Square roots mod m for general $m \in \mathbb{Z}$.

$m = p^k$ $\quad$ p prime

Thm For $m = p^k$, can find square roots mod m in randomized poly $(\log m)$ time.

Given x, find y s.t. $y^2 \equiv x \pmod{m}$.

Algorithm

Input $x \in \mathbb{Z}$.

1. Find y_1 s.t. $y_1^2 \equiv x \pmod{p}$.
   (By Berlekamp's square root alg. for $\mathbb{F}_p$)

2. Try to find $y_2 = (y_1 + z \cdot p)$ s.t.

$$y_2^2 \equiv x \pmod{p^2}$$

Want $z \in \mathbb{F}_p$ s.t.

$$(y_1 + z \cdot p)^2 = x \pmod{p^2}.$$

$$y_1^2 + 2zy_1p + \cancel{z^2p^2}$$

$$\Big\| \pmod{p^2}$$

$$\boxed{y_1^2} + 2zy_1p \pmod{p^2}$$

$\boxed{y_1^2} = (x+\lambda p)$

$2zy_1p \rightarrow \square \cdot p$

Need to choose z s.t.

$$2zy_1 \equiv -\lambda \pmod{p}$$

$$z = \frac{-\lambda}{2y_1} \pmod{p}$$

Can do this if $p \nmid y_1$

$p \neq 2$.

If $p \mid y_1$, then $p \mid x$, do something else

If $p = 2$ then too something else.

Step 3 Find $y_3 = (y_2 + z \cdot p^2)$ s.t.

$$y_3^2 \equiv x \pmod{p^3}$$

This also succeeds if

$p \nmid y$, and $p \neq 2$.

So on mod p^i for all i upto k.

Final Thm If $p \nmid x$ and $p \neq 2$,

then x is a perfect square mod p^k

iff x - - - - - - - p

and we can find the square root in polylog(p) time.

If $p^2 \mid x$, then $\sqrt{x} \bmod p^k$

$= \left[\left(\sqrt{\frac{x}{p^2}}\right) \pmod{p^k}\right] \cdot p$

If $p \mid x$ and $p^2 \nmid x$, then x is

not a perfect sq. mod p^k.
($k \geq 2$).

---

2 is special, need to lift from solutions mod 8.

General m

Thm If there is an algorithm $A(x, m)$ ($0 \leq x < m$) that finds a y s.t. $y^2 \equiv x \bmod m$ in time polylog (m), then there is an algorithm $B(m)$ that finds a nontrivial factorization of m if m is not prime in time polylog (m).

Proof

If $m = \prod_{i=1}^{\ell} p_i^{e_i}$

then

$\mathbb{Z}/_{m} \simeq \bigoplus^{\ell} \mathbb{Z}/_{p_i}$.

$\mathbb{Z}/m\mathbb{Z} \cong \bigoplus_{i=1}^{\ell} \mathbb{Z}/p_i^{e_i}\mathbb{Z}$

and the perfect squares mod m are those that are perfect squares mod $p_i^{e_i}$ for each i.

$$a \longmapsto (a_1, a_2, \ldots, a_\ell) \in \bigoplus_i \mathbb{Z}/p_i^{e_i}$$

$$a^2 \longmapsto (a_1^2, a_2^2, \ldots a_\ell^2)$$

and the square roots are

$$(\pm a_1, \pm a_2, \ldots, \pm a_\ell)$$

all 2^ℓ (typically) combinations.

If we had our hands on 2 square roots a, a' of the same x, then

$(a_1 \dots a_\ell)$ $(a_1' \dots a_\ell')$ $a + a'$, if it is not $0 \bmod m$,

has nontrivial GCD with m.

(since mod some $p_i^{e_i}$, $a_i = -a_i'$

If $m \mid a^2 - (a')^2 = (a - a')(a + a')$

then we want $m \nmid a - a'$

$m \nmid a + a'$

and then $GCD(m, a + a') \neq 1, m$.

Fact If m_1 is odd and not a prime power, then for a random $a \in \mathbb{Z}_m$,

a^2 has ≥ 4 square roots.

w.h.p.

Algorithm B (m)

0. If $2 \mid m$, output 2.

1. Pick $a \in \mathbb{Z}_m$ uniformly at random

1.5 Let $u = a^2 \in \mathbb{Z}_m$

2. Let $y = A(u, m)$

If $GCD(a,m) \neq 1$, output $GCD(a,m)$

3. If $a \equiv y$ or $a \equiv -y \bmod m$,

FAIL.

4 Else output $GCD(a+y, m)$.

Claim B succeeds in finding a nontrivial factor with prob $\geq \frac{1}{4}$.

Proof

For analysis, first pick $u \in \mathbb{Z}_m$ according to the distribution of $a^2 \pmod m$ for uniformly random $a \in \mathbb{Z}_m$, $GCD(a,m) = 1$.

Then the conditional distribution of $a \mid u$ is uniform on the

square roots of u mod m.

There are ≥ 4 such square roots, and 2 of them are $A(u,m)$ and $-A(u,m)$.

$$\Pr\left[a = A(u,m) \quad \vee \quad a = -A(u,m)\right] \leq \frac{2}{4}.$$

So w.p. $\geq \frac{1}{2}$, $a \neq A(u,m)$

has nontrivial GCD with m.