# Factoring Polynomials over Finite Fields

## First Square roots mod p.

Given odd prime $p$, $a \in \mathbb{F}_p$.

$\mathbb{F}_p = \{0, 1, \ldots, p-1\}$ with operations mod $p$.

Goal: Find $x \in \mathbb{F}_p$ s.t. $x^2 = a \pmod p$.

Ideal running time: poly $(\log p)$ time.

This is open!

$\mathbb{F}_p = \{0, 1, \ldots p-1\}$

$\mathbb{F}_p^* = \{1, 2, \ldots, p-1\}$

a group under multiplication.

$\mathbb{Z}/p-1$

Equivalently, $\exists g \in \mathbb{F}_p^*$ s.t.

$$\{1, g, g^2, \ldots, g^{p-2}\} = \mathbb{F}_p^*.$$

$$\{\text{Nonzero Perfect squares}\} = \{g^{2i} : 0 \le i \in p-2\}$$

$$= \{g^{2i} : 0 \le i \le \left[\frac{p-2}{2}\right]\}$$

$\frac{p-1}{2}$ of them.

---

Test for whether $a \in \mathbb{F}_p^*$ is a perfect Squares

Consider $b = a^{\frac{p-1}{2}}$

Nonsquares → If $a = g^{\text{odd}}$, $b = g^{\frac{p-1}{2}} = -1$

Squares → If $a = g^{\text{even}}$, $b = a^0 = 1$

How do we find $a^{\frac{p-1}{2}}$ ?

## Repeated Squaring

First find $a, a^2, a^4, a^8, \cdots, a^{2^{\lceil \log p \rceil}}$.

by $a^{2i} = (a^i)^2$

Then find $a^{\frac{p-1}{2}} = \prod a^{2^j}$

certain $j$'s.

Whole thing takes poly(log p) time.

---

If $p \equiv 3 \bmod 4$,

$$\left(a^{\frac{p+1}{4}}\right)^2 = a^{\frac{p+1}{2}}$$

$$= a^{\frac{p-1}{2}} \cdot a$$

$$= (+1) \cdot a$$ → If $a$ is a square

$= a.$

So $a^{\frac{p+1}{4}} = \sqrt{a} \mod p.$

---

If $p \equiv 5 \mod 8$, algorithm to find square roots in poly log $(p)$ time

There is an algorithm that runs in time poly $(a, \log p)$ that finds $\sqrt{a} \mod p$

Schoof, via Elliptic Curves.

---

Today Randomized poly $(\log p)$ time algorithm for square roots mod $p$.

An algorithm $F(a, p, y)$ where

$p$ prime, $a \in \mathbb{F}_p$, $y \in \{0,1\}^{\text{polylog } p}$.

s.t.

$\forall\, p$, $\forall\, a \in \mathbb{F}_p$ a perfect square,

$$\Pr_{y \in \{0,1\}^{\text{polylog } p}}\left[ F(a,p,y) \neq \text{a square root of } a \text{ in } \mathbb{F}_p \right] \leq 0.1.$$

---

Consider $Q(X) = X^{\frac{p-1}{2}} - 1$

Distinct roots: 0. Roots of $Q(X)$ are the $\frac{(p-1)}{2}$ perfect squares in $\mathbb{F}_p$.

Input-ant:

1. $Q(X)$ has $\Omega(1)$ and $1-\Omega(1)$ fraction roots in $\mathbb{F}_p$.

2. $Q(X)$ is sparse.

Consider $f(x) = x^2 - a$.

$= (x - \alpha)(x + \alpha)$

where $\alpha = \sqrt{a}$

Idea1: Compute $GCD(Q(x), f(x))$

If it is degree 1, then we found a nontrivial factor of $f(x)$, hooray!

Idea2 Randomize the roots of $f(x)$ by looking at $\tilde{f}(x) = f(cx + d)$ for random $c, d \in \mathbb{F}_p$.

---

If $\alpha, \beta \in \mathbb{F}_p$ $\alpha \neq \beta$.

then for uniformly random $c, d \in \mathbb{F}_p$,

$(c\alpha + d,\ c\beta + d)$ is uniformly distributed in $\mathbb{F}_p^2$.

$$\begin{bmatrix} \alpha & 1 \\ \beta & 1 \end{bmatrix} \begin{pmatrix} c \\ d \end{pmatrix}$$

$\eta$

invertible

---

So the chance that exactly one of $\{c\alpha + d,\ c\beta + d\}$ is a root of $Q(x)$

is $= \frac{1}{2} + O\left(\frac{1}{p}\right)$.

---

To find $\mathrm{GCD}\left(Q(x),\ \tilde{f}(x)\right)$

need to find $x^{\frac{p-1}{2}} - 1 \bmod \tilde{f}(x)$

$\eta$ $\eta$

deg 2

First find $X, X^2, X^4, \ldots X^{2^i} \pmod{\tilde{f}(x)}$.

as deg 1 polys mod $\tilde{f}(x)$.

Find $X^{\frac{p^l-1}{2}} \pmod{\tilde{f}(x)}$ as a product of

$\leq \log p$ of these.

mod $\tilde{f}(x)$.

---

Find roots of $f(x)$ reduces to finding roots of $\tilde{f}(x)$ provided $c \neq 0$. (this holds w. prob $1 - \frac{1}{p}$).

---

Berlekamp's algorithm 1970

Factoring polys over finite fields.

Above alg. easily generalizes to finding roots in $\mathbb{F}_p$ of any polynomial. (odd prime $p$).

Also to $\mathbb{F}_q$ for odd prime powers $q$.

Also to $\mathbb{F}_q$ for even prime powers $q$.

( FACT : In $\mathbb{F}_{2^m}$, the polynomial

$$Tr_{\mathbb{F}_{2^m}/\mathbb{F}_2}(X) = X + X^2 + X^4 + X^8 + \cdots + X^{2^{m-1}}$$

has $2^{m-1}$ roots in $\mathbb{F}_{2^m}$

and has only $m = \log(2^m)$ monomials).

Next time: Factoring.