Lec18A Cantor Zassenhaus Factorization, Michael Monagan

March 18, 2021 11:30 AM

Polynomial Factorization in $\mathbb{Z}_p[x]$ and $GF(q)[x]$.

Let $a \in \mathbb{Z}_p[x]$, $d = \deg(a)$, $d > 0$. Suppose $\gcd(a, a') = 1$. (a has no repeated factors)

How can we compute the linear factors of a in $\mathbb{Z}_p[x]$?

Test if $a(0) = 0$, $a(1) = 0$, ..., $a(p-1) = 0$?

This costs $p \cdot O(d) = O(pd)$ arithmetic ops in $\mathbb{Z}_p$.

Expensive if $p = 2^{31} - 1$.

Fermat's "little" Theorem (FLT): if p is prime and $0 < a < p$ then

$a^{p-1} \equiv 1 \pmod p$. E.g. $p=7, a=3$. $3^6 = (\underset{9}{3^2})^3 = (2)^3 = \underset{8}{} \equiv 1 \pmod 7$.

$\Rightarrow a^p \equiv a \pmod p$ for $0 \le a < p$

$\Rightarrow a^p - a = 0$ in $\mathbb{Z}_p$.

$\Rightarrow x^p - x = x(x-1)(x-2) \cdots (x-(p-1))$ in $\mathbb{Z}_p[x]$

has roots $0 \le a < p$. is the $\prod$ of all linear factors.

Idea ①. Let $g = \gcd(a, x^p - x) = \prod$ of all linear factors of a.

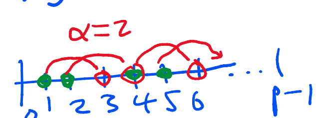
How do we factor g? Suppose $p \ne 2$ and $x \nmid a$. ← not a bother.

$$x^p - x = x \cdot (x^{p-1} - 1) = x(x^{\frac{p-1}{2}} - 1)(x^{\frac{p-1}{2}} + 1)$$

even — half of the linear factors — other half.

$\Rightarrow \gcd(g, x^{\frac{p-1}{2}} - 1) = \{ 1, g, \text{proper factor of } g \}$

Idea ② Pick $\alpha \in \mathbb{Z}_p$ at random.



Let $h = \gcd(g, (x+\alpha)^{\frac{p-1}{2}} - 1) = \{1, g, \text{proper factor of } g\}$.

a random shift

If $h = 1$ or $h = g$ then try again with a new α

Otherwise $g = h \cdot \frac{g}{h}$. Let's factor h and $\frac{g}{h}$ recursively.

See Example in Maple.

Theorem 8.14 (over $\mathbb{Z}_p$ and $GF(q)$).

In $\mathbb{Z}_p[x]$, $x^{p^k} - x$ is the product of all monic irreducible polynomials in $\mathbb{Z}_p[x]$ of degree $d | k$.

$\leftarrow k=1 \Rightarrow d=1$

$\Rightarrow x^{p}-x$ is the Π of all linear polynomials. $g_1=\gcd(a,x^{p}-x)$. $a\leftarrow a/g_1$

$\leftarrow k=2 \quad d=1,2$

$\Rightarrow x^{p^2}-x$ is the Π of all linear & quad polys. $\rightarrow g_2=\gcd(a,x^{p^2}-x)$. $a\leftarrow a/g_2$

all quadratics in a.

$\leftarrow$ all cubics in a.

$\Rightarrow x^{p^3}-x$ is the Π of all linear & cubic polys. $g_3=\gcd(a,x^{p^3}-x)$. $a\leftarrow a/g_3$

$\Rightarrow x^{p^4}-x$ is the Π of all linear, quad, quartics. $g_4=\gcd(a,x^{p^4}-x)$. $a\leftarrow a/g_4$

What if k is large? $k=100, 1000$.

$$\gcd(\underbrace{a, x^{p^k}-x}_{\text{High Deg.}}) = \gcd(\text{rem}(x^{p^k}-x, a), a) \quad \deg a > 1.$$

$$= \gcd(\text{rem}(x^{p^k}, a)-x, a)$$

$$\underbrace{(((x^p)^p)^p \dots)^p}_{k \text{ times}} \bmod a.$$

Fermat's little Theorem in $GF(q)$

Let $GF(q)$ be a finite field with q elements ($q=p$ or $q=p^k$) ($q=p$: $\mathbb{Z}_p$)

Let $a \in GF(q)$, $a\neq 0$.

Then $a^{q-1}=1 \Rightarrow a^q=a$. (also true for $a=0$)

Proof. Let $GF(q)=\{0, x_1, x_2, \dots, x_{q-1}\}$ where $x_i \neq x_j \neq 0$.

Let $A=\{a\cdot x_1, a\cdot x_2, \dots, a\cdot x_{q-1}\}$. $|A|=q-1$

Suppose $\cancel{a}\cdot x_i = \cancel{a}\cdot x_j \Rightarrow x_i = x_j$ $\boxtimes$

$GF(q)$ is a field $\Rightarrow$ Can Law holds.

Also $0 \notin A$. $\underset{\neq 0}{a}\cdot \underset{\neq 0}{x_i} \neq 0$. $\Rightarrow A=\{x_1, x_2, \dots, x_{q-1}\}$.

Eg. In $\mathbb{Z}_7$ $a=3$

$A=\{3\cdot 1, 3\cdot 2, 3\cdot 3, 3\cdot 4, 3\cdot 5, 3\cdot 6\}$
$=\{3, 6, 2, 5, 1, 4\} = \mathbb{Z}_7 \setminus \{0\}$.

Therefore $(a\cdot x_1)\cdot(a x_2)\cdot \dots \cdot (a\cdot x_{q-1}) = x_1 \cdot x_2 \cdot \dots \cdot x_{q-1}$

CAN LAW $\Rightarrow$ $\cancel{x_1}\cdot(\cancel{x_2}\cdot \dots \cdot \cancel{x_{q-1}}\cdot a^{q-1}) = \cancel{x_1}(\cancel{x_2}\cdot \dots \cdot \cancel{x_{q-1}})$

$\Rightarrow a^{q-1}=1$.

Theorem 8.14. Let $f=x^{p^k}-x \in \mathbb{Z}_p[x]$, $k>0$. Let $m(x)\in\mathbb{Z}_p[x]$ be irreducible of degree $d>0$. Then $d|k \Leftrightarrow m \,|\, f=x^{p^k}-x$.

Proof ($\Rightarrow$) Let $F=\mathbb{Z}_p[x]/m$. F is a field with $|F|=\underset{q}{p^d}$ elements.

Let $v\in F$. FLT $\Rightarrow v^{p^d}=v$ in F.

Now $d|k \Rightarrow k=d\cdot q$ for some $q\in\mathbb{Z}$.

Let $v \in F$. $F\ell T \Rightarrow v^{p^d} = v$ in ...

Now $d \mid k \Rightarrow k = d \cdot q$ for some $q \in \mathbb{Z}$.

$$\Rightarrow v^{p^k} = (\overbrace{((v^{p^d})^{p^d})^{p^d} \cdots}^{q \text{ times}})^{p^d} = v \quad F\ell T$$

$$\Rightarrow v^{p^k} - v = 0 \text{ in } F = \mathbb{Z}_p[x]/m$$

$$\Rightarrow \boxed{m \mid v^{p^k} - v} \text{ in } \mathbb{Z}_p[x] \quad \text{for all } v \in F = \{0, 1, x, x+1, \dots\}$$

Take $v = x$

$$\Rightarrow m \mid x^{p^k} - x.$$

($\Leftarrow$) [Proof in book].

How do we split $g_k \in \mathbb{Z}_p[x]$ a $\prod$ of irreducible factors of degree k ?

Th 8.14 If m is irreducible of degree k then $m \mid x^{p^k} - x$ in $\mathbb{Z}_p[x]$.

If $p \neq 2$ Then

$$x^{p^k} - x = x(x^{p^k - 1} - 1) = x(x^{\frac{p^k-1}{2}} - 1)(x^{\frac{p^k-1}{2}} + 1)$$

even

A. $\prod$ of all deg k factors

B. $\prod$ half of deg k factors

C. $\prod$ other half degree factors.

Consider $\gcd(a, x^{\frac{p^k-1}{2}} + 1) = \{1, a, \text{proper factor}\}$.

Also $\boxed{m \mid v^{p^k} - v} = v \cdot (v^{\frac{p^k-1}{2}} - 1)(v^{\frac{p^k-1}{2}} + 1)$ for all $v \in F$.

Theorem 8.11 To split $g_k \in \mathbb{Z}_p[x]$ a $\prod$ of ≥ 2 irreducible polynomials of degree k, pick $v \in \{x^k + v_{k-1}x^{k-1} + \dots + v_1 x + v_0 \in \mathbb{Z}_p[x]\}$ at random. Then

$$\text{Prob}\left[\gcd(g_k, v^{\frac{p^k-1}{2}} \pm 1) \notin \{1, g_k\}\right] > \frac{1}{2} - \frac{1}{2p^2} \geq \frac{1}{2} - \frac{1}{18} = \boxed{\frac{4}{9}}.$$

$p=3$ close to $\frac{1}{2}$

$k=1$ $\gcd(g_1, (x^1+\alpha)^{\frac{p^1-1}{2}} \pm 1)$ for $\alpha \in \mathbb{Z}_p$ chosen at random

$k=2$ $\gcd(g_2, (x^2+\alpha x+\beta)^{\frac{p^2-1}{2}} \pm 1)$ $\alpha, \beta \in \mathbb{Z}_p$

$k=3$ $\gcd(g_3, (x^3+\alpha x^2+\beta x+\gamma)^{\frac{p^3-1}{2}} \pm 1)$ $\alpha, \beta, \gamma \in \mathbb{Z}_p$.

- This is an example of a Las Vegas algorithm. The probability that it succeeds is $\geq 4/9$.
- Cost $O(d^3 \log p)$ arithmetic operations in $\mathbb{Z}_p$ on average.