6 - Rachunek indeksów

Friday, 21 June 2024 16:16

Chcemy policzyć Discrete-Log w $\mathbb{Z}_p$.

Factor Base

Wybieramy mały zbiór liczb pierwszych. $np \leq B$

$Q = \{q_1, \dots, q_r\}$

Dla różnych (losowych) k, obliczamy a^k szukając liczb Q-gładkich.

Jeśli a^k jest Q-gładka:

$k = \beta_1 \log q_1 + \dots + \beta_r \log q_r$

Znamy β_i, nie znamy $\log q_i$.

Znajdujemy ~$3r$ takich równań i rozwiązujemy układ równań.

Mamy zatem wyliczone logarytmy dyskretne dla małych liczb.

Chcemy znaleźć u, v takie, że $b^u a^v$ jest Q-gładka.

$b^u a^v = q_1^{\beta_1} \dots q_r^{\beta_r}$

$u \log b + v \log a = \beta_1 \log q_1 + \dots + \beta_r \log q_r$

Wtedy $\log b = u^{-1} (\beta_1 \log q_1 + \dots + \beta_r \log q_r - v)$ □

$\log_a a = 1$:)