LECTURE 07

2/29/2012

Note Title 2/27/2012

TODAY

FACTORIZATION OF POLYNOMIALS

- Quadratics
- Linear Factors
- General Case

Simple Case: $q = \text{odd}$;

Input: $x^2 + ax + b \quad [= (x-\alpha)\cdot(x-\beta)]$

"random"

Goal: $x-\alpha, \quad x-\beta$

- Key to all factorization alg (over $\mathbb{F}_q[x]$)

$$x^q - x = x \cdot \left(x^{\frac{q-1}{2}} - 1\right) \cdot \left(x^{\frac{q-1}{2}} + 1\right)$$

- Why is this useful?
  - Contains all linear factors
  - Sparse

- Idea / Hope:

$(x-\alpha) \mid x^{\frac{q-1}{2}} - 1$

but not $x-\beta$

- Assuming above

$$\gcd\left(x^{\frac{q-1}{2}} - 1,\ x^2 + ax + b\right) = x - \alpha$$

- Implementation
  - Compute $x^{\frac{q-1}{2}} \pmod{x^2+ax+b} = g(x)$

by repeated squaring

- Compute $\gcd\left(g-1, (x^2+ax+b)\right)$

- Works if $\alpha = QR$

  $\beta \neq QR$

- General Case? ... shortly

Aside: $q = 2^l$

Use the identity

$$(x^q - x) = Tr(x)\left(Tr(x)-1\right)$$

where

$$Tr(x) = x + x^2 + x^4 + \cdots x^{q/2}$$

Details omitted (easy, no surprises)

Rest of lecture - odd case

General Quadratic : $x^2 + ax + b = f$

Case 1: No linear factors?

Test: $\gcd(f, x^q - x) = ?$

- ✓ $\gcd = 1 \Rightarrow f$ is irreducible
- ? $\gcd = f \Rightarrow f$ has two distinct linear factors.
- ✓ $\gcd = (x-\alpha) \Rightarrow f = (x-\alpha)^2$

Only need to deal with middle case.

Remaining Case: $f = (x-\alpha)(x-\beta)$

$\alpha \neq \beta$.

Idea: Map roots to two random pts.

$$\alpha \longrightarrow \alpha \cdot c + d$$

$$\beta \longrightarrow \beta \cdot c + d$$

How? Let

$$h(x) = f\left(\frac{x-d}{c}\right).$$

Then $h(x) = \left(\frac{x-d}{c} - \alpha\right)\left(\frac{x-d}{c} - \beta\right)$

$$= \frac{1}{c^2}\left(x - (\alpha c + d)\right)\left(x - (\beta c + d)\right)$$

Key Observation:

$c \in \mathbb{F}_q^*$; $d \in \mathbb{F}_q$ random

$\Rightarrow \alpha c + d$ & $\beta c + d$ are random & independent.

$\Rightarrow$ w.p. $\geq 1/4$ $\quad \alpha c+d = QR$

$\beta c+d \neq QR$

$\Rightarrow$ Reduces to simple case!

Algorithm dates back to [Berlekamp '72]

Algorithm Summarized

FACTOR $\left(f(x) = x^2 + ax + b\right)$

- if $\gcd(f, x^q - x) = 1 \Rightarrow$ irreducible
- " $= (x-\alpha) \Rightarrow f = (x-\alpha)^2$
- Else

  Repeat till success

  - Pick $c \leftarrow \mathbb{F}^*$, $d \leftarrow \mathbb{F}$ randomly
  - if $\gcd\left(f\left(\frac{x-d}{c}\right), x^{\frac{q-1}{2}} - 1\right)$

    $= (x-\gamma)$

    output $\left(f_1 = x - \left(\frac{\gamma - d}{c}\right);\ f/f_1\right)$ & STOP
  - continue

Towards higher-degree polynomials

Case 1: f splits into linear factors.

- Above algorithm still makes progress.

Case 2: f has irreducible factors of distinct degrees.

- Use the fact that

  f_i irred. of deg d

  $\iff$ d is the least integer s.t.

  $$f_i \mid x^{q^d} - x$$

- Fact above + gcd's give non-trivial factorization .... makes progress.

irred.

Case 3: All factors of f have same degree d, but some maybe repeated.

Calculus in Algebra:

Definition
- Derivative of $x^i = i \cdot x^{i-1}$
- Extend linearly $(\alpha x^i)' = i\alpha x^{i-1}$

$$(f+g)' = f' + g'$$

Prop.
- Product rule holds: $(f \cdot g)' = f'g + g'f$
- $g^2 \mid f \Rightarrow g \mid f'$

$$\Rightarrow g \mid \gcd(f, f')$$

- $g^i \nmid f$ & $g^{i-1} \mid f$ $\Longrightarrow g^{i-1} \nmid \gcd(f, f')$. (for irreal. g)

Use calculus / gcd (f, f') to eliminate repeated factors.

Case 4: (the interesting case)

f has distinct irred. factors all of same degree d.

Inspiration:

- Should be able to factor f over extension field of size q^d.
- f will have linear factors there.
- Use idea of minimal polynomials to get back solution over $\mathbb{F}_q$

Hurdles:

- Don't have $\mathbb{F}_{q^d}$ explicitly.
- Computing minimal poly? How?

Direct approach: $f = f_1 \cdot f_2$

$\deg(f_i) = d$.

- Pick random poly g of deg $2d-1$
- Chinese Remainder Theorem

$\Rightarrow (g \bmod f_1), (g \bmod f_2)$

uniquely specify $g_i = (g \bmod f)$

$\Rightarrow g_1 = g \bmod f_1$ & $g_2 = g \bmod f_2$

are random & independent.

- W.p. $\geq \frac{1}{4}$

g_1 is a QR in $\mathbb{F}_q[x]/f_1$

g_2 is not a QR in $\mathbb{F}_q[x]/f_2$

$\Rightarrow \gcd\left(g^{\frac{q^d-1}{2}} - 1, f\right) =$ non-trivial

⊠

Summary

- Can factor poly of deg n in $\mathbb{F}_q$ using $\text{poly}(n, \log q)$ operations over $\mathbb{F}_q$
- # operations depends on q!
- Next lectures:
  1. Deterministic algorithms running in time $\text{poly}(n, \ell, p)$ if $q = p^\ell$
  2. Factorization of bivariate polynomials
  3. Factorization of rational ...