15.2. Dixon's random squares method

References: - Chapter 19.5 in "Modern computer algebra"
- Dixon: Asymptotically fast factorization of integers

Reminder.

Lemma 15.2.1 Let $n = p_1^{e_1} \cdots p_k^{e_k}$ odd ($k \geq 2$). Let a be a uniformly random element of $(\mathbb{Z}/n\mathbb{Z})^\times[2] \cong \underbrace{\{\pm 1\} \times \cdots \times \{\pm 1\}}_{k}$. Then,

$1 < \gcd(a-1, n) < n$ with probability $1 - \frac{1}{2^{k-1}} \geq \frac{1}{2}$.

Pf There are exactly 2^k bad a:

$a = 1$: $\gcd = n$

$a = -1$: $\gcd = 1$.

□

How to construct a 2-torsion element:

Find $a, b \in (\mathbb{Z}/n\mathbb{Z})^\times$ with $a^2 \equiv b^2 \bmod n$. Then, $\frac{a}{b} \in (\mathbb{Z}/n\mathbb{Z})^\times[2]$.

Birthday paradox: need to choose $\sim \sqrt{|(\mathbb{Z}/n\mathbb{Z})^\times|}$ random elements $a_i \in (\mathbb{Z}/n\mathbb{Z})^\times$ until finding two with the same square.

Idea Try to find numbers $a_1, \ldots, a_r \bmod n$ s.t.

$$\underbrace{(a_1^2 \bmod n)}_{\in \{1, \ldots, n\}} \cdots \underbrace{(a_r^2 \bmod n)}_{\in \{1, \ldots, n\}} = b^2 \text{ for an integer } b.$$

(!!!)

This is equivalent to the condition that the LHS is divisible by every prime q an even number of times.

We'll only allow a_i such that $(a_i^2 \bmod n) \in \{1, \ldots, n\}$ has only prime factors $q < B$.

(small)

Alg 15.2.2

Given: odd integer $n \geq 3$, composite, not a prime power,

some $B \geq 2$.

1) Compute the primes $p_1, \dots, p_r \leq B$.

Lemma 15.2.2 Let $n = p_1^{e_1} \cdots p_u^{e_u}$ odd, $k \geq 2$.

Let $q_1 < \dots < q_r$ be (small) primes [not dividing n].

The following alg. returns a uniformly random element of $(\mathbb{Z}/n\mathbb{Z})^\times[2]$.

Alg (15.2.2)

1) Find uniformly random elements $b_1, \dots, b_{r+1} \in (\mathbb{Z}/n\mathbb{Z})^\times$ subject to the condition that for each i $(b_i^2 \bmod n)$ can be written as $(b_i^2 \bmod n) = q_1^{f_{i1}} \cdots q_r^{f_{ir}}$:

Just pick random $b \in (\mathbb{Z}/n\mathbb{Z})^\times$, compute $b^2 \bmod n$, find the number of times this integer is divisible by each q_i by trial division, until you've found $r+1$ good residue classes b_i. [This terminates because $b = 1$ is possible.]

2) Using Gaussian elimination, find the kernel of the map $\mathbb{F}_2^{r+1} \to \mathbb{F}_2^r$

$$(v_i)_{i=1,\dots,r+1} \mapsto \left(\sum_i v_i f_{ij} \right)_{j=1,\dots,r}$$

3) Pick a uniformly random nonzero element $v=(v_i)_i \in \mathbb{F}_2^{r+1}$ of the kernel. Let $S = \{i \mid v_i = 1\} \subseteq \{1,\dots,r+1\}$. $\neq \emptyset$

$(\Rightarrow \sum_{i \in S} f_{ij} \equiv 0 \bmod 2$ for all j.)

$\sum_{i \in S} f_{ij}$

4) Let $t_j = \frac{1}{2} \sum_{i \in S} f_{ij}$.

$(\Rightarrow \prod_{i \in S} (b_i^2 \bmod n) = \prod_{i \in S} \prod_j q_j^{f_{ij}} = \prod_j q_j^{2t_j} = \left(\prod_j q_j^{t_j}\right)^2$.)

5) Return $c := \dfrac{\prod_{i \in S} b_i}{\prod_j q_j^{t_j}} \bmod n$.

Pf The result c is an el. of $(\mathbb{Z}/n\mathbb{Z})^\times \setminus \mathbb{Z}$ because

$$\left(\prod_{i \in S} b_i\right)^2 \equiv \left(\prod_j q_j^{t_j}\right)^2 \bmod n.$$

~~We'll show that for any fixed set $S \neq \emptyset$, all elements of $(\mathbb{Z}/n\mathbb{Z})^\times$ are equally likely. Fix any $i_0 \in S$.~~

~~Fix the set S and any $i_0 \in S$ and the value $d = (b_{i_0}^2 \bmod n)$. Also fix all b_j with $j \neq i_0$.~~

~~$\Rightarrow b_{i_0}$ is determined by its square d up to mult. by an el. of $(\mathbb{Z}/n\mathbb{Z})^\times$~~ (Thm)

~~All square roots of $d \bmod n$ are equally likely to be the value of b_{i_0}~~

~~$\Rightarrow$ All elements d of $(\mathbb{Z}/n\mathbb{Z})^\times \setminus \mathbb{Z}$ occur with the same probability.~~

□

~~We'll show that for any fixed $S, c \in \{\pm b\}$~~

We'll show that c is a uniformly random element of $(\mathbb{Z}/n\mathbb{Z})^\times[2]$, even ~~[redacted]~~ for ~~[redacted]~~

~~$S \ni i_0$, for all $i \neq i_0$, $d_{i_0} = (b_{i_0}^2 \bmod n)$~~

~~Note that S can be determined from~~

particular fixed values $d_i = (b_i^2 \bmod n)$.

Note that, S only depends on these values (and randomness the set not on the square roots b_i of d_i.

~~[redacted]~~ The b_i are uniformly random square roots of the d_i.

$\Rightarrow$ ~~[redacted]~~ $\prod_{i \in S} b_i$ is a uniformly distributed random square root of $\prod_{i \in S} d_i$ (even if we pick $i_0 \in S$ and fix all b_i with $i \neq i_0$).

□

Rmk We could have chosen r (and therefore S) deterministically, as long as the choice only depends on $d_1, \ldots, d_{r+1}$, not on $b_1, \ldots, b_{r+1}$.

Question For what fraction of elements $b \in (\mathbb{Z}/n\mathbb{Z})^\times$ can $(b^2 \bmod n)$ be written as $q_1^{f_1} \cdots q_r^{f_r}$?

I.e. how long does step 1 take?

Remark Assume $q_1 < \dots < q_r$ and $q_r^t \le n$. Then,

$$\#\{1 \le a \le n \mid a = q_1^{f_1} \cdots q_r^{f_r} \text{ for some } f_1, \dots, f_r \ge 0\}$$

$$\ge \#\{(f_1, \dots, f_r) \mid f_1, \dots, f_r \ge 0,\ f_1 + \dots + f_r \le t\}$$

$$= \binom{t+r}{t} \ge \frac{r^t}{t!} \qquad (\text{"close to } \tfrac{n}{t!}\text{"})$$

But we need to prove that many of these $1 \le a \le n$ are quadratic residues mod n.

(invertible) Idea (quadr. nonres. mod p_i) · (quadr. nonres) = (quadr. res

Lemma 15.2.3 Assume $q_1 < \dots < q_r$ and $q_r^{2t} \le n$ and that no q_i divides n. Then,

$$\#\{a \in (\mathbb{Z}/n\mathbb{Z})^\times \mid a = q_1^{f_1} \cdots q_r^{f_r} \text{ for some } f_1, \dots, f_r \text{ and } \dots\}$$

(quadr. res)

$$\#\{1 \le a \le n \mid a = q_1^{f_1} \cdots q_r^{f_r} \text{ for some } f_1, \dots, f_r \text{ and } \dots\}$$

$$\#\{b \in (\mathbb{Z}/n\mathbb{Z})^\times \mid (b^2 \bmod n) = q_1^{f_1} \cdots q_r^{f_r} \text{ for some } f_1, \dots, f_r \ge 0\}$$

$$\ge \frac{r^{2t}}{(2t)!}. \qquad (\text{"close to } \tfrac{n}{(2t)!}\text{"})$$

Write $n = p_1^{e_1} \cdots p_r^{e_r}$. $\rightsquigarrow (\mathbb{Z}/n\mathbb{Z})^\times \cong C_{\varphi(p_1^{e_1})} \times \cdots \times C_{\varphi(p_r^{e_r})}$.

Pf Consider the map

$$\chi : (\mathbb{Z}/n\mathbb{Z})^\times \longrightarrow (\mathbb{Z}/n\mathbb{Z})^\times / (\mathbb{Z}/n\mathbb{Z})^{\times 2} \cong \underbrace{C_2 \times \cdots \times C_2}_{k} =: G$$

($(\mathbb{Z}/n\mathbb{Z})^{\times 2}$: quadr. res)

with kernel $(\mathbb{Z}/n\mathbb{Z})^{\times 2}$.

For any $g \in G$, let

$$U_g := \chi^{-1}(g).$$

If $a_1, a_2 \in U_g$, then $\chi(a_1 a_2) = \chi(a_1)\chi(a_2) = g^2 = e$, so $a_1 a_2 \in \ker = (\mathbb{Z}/n\mathbb{Z})^{\times 2}$ is a quadratic residue, with 2^k square roots.

Let $T := \{ a = q_1^{f_1} \cdots q_r^{f_r}$ for some $f_1, \dots, f_r \geq 0$ with $f_1 + \cdots + f_r$ even $\}$.

$(\Rightarrow 1 \leq a \leq \sqrt{n})$

If $a_1, a_2 \in U_g \cap T$, then

$$a_1 a_2 \in W := \{ 1 \leq a \leq n \mid a = q_1^{f_1} \cdots q_r^{f_r}, \ f_1 + \cdots + f_r = 2\epsilon, \ a \in (\mathbb{Z}/n\mathbb{Z})^{\times 2} \}.$$

Hence, we obtain a map

$$\rho : \bigsqcup_{g \in G} (U_g \cap T) \times (U_g \cap T) \longrightarrow W.$$

$$(a_1, a_2) \longmapsto a_1 a_2$$

[Crude estimate:] Any $a = q_1^{f_1} \cdots q_r^{f_r} \in W$ (with $f_1 + \cdots + f_r \leq 2t$) has at most $\binom{2t}{t} = \frac{(2t)!}{t!^2}$ preimages (choose which of the $2t$ prime factors of a go into a_1).

$$\Rightarrow \sum_{g \in G} |U_g \cap T|^2 \le |W| \cdot \frac{(2t)!}{t!^2}.$$

AM-QM ineq: $\left(\frac{\sum_{g \in G} |U_g \cap T|}{|G|} \right)^2 \le \frac{\sum_{g \in G} |U_g \cap T|^2}{|G|}$.

$(\mathbb{Z}/n\mathbb{Z})^\times = \bigsqcup_{g \in G} U_g$ $\rightarrow$ $\left(\frac{|T|}{|G|} \right)^2$ $\le$ $\frac{|W|}{|G|} \cdot \frac{(2t)!}{t!^2}$

$$\Rightarrow \#\{b \in (\mathbb{Z}/n\mathbb{Z})^\times \mid (b^2 \bmod n) = q_1^{f_1} \cdots q_r^{f_r} \cdots\}$$

$$\ge 2^k \cdot |W| \ge \frac{2^k \cdot |T|^2}{|G| \cdot (2t)!/t!^2} = \binom{t+r-1}{t}^2 \cdot \frac{t!^2}{(2t)!}$$

$$\ge \frac{r^{2t}}{t!^2} \cdot \frac{t!^2}{(2t)!} = \frac{r^{2t}}{(2t)!}$$

□