Polynomial factorization over finite fields

Pierre Lairez
Factorization reveals interesting phenomena

1. pick a random $f \in \mathbb{Q}[t, x, y]$
2. compute $\Delta = \text{disc}_x(\text{disc}_y(f))$
3. compute the irreducible factors of $\Delta$
Factorization reveals interesting phenomena

1. pick a random \( f \in \mathbb{Q}[t, x, y] \)
2. compute \( \Delta = \text{disc}_x(\text{disc}_y(f)) \)
3. compute the irreducible factors of \( \Delta \)

How to compute the irreducible factors of \( \Delta \)?

1st step: factorization over \( \mathbb{F}_q \), \( q \) odd
2nd step: factorization over \( \mathbb{Q} \)

Much easier than factorization over $\mathbb{Z}$!

$\mathbb{F}_p[x]$ has many similarities with $\mathbb{Z}$:

- Euclidean division
- the degree in $\mathbb{F}_p[x]$ matches the absolute value in $\mathbb{Z}$
- similar data representation
- similar (fast) multiplication algorithms
- (sometimes) similar algorithms for matrices over $\mathbb{F}_p[x]$ or $\mathbb{Z}$

Factorization is where analogy breaks down!
General factorization is undecidable

**Theorem (Van der Waerden 1930)**

There exist an effective field $K$ such that irreducibility in $K[x]$ is undecidable.

Proof:

Take $K = \mathbb{Q} \left\langle \prod_{i=1}^{p_{p_1} \cdot p_{p_2} \cdot \cdots} \right\rangle$, where $p_i$ is the $i$th prime number and $p_{p_1} \cdot p_{p_2} \cdot \cdots$ is an enumeration of the indices of the Turing machines that halt. For a given $n$, does $X^2 - n$ split over $K$?

The example itself is irrelevant. Interesting conclusion: No factorization algorithm for abstract fields.

General factorization is undecidable

**Theorem (Van der Waerden 1930)**

There exist an effective field $K$ such that irreducibility in $K[x]$ is undecidable.

**Proof**

Take $K = \mathbb{Q}[\sqrt{p_{i_1}}, \sqrt{p_{i_2}}, \ldots ]$, where $p_i$ is the $i$th prime number and $i_1, i_2, \ldots$ is an enumeration of the indices of the Turing machines that halt. For a given $n$, does $X^2 - n$ splits over $K$?
General factorization is undecidable

**Theorem (Van der Waerden 1930)**

There exist an effective field $K$ such that irreducibility in $K[x]$ is undecidable.

**Proof**

Take $K = \mathbb{Q}[\sqrt[p_{i_1}]{}, \sqrt[p_{i_2}]{}, \ldots ]$, where $p_i$ is the $i$th prime number and $i_1, i_2, \ldots$ is an enumeration of the indices of the Turing machines that halt. For a given $n$, does $X^2 - n$ splits over $K$?

The example itself is irrelevant. Interesting conclusion:

⚠️ No factorization algorithm for abstract fields.

We will deal with specific properties of finite fields.

1. Introduction

2. Basic algebra
   2.1 Finite fields
   2.2 Polynomials

3. Factorization algorithms
   3.1 Reduction to the squarefree case
   3.2 Berlekamp’s approach
   3.3 Cantor and Zassenhaus’ algorithm
   3.4 The full algorithm

4. Bonus
Lemma

If $K$ is a finite field, then $|K|$ is a power of a prime number.

Proof

$K$ is a $\mathbb{F}_p$-linear space, with $p = \text{char } K$, so $|K| = |\mathbb{F}_p|^\text{dim } K$. \qed
Lemma
If $K$ is a finite field, then $|K|$ is a power of a prime number.

Proof
$K$ is a $\mathbb{F}_p$-linear space, with $p = \text{char} K$, so $|K| = |\mathbb{F}_p|^\dim K$. □

We fix a prime number $p$ and an algebraic closure $\overline{\mathbb{F}}_p$ of $\mathbb{F}_p$.

Lemma
For any $q = p^n$, the set $\{x \in \overline{\mathbb{F}}_p \mid x^q = x\}$ is a subfield of $\overline{\mathbb{F}}_p$.

Proof
It is closed under multiplication, inverse and addition because $x \mapsto x^q$ is a field endomorphism.
Finite field II

**Definition**

For any prime power $q = p^n$, $\mathbb{F}_q \doteq \{ x \in \mathbb{F}_p | x^q = x \}$
Finite field II

Definition
For any prime power $q = p^n$, $\mathbb{F}_q \doteq \{ x \in \overline{\mathbb{F}}_p \mid x^q = x \}$

Theorem
For any finite field $K$, $K \cong \mathbb{F}_{|K|}$.

Proof
Let $q = p^n = |K|$. Since $K$ is a finite set, it is an algebraic extension of its prime field $\mathbb{F}_p$. So there is an embedding $\phi : K \hookrightarrow \overline{\mathbb{F}}_p$. Note that $K \cong \phi(K)$.

By Lagrange’s theorem applied to the multiplicative group $K^\times$, we have $x^q = x$ for any $x \in K$. So $\phi(K) \subseteq \mathbb{F}_q$. By equality of cardinality, $\phi(K) = \mathbb{F}_q$. $\square$
Irreducible polynomials I

Let $K$ be a field.
A polynomial $f \in K[x]$ is irreducible (over $K$) if it is not the product of two nonconstant polynomials.

**Lemma**

A polynomial $f \in K[x]$ is irreducible if and only if the quotient ring $K[x]/(f)$ is a field.

**Theorem**

For any $f \in K[x]$, there are distinct monic irreducible polynomials $g_1, \ldots, g_r$ and positive integers $e_1, \ldots, e_r$ such that $f = \text{lcm}(f)g_1^{e_1} \cdots g_r^{e_r}$.

They are uniquely determined up to permutation.
A polynomial $f \in K[x]$ is **squarefree** if $f$ is not divided by $h^2$ for any nonconstant $h \in K[x]$.

**Lemma**

Let $f \in K[x]$. The following are equivalent:

1. $f$ is squarefree;
2. the exponents in the irreducible factorization of $f$ are 1;
3. the quotient ring $K[x]/(f)$ is isomorphic to a product of fields;
4. zero is the only nilpotent element of $K[x]/(f)$.

For a polynomial $f$ which factors as $c \prod_i g_i^{e_i}$, the **squarefree part** of $f$ is $\prod_i g_i$.

⚠️ $\gcd(f, f') = 1 \Rightarrow f$ is squarefree. The converse is not true.
Squarefree polynomials II

Proof
Let \( f = c \prod_i g_i^{e_i} \) be the irreducible factorization of \( f \).

1 \( \Rightarrow \) 2. If \( e_i > 1 \) then \( g_i^2 \) divides \( f \), so \( f \) is not squarefree.

2 \( \Rightarrow \) 3. If \( f = c \prod_i g_i \) then \( K[x]/(f) = \prod_i K[x]/(g_i) \). Since \( g_i \) is irreducible, \( K[x]/(g_i) \) is a field.

3 \( \Rightarrow \) 4. Let \( (\alpha_1, \ldots, \alpha_r) \) be a nilpotent element of a product \( K_1 \times \cdots \times K_r \) of fields. That is \( (\alpha_1^n, \ldots, \alpha_r^n) = (0, \ldots, 0) \) for some \( n \geq 1 \). Since each \( K_i \) is a field, this implies \( \alpha_i = 0 \).

4 \( \Rightarrow \) 1. Assume, for contradiction, that there is some nonconstant polynomial \( h \) such that \( h^2 | f \). Write \( f = ah^2 \). Then \( ah \) is nilpotent in \( K[x]/(f) \). By hypothesis, \( ah \) is zero in this ring. So \( ah \) is divisible by \( f \). But \( \deg(ah) < \deg(f) \). \( \square \)
1. Introduction

2. Basic algebra
   2.1 Finite fields
   2.2 Polynomials

3. Factorization algorithms
   3.1 Reduction to the squarefree case
   3.2 Berlekamp’s approach
   3.3 Cantor and Zassenhaus’ algorithm
   3.4 The full algorithm

4. Bonus
Finite fields are perfect

Let \( q = p^n \) be a prime power.

**Lemma**

On \( \mathbb{F}_q \), the field endomorphism \( \text{Frob} : \alpha \mapsto \alpha^p \) is bijective with inverse \( \text{Frob}^{n-1} : \alpha \mapsto \alpha^{p^{n-1}} \).

**Proof**

\( \text{Frob} \) is injective, as any field endomorphism, and so bijective because \( \mathbb{F}_q \) is finite. \( \text{Frob}^n(\alpha) = \alpha^q = \alpha \) (Lagrange’s theorem), so \( \text{Frob}^{-1} = \text{Frob}^{n-1} \).

**Lemma**

For any \( f \in \mathbb{F}_q[x] \), if \( f' = 0 \), then \( f = g^p \) for some \( g \in \mathbb{F}_q[x] \).

**Proof**

Let \( f = \sum_i a_i x^i \). If \( f' = 0 \), then \( a_i = 0 \) unless \( p | i \).

So \( f = \sum_i a_{pi} x^{pi} = (\sum_i \text{Frob}^{-1}(a_{pi})x_i)^p \).
Reduction to squarefree

1:  **procedure** SquarefreePart($f$)
2:    if $f$ and $f'$ are coprime then
3:      return $f$
4:    else if $f' = 0$ then
5:      compute $g$ such that $f = g^p$
6:      return SquarefreePart($g$)
7:    else
8:      $h \leftarrow f / \gcd(f, f')$;  $g \leftarrow f / \gcd(f, h^{\deg f})$
9:      return $h \cdot $ SquarefreePart($g$)  \hspace{1cm} \triangleright \text{NB: } g' = 0

**Theorem**

On input $f \in \mathbb{F}_q[x]$ nonzero of degree $d$, SquarefreePart outputs the squarefree part of $f$ and performs $O(M(d) \log d + dp^{-1} \log q)$ operations in $\mathbb{F}_q$. 
Recap

\[ f \in \mathbb{F}_q[x] \]

\[ M(d) \log d + \frac{d}{p} \log q \]

squarefree part of \( f \)

\[ \text{irreducible factors of } f \]

\[ dM(d) \text{ with the naive algorithm} \]

irreducible decomposition of \( f \)
Berlekamp’s irreducibility test

Let $f \in \mathbb{F}_q[x]$ squarefree.
The map $Q : \alpha \mapsto \alpha^q$ is a $\mathbb{F}_q$-linear map on $\mathbb{F}_q[x]/(f)$.

**Theorem (Berlekamp 1967)**

$\dim_{\mathbb{F}_q} \ker(Q - \text{id})$ equals the number of irreducible factors of $f$.

**Proof**

Decompose $\mathbb{F}_q[x]/(f)$ as $L_1 \times \cdots \times L_r$, where each $L_i$ is an algebraic extension of $\mathbb{F}_q$. Each factor $L_i$ is stable under $Q$. In particular

$$\ker(Q - \text{id}) \simeq \prod_i \ker(Q - \text{id})|_{L_i}$$

$$= \prod_i \{\alpha \in L_i \mid \alpha^q = \alpha\} = \mathbb{F}_q^r. \quad \Box$$
Berlekamp’s irreducibility test

Let $f \in \mathbb{F}_q[x]$ squarefree.
The map $Q : \alpha \mapsto \alpha^q$ is a $\mathbb{F}_q$-linear map on $\mathbb{F}_q[x]/(f)$.

**Theorem (Berlekamp 1967)**

$\dim_{\mathbb{F}_q} \ker(Q - \text{id})$ equals the number of irreducible factors of $f$.

**Corollary**

Irreducibility in $\mathbb{F}_q[x]$ is decidable with $O(d^\omega + M(d) \log q)$ operations in $\mathbb{F}_q$, where $d$ is the degree.

Leads to a factorization algorithm, but we skip this part.

The quotient ring of a squarefree polynomial

\[ \mathbb{F}_q[x]/(f) \cong \mathbb{F}_q \times \mathbb{F}_q \times \mathbb{F}_q^2 \times \mathbb{F}_q^5 \times \mathbb{F}_q^5 \times \mathbb{F}_q^5 \]
The quotient ring of a squarefree polynomial

\[ \mathbb{F}_q / (f) \cong \mathbb{F}_q \times \mathbb{F}_q \times \mathbb{F}_{q^2} \times \mathbb{F}_{q^5} \times \mathbb{F}_{q^5} \times \mathbb{F}_{q^5} \]

\( Frob^n \) stabilizes the bottom row

\[ \ker(Frob^n - \text{id}) \]

\[ \mathbb{F}_q \times \mathbb{F}_q \times \mathbb{F}_q \times \mathbb{F}_q \times \mathbb{F}_q \times \mathbb{F}_q \]
1. Introduction

2. Basic algebra
   2.1 Finite fields
   2.2 Polynomials

3. Factorization algorithms
   3.1 Reduction to the squarefree case
   3.2 Berlekamp’s approach
   3.3 Cantor and Zassenhaus’ algorithm
   3.4 The full algorithm

4. Bonus
Distinct-degree factorization

\[ \eta \leftarrow \text{class of } x \]

\[
\mathbb{F}_q[x]/(f) \cong \mathbb{F}_q \times \mathbb{F}_q \times \mathbb{F}_q^2 \times \mathbb{F}_q^5 \times \mathbb{F}_q^5 \times \mathbb{F}_q^5
\]
Distinct-degree factorization

\[ \eta \leftarrow \text{class of } x \]
\[ \eta \leftarrow \eta^q \]

\[ \mathbb{F}_q \rightarrow x \rightarrow f \rightarrow \eta \]

\[ \mathbb{F}_q[\alpha]/(f) \cong \mathbb{F}_q \times \mathbb{F}_q \times \mathbb{F}_q^2 \times \mathbb{F}_q^5 \times \mathbb{F}_q^5 \times \mathbb{F}_q^5 \]
Distinct-degree factorization

\[ \eta \leftarrow \text{class of } x \]

\[ \eta \leftarrow \eta^q \]

\[ \eta \leftarrow \eta^q \]

\[ \mathbb{F}_q \beta^4 \]
\[ \mathbb{F}_q \beta^4 \]
\[ \mathbb{F}_q \beta^4 \]

\[ \mathbb{F}_q \beta^3 \]
\[ \mathbb{F}_q \beta^3 \]
\[ \mathbb{F}_q \beta^3 \]

\[ \mathbb{F}_q \beta^2 \]
\[ \mathbb{F}_q \beta^2 \]
\[ \mathbb{F}_q \beta^2 \]

\[ \mathbb{F}_q \alpha \]
\[ \mathbb{F}_q \beta \]
\[ \mathbb{F}_q \beta \]
\[ \mathbb{F}_q \beta \]

\[ \mathbb{F}_q \]
\[ \mathbb{F}_q \]
\[ \mathbb{F}_q \]
\[ \mathbb{F}_q \]
\[ \mathbb{F}_q \]
\[ \mathbb{F}_q \]

\[ \mathbb{F}_q[x]/(f) \cong \mathbb{F}_q \times \mathbb{F}_q \times \mathbb{F}_q^2 \times \mathbb{F}_q^5 \times \mathbb{F}_q^5 \times \mathbb{F}_q^5 \]
Distinct-degree factorization

\[ \eta \leftarrow \text{class of } x \]
\[ \eta \leftarrow \eta^q \]
\[ \eta \leftarrow \eta^q \]
\[ \eta \leftarrow \eta^q \]

\[ \mathbb{F}_q \beta^4 \]
\[ \mathbb{F}_q \beta^4 \]
\[ \mathbb{F}_q \beta^4 \]

\[ \mathbb{F}_q \beta^3 \]
\[ \mathbb{F}_q \beta^3 \]
\[ \mathbb{F}_q \beta^3 \]

\[ \mathbb{F}_q \beta^2 \]
\[ \mathbb{F}_q \beta^2 \]
\[ \mathbb{F}_q \beta^2 \]

\[ \mathbb{F}_q \alpha \]
\[ \mathbb{F}_q \beta \]
\[ \mathbb{F}_q \beta \]
\[ \mathbb{F}_q \beta \]

\[ \mathbb{F}_q \]
\[ \mathbb{F}_q \]
\[ \mathbb{F}_q \]
\[ \mathbb{F}_q \]
\[ \mathbb{F}_q \]
\[ \mathbb{F}_q \]

\[ \mathbb{F}_q[x]/(f) \cong \mathbb{F}_q \times \mathbb{F}_q \times \mathbb{F}_q^2 \times \mathbb{F}_q^5 \times \mathbb{F}_q^5 \times \mathbb{F}_q^5 \]
Distinct-degree factorization

$$\eta \leftarrow \text{class of } x$$

$$\eta \leftarrow \eta^q$$

$$\eta \leftarrow \eta^q$$

$$\eta \leftarrow \eta^q$$

$$\eta \leftarrow \eta^q$$

$$\mathbb{F}_q \beta^4 \times \mathbb{F}_q \beta^4 \times \mathbb{F}_q \beta^4$$

$$\mathbb{F}_q \beta^3 \times \mathbb{F}_q \beta^3 \times \mathbb{F}_q \beta^3$$

$$\mathbb{F}_q \beta^2 \times \mathbb{F}_q \beta^2 \times \mathbb{F}_q \beta^2$$

$$\mathbb{F}_q \alpha \times \mathbb{F}_q \beta \times \mathbb{F}_q \beta \times \mathbb{F}_q \beta$$

$$\mathbb{F}_q \times \mathbb{F}_q \times \mathbb{F}_q^2 \times \mathbb{F}_q^5 \times \mathbb{F}_q^5 \times \mathbb{F}_q^5$$

$$\mathbb{F}_q[x]/(f) \cong \mathbb{F}_q \times \mathbb{F}_q \times \mathbb{F}_q^2 \times \mathbb{F}_q^5 \times \mathbb{F}_q^5 \times \mathbb{F}_q^5$$
Distinct-degree factorization

\[ \eta \leftarrow \text{class of } x \]
\[ \eta \leftarrow \eta^q \]
\[ \eta \leftarrow \eta^q \]
\[ \eta \leftarrow \eta^q \]
\[ \eta \leftarrow \eta^q \]
\[ \eta \leftarrow \eta^q \]

\[ \mathbb{F}_q \beta^4 \]
\[ \mathbb{F}_q \beta^4 \]
\[ \mathbb{F}_q \beta^4 \]
\[ \mathbb{F}_q \beta^3 \]
\[ \mathbb{F}_q \beta^3 \]
\[ \mathbb{F}_q \beta^3 \]
\[ \mathbb{F}_q \beta^2 \]
\[ \mathbb{F}_q \beta^2 \]
\[ \mathbb{F}_q \beta^2 \]
\[ \mathbb{F}_q \alpha \]
\[ \mathbb{F}_q \beta \]
\[ \mathbb{F}_q \beta \]
\[ \mathbb{F}_q \beta \]
\[ \mathbb{F}_q \]
\[ \mathbb{F}_q \]
\[ \mathbb{F}_q \]
\[ \mathbb{F}_q \]
\[ \mathbb{F}_q \]
\[ \mathbb{F}_q \]
\[ \mathbb{F}_q \]
\[ \mathbb{F}_q \]
\[ \mathbb{F}_q \]

\[ \mathbb{F}_q [x] / (f) \simeq \mathbb{F}_q \times \mathbb{F}_q \times \mathbb{F}_q^2 \times \mathbb{F}_q^5 \times \mathbb{F}_q^5 \times \mathbb{F}_q^5 \]
A formula for irreducible polynomials I

As usual, let \( q = p^n \) be a prime power.

**Lemma**

Let \( \mathcal{P}_d = \{ g \in \mathbb{F}_q[x] \mid g \text{ is monic, irreducible and of degree } d \} \).

For any \( d \geq 1 \),

\[
x^{q^d} - x = \prod_{s \mid d} \prod_{g \in \mathcal{P}_s} g.
\]

A complete description of the irreducible polynomials over \( \mathbb{F}_q \)!

**Proof**

Omitted (we don’t really need it).
A trivial but key idea

**Lemma**

Let \( f \in K[x] \) be a squarefree polynomial. Let \( f = g_1 \cdots g_r \) be its irreducible decomposition.

Let \( \eta \in K[x]/(f) \) and \( (\eta_1, \ldots, \eta_r) \) the corresponding tuple under the isomorphism \( K[x]/(f) \cong K[x]/(g_1) \times \cdots \times K[x]/(g_r) \).

Then \( \gcd(f, \eta) = \prod_{i \text{ s.t. } \eta_i = 0} g_i \).

**Proof**

\( \eta_i = 0 \iff g_i | \eta \).

We want to find an \( \eta \) with some but not all zero components.
Distinct-degree factorization, the algorithm

**input** $f \in \mathbb{F}_q[x]$ monic and squarefree

**output** $g_1, \ldots, g_s \in \mathbb{F}_q[x]$ such that $f = g_1 \cdots g_s$ and the irreducible factors of $g_i$ have degree $i$.

1: $s \leftarrow 0$
2: $\eta \leftarrow x$
3: while $f$ is not constant do
4: \hspace{1em} $s \leftarrow s + 1$
5: \hspace{1em} $\eta \leftarrow \eta^q \mod f$
6: \hspace{1em} $g_s \leftarrow \gcd(\eta - x, f)$
7: \hspace{1em} $f \leftarrow f / g_s$
8: return $(g_1, \ldots, g_s)$

**Theorem**

The algorithm is correct and performs $O(dM(d) \log d + dM(d) \log q)$ operations in $\mathbb{F}_q$. 
Squares in $\mathbb{F}_q$

⚠️ Assumption: $q$ is odd

**Lemma**

Let $S_+ = \left\{ \alpha \in \mathbb{F}_q^\times \middle| \alpha^{\frac{q-1}{2}} = 1 \right\}$ and $S_- = \left\{ \alpha \in \mathbb{F}_q^\times \middle| \alpha^{\frac{q-1}{2}} = -1 \right\}$. Then

1. $\#S_+ = \#S_- = \frac{q-1}{2}
2. $\mathbb{F}_q^\times$ is the disjoint union of $S_+$ and $S_-$.

**Proof**

As the zero set of polynomials of degree $\frac{q-1}{2}$, $S_+$ and $S_-$ contain at most $\frac{q-1}{2}$ elements each.

For any $\alpha \in \mathbb{F}_q^\times$, $1 = \alpha^{q-1} = (\alpha^\frac{q-1}{2})^2$, so $\mathbb{F}_q^\times = S_+ \cup S_-$. The union is clearly disjoint. For cardinality reasons, $\#S_+ = \#S_- = \frac{q-1}{2}$. 

Polynomial factorization I | Factorization algorithms
Cantor and Zassenhaus’ idea

⚠ Assumption: \( q \) is odd

\[
\mathbb{F}_q[x]/(f) \simeq \mathbb{F}_{q^3} \times \mathbb{F}_{q^3} \times \mathbb{F}_{q^3} \times \mathbb{F}_{q^3} \times \mathbb{F}_{q^3}
\]
Cantor and Zassenhaus’ idea

⚠️ Assumption: $q$ is odd

\[
\mathbb{F}_q[x]/(f) \cong \mathbb{F}_{q^3} \times \mathbb{F}_{q^3} \times \mathbb{F}_{q^3} \times \mathbb{F}_{q^3} \times \mathbb{F}_{q^3}
\]

1. pick $\eta$ at random
Cantor and Zassenhaus’ idea

⚠️ Assumption: \( q \) is odd

\[
\begin{array}{ccccc}
= 0 & \neq 0 & \neq 0 & \neq 0 & \neq 0 \\
0 & * & * & * & * \\
0 & * & * & * & * \\
0 & * & * & * & * \\
\end{array}
\]

\[
\mathbb{F}_q[x]/(f) \cong \mathbb{F}_{q^3} \times \mathbb{F}_{q^3} \times \mathbb{F}_{q^3} \times \mathbb{F}_{q^3} \times \mathbb{F}_{q^3}
\]

1. pick \( \eta \) at random
Cantor and Zassenhaus’ idea

Assumption: \( q \) is odd

\[
\begin{align*}
\mathbb{F}_q[x]/(f) &\cong \mathbb{F}_{q^3} \times \mathbb{F}_{q^3} \times \mathbb{F}_{q^3} \times \mathbb{F}_{q^3} \times \mathbb{F}_{q^3}
\end{align*}
\]

1. pick \( \eta \) at random
Cantor and Zassenhaus’ idea

⚠️ Assumption: $q$ is odd

\[
\begin{align*}
0 & \in S_+ & 0 & \in S_+ & 0 & \in S_- & 0 & \in S_+ \\
0 & 0 & 0 & 0 & 0 & 0 & & \\
0 & 0 & 0 & 0 & 0 & 0 & & \\
0 & 1 & 1 & -1 & 1 & & & \\
\end{align*}
\]

\[
\mathbb{F}_q[x]/(f) \simeq \mathbb{F}_{q^3} \times \mathbb{F}_{q^3} \times \mathbb{F}_{q^3} \times \mathbb{F}_{q^3} \times \mathbb{F}_{q^3}
\]

1. pick $\eta$ at random

2. $\eta \leftarrow \eta^{\frac{q^3-1}{2}}$
Cantor and Zassenhaus’ idea

⚠️ Assumption: $q$ is odd

\[
\begin{align*}
= 0 & \in S_+ & \in S_+ & \in S_\_ & \in S_+ \\
0 & 0 & 0 & 0 & 0 \\
0 & 0 & 0 & 0 & 0 \\
0 & 1 & 1 & -1 & 1 \\
\end{align*}
\]

\[
\mathbb{F}_q[x]/(f) \simeq \mathbb{F}_{q^3} \times \mathbb{F}_{q^3} \times \mathbb{F}_{q^3} \times \mathbb{F}_{q^3} \times \mathbb{F}_{q^3}
\]

1. pick $\eta$ at random
2. $\eta \leftarrow \eta^{\frac{q^3-1}{2}}$
3. $f = \gcd(f, \eta) \gcd(f, \eta - 1) \gcd(f, \eta + 1)$
Cantor and Zassenhaus’ theorem I

⚠️ Assumption: $q$ is odd

**Theorem (Cantor, Zassenhaus 1981)**

Let $f \in \mathbb{F}_q[x]$ of degree $d$ such that all irreducible factors of $f$ have degree $s < d$. (Note that $s \mid d$.)

Let $\eta \in \mathbb{F}_q[x]$ be a polynomial of degree less than $d$.

Then

1. $f = \gcd(f, \eta) \cdot \gcd(f, \eta^{\frac{q^s-1}{2}} - 1) \cdot \gcd(f, \eta^{\frac{q^s-1}{2}} + 1)$

2. for at least 50% of the $q^d$ possible choice of $\eta$, the factorization above is nontrivial.

Cantor and Zassenhaus’ theorem II

Proof
We just proved the first point.
Concerning the second point, let $\eta \in \mathbb{F}_q[x]/(f)$ and $(\eta_1, \ldots, \eta_r)$ its decomposition in $\prod_i \mathbb{F}_q[x]/(g_i) = (\mathbb{F}_{q^s})^r$, where $f = g_1 \cdots g_r$. We have a trivial factorization if and only if the $\eta_i$ are all zero, or all in $S_+$ or all in $S_-$. Therefore

$$\operatorname{Prob} (\text{trivial factorization}) = \frac{1 + \# S_+^r + \# S_-^r}{\text{total number of choice}}$$

$$= q^{-d} \left( 1 + 2 \left( \frac{q^s - 1}{2} \right)^r \right)$$

$$\leq q^{-d} \left( 2^{1-r}(q^s)^r \right) = 2^{1-r} \leq \frac{1}{2}. \qed$$
Cantor and Zassenhaus’ algorithm

\textit{input} \; f \in \mathbb{F}_q[x] \text{ squarefree, } s < \deg f \text{ such that the irreducible factors of } f \text{ have degree } s

\textit{output} \; \text{the irreducible factors of } f

1: \textbf{procedure} \; \text{CZ}(f, s)
2: \quad \textbf{if} \; s = \deg f \; \textbf{then return} \; \{f\}
3: \quad \textbf{else if} \; f \; \textbf{is constant} \; \textbf{then return} \; \emptyset
4: \quad \textbf{else}
5: \quad \quad \text{pick } a_0, \ldots, a_{\deg f - 1} \in \mathbb{F}_q \text{ uniformly at random}
6: \quad \quad \eta \leftarrow \sum_{i=0}^{\deg f - 1} a_ix^i; \quad \eta \leftarrow \eta \frac{q^s - 1}{2} \mod f
7: \quad g_0 \leftarrow \gcd(f, \eta)
8: \quad g_+ \leftarrow \gcd(f, \eta - 1)
9: \quad g_- \leftarrow \gcd(f, \eta + 1) \quad \triangleright g_- = f / g_0 / g_+
10: \quad \textbf{return} \; \text{CZ}(g_0, s) \cup \text{CZ}(g_+, s) \cup \text{CZ}(g_-, s)
Complexity analysis

Excluding recursive calls, each call performs:

- $O(M(d) \log d)$ ops in $\mathbb{F}_q$ for the gcd computations
- $O(M(d) s \log q)$ ops in $\mathbb{F}_q$ for the exponentiation

A recursive call is trivial if the degree of its argument has not decreased. On average, there is no more than 50% trivial calls. There are $O(d)$ nontrivial calls. So there are $O(d)$ calls on average. This leads to a $O(sdM(d) \log q + dM(d) \log d)$ total average complexity.

⚠️ This is not a tight analysis!
Refined complexity analysis

Imagine a biased dice with 3 facets:
- a facet $\circ$ with probability $q^{-s} \leq \frac{1}{3}$
- two equiprobable facets $\oplus$ and $\ominus$

Game

Draw $r$ rows. At each turn, draw one dice for each row, and draw the corresponding symbol. Stop when each row is different.

Lemma

The game stops after $O(\log r)$ iterations on average.

Proof

The probability that the columns $i$ and $j$ are equal after $k$ iterations is at most $2^{-k}$. The probability that the columns are not all different after $k$ iterations is at most $r^22^{-k}$. □
Let us play
Let us play
Let us play
Let us play
Let us play
Let us play

Polynomial factorization I | Factorization algorithms
Let us play

(Probably more ○ than what would happen in practice.)
Another view of the game

This is the tree of recursive calls in CZ algorithm. The tree has height $O(\log r)$ on average. The sum of the cost of all computations at a given depth is $O(M(d)s \log q + M(d) \log d)$. Total average complexity: $O(\left((M(d)s \log q + M(d) \log d) \log r\right))$. 
The full algorithm...

1: **procedure** Factor($f$)
2: $f_{\text{squarefree}} \leftarrow \text{SquarefreePart}(f)$
3: $g_1, \ldots, g_s \leftarrow \text{DistinctDegreeFactor}(f_{\text{squarefree}})$
4: $\mathcal{I} \leftarrow \emptyset$
5: **for** $i \in \{1, \ldots, s\}$ **do**
6: $\mathcal{I} \leftarrow \mathcal{I} \cup \text{CZ}(g_i, i)$
7: $\mathcal{J} \leftarrow \emptyset$
8: **for** $g \in \mathcal{I}$ **do**
9: $e \leftarrow 0$
10: **repeat**
11: $f \leftarrow f / g$
12: $e \leftarrow e + 1$
13: **until** $g$ does not divides $f$
14: $\mathcal{J} \leftarrow \mathcal{J} \cup \{(g, e)\}$
15: **return** $\mathcal{J}$
...and its complexity

**Theorem (Cantor, Zassenhaus 1981)**

The algorithm above, on input \( f \in \mathbb{F}_q[x] \), outputs the irreducible factorization of \( f \) after \( O(dM(d)(\log d + \log q)) \) operations in \( \mathbb{F}_q \), where \( d = \deg f \).

**Major open question**

Can we factor polynomials over \( \mathbb{F}_q \) in deterministic polynomial time?

The iterated Frobenius algorithm

\[
\text{input } f \in \mathbb{F}_q[x], \eta \in \mathbb{F}_q[x], \text{ and } s \geq 1, \text{ with } \deg \eta < \deg f \\
\text{output } \eta^{q^{s-1}} \mod f
\]

1: \textbf{procedure} SuperFastExponentiation($f$, $\eta$, $s$)
2: \quad $\gamma_0 \leftarrow x$
3: \quad $\gamma_1 \leftarrow x^q \mod f$
4: \quad \textbf{while } $i \leq s - 1$ \textbf{do}
5: \quad \hspace{1em} \text{\smaller \textgreater multipoint evaluation over the ring } \mathbb{F}_q[x]/(f)
6: \quad \hspace{1em} \textbf{for } j \in \{1, \ldots, i\} \textbf{ do}
7: \quad \hspace{2em} $\gamma_{i+j} \leftarrow \gamma_i(\gamma_j) \mod f$
8: \quad \hspace{1em} $i \leftarrow 2i$
9: \quad \textbf{for } i \in \{1, \ldots, s\} \textbf{ do} \quad \text{\smaller \textgreater multipoint evaluation}
10: \quad \hspace{1em} $\alpha_i \leftarrow \eta(\gamma_i) \mod f$
11: \quad \textbf{return } (\alpha_0 \cdots \alpha_{s-1})^{q-1} \mod f
What is going on?

1. For any $\eta \in \mathbb{F}_q[x]$, $\eta^{q^j} \equiv \eta(x^{q^j}) \equiv \eta(x^{q^j} \mod f) \mod f$
What is going on?

1. For any $\eta \in \mathbb{F}_q[x]$, $\eta^{q^j} \equiv \eta(x^{q^j}) \equiv \eta(x^{q^j} \pmod f) \mod f$

2. Let $\gamma_i = x^{q^i} \mod f$.
   Using with $\eta = \gamma_i$, we have $\gamma_{i+j} \equiv (x^{q^i})^{q^j} \equiv \gamma_i \gamma_j \mod f$
What is going on?

1. For any $\eta \in \mathbb{F}_q[x]$, $\eta^{q^j} \equiv \eta(x^{q^j}) \equiv \eta(x^{q^j} \pmod{f}) \pmod{f}$

2. Let $\gamma_i = x^{q^i} \pmod{f}$.
   Using with $\eta = \gamma_i$, we have $\gamma_{i+j} \equiv (x^{q^i})^{q^j} \equiv \gamma_i(\gamma_j) \pmod{f}$

3. 
   
   $\eta^{q^{s-1}/2} = \left( \prod_{i=0}^{s-1} \eta^{q^i} \right)^{q^{-1}/2} 
   
   \equiv \left( \prod_{i=0}^{s-1} \eta(\gamma_i) \right)^{q^{-1}/2}$