Factoring polynomials over finite fields

Over a finite field $\mathbb{F}_q$, we saw a sketch of how to find $\mathbb{F}_q$-roots of a polynomial $f(x) \in \mathbb{F}_q[x]$ of degree d in $\text{poly}(d)$ $\mathbb{F}_q$-operations.

Algorithm

1. Define $Q(x) = x^{\frac{q-1}{2}} - 1$ if q is odd
$= x + x^2 + x^4 + \cdots + x^{q/2}$ if q even

2. Consider $f'(x) = GCD\left(Q(x), f(cx+d)\right)$
for random $c, d \in \mathbb{F}_q$

3. If GCD has degree >0 but

$< d$, we reduced to a smaller degree poly f'.

What is $\mathbb{F}_q$? How do we work with it algorithmically?

q is a prime power $= p^m$
p prime.

Then $\mathbb{F}_q$, the finite field with q elements, is a set of size q with $+, \cdot$ satisfying field axioms, and looks like:

$$\mathbb{F}_q \cong \mathbb{F}_p[X]/E(X) = \{\text{polynomials in } \mathbb{F}_p[X] \text{ of degree} \leq m-1 \text{ \& operations mod } E(X)\}.$$

$\downarrow$

irreducible poly in $\mathbb{F}_q[X]$ of degree m.

To realize $\mathbb{F}_q$, we need an irreducible

$E(X)$ of degree m.

Question Given q as input ($\log q$ bits long)

can we find irreducible $E(X)$ of degree m in time $\text{poly}(\log q) = \text{poly}(m, \log p)$?

Open!

For $m=2$, p prime, it is the question of finding a quadratic nonresidue in $\mathbb{F}_p$.

Thm (Ankeny): Under GRH,

one of $\{1, 2, \ldots, O(\log^2 p)\}$ is a quadratic nonresidue in $\mathbb{F}_p$.

What is the least quadratic nonresidue? Famous Open Problem!

to show $p^{O(1)}$.

Best known $\leq p^{\frac{1}{4\sqrt{e}}}$.

Find a prime $\in [n, 2n]$ in time polylog(n)?

Open.

Randomized alg to find primes/irred polys.

1. Pick a uniformly random $E(X) \in \mathbb{F}_p[X]$ of degree n

   or $p \in [n, 2n]$.

2. Check if E is irreducible / p is prime

Done

Thm # primes $\in (n, 2n] = \Omega\left(\frac{n}{\log n}\right)$

$\longrightarrow$ (follows from PNT)

Thm # monic irreducible polys in $\mathbb{F}_p[X]$ of degree m is $\frac{p^m}{m}(1+o(1))$, $m \to \infty$

$\longrightarrow$

Important thms to be proved:

1. Can check irreducibility of degree m poly in time poly$(m, \log p)$

NOW, EASY

2. ——— primality of p in time poly$(\log p)$.

Deterministically!

LATER, IMPORTANT, AMAZING

Facts about finite fields

$$\prod_{\alpha \in \mathbb{F}_p} (X - \alpha) = X^p - X.$$

$$\prod_{\alpha \in \mathbb{F}_q} (X - \alpha) = X^q - X$$

$\alpha = 0 \Rightarrow \alpha^q = \alpha$

$\alpha \neq 0 \Rightarrow \alpha^{q-1} = 1$ (since $|\mathbb{F}_q^*| = q-1$)

$\in \mathbb{F}_q \Rightarrow \alpha^q = \alpha.$

Take $\alpha \in \mathbb{F}_q$.

Consider its minimal poly $G(X)$ over $\mathbb{F}_p$.

Then $G(\alpha) = 0$

$G(\alpha^p) = (G(\alpha))^p = 0.$

$u \mapsto u^p$ is $\mathbb{F}_p$-linear

So $\alpha, \alpha^p, \alpha^{p^2}, \ldots$ are roots of $G(X)$.

$\leq n$

If $\alpha^p = \alpha$, then

$$G(X) = (X-\alpha)(X-\alpha^p)\cdots(X-\alpha^{p^{s-1}})$$

(Just need to show that ↑ has $\mathbb{F}_p$ coefficients)

$$\left(\text{For } \beta \in \mathbb{F}_q, \quad (\beta \in \mathbb{F}_p) \Leftrightarrow (\beta^p = \beta)\right)$$

$$\prod_{\alpha \in \mathbb{F}_q} (X-\alpha) = X^q - X$$

$$\Updownarrow$$

$$\prod_{\text{monic irreducibles } G(X) \text{ of degree dividing } m} \left(\prod_{\text{roots } \alpha \text{ of } G(X)} (X-\alpha)\right) = X^q - X.$$

Any irreducible $G(X) \in \mathbb{F}_q[X]$ which has a root in $\mathbb{F}_q$, has all roots in $\mathbb{F}_q$.

~~$\alpha \in \mathbb{F}_q$~~

$$\prod_{\substack{\text{monic irreducibles} \\ G(x) \text{ of degree} \\ \text{dividing } m}} G(x) = x^{q^m} - x$$

This gives an irreducibility test.

Given $E(x)$ of degree m,

1. Check that $E(x) \mid x^{p^m} - x$.

2. For each $k < m$,

   check that $\gcd(x^{p^k} - x, E(x)) = 1$

   (E is not a product of lower degree irreducibles).

$m = 2$ case of identity

WTS $\prod_{G(x)} G(x) = x^{p^2} - x$

monic
irreducibles $G(X)$
of degree 1 or 2.

Know

$$\prod_{\alpha \in \mathbb{F}_{p^2}} (X-\alpha) = X^{p^2} - X.$$

$$\left(\prod_{\alpha \in \mathbb{F}_p} (X-\alpha) \right) \cdot \left(\prod_{\alpha \in \mathbb{F}_{p^2} \setminus \mathbb{F}_p} (X-\alpha) \right) = X^{p^2} - X.$$

degree 1 monic irreds.

Splits into pairs of the form

$$(X-r)(X-r^p) = \text{monic irred of degree 2.}$$

For each $\alpha \in \mathbb{F}_{p^m}$.

consider smallest $k(\alpha)$ s.t. $\alpha^{p^k} = \alpha$.

$\Leftrightarrow \quad \mathbb{F}_p(\alpha) = \mathbb{F}_{p^k}$.

$\alpha^{p^m} = \alpha$.

$k(\alpha) \mid m$.

Orbit(α) = $\{\alpha, \alpha^p, \dots, \alpha^{p^{k(\alpha)-1}}\}$

$$X^{p^m} - X = \prod_{\alpha \in \mathbb{F}_{p^m}} (X - \alpha)$$

$$= \prod_{k \mid m} \left(\prod_{\substack{\alpha \text{ s.t.} \\ k(\alpha) = k}} (X - \alpha) \right)$$

$$= \prod_{k \mid m} \left(\prod_{\text{orbits } \mathcal{O} \text{ of size } k} \left(\prod_{\beta \in \text{orbit}} (X - \beta) \right) \right)$$

$$= \prod_{k \mid m} \left(\prod_{\substack{\text{various} \\ \text{irreducibles } G(X) \\ \text{of degree } k}} G(X) \right)$$