3 - Sito Kwadratowe

Friday, 21 June 2024 14:01

Chcemy rozłożyć N na czynniki.

Mając nietrywialne rozwiązanie $x^2 = y^2 \pmod N$

$\gcd(x-y, N)$ lub $\gcd(x+y, N)$ daje nietrywialny dzielnik N.

Wybieramy $a_1, \dots, a_k$ i obliczamy $b_i = a_i^2 \pmod N$ $\quad a_i > \sqrt{N}$

Chcemy wybrać taki podzbiór $I \subseteq [k]$: $\prod_{i \in I} b_i = z^2$

Ustalmy B; zbiór liczb pierwszych $\leq B$: $p_1, \dots, p_\pi$

Liczby B-gładkie - faktoryzujące się na składniki $\leq B$.

Jeśli mamy zbiór liczb B-gładkich o mocy większej niż $\pi(B)$

to możemy takie I wybrać: powyżej wykładniki to przestrzeń $\mathbb{Z}_2^{\pi(B)}$.

Niech $x = \prod_{i \in I} a_j \pmod N$; $y = \sqrt{\prod_{i \in I} b_j} \pmod N$

Jeśli $x \neq \pm y$ to mamy nietrywialny dzielnik.

Jak znaleźć $a_1, \dots, a_k$?

$X_j = \lceil \sqrt{N} \rceil + j$ dla $j \leq K$ (jakaś stała)

$Y_j = X_j^2 \pmod N \Rightarrow Y_j = X_j^2 - N$

Chcemy zobaczyć, czy wśród Y_j jest wystarczająco dużo B-gładkich.

$Y_j = X_j^2 - N \Rightarrow \left(p \mid Y_j \Rightarrow X_j^2 = N \pmod p\right)$

Zatem N jest resztą kwadratową mod p. Jeśli nie, to nie musimy rozpatrywać p.

Jeśli N jest resztą kwadratową, to możemy znaleźć x: $x^2 = N \pmod p$

Zatem jedyne liczby Y_j podzielne przez p, to takie, że $X_j = \pm x$

Możemy operować na logach, ale musimy wyłuskać max potęgę p.

Złożoność: „Opłaca się" zabrać ograniczenie na K i $B \sim e^{\sqrt{\ln N \ln\ln N}}$

Wtedy oczekiwana złożoność to $O\left(e^{(1+o(1))\sqrt{\ln N \ln\ln N}}\right)$

Jest zatem podwykładniczy. $\square$