8. Factoring polynomials over finite fields

CS-E4500 Advanced Course on Algorithms
Spring 2019

Petteri Kaski
Department of Computer Science
Aalto University

Lecture schedule

Tue 15 Jan:	1. Polynomials and integers
Tue 22 Jan:	2. The fast Fourier transform and fast multiplication
Tue 29 Jan:	3. Quotient and remainder
Tue 5 Feb:	4. Batch evaluation and interpolation
Tue 12 Feb:	5. Extended Euclidean algorithm and interpolation from erroneous data
Tue 19 Feb:	*Exam week — no lecture*
Tue 27 Feb:	6. Identity testing and probabilistically checkable proofs
Tue 5 Mar:	*Break — no lecture*
Tue 12 Mar:	7. Finite fields
Tue 19 Mar:	8. Factoring polynomials over finite fields
Tue 26 Mar:	9. Factoring integers

CS-E4500 Advanced Course in Algorithms (5 ECTS, III–IV, Spring 2019)

2019	KALENTERI				2019
Tammikuu	**Helmikuu**	**Maaliskuu**	**Huhtikuu**	**Toukokuu**	**Kesäkuu**
1 Ti Uudenvuodenpäivä	1 Pe	1 Pe	1 Ma Vk 14 T9	1 Ke Vappu	1 La
2 Ke	2 La	2 La	2 Ti	2 To	2 Su
3 To	3 Su D3	3 Su	3 Ke	3 Pe	3 Ma Vk 23
4 Pe	4 Ma Vk 06 T3	4 Ma Vk 10	4 To	4 La	4 Ti
5 La	5 Ti L4	5 Ti Laskiainen	5 Pe	5 Su	5 Ke
6 Su Loppiainen	6 Ke	6 Ke	6 La	6 Ma Vk 19	6 To
7 Ma Vk 02	7 To Q4	7 To	7 Su	7 Ti	7 Pe
8 Ti	8 Pe	8 Pe	8 Ma Vk 15	8 Ke	8 La
9 Ke	9 La	9 La	9 Ti	9 To	9 Su Helluntaipäivä
10 To	10 Su D4	10 Su D6	10 Ke	10 Pe	10 Ma Vk 24
11 Pe	11 Ma Vk 07 T4	11 Ma Vk 11 T6	11 To	11 La	11 Ti
12 La	12 Ti L5	12 Ti L7	12 Pe	12 Su Äitienpäivä	12 Ke
13 Su	13 Ke	13 Ke	13 La	13 Ma Vk 20	13 To
14 Ma Vk 03	14 To Q5	14 To Q7	14 Su Palmusunnuntai	14 Ti	14 Pe
15 Ti L1	15 Pe	15 Pe	15 Ma Vk 16	15 Ke	15 La
16 Ke	16 La	16 La	16 Ti	16 To	16 Su
17 To Q1	17 Su	17 Su D7	17 Ke	17 Pe	17 Ma Vk 25
18 Pe	18 Ma Vk 08	18 Ma Vk 12 T7	18 To	18 La	18 Ti
19 La	19 Ti	19 Ti L8	19 Pe Pitkäperjantai	19 Su Kaatuneiden muistopäivä	19 Ke
20 Su D1	20 Ke	20 Ke Kevätpäiväntasaus	20 La	20 Ma Vk 21	20 To
21 Ma Vk 04 T1	21 To	21 To Q8	21 Su Pääsiäispäivä	21 Ti	21 Pe Kesäpäivänseisaus
22 Ti L2	22 Pe	22 Pe	22 Ma 2. pääsiäispäivä	22 Ke	22 La Juhannus
23 Ke	23 La	23 La	23 Ti	23 To	23 Su
24 To Q2	24 Su D5	24 Su D8	24 Ke	24 Pe	24 Ma Vk 26
25 Pe	25 Ma Vk 09 T5	25 Ma Vk 13 T8	25 To	25 La	25 Ti
26 La	26 Ti L6	26 Ti L9	26 Pe	26 Su	26 Ke
27 Su D2	27 Ke	27 Ke	27 La	27 Ma Vk 22	27 To
28 Ma Vk 05 T2	28 To Q6	28 To Q9	28 Su	28 Ti	28 Pe
29 Ti L3		29 Pe	29 Ma Vk 18	29 Ke	29 La
30 Ke		30 La	30 Ti	30 To Helatorstai	30 Su
31 To Q3		31 Su Kesäaika alkaa D9		31 Pe	

Exam week (Helmikuu 18–22)

Break (Maaliskuu 4–8)

L = Lecture; hall T5, Tue 12–14
Q = Q & A session; hall T5, Thu 12–14
D = Problem set deadline; Sun 20:00
T = Tutorial (model solutions); hall T6, Mon 16–18

Recap of last week

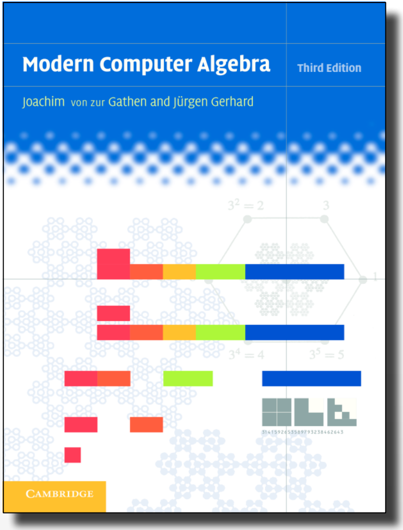
- Prime fields (the integers modulo a prime)
- **Irreducible polynomial**, existence of irreducible polynomials
- **Fermat's Little Theorem** and its generalization (exercise)
- **Finite fields** of **prime power order** via irreducible polynomials (exercise)
- The **characteristic** of a ring; fields have either zero or prime characteristic
- **Extension field**, **subfield**, **degree** of an extension
- **Algebraic** and **transcendental** elements of a field extension;
  the **minimal polynomial** of an algebraic element
- **Multiplicative order** of a nonzero element in a finite field;
  the multiplicative group of a finite field is cyclic
- **Formal derivative** of a polynomial with coefficients in a field (exercise)

Motivation for this and next week

- A tantalizing case where the connection between polynomials and integers apparently breaks down occurs with **factoring**
- Namely, it is known how to efficiently factor a given univariate polynomial over a finite field into its irreducible components, whereas no such algorithms are known for factoring a given integer into its prime factors
- This week we develop one efficient factoring algorithm for univariate polynomials over a finite field
- The best known algorithms for factoring integers run in time that scales moderately exponentially in the number of digits in the input; next week we study one such algorithm

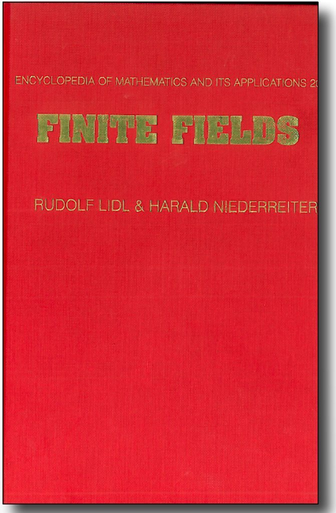
Factoring polynomials over finite fields

(von zur Gathen and Gerhard [11],
Sections 14.1–3, 14.6)



Finite fields

(Lidl and Niedderreiter [19])



Key content for Lecture 8

- **Factoring** a monic polynomial into monic **irreducible polynomials** over a finite field
- **Square-and-multiply** algorithm for **modular exponentiation** (exercise)
- The **squarefree part** of a polynomial
  - Computing the squarefree part using the **formal derivative**, greatest common divisors, and modular exponentiation (exercise)
- The **distinct-degree factorization** of a squarefree polynomial
  - Computing the distinct-degree factorization using **extended Fermat's little theorem**, modular exponentiation, and greatest common divisors
- The **equal-degree factorization** of a polynomial with known identical degrees for the irreducible factors
  - **Cantor–Zassenhaus algorithm** and random **splitting polynomials** (analysis: exercise)

Irreducible polynomial

- Let q be a prime power
- Let $\mathbb{F}_q$ be the finite field with q elements
- We say that a polynomial $f \in \mathbb{F}_q[x]$ is **irreducible** if $f \notin \mathbb{F}_q$ and for any $g, h \in \mathbb{F}_q[x]$ with $f = gh$ we have $g \in \mathbb{F}_q$ or $h \in \mathbb{F}_q$

- Let us also recall that we say that $f \in \mathbb{F}_q[x]$ is **monic** if its leading coefficient is 1

Factorization into irreducible polynomials

- Let $f \in \mathbb{F}_q[x]$
- The **factorization** of f consists of distinct monic irreducible polynomials $f_1, f_2, \ldots, f_r \in \mathbb{F}_q[x]$ and integers $d_1, d_2, \ldots, d_r \in \mathbb{Z}_{\geq 1}$ such that

$$f = \mathrm{lc}(f) f_1^{d_1} f_2^{d_2} \cdots f_r^{d_r}$$

- The factorization of f is unique up to ordering of the irreducible factors
- The polynomial f is **squarefree** if $d_1 = d_2 = \cdots = d_r = 1$

Example: Factorization into irreducible polynomials

- The factorization of

$$f = 2 + 2x + x^2 + 2x^4 + 2x^5 + 2x^6 + 2x^8 + 2x^9 + x^{10} + x^{11} + x^{12} + x^{13} \in \mathbb{F}_3[x]$$

  is

$$f = (1+x)^3(x^2+x+2)(x^2+1)(x^3+2x+2)^2$$

- Or what is the same,

$$\begin{aligned} f_1 &= 1 + x\,, & d_1 &= 3\,, \\ f_2 &= x^2 + x + 2\,, & d_2 &= 1\,, \\ f_3 &= x^2 + 1\,, & d_3 &= 1\,, \\ f_4 &= x^3 + 2x + 2\,, & d_4 &= 2 \end{aligned}$$

Preliminaries: Fast modular exponentiation

- Let $f, g \in \mathbb{F}_q[x]$ with $g \neq 0$, $\deg f, \deg g \leq d$ and $m \in \mathbb{Z}_{\geq 0}$
- Then, there exists an algorithm that computes $f^m \operatorname{rem} g$ in $O(M(d) \log m)$ operations in $\mathbb{F}_q$ (exercise)

Preliminaries: Greatest common divisor

- Let $f, g \in \mathbb{F}_q[x]$ such that at least one of f, g is nonzero
- Let us write $\gcd(f, g)$ for the monic greatest common divisor of f and g
- That is, in what follows we assume that $\mathrm{lc}(\gcd(f, g)) = 1$

Squarefree part

- Let $f = \mathrm{lc}(f) f_1^{d_1} f_2^{d_2} \cdots f_r^{d_r}$ be the factorization of $f \in \mathbb{F}_q[x]$
- The **squarefree part** of f is the (monic) polynomial $f_1 f_2 \cdots f_r$
- To factor f, it suffices to factor the squarefree part of f since f and its squarefree part have the same irreducible factors
- Indeed, given an irreducible factor f_j of f, it is easy to determine the maximum exponent $d_j \in \mathbb{Z}_{\geq 1}$ such that $f_j^{d_j}$ divides f

Example: Squarefree part

- The squarefree part of

$$2 + 2x + x^2 + 2x^4 + 2x^5 + 2x^6 + 2x^8 + 2x^9 + x^{10} + x^{11} + x^{12} + x^{13} \in \mathbb{F}_3[x]$$

is

$$1 + x + 2x^2 + x^5 + 2x^7 + x^8 \in \mathbb{F}_3[x]$$

The squarefree part and the formal derivative (1/2)

- Let p be the characteristic of $\mathbb{F}_q$; that is, q is a power of the prime p
- Let $f \in \mathbb{F}_q[x]$ be monic with factorization $f = f_1^{d_1} f_2^{d_2} \cdots f_r^{d_r}$
- Then, we have (exercise)

$$f' = \sum_{j=1}^{r} d_j f_j' \frac{f}{f_j} \tag{35}$$

- Furthermore, for all $i, j = 1, 2, \ldots, r$ we have that $f_i^{d_i}$ divides $d_j f_j' \frac{f}{f_j}$ when $i \neq j$
- When $i = j$, clearly $f_j^{d_j - 1}$ divides $d_j f_j' \frac{f}{f_j}$;
  furthermore, we have that $f_j^{d_j}$ divides $d_j f_j' \frac{f}{f_j}$ if and only if f_j divides $d_j f_j'$;
  since $\deg f_j' < \deg f_j$, we have that f_j divides $d_j f_j'$ if and only if p divides d_j

The squarefree part and the formal derivative (2/2)

- Set $u \leftarrow \gcd(f, f')$ and $v \leftarrow f/u$
- For $j = 1, 2, \ldots, r$, let

$$\delta_j = \begin{cases} 1 & \text{if } p \text{ does not divide } d_j; \\ 0 & \text{if } p \text{ divides } d_j \end{cases}$$

- We have

$$u = f_1^{d_1-\delta_1} f_2^{d_2-\delta_2} \cdots f_r^{d_r-\delta_r}$$
$$v = f_1^{\delta_1} f_2^{\delta_2} \cdots f_r^{\delta_r}$$

- In particular, v is the squarefree part of f if $\delta_1 = \delta_2 = \cdots = \delta_r = 1$
- Otherwise, that is, when $\delta_j = 0$ for at least one j, we need to do some more work ...

Extracting a p^{th} power

- Recall that we have
$$f = f_1^{d_1} f_2^{d_2} \cdots f_r^{d_r}$$
$$v = f_1^{\delta_1} f_2^{\delta_2} \cdots f_r^{\delta_r}$$
- Let $w \leftarrow f / \gcd(f, v^{\deg f})$
(exercise: how do you compute w fast given f and v as input?)
- We have
$$w = f_1^{(1-\delta_1)d_1} f_2^{(1-\delta_1)d_2} \cdots f_r^{(1-\delta_r)d_r} = \prod_{p \mid d_j} f_j^{d_j}$$
- That is, we have that w is the p^{th} power of the polynomial $\prod_{p \mid d_j} f_j^{d_j/p}$
- To access the squarefree part of w (which, when multiplied with v, forms the squarefree part of f), it suffices to recurse on a p^{th} root of w
- Next we look at how to compute p^{th} roots ...

The structure of a p^{th} power in characteristic p

- Let p be the characteristic of $\mathbb{F}_q$
- Let $g = \sum_{i=0}^{d} \psi_i x^i \in \mathbb{F}_q[x]$
- By the multinomial theorem, we have

$$g^p = \sum_{\substack{0 \le j_0, j_1, \ldots, j_d \le p \\ j_0 + j_1 + \ldots + j_d = p}} \binom{p}{j_0, j_1, \ldots, j_d} \psi_0^{j_0} \psi_1^{j_1} \cdots \psi_d^{j_d} x^{\sum_{k=0}^{d} k j_k}$$

- Since p is prime, we have that p divides $\binom{p}{j_0, j_1, \ldots, j_d} = \frac{p!}{j_0! j_1! \cdots j_d!}$ unless there exists a $k = 0, 1, \ldots, d$ with $j_k = p$, in which case $\binom{p}{j_0, j_1, \ldots, j_d} = 1$
- Thus, we have

$$g^p = \sum_{i=0}^{d} \psi_i^p x^{pi}$$

Computing a p^{th} root of a p^{th} power in characteristic p

- Let p be the characteristic of $\mathbb{F}_q$
- Let $g = \sum_{i=0}^{d} \psi_i x^i \in \mathbb{F}_q[x]$
- From the previous slide, we have $g^p = \sum_{i=0}^{d} \psi_i^p x^{pi}$
- Suppose we are given $h = \sum_{i=0}^{d} \eta_i x^{pi}$ as input and we want to compute a p^{th} root of h
- By Fermat's little theorem, for $\eta = \psi^p$ with $\psi \in \mathbb{F}_q$ we have $\eta^{q/p} = (\psi^p)^{q/p} = \psi^q = \psi$
- Thus, we have $h = g^p$ for

$$g = \sum_{i=0}^{d} \eta_i^{q/p} x^i$$

(exercise: how do you compute $\eta^{q/p}$ fast, given $\eta \in \mathbb{F}_q$ together with q and p as input?)

Example: Computing the squarefree part

- Let us compute the squarefree part of $f = 2 + 2x + x^2 + 2x^4 + 2x^5 + 2x^6 + 2x^8 + 2x^9 + x^{10} + x^{11} + x^{12} + x^{13} \in \mathbb{F}_3[x]$
- We have

$$f' = 2 + 2x + 2x^3 + x^4 + x^7 + x^9 + 2x^{10} + x^{12}$$

- And thus

$$\begin{aligned} u &= \gcd(f, f') = 2 + 2x + 2x^4 + x^6 \\ v &= f/u = 1 + 2x^2 + x^3 + 2x^4 + 2x^5 + x^6 + x^7 \\ w &= 1 + x^3 \end{aligned}$$

- Since $w \neq 1$ we proceed to take the p^{th} root for $p = 3$, and obtain $w^{1/3} = 1 + x$
- The squarefree part of $w^{1/3}$ is trivially $1 + x$, so we obtain that

$$(1 + x)v = 1 + x + 2x^2 + x^5 + 2x^7 + x^8$$

is the squarefree part of f

Distinct-degree decomposition of a squarefree polynomial

- Let $g \in \mathbb{F}_q[x]$ be monic and squarefree of degree at least 1
- The **distinct-degree decomposition** of g is the sequence $g_1, g_2, \ldots, g_s \in \mathbb{F}_q[x]$ such that $g_s \neq 1$ and for all $i = 1, 2, \ldots, s$ we have that g_i is the product of all monic irreducible polynomials of degree i that divide g
- The distinct-degree decomposition of g is unique
- We also have $g = g_1 g_2 \cdots g_s$
- To factor g it suffices to factor each of $g_1, g_2, \ldots, g_s$

Example: Distinct-degree decomposition

- The polynomial

$$g = 1 + x + 2x^2 + x^5 + 2x^7 + x^8 \in \mathbb{F}_q[x]$$

  is monic and squarefree of degree at least 1

- The distinct-degree decomposition of g is

$$\begin{aligned} g_1 &= 1 + x \\ g_2 &= 2 + x + x^3 + x^4 \\ g_3 &= x^3 + 2x + 2 \end{aligned}$$

Extended Fermat's little theorem

Theorem 18 (Extended Fermat's little theorem)

Let q be a prime power and let $d \in \mathbb{Z}_{\geq 1}$. Then, $x^{q^d} - x \in \mathbb{F}_q[x]$ is the product of all monic irreducible polynomials in $\mathbb{F}_q[x]$ whose degree divides d

Proof.

(Exercise in last week's problem set) □

Computing the distinct-degree decomposition

- Let $g \in \mathbb{F}_q[x]$ be monic and squarefree of degree at least 1 given as input

1. Set $f \leftarrow g$, $h \leftarrow x$, and $i \leftarrow 1$
2. while $f \neq 1$ do
   a. Set $h \leftarrow h^q \operatorname{rem} f$ using fast modular exponentiation
   b. Set $g_i \leftarrow \gcd(h - x, f)$
   [here we have the invariants that $h - x \equiv x^{q^i} - x \pmod{f}$ and f has no irreducible factors of degree less than i]
   c. Set $f \leftarrow f/g_i$
   d. Set $i \leftarrow i + 1$
3. Set $s \leftarrow i - 1$
4. Output $g_1, g_2, \ldots, g_s$ as the distinct-degree decomposition of g and stop

Equal-degree factorization

- Let $f \in \mathbb{F}_q[x]$ be monic and squarefree of degree $n \in \mathbb{Z}_{\geq 1}$ such that all irreducible factors of f have degree $d \in \mathbb{Z}_{\geq 1}$
- The **equal-degree factorization** task is to factor f given both f and d as input
- Clearly we must have that d divides n, and the task is trivial if $d = n$
- Let us next look at one possible algorithm for equal-degree factorization ...

The Cantor–Zassenhaus algorithm (1/2)

- Let q be an **odd** prime power
- Let $f \in \mathbb{F}_q[x]$ be monic of degree $n = dr$ such that all $r \geq 2$ irreducible factors of f have degree d

1. Let $a \in \mathbb{F}_q[x]$ be a uniform random nonzero polynomial of degree at most $n - 1$
2. Let $g \leftarrow \gcd(a, f)$. If $g \neq 1$, then output g and stop
3. Compute $s \leftarrow a^{(q^d-1)/2} \operatorname{rem} f$ using fast modular exponentiation
4. Let $g \leftarrow \gcd(s - 1, f)$. If $g \neq 1$ and $g \neq f$, then output g and stop
5. Assert failure and stop

The Cantor–Zassenhaus algorithm (2/2)

- The Cantor–Zassenhaus algorithm outputs a proper divisor g of f (a **splitting polynomial** for f) with probability at least $1/2$
- We can repeat the algorithm until a proper divisor g is found, and then recurse on g and f/g as appropriate to complete the equal-degree factorization of f into the r irreducible factors, each of degree d

Analysis of the Cantor–Zassenhaus algorithm I

- Let $f = f_1 f_2 \dots f_r$ be the factorization of the input f
- Let a be a uniform random nonzero polynomial of degree at most $n - 1$
- If the algorithm stops in Step 2 we have that g splits f
- So suppose that we continue to Step 3; in this case a and f are coprime and thus a and f_j are coprime for each $j = 1, 2, \dots, r$
- By the Chinese Remainder Theorem, we have the isomorphism
$$\chi : \mathbb{F}_q[x]/\langle f \rangle \to \mathbb{F}_q[x]/\langle f_1 \rangle \times \mathbb{F}_q[x]/\langle f_2 \rangle \times \cdots \times \mathbb{F}_q[x]/\langle f_r \rangle$$
given for all $h \in \mathbb{F}_q/\langle f \rangle$ by $\chi(h) = (\chi_1(h), \chi_2(h), \dots, \chi_r(h))$ with $\chi_i(h) = h \operatorname{rem} f_i$ for all $i = 1, 2, \dots, r$
- Since each $f_i \in \mathbb{F}_q[x]$ is irreducible of degree d, we have that each $\mathbb{F}_q[x]/\langle f_i \rangle$ is isomorphic to $\mathbb{F}_{q^d}$

Analysis of the Cantor–Zassenhaus algorithm II

- We have $\chi_i(h) = 0$ if and only if f_i divides h
- In particular, h is a splitting polynomial for f if and only if there exist $i_0, i_{\neq 0} \in \{1, 2, \ldots, r\}$ such that $\chi_{i_0}(h) = 0$ and $\chi_{i_{\neq 0}}(h) \neq 0$
- Since χ is an isomorphism and a is coprime to each of $f_1, f_2, \ldots, f_r$, we have that $\chi_1(a), \chi_2(a), \ldots, \chi_r(a)$ are mutually independent uniform random elements in the multiplicative groups of $\mathbb{F}_q[x]/\langle f_1\rangle, \mathbb{F}_q[x]/\langle f_2\rangle, \ldots, \mathbb{F}_q[x]/\langle f_r\rangle$, each of which is isomorphic to the multiplicative group $\mathbb{F}_{q^d}^\times$
- Since q is odd and the multiplicative group $\mathbb{F}_{q^d}^\times$ is cyclic (recall last week), for a uniform random $b \in \mathbb{F}_{q^d}^\times$ we have $\Pr(b^{(q^d-1)/2} = 1) = \Pr(b^{(q^d-1)/2} = -1) = 1/2$ (exercise)
- Thus, we have that $\chi(a^{(q^d-1)/2})$ is a uniform random vector with entries in $\{-1, 1\}$
- In particular, with probability at least $1 - 2^{1-r}$ the vector $\chi(a^{(q^d-1)/2})$ has at least one 1-entry and at least one (-1)-entry

Analysis of the Cantor–Zassenhaus algorithm III

- Thus, since χ is an isomorphism, with probability at least $1 - 2^{1-r}$ the vector $\chi(a^{(q^d-1)/2} - 1)$ has at least one zero entry and at least one nonzero entry
- The algorithm thus outputs a splitting polynomial and stops in Step 4 with probability at least $1 - 2^{1-r} \geq 1/2$ since $r \geq 2$

Summary: Factoring a polynomial over a finite field (1/2)

- Let a monic $f \in \mathbb{F}_q[x]$ be given as input

1. Compute the squarefree part $g \in \mathbb{F}_q[x]$ of f
2. Compute the distinct-degree decomposition $g_1, g_2, \ldots, g_s \in \mathbb{F}_q[x]$ of g
3. For each $i = 1, 2, \ldots, s$, run an equal-degree factorization algorithm to factor g_i (e.g., for odd q, run Cantor–Zassenhaus algorithm)
4. Assemble all the monic irreducible factors $f_1, f_2, \ldots, f_r \in \mathbb{F}_q[x]$ obtained in Step 3
5. For each $j = 1, 2, \ldots, r$, compute the maximum exponent $d_j \in \mathbb{Z}_{\geq 1}$ such that $f_j^{d_j}$ divides f
6. Return the factorization $f = f_1^{d_1} f_2^{d_2} \cdots f_r^{d_r}$

Summary: Factoring a polynomial over a finite field (2/2)

- We have presented one possible algorithm for efficiently factoring a given polynomial $f \in \mathbb{F}_q[x]$ into its irreducible factors
- Here by efficient we mean that the number of operations in $\mathbb{F}_q$ executed by the algorithm is bounded by a polynomial in $\deg f$ and $\log q$
- More efficient algorithms are known (cf. von zur Gathen and Gerhard [11] and Kedlaya and Umans [16])

Three applications

- Find all roots of a polynomial
  - The irreducible factors of degree 1 correspond to the distinct roots
- Testing for irreducibility
  - Test that the squarefree part agrees with the polynomial and then compute a distinct-degree decomposition to decide irreducibility
- Constructing an irreducible monic polynomial of degree n
  - Draw a uniform random monic polynomial of degree n, and test for irreducibility using the test above; repeat until an irreducible polynomial is found
  - Recalling the counting lemma for irreducible polynomials from the previous lecture, in expectation $O(n)$ repeats are required

Recap of Lecture 8

- **Factoring** a monic polynomial into monic **irreducible polynomials** over a finite field
- **Square-and-multiply** algorithm for **modular exponentiation** (exercise)
- The **squarefree part** of a polynomial
  - Computing the squarefree part using the **formal derivative**, greatest common divisors, and modular exponentiation (exercise)
- The **distinct-degree factorization** of a squarefree polynomial
  - Computing the distinct-degree factorization using **extended Fermat's little theorem**, modular exponentiation, and greatest common divisors
- The **equal-degree factorization** of a polynomial with known identical degrees for the irreducible factors
  - **Cantor–Zassenhaus algorithm** and random **splitting polynomials** (analysis: exercise)