1. Obliczamy po kolei kolejne wartości 5^{2k}, k=0,1,... (dla wykładnika 41 k=0,1,2,3,4,5 bo $41 = 1 + 2^3 + 2^5$)

$$5^1 \bmod 137 = 5 \tag{6}$$
$$5^2 \bmod 137 = (5^1)^2 \bmod 137 = 25\text{mod } 137 = 25 \tag{7}$$
$$5^4 \bmod 137 = (5^2)^2 \bmod 137 = 25^2\text{mod } 137 = 77 \tag{8}$$
$$5^8 \bmod 137 = (5^4)^2 \bmod 137 = 77^2\text{mod } 137 = 38 \tag{9}$$
$$5^{16} \bmod 137 = (5^8)^2 \bmod 137 = 38^2\text{mod } 137 = 74 \tag{10}$$
$$5^{32} \bmod 137 = (5^{16})^2 \bmod 137 = 74^2\text{mod } 137 = 133 \tag{11}$$
$$\tag{12}$$

2. Korzystając z powyżej obliczonych wielkości otrzymujemy $5^{41}\text{mod } 137 = 5^1 * 5^8 * 5^{32}\text{mod } 137 = 133 * 38 * 5\text{mod } 137 = 62$. Proszę zwrócić uwagę, że wykonanie pierwszego kroku nie stanowi problemu. W każdym następnym kroku obliczeń

korzystamy z wyniku kroku poprzedniego. Przykładowe wyniki dla $1567^{70423-1}$mod 70423

$$
\begin{aligned}
&1567^1 \bmod 70423 = 1567 && (13)\\
&1567^2 \bmod 70423 = (1567^1)^2 \bmod 70423 = 61107\text{mod } 70423 = 61107 && (14)\\
&1567^4 \bmod 70423 = (1567^2)^2 \bmod 70423 = 61107^2\text{mod } 70423 = 26720 && (15)\\
&1567^8 \bmod 70423 = (1567^4)^2 \bmod 70423 = 26720^2\text{mod } 70423 = 10026 && (16)\\
&1567^{16} \bmod 70423 = (1567^8)^2 \bmod 70423 = 10026^2\text{mod } 70423 = 27055 && (17)\\
&1567^{32} \bmod 70423 = (1567^{16})^2 \bmod 70423 = 27055^2\text{mod } 70423 = 66786 && (18)\\
&1567^{64} \bmod 70423 = (1567^{32})^2 \bmod 70423 = 66786^2\text{mod } 70423 = 58668 && (19)\\
&1567^{128} \bmod 70423 = (1567^{64})^2 \bmod 70423 = 58668^2\text{mod } 70423 = 10099 && (20)\\
&1567^{256} \bmod 70423 = (1567^{128})^2 \bmod 70423 = 10099^2\text{mod } 70423 = 17297 && (21)\\
&1567^{512} \bmod 70423 = (1567^{256})^2 \bmod 70423 = 17297^2\text{mod } 70423 = 29305 && (22)\\
&1567^{1024} \bmod 70423 = (1567^{512})^2 \bmod 70423 = 29305^2\text{mod } 70423 = 44963 && (23)\\
&1567^{2048} \bmod 70423 = (1567^{1024})^2 \bmod 70423 = 44963^2\text{mod } 70423 = 38308 && (24)\\
&1567^{4096} \bmod 70423 = (1567^{2048})^2 \bmod 70423 = 38308^2\text{mod } 70423 = 28390 && (25)\\
&1567^{8192} \bmod 70423 = (1567^{4096})^2 \bmod 70423 = 28390^2\text{mod } 70423 = 865 && (26)\\
&1567^{16384} \bmod 70423 = (1567^{8192})^2 \bmod 70423 = 865^2\text{mod } 70423 = 43995 && (27)\\
&1567^{33668} \bmod 70423 = (1567^{16384})^2 \bmod 70423 = 43995^2\text{mod } 70423 = 54293 && (28)\\
&1567^{67336} \bmod 70423 = (1567^{33668})^2 \bmod 70423 = 54293^2\text{mod } 70423 = 34338 && (29)\\
& && (30)
\end{aligned}
$$

Po wykonaniu działania $1567^{70423-1}$mod $70423 = 1$. Inne przykłady

(a) 1567^{704567}mod $7048765 = 4254808$

(b) 15^{12347}mod $707 = 113$

(c) $73^{7789653217}$mod $613 = 109$

(d) $587^{4432679}$mod $997 = 271$

Analogicznie można postąpić dla dowolnej liczby a podniesionej do potęgi k liczonej modulo n $a^k \text{mod} n$
Test Millera-Rabina opiera się na małym twierdzeniu Fermata

$$a^{n-1} \equiv 1 \text{ mod n}, \tag{31}$$

gdzie n jest liczbą pierwszą. Załóżmy, że $n > 2$. Ponieważ n jest liczbą nieparzystą to można ją przedstawić w postaci

$$n - 1 = 2^d q, \tag{32}$$

gdzie q będzie liczbą nieparzystą. Rozważmy następujący ciąg liczb

$$a^q \text{mod n},\ a^{2q}\text{mod n},\ a^{2^2 q}\text{mod n}, ..., a^{2^d q}\text{mod n} = a^{n-1}\text{mod n} \tag{33}$$

Z małego twierdzenia Fermata wiemy, że ostani element ciągu $a^{2^d q}\text{mod n} = a^{n-1}\text{mod n} = 1$. Dodatkowo, każdy następny element ciągu jest kwadratem poprzedniego elementu. Jeżeli n jest liczbą pierwszą to z równania

$$x^2 \equiv 1\text{mod n} \tag{34}$$

otrzymać możemy jedynie dwa rozwiązania

$$
\begin{aligned}
&x \equiv 1 \text{ mod n}\\
&\text{lub}\\
&x \equiv -1 \text{ mod n}
\end{aligned}
$$

Wracając do naszego ciągu, mamy dwie możliwe sytuacje:

1. Pierwszy element ciągu $a^q \equiv 1$mod n. Każdy następny element jest kwadratem poprzedniego, więc otrzymywać będziemy same jedynki

2. Jeżeli pierwszy element ciągu $a^q \not\equiv 1 \text{mod n}$, jeden z elementów ciągu musi być równy -1 (w sensie mod n). Taki element podniesiony do kwadratu da 1 (w sensie mod n) co zapewni nam $a^{2^d q} \text{mod n} = a^{n-1} \text{mod n} = 1$

Test Millera-Rabina bazuje na zaprzeczeniu powyższego rozumowania. Jeżeli dla danej liczby n potrafimy znaleźć taką liczbę a spełniającą dwa warunki

1. $a^q \not\equiv 1 \text{mod n}$ i
2. $a^{2^i q} \not\equiv -1 \text{mod n}$ dla wszystkich i $0 \leqslant i \leqslant d-1$,

to liczba n **jest** liczbą złożoną. Jeżeli nie to liczba n może być liczbą pierwszą - ale nie musi. Istnieją przypadki, w których liczba złożona n może przejść powyższy test dla danej liczby a. Istnieje twierdzenie, które mówi o tym, że zdarza się to dla co najwyżej $\frac{1}{4}$ liczb a z zakresu $0 < a < n$. W celu uzyskania wyższego prawdopodobieństwa, że liczba n jest pierwsza należy wykonać powyższy test dla kilku liczb a.
Skrótowo algorytm można przedstawić w następujących krokach.

1. Dla liczby n wybierz liczbę b taką że $1 < b < n-1$.
2. Przedstaw n-1=2^d*q
3. Oblicz ciąg b^q mod n, b^{2q} mod n, .. $b^{2^d q}$ mod n. Jeżeli
   - pierwsza reszta jest równa 1 (mod n)
   - lub któraś z pozostałych jest równa n-1 ≡ -1 mod n

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

Punktacja:

1. Napisanie funkcji potęgowania modulo 3 punkty
2. Napisanie testu Millera-Rabina (maksymalnie 7 punktów):
   - działającego dla liczb z zakresu 3-999 - 2 punkty
   - działającego dla liczb z zakresu 1000-9999 - 4 punkty
   - działającego dla liczb z zakresu 10 000-32 000 i więcej - 7 punktów