

CS 4424

Finite fields – factorization

Goal

Final goal: factoring in $\mathbb{Q}[X]$.

Today

- more on finite fields \mathbb{F}_p
- factorization in $\mathbb{F}_p[X]$

Next

- lifting factors
- recombination

Example

Let $F = x^4 - 2x^3 + 9x^2 - 8x + 20$.

Factorization mod 5. Modulo $p = 5$, we have

$$F \equiv x(x+1)(x+3)(x+4) \pmod{5}.$$

Then we get.

- $F \equiv (x+10)(x+11)(x+13)(x+14) \pmod{5^2}$
- $F \equiv (x+260)(x+261)(x+363)(x+364) \pmod{5^4}$
- $F \equiv (x+220885)(x+220886)(x+169738)(x+169739) \pmod{5^8}$

Example

We shift back all coefficients between -195312 and 195312:

$$\begin{aligned} F &\equiv (x - 169740)(x - 169739)(x + 169738)(x + 169739) \pmod{5^8} \\ &\equiv f_1 f_2 f_3 f_4 \pmod{5^8}. \end{aligned}$$

Trying **all combinations**, we find

$$f_2 f_4 \equiv x^2 + 4 \pmod{5^8} \quad \text{and} \quad f_1 f_3 \equiv x^2 - 2x + 5 \pmod{5^8}.$$

That's the factorization.

Where are the problems

- Factorization mod p is relatively well understood.
- Factorization modulo $p \rightarrow$ Factorization modulo p^2 : Newton
- Recombination is slow; there are better but harder solutions.

Factorization

Irreducibility and divisibility

Here, k is a field.

Lemma

- If $P \in k[X]$ is irreducible, and P divides AB , then P divides A or B .

Proof.

- $AB = 0$ in $k[X]/P$
- so either $A = 0$ or $B = 0$ in $k[X]/P$ (because $k[X]/P$ is a field)

Remark: actually, this is a direct consequence of an XGCD identity.

Existence, uniqueness

Prop. Any non-zero polynomial P in $k[X]$ can be factored uniquely (up to permutation) as

$$P = \alpha P_1^{e_1} \cdots P_s^{e_s},$$

with

- α in k
- P_i monic, irreducible
- $P_i \neq P_j$ for $i \neq j$
- e_i integer ≥ 1 .

Proof.

- existence by induction on the degree
- uniqueness from the previous lemma

Squarefree polynomials

Def.

- A polynomial P is squarefree if it does not have any factor of the form Q^2 , with $\deg(Q) > 0$.

Prop.

- P is squarefree if and only if $e_i = 1$ for all i in the factorization

$$P = \alpha P_1^{e_1} \cdots P_s^{e_s},$$

that is,

$$P = \alpha P_1 \cdots P_s.$$

Proof.

- easy!

Making a polynomial squarefree

Prop.

- if

$$P = P_1^{e_1} \cdots P_s^{e_s}$$

and if e_1, \dots, e_s are non-zero in k , then

$$\frac{P}{\gcd(P, P')} = P_1 \cdots P_s.$$

Proof.

- $P' = e_1 P_1' P_1^{e_1-1} P_2^{e_2} \cdots P_s^{e_s} + \cdots + e_s P_s' P_1^{e_1} \cdots P_{s-1}^{e_{s-1}} \cdots P_s^{e_s-1}$
- rewrite it as

$$P' = P_1^{e_1-1} \cdots P_s^{e_s-1} (e_1 P_1' P_2 \cdots P_s + \cdots + e_s P_1 \cdots P_{s-1} P_s')$$

- so $\gcd(P, P') = P_1^{e_1-1} \cdots P_s^{e_s-1}$

Chinese Remainder Theorem

Th.

- suppose that $P = P_1 \cdots P_s$, with P_i irreducible, $P_i \neq P_j$
- let A be in $k[X]$
- then $A \bmod P = 0$ if and only if $A \bmod P_i = 0$ for all i

Proof.

- left to right: easy
- right to left: if P and Q divide A , and $\gcd(P, Q) = 1$ then PQ divide A
- follows from an XGCD identity

Finite fields

Building fields

Lemma 1

- If p is a prime number, then $\mathbb{Z}/p\mathbb{Z}$ is a field.

Lemma 2

- If k is a field and P is an irreducible polynomial, then $k[X]/P$ is a field.

They are mostly the same thing. We prove 2.

- We already saw that it is a ring
- So we need to prove that it is a field: any non-zero element has an inverse
- The extended GCD algorithm computes the inverse

\mathbb{F}_p and $\mathbb{F}_p[X]/P$

1. If p is a prime, we rather write $\mathbb{F}_p = \mathbb{Z}/p\mathbb{Z}$. So, \mathbb{F}_p is a finite field, of cardinality p .
2. If P is an irreducible polynomial in $\mathbb{F}_p[X]$, then $\mathbb{F}_p[X]/P$ is a field.

Lemma

- $\mathbb{F}_p[X]/P$ is a finite field, of cardinality p^d , with $d = \deg(P)$.

Proof.

- the elements of $\mathbb{F}_p[X]/P$ have the form $a_0 + \cdots + a_{d-1}X^{d-1}$
- we have p possibilities for each a_i

Little Fermat

Prop.

- For any a in $\mathbb{F}_p - \{0\}$, we have $a^{p-1} = 1$.

Proof.

- there exists $k > 0$ such that $a^k = 1$, and $a^{k'} \neq 1$ for $0 < k' < k$
- so the elements $1, a, a^2, \dots, a^{k-1}$ form a cycle for “multiplication by a ”
- for b in $\mathbb{F}_p - \{0\}$, let $C_b = \{b, ab, \dots, a^{k-1}b\}$
- prove that $|C_b| = k$
- prove that if C_b and $C_{b'}$ intersect, they are equal
- so k divides $p - 1$.

Roots of $X^p - X$

Coro.

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

Proof.

- every a in $\mathbb{F}_p - \{0\}$ is a root of $X^p - X$ (little Fermat)
- 0 is a root as well

Binomial coefficients mod p

Coro.

- For $0 < i < p$, the binomial coefficient $\binom{p}{i}$ is 0

Proof.

- $(X + 1)^p = 1 + \binom{p}{1}X + \cdots + \binom{p}{p-1}X^{p-1} + X^p$
- $X^p - X = \prod_{a \in \mathbb{F}_p} (X - a) = \prod_{a \in \mathbb{F}_p} (X - 1 - a)$
- replace X by $X + 1$: $(X + 1)^p - (X + 1) = X^p - X$
- so $(X + 1)^p = X^p + 1$

Linearity of the p -power

Prop.

- For any polynomials a, b in $\mathbb{F}_p[X]$, and any λ, μ in \mathbb{F}_p ,

$$(\lambda a + \mu b)^p = \lambda a^p + \mu b^p$$

- For any polynomial P in $\mathbb{F}_p[X]$ and a, b in $\mathbb{F}_p[X]/P$, we have

$$(\lambda a + \mu b)^p = \lambda a^p + \mu b^p.$$

Proof.

- binomial expansion

Remark: this means that p -powering is an \mathbb{F}_p -linear map.

Berlekamp's algorithm

Main result

Prop.

- suppose that P is a squarefree polynomial in $\mathbb{F}_p[X]$, of degree d
- then one can find a proper factor of P using $O(n^3 + pM(n) \log(n))$ operations in \mathbb{F}_p

Coro.

- suppose that P is a squarefree polynomial in $\mathbb{F}_p[X]$, of degree d
- then one can find the irreducible factorization of P for d times the previous cost.

Remark:

- if you don't care about complexity, finding the factorization is an easy problem:
- try all possible factors

The Berlekamp map

We let $P = P_1 \cdots P_s$ be as above.

Consider the map

$$\begin{aligned} \phi : \mathbb{F}_p[X]/P &\rightarrow \mathbb{F}_p[X]/P \\ a &\mapsto a^p - a \end{aligned}$$

Remark:

- if P is irreducible, then

$$\phi(a) = 0 \iff a \in \mathbb{F}_p$$

because $\mathbb{F}_p[X]/P$ is a field

- ϕ is an \mathbb{F}_p -linear map

The nullspace of ϕ

Prop.

- $\phi(a) = 0$ if and only if $a \bmod P_i$ is in \mathbb{F}_p for all i
- then, we write $a_i = a \bmod P_i$

Proof.

- $\phi(a) = 0$ if and only if $a^p - a = 0 \bmod P$
- if and only if $a^p - a = 0 \bmod P_i$ for all i (Chinese Remainder)
- if and only if $(a \bmod P_i)$ is in \mathbb{F}_p for all i (P_i irreducible)

Coro.

- the dimension of the nullspace of ϕ is s (the number of irreducible factors)
- so we'll be able to count them

Non-constant elements in the kernel

We suppose that P is not irreducible

Prop.

- suppose that $\phi(a) = 0$, and that $\deg(a) > 0$
- then there exists i, j such that $a_i \neq a_j$

Proof.

- contrapositive: if all a_i are equal, then $\deg(a) = 0$
- $a - a_i = 0 \pmod{P_i}$ for all i , so $a - a_i = 0 \pmod{P}$
- $\deg(a) < \deg(P)$ so $a = a_i$

Splitting P

Prop.

- For α in \mathbb{F}_p , $\gcd(P, a - \alpha)$ is the product of all P_i such that $a_i = \alpha$

Proof.

- $\gcd(P, a - \alpha)$ is the product of the $\gcd(P_i, a - \alpha)$
- $\gcd(P_i, a - \alpha) = \gcd(P_i, a - \alpha \bmod P_i) = \gcd(P_i, a_i - \alpha)$
- so it is equal to P_i if $a_i = \alpha$ and 1 otherwise

Remark:

- if $\deg(a) > 0$, then not all a_i are the same
- so $\gcd(P, a - \alpha) \neq P$

Algorithm

1. find a such that $\phi(a) = 0$ and $\deg(a) > 0$
2. for α in \mathbb{F}_p , compute $P_\alpha = \gcd(P, a - \alpha)$; stop when $\deg(P_\alpha) > 0$

Prop.

- there exists α such that $\deg(P_\alpha) > 0$
- for any such α , we have $0 < \deg(P_\alpha) < \deg(P)$
- so P_α and P/P_α are “proper” factors of P