Last time

Discrete log in $\mathbb{Z}_n^*$ for n prime,

with preprocessing, running in randomized time $2^{O(\sqrt{\log n}\,(\text{polyloglog } n))}$.

Def m is y-smooth if all prime factors of m are $\leq y$.

Fact Given m, y as input, can determine if m is y-smooth, and if so, its factorization into primes in time $\text{poly}(y, \log m)$.

Algorithm:

- Given input x, g
- Set $B = 2^{O(\sqrt{\log n})}$ → Where ϵ = fraction of B-smooth #'s $< n$
- Repeat $1/\epsilon$ times:
  - Pick $a \in [n-1]$ uniformly at random.

- Consider $z = x \cdot g^a$
- If z is B-smooth and $z = \prod p_i^{e_i}$ for $p_i < B$ then $\log_g x = \left(\left(\sum e_i \log_g p_i\right) - a\right) \bmod (n-1)$

Runtime = $\text{poly}(B, 1/\epsilon, \log n)$.

Need to set B so that B is not too big, ϵ not too small.

How many B-smooth #s $< n$ are there?

Want a lower bound.

Suppose $B^k \approx n$

Take any k primes less than B, and multiply them.

There are $\binom{\pi(B)}{k}$ such products. ($\pi(B)$ = # primes $< B$)

$$\geq \left(\frac{B}{k \log B}\right)^k \geq \frac{n}{(k \log B)^k}$$

For $B = 2^{\sqrt{\log n}}$ $\quad B^k \geq \frac{n}{2}$

$k = \sqrt{\log n}$

$$(k \log B)^k = 2^{k(\log k + \log\log B)}$$

$$= 2^{\sqrt{\log n} \cdot (\log\log n + \log\log n)}$$

$$= 2^{\sqrt{\log n}\,(\text{polyloglog } n)}.$$

$$\epsilon = \frac{1}{B^{\text{polyloglog } n}}$$

So runtime of alg $= 2^{\sqrt{\log n}\,(\text{polyloglog } n)}$.

Removing the preprocessing

Repeat lots of times:

Pick $r \in [n-1]$ uniformly at random.

Consider $z = g^r$.

If it is B-smooth, and

$$z = \prod_{p<B} p^{e(p)}$$

then $$r = \sum_{p<B} e(p) \log_g p \quad \cdots (*)$$

Add $(*)$ to our list of equations relating the $\{\log p\}_{p<B}$

Plan:
Solve these equations, get $\{\log p\}_{p<B}$.

May be too much to ask for, aim lower.

Initial Training phase

Collect equations:

$r \longrightarrow e_r \in \mathbb{Z}_{n-1}^{\pi(B)}$

" the powers of p's multiplied to give g^r.

Collected $r_1, r_2, \ldots \in [n-1]$

and $e_{r_1}, e_{r_2}, \ldots \in \mathbb{Z}_{n-1}^{\pi(B)}$

Doing phase

Next we get random $z = x \cdot g^a$ which is B-smooth, we factor it as $z = \prod_{p<B} p^{f(p)}$

$f \in \mathbb{Z}_{n-1}^{\pi(B)}$

If can write $f = \sum u_i e_{r_i}$

for $u_i \in \mathbb{Z}$,

then $\log_g z = \sum_i u_i r_i$

$g^{r_1} = 2^2 \cdot 3^3$

$g^{r_2} = 2^5 \cdot 3^1$

then

$g^{r_1+r_2} = 2^7 \cdot 3^4$

Analysis

Let $G_1 \subseteq G_2 \subsetneq \cdots \subsetneq G_i \cdots \subseteq G_K$.

be the subgroups of

$\mathbb{Z}_{n-1}^{\pi(B)}$

generated by

$\{e_{r_1}\}, \{e_{r_1}, e_{r_2}\}, \ldots$

respectively.

Each e_{r_i} is an independent sample from the same distribution. (the distribution of exponents in the prime factorization of unif. Random B-smooth numbers $< n$).

Next, we sample an f from the same distribution $\mathcal{U}$.

$$\Pr[f \in G_K] ?$$

Let X_i be the indicator for $G_i \neq G_{i-1}$.

$$\sum_i X_i \leq \Pi(\mathcal{B}) \log n.$$

If $\Pr[X_i = 1 \mid r_1, r_2, \ldots r_{i-1}] < \epsilon$,

then $\Pr[f \in G_K] < \epsilon$.

$\Pr[X_i = 1 \mid r_1, \ldots r_{i-1}]$ is nonincreasing

If $\Pr\left[X_K = 1 \mid r_1 \cdots r_{K-1} \right] \geq \epsilon$,

then at least $K - \pi(B) \log n$

chances to grow w.p prob $(1-\epsilon)$ failed. So this is very unlikely

$$\Pr_{r_1 \cdots r_K}\left[\Pr\left[f_K(r_K) > \epsilon \right] \right]$$

$$\leq \binom{K}{\pi(B)\log n} (1-\epsilon)^{K - \pi(B)\log n}$$

$$\leq \left(\frac{K}{\pi(B)\log n} \right)^{\pi(B)\log n} (1-\epsilon)^{K-\pi(B)\log n}$$

$$\leq e^{\pi(B)\log n \log K} \cdot e^{-\epsilon\left(K - \pi(B)\log n\right)}$$

Setting $\boxed{K = \left(\pi(B)\log n\right)^3}$

this is $\leq e^{-\pi(B)^2}$

$= o(1)$.