Dixon's Alg for factoring integers.

Given n, in a randomized $2^{O(\sqrt{\log n \log\log n})}$ time & space we will find the prime factorization of n.

Algorithm $\rightarrow$ Recall: About $\frac{1}{B}$ fraction of $\{1,2,\dots,n\}$ is B-smooth

- $B = 2^{O(\sqrt{\log n \log\log n})}$
- If some $\# < B$ divides n, done // poly(B)

Repeat $(\pi(B)+1)K$ times:

- Sample random $x_i \in \{1,2,\dots,n-1\}$
- Check if $x_i^2 \pmod n$ is B-smooth and if so:

  write $x_i^2 = \prod_{p<B} p^{e_i(p)}$.

- Consider the $\vec{e_i}$ vectors so obtained. $\in \mathbb{N}^{\pi(B)}$
- Find $a_i \in \{0,1\}$ s.t.

$\sum a_i \vec{e}_i$ is all even.

(linear algebra over $\mathbb{F}_2$, succeeds if we have $> \pi(B)$ such $\vec{e}_i$)

- Then $\prod_i (x_i^2)^{a_i} \equiv \prod_i \left(\prod_{p<B} p^{e_i(p)} \right)^{a_i} \bmod n$

$\left(\prod_i x_i^{a_i} \right)^2 = x^2$

$= \prod_{p<B} p^{\sum a_i e_i(p)}$

$= \prod_p p^{\text{something even}}$

$= y^2.$

So $x^2 \equiv y^2 \bmod n$

- Take GCD of $x-y$ and n and if it is a nontrivial factor of n.

output it

else fail.

Main question

$$\Pr_{x \in \{1,2,\ldots n\}} \left[x^2 \bmod n \text{ is } B\text{-smooth} \right] \geq \frac{1}{\text{poly}(B)} ?$$

Want to exhibit many B-smooth squares mod n.

Try 1: Take B-smooth smooth #s $< \sqrt{n}$.

Square them.

How many #s do we get?

$\geq \sqrt{n} - n^{1/2 - o(1)}$

$\geq \frac{n}{B}$ — ..

But we need to find $\geq \frac{n}{\text{poly}(B)}$

$= n^{1-o(1)}$ many

B-smooth squares mod n.

Try 2 Let $n = \prod_{i=1}^{\ell} q_i^{e_i}$

Then $\mathbb{Z}_n^* = \bigoplus_{i=1}^{\ell} \mathbb{Z}_{q_i^{e_i}}^*$

Consider $\chi_i : \mathbb{Z}_{q_i^{e_i}}^* \to \{\pm 1\}$

the quadratic residue character.

Then $\chi : \mathbb{Z}_n^* \to \{\pm 1\}^{\ell}$

given by $\chi(a) = (\chi_1(a), \chi_2(a), \ldots)$

determines perfect squareness mod n.

($a \in \mathbb{Z}_n^*$ is a perfect sq. iff $\chi(a) = (+1, +1, \ldots, +1)$)

$\chi(a)$ (,) -) .

Key Observation

Consider any two B-smooth numbers a, b at most $\sqrt{n}$ with $\chi(a) = \chi(b)$.

Then $a \cdot b$ is B-smooth, $\leq n$,

and a perfect square mod n.

How do we count the number of **distinct** such numbers produced?

For each $v \in \{\pm 1\}^\ell$, let

$$S_v = \{ z \leq \sqrt{n} : z \text{ is B-smooth}, \chi(z) = v \}.$$

$$\bigcup_{v \in \{\pm 1\}^\ell} S_v = \{ \text{B-smooth } \#\text{'s} < \sqrt{n} \}$$

Similarly worse to case:

$\forall \{z_1, z_2, z_3, z_4\}$ s.t.

$\chi(z_1) = \chi(z_2)$, $\chi(z_3) = \chi(z_4)$

we have $z_1 z_2 \neq z_3 z_4$

then the # of B-smooth squares mod n we get is

$$\geq \frac{1}{2}\left(\sum_v |S_v|^2\right) \geq \frac{1}{2}\left(\frac{\sum_v |S_v|}{2^\ell}\right)^2 \cdots \left(\begin{array}{l}\left(\sum |S_v| \cdot 1\right)^2 \\ \leq \left(\sum |S_v|^2\right)\left(\sum 1^2\right)\end{array}\right)$$

$$\geq \frac{1}{2^{\ell+1}} \cdot \left(\begin{array}{c}\#\text{ B-smooth \#s} \\ \leq \sqrt{n}\end{array}\right)^2$$

$$\geq \frac{1}{2^{\ell+1}} \cdot \left(\frac{\sqrt{n}}{B}\right)^2$$

$$\geq \frac{1}{2^{\ell+1}} \quad \frac{n}{B^2}.$$

If $\ell \leq \sqrt{\log n \log\log n}$, then this is

n ___

poly(B).

If $\ell \geq \sqrt{\log n \log\log n}$, then some prime factor $\leq n^{1/\ell} \leq 2^{\sqrt{\frac{\log n}{\log\log n}}}$

$\leq B$.

Real argument (without toy simplification)

For any $a \in \mathbb{N}$, let $\gamma(a)$ be the number of divisors of a.

$$\gamma(a) = \prod (e_i + 1) \quad \text{if } a = \prod \underbrace{p_i}^{e_i}$$

Fun fact (1) $\gamma(a) \leq a^{O(1/\log\log(a))}$

and is tight for some a's.

(2) $$\sum_{a \leq m} \gamma(a) = \#\{(u,v) \text{ s.t. } u \cdot v \leq m\} \in \mathbb{N}^2$$

$\approx m \log m$.

(3) $\gamma(a \cdot b) \leq \gamma(a) \cdot \gamma(b)$

Plan Every number c produced by the procedure:

1. Pick $v \in \{\pm 1\}^\ell$
2. Pick $a, b \in S_v$
3. Output $a \cdot b$

we will give a weight

$\leq \frac{1}{\gamma(c)}$.

Let $W = \{B\text{-smooth squares mod } n\}$.

$$\sum_{v \in \{\pm 1\}^\ell} \sum_{a,b \in S_v} \frac{1}{\gamma(ab)}$$

$$= \sum_{c \in W} \frac{1}{\gamma(c)} \cdot \left(\#\text{ times } \frac{1}{\gamma(c)} \text{ appears in the above} \right.$$

sum)

$$\leq \sum_{c \in W} \frac{1}{\gamma(c)} \cdot \left(\#\, a,b \text{ s.t. } a \cdot b = c \right)$$

$$\leq \sum_{c \in W} \frac{\gamma(c)}{\gamma(c)} = |W|.$$

WTS: $\sum_{v} \sum_{a,b \in S_v} \frac{1}{\gamma(ab)}$ is big.

$$\geq \sum_{v} \sum_{a,b \in S_v} \frac{1}{\gamma(a)\gamma(b)}$$

$$= \sum_{v} \left(\sum_{a \in S_v} \frac{1}{\gamma(a)} \right)^2$$

AM-HM inequality applied to $\{\gamma(a) : a \in S_v\}$

$$\frac{|S_v|}{\sum \frac{1}{\gamma(a)}} \leq \frac{\sum_{a \in S_v} \gamma(a)}{|S_v|}$$

$$\sum_{a \in S_v} \frac{1}{y(a)} \geq \frac{|S_v|^2}{\sum_{a \in S_v} y(a)}$$

$$\geq \frac{\left(\sum_v \sum_{a \in S_v} \frac{1}{y_a} \right)^2}{2^\ell}$$

$$\geq \frac{1}{2^\ell} \left(\sum_{a \in B\text{-smooth}, \leq \sqrt{n}} \frac{1}{y_a} \right)^2 \quad \cdots \quad (*)$$

$$\left(\sum_{\substack{a \in B\text{-smooth} \\ a \leq \sqrt{n}}} \frac{1}{y_a} \right) \geq \frac{\left(\#\, B\text{-smooth}_{\leq} \leq \sqrt{n} \right)^2}{\left(\sum_{\substack{a \in B\text{-smooth} \\ a \leq \sqrt{n}}} y_a \right)}$$

$$\geq \frac{\left(\frac{\sqrt{n}}{B}\right)^2}{\sum_{a \leq \sqrt{n}} s_a} \geq \frac{\left(\frac{\sqrt{n}}{B}\right)^2}{\sqrt{n}\log n}$$

$$\geq \frac{1}{B^2 \log n}\sqrt{n}.$$

Plugging into (*)

$$\sum_v \sum_{a,b \in S_v} \frac{1}{J(ab)} \geq \frac{1}{2^\ell} \cdot \left(\frac{\sqrt{n}}{B^2 \log n}\right)^2$$

$$\geq \frac{1}{2^\ell} \cdot \frac{1}{B^4 \cdot \log^2 n} \cdot n$$

$$\geq \frac{n}{\cdot}$$

poly (B)

if $\ell \leq \sqrt{\log n}$.