Znajdowanie (generowanie) dużych losowych liczb pierwszych (np liczb pierwszych k-cyfrowych) np $k \geq 1024$

$\pi(n)$ – ilość liczb pierwszych w $[0, n]$

$$\pi(n) \sim \frac{n}{\ln n}$$

Test Millera - Rabina (n)

1° Jeżeli $2 \mid n$ to n - złożona

2° $n - 1 = 2^k m$ (m - nieparzyste)

3° Losujemy $a < n$

4° Obliczamy $a^m, a^{2m}, a^{2^2 m}, \ldots, a^{2^k m} \mod n$

5° Jeżeli $a^{2^k m} \neq 1$ to n - złożona

6° Jeżeli $a^{2^k m} = 1$ i $a^{2^{k-1} m} \neq \pm 1$ to n - złożona

$a^m, a^{2m}, \ldots, a^{2^k m}$

$-1, 1, 1, 1$

n - pierwsze

$x \quad x^2 \equiv_n 1$ mody

Tw 1: Liczba pierwsza $\Leftarrow$

n wtedy wtw $x = \pm 1$

okazuje się 2 rozw w teście M-R

Dowód

- 1° jeżeli n - pierwsza, to $2 \nmid n$
- 5° jeżeli n - pierwsza, to $a^{n-1} \equiv_n 1$
- 6° jeżeli n-pierwsza, to $x^2 \equiv_n 1 \Rightarrow x = \pm 1$

Tw 2: Jeżeli n - złożona, to Test M-R wykrywa to z pr. $\geq \frac{1}{2}$

2 przypadki

1° $n = p^{\alpha}$

2° $n = n_1 \cdot n_2$ gdzie $n_1 \perp n_2$

1° G - grupa i H - podgrupa G

Fakt: Jeżeli istnieje $g \in G \setminus H$, to $|H| \leq \frac{|G|}{2}$

$\Rightarrow$ przypadkowy el G należy do H z pr. $\leq \frac{1}{2}$

$G = \mathbb{Z}_{p^\alpha}^*$ $\quad H = \{a \in G : a^{p^{\alpha-1}} \equiv 1\}$

G jest cykliczna rzędu $p^\alpha - p^{\alpha-1}$

Generator g ma rząd $p^\alpha - p^{\alpha-1}$ wtedy

$$g^{p^{\alpha-1}} \equiv g^{p^{\alpha-1}-1} \not\equiv 1$$

2° $n = n_1 \cdot n_2$ $\quad n_1 \perp n_2$

2.1 $\exists a \quad a^{n-1} = a^{2^k m} \not\equiv 1 \mod n$

$$H = \{a \in \mathbb{Z}_n^* : a^{n-1} \equiv 1\}$$

H jest podgrupą $\mathbb{Z}_n^*$

$$|H| \leq \frac{|\mathbb{Z}_n^*|}{2}$$

$$a \notin \mathbb{Z}_n^* \Rightarrow \exists\, d = a \perp n > 1 \Rightarrow$$

$$a^{n-1} \equiv d^{n-1} \not\equiv 1 \mod n$$

Losujemy $a < n$

$$Pr(a \in H) < \frac{1}{2}$$

2.2 $\forall a \in \mathbb{Z}_n^* \quad a^{n-1} = a^{2^k m} \underset{n}{\equiv} 1$

Niech L będzie najmniejsze, takie że $\forall a \in \mathbb{Z}_n^* \; a^{2^L m} \equiv 1$

$$a^m \quad a^{2m} \quad a^{4m} \quad \ldots a^{2^l m} \quad \ldots \quad a^{2^k m}$$

$*, 1, 1, \ldots, 1$

↑ może być $\neq 1$

$l > 0$, bo $(-1)^m \equiv_n -1 \neq 1$

$$H = \left\{ a \in \mathbb{Z}_n^* : a^{2^{l-1} m} \equiv_n \pm 1 \right\}$$

Jeżeli n nie jest cyklezyjna w teście M-R jako złożone dla a, to $a \in H$

Jeżeli pokażemy istnienie $a \in \mathbb{Z}_n^*$ takiego, że $a \in H$, to pokażemy, że test M-R wykaże złożoność n z pr. $> \frac{1}{2}$

Rozważmy jakiekolwiek a:

$a^{2^{l-1}m} \not\equiv_n 1$.

jeżeli $a^{2^{l-1}m} \not\equiv -1$ to znaleźliśmy poszukiwane a

jeżeli $a^{2^{l-1}m} \equiv_n -1$

Skorzystamy z Chińskiego tw o
resztach. Możemy a przedstawić
jako parę $(a_1, a_2) = (a \bmod n_1, a \bmod n_2)$

$a_1^{2^{L-1} m} \equiv_{n_1} -1$ $\quad$ $a_2^{2^{L-1} m} \equiv_{n_2} -1$

z tw o r istnieje b, że

$b \equiv a_1 \bmod n_1$ i $b \equiv 1 \bmod n_2$

Wtedy $b^{2^{L-1} m} \equiv_{n_1} -1$ $\quad$ $b^{2^{L-1} m} \equiv_{n_2} 1$

$b^{2^{L-1} m} \not\equiv \pm 1 \bmod n$

Zatem $b \notin H$

Faktoryzacja $n = p \cdot q$

Algorytm $p-1$

Dla losowego a

Dla $b = 2, 3, 4, \ldots, B$

$a \leftarrow a^b \bmod n$

Jeżeli $NWD(a-1, n) > 1$

Zwróć $NWD(a-1, n)$ jako dzielnik

$$a = (a_p, a_q) = (a \bmod p, a \bmod q)$$

w kolejnych b $a = (a_p^{b!}, a_q^{b!})$

p III HH
1 1

$$NWD(a-1, n) = p$$

Dla jakich n ten algorytm najlepiej działa?

Odp gdy $p-1$ ma rozkład na małe czynniki pierwsze

Wniosek: Należy stosować p, q, że

$p-1$, $q-1$ nie mają rozkładu na małe $\mathbb{Z}$ pierwsze.

Dlatego generowane są liczby p, q i że $p = 2p' + 1$, $q = 2q' + 1$.

Algorytm sita kwadratowego (2 Pozomerowski) ma $O(e^{c\sqrt{\ln n \ln\ln n}})$

Alg ten działa w dwóch fazach

$B \approx C e^{c'\sqrt{\ln n \ln\ln n}}$

faza pierwsza

Powtórz wiele razy

Wybierz y

Oblicz $y^2 \bmod n = y'$

Jeżeli y' ma rozkład na czynniki $\leq B$, to zapamiętaj y wraz z tym rozkładem

Skończ gdy zgromadzisz $B+C$ liczb y

faza 2

Niech $p_1\ p_2 - \dots - p_s$ - liczby pierwsze mniejsze niż B

$$y_i^2 \underset{n}{\equiv} p_1^{\alpha_{1i}}\ p_2^{\alpha_{2i}} \cdots p_s^{\alpha_{si}}$$

$$y_i \sim (\underset{\text{mod}2}{\alpha_{1i}}, \underset{\text{mod}2}{\alpha_{2i}}, \dots, \underset{\text{mod}2}{\alpha_{si}}) = \vec{\alpha_i}$$

$$(1, 0, 0, 1, 1 - \dots 0, 0)$$

Rozwiązując układ równań liniowych obliczamy $b_1 - \dots - b_{s+1} \in \{0, 1\}$

$$b_1\vec{\alpha_1} +_2 b_2\vec{\alpha_2} +_2 \dots - \dots +_2 b_{s+1}\vec{\alpha_{s+1}} = (0, 0 \dots 0)$$

$$y_1^{2b_1} \cdot y_2^{2b_2} \cdots y_{s+1}^{2b_{s+1}} = Y^2$$

$\Rightarrow$ pary ste

$$Y^2 = \prod_{i=1}^{s+1} p_i^{\sum_i \alpha_{ij} b_j} = \left(\prod_{i=1}^{s+1} p_i^{k_i} \right)^2$$

$$= Z^2$$

$$Y^2 \underset{n}{=} Z^2$$

$$Y \underset{n}{=} \pm Z \Rightarrow \text{to nam nic nie daje}$$

$$Y \neq \pm Z \Rightarrow \text{to daje faktoryzację}$$

$n \mid Y^2 - Z^2 \iff n \mid (Y-Z)(Y+Z)$

$n \mid (Y-Z) \iff Y \underset{n}{\equiv} Z \quad n \mid (Y+Z) \iff Y \underset{n}{\equiv} -Z$

$NWD(n, Y \pm Z)$ — nietrywialny dzielnik n

Lepszy jest algorytm sita ciała liczbowego — złożoność

$e^{\sqrt[3]{\ln n \ln\ln n}}$