Factoring Polynomials over Finite Fields

Enver Ozdemir

Enver, Ozdemir Factoring Polynomials over Finite Fields

イロト 不得 とくほ とくほとう

ъ

$\bigcirc \mathbb{F}_{p}, p \text{ is an odd prime.}$

- $f(x) \in \mathbb{F}_p[x]$
- **The Problem:** Find $f_i(x) \in \mathbb{F}_p[x]$, $f(x) = f_1(x) \dots f_n(x)$, $f_i(x)$ irreducible and coprime.

イロト 不得 とくほ とくほ とう

$\bigcirc \mathbb{F}_{p}, p \text{ is an odd prime.}$

2 $f(x) \in \mathbb{F}_{p}[x]$

The Problem: Find $f_i(x) \in \mathbb{F}_p[x]$, $f(x) = f_1(x) \dots f_n(x)$, $f_i(x)$ irreducible and coprime.

イロン 不得 とくほ とくほ とうほ

- $\bigcirc \mathbb{F}_{p}, p \text{ is an odd prime.}$
- 2 $f(x) \in \mathbb{F}_p[x]$
- **3** The Problem: Find $f_i(x) \in \mathbb{F}_p[x]$, $f(x) = f_1(x) \dots f_n(x)$, $f_i(x)$ irreducible and coprime.

イロト イポト イヨト イヨト

Berlekamp and Cantor-Zassenhaus (PARI etc.)

3 Berlekamp: Find $h(x) \in \mathbb{F}_p[x], h^p(x) \equiv h(x) \pmod{f(x)}$

$$gcd(h(x) - t, f(x))$$

- Cantor-Zassenhaus: $gcd(h(x)^{(p^d-1)/2} 1, f(x))$ each irreducible factor of f(x) is of degree *n*.
- probabilistic, $\sim 1/2$ chance for h(x)

ヘロン ヘアン ヘビン ヘビン

ъ

- Berlekamp and Cantor-Zassenhaus (PARI etc.)
- **2** Berlekamp: Find $h(x) \in \mathbb{F}_p[x]$, $h^p(x) \equiv h(x) \pmod{f(x)}$
- $3 \ \, \gcd(h(x)-t,f(x))$
- Cantor-Zassenhaus: $gcd(h(x)^{(p^d-1)/2} 1, f(x))$ each irreducible factor of f(x) is of degree *n*.
- probabilistic, $\sim 1/2$ chance for h(x)

<ロ> (四) (四) (三) (三) (三)

- Berlekamp and Cantor-Zassenhaus (PARI etc.)
- **2** Berlekamp: Find $h(x) \in \mathbb{F}_p[x]$, $h^p(x) \equiv h(x) \pmod{f(x)}$
- Cantor-Zassenhaus: $gcd(h(x)^{(p^d-1)/2} 1, f(x))$ each irreducible factor of f(x) is of degree *n*.
- **o** probabilistic, $\sim 1/2$ chance for h(x)

◆□ ▶ ◆□ ▶ ◆ □ ▶ ◆ □ ▶ ● □ ● ● ● ●

- Berlekamp and Cantor-Zassenhaus (PARI etc.)
- **2** Berlekamp: Find $h(x) \in \mathbb{F}_p[x]$, $h^p(x) \equiv h(x) \pmod{f(x)}$

$$gcd(h(x) - t, f(x))$$

- Cantor-Zassenhaus: $gcd(h(x)^{(p^d-1)/2} 1, f(x))$ each irreducible factor of f(x) is of degree *n*.
- **o** probabilistic, $\sim 1/2$ chance for h(x)

イロト 不得 とくほ とくほ とう

э.

What is a hyperelliptic curve The Jacobian Factoring f(x)

k is a finite field of characteristic different from 2.

- 2 $H: y^2 = f(x)$
- If (x) is a monic polynomial with simple roots and deg(f(x)) = 2g + 1

<ロ> (四) (四) (注) (注) (注) (注)

What is a hyperelliptic curve The Jacobian Factoring f(x)

k is a finite field of characteristic different from 2. H: y² = f(x)

If (x) is a monic polynomial with simple roots and deg(f(x)) = 2g + 1

イロン 不得 とくほ とくほ とうほ

What is a hyperelliptic curve The Jacobian Factoring f(x)

k is a finite field of characteristic different from 2.

2
$$H: y^2 = f(x)$$

f(x) is a monic polynomial with simple roots and deg(f(x)) = 2g + 1

イロト 不得 とくほ とくほ とう

What is a hyperelliptic curve The Jacobian Factoring f(x)

- $Iac(H) = \operatorname{Pic}^o(H)$
- Pic(*H*) = the group of all isomorphism classes of invertible $k[x, y]/(y^2 f(x))$ -modules.
- 3 $D \in \operatorname{Jac}(H)$
- the Mumford Representation: Unique pair of polynomials (u(x), v(x)) satisfying the followings
 - u(x) is monic
 - $\deg v(x) < \deg u(x) \le g$
 - $f(x) v(x)^2$ is a multiple of u(x)
- Cantor's Algorithm: Computing in Jac(H), only polynomial arithmetics

・ロ・ ・ 同・ ・ ヨ・ ・ ヨ・

What is a hyperelliptic curve The Jacobian Factoring f(x)

- $Iac(H) = \operatorname{Pic}^o(H)$
- Pic(*H*) = the group of all isomorphism classes of invertible $k[x, y]/(y^2 f(x))$ -modules.
- O ∈ Jac(H)
- the Mumford Representation: Unique pair of polynomials (u(x), v(x)) satisfying the followings
 - u(x) is monic
 - $\deg v(x) < \deg u(x) \le g$
 - $f(x) v(x)^2$ is a multiple of u(x)
- Cantor's Algorithm: Computing in Jac(H), only polynomial arithmetics

・ロ・ ・ 同・ ・ ヨ・ ・ ヨ・

What is a hyperelliptic curve The Jacobian Factoring f(x)

- $Iac(H) = \operatorname{Pic}^o(H)$
- Pic(*H*) = the group of all isomorphism classes of invertible $k[x, y]/(y^2 f(x))$ -modules.
- $D \in \operatorname{Jac}(H)$
- the Mumford Representation: Unique pair of polynomials (u(x), v(x)) satisfying the followings
 - u(x) is monic
 - $\deg v(x) < \deg u(x) \le g$
 - $f(x) v(x)^2$ is a multiple of u(x)
- Cantor's Algorithm: Computing in Jac(H), only polynomial arithmetics

What is a hyperelliptic curve The Jacobian Factoring f(x)

- $Iac(H) = \operatorname{Pic}^o(H)$
- Pic(*H*) = the group of all isomorphism classes of invertible $k[x, y]/(y^2 f(x))$ -modules.
- $D \in \operatorname{Jac}(H)$
- the Mumford Representation: Unique pair of polynomials (u(x), v(x)) satisfying the followings
 - u(x) is monic
 - $\deg v(x) < \deg u(x) \le g$
 - $f(x) v(x)^2$ is a multiple of u(x)
- Cantor's Algorithm: Computing in Jac(H), only polynomial arithmetics

What is a hyperelliptic curve The Jacobian Factoring f(x)

- $Iac(H) = \operatorname{Pic}^o(H)$
- Pic(*H*) = the group of all isomorphism classes of invertible $k[x, y]/(y^2 f(x))$ -modules.
- $D \in \operatorname{Jac}(H)$
- the Mumford Representation: Unique pair of polynomials (u(x), v(x)) satisfying the followings
 - u(x) is monic
 - $\deg v(x) < \deg u(x) \le g$
 - $f(x) v(x)^2$ is a multiple of u(x)
- Cantor's Algorithm: Computing in Jac(H), only polynomial arithmetics

What is a hyperelliptic curve The Jacobian Factoring f(x)

- $Iac(H) = \operatorname{Pic}^o(H)$
- Pic(*H*) = the group of all isomorphism classes of invertible $k[x, y]/(y^2 f(x))$ -modules.
- $D \in \operatorname{Jac}(H)$
- the Mumford Representation: Unique pair of polynomials (u(x), v(x)) satisfying the followings
 - u(x) is monic
 - $\deg v(x) < \deg u(x) \le g$
 - $f(x) v(x)^2$ is a multiple of u(x)
- Cantor's Algorithm: Computing in Jac(H), only polynomial arithmetics

What is a hyperelliptic curve The Jacobian Factoring f(x)

- $Iac(H) = \operatorname{Pic}^o(H)$
- Pic(*H*) = the group of all isomorphism classes of invertible $k[x, y]/(y^2 f(x))$ -modules.
- $D \in \operatorname{Jac}(H)$
- the Mumford Representation: Unique pair of polynomials (u(x), v(x)) satisfying the followings
 - u(x) is monic
 - $\deg v(x) < \deg u(x) \le g$
 - $f(x) v(x)^2$ is a multiple of u(x)
- Solution Cantor's Algorithm: Computing in Jac(H), only polynomial arithmetics

What is a hyperelliptic curve The Jacobian Factoring f(x)

• f(x) is square-free and reducible in k[x]

- $eqtint{black} 0 eqtilde{A} = 2g + 1 eqtilde$
- 3 $H: y^2 = f(x)$ over *k*
- 2-torsion points of Jac(H):
 - (u(x), 0)
 - deg $u(x) \leq g$
 - *f*(*x*) is divisible by *u*(*x*)

・ロト ・ 理 ト ・ ヨ ト ・

What is a hyperelliptic curve The Jacobian Factoring f(x)

• f(x) is square-free and reducible in k[x]

- 2 $\deg f(x) = 2g + 1$
- 3 $H: y^2 = f(x)$ over *k*
- 2-torsion points of Jac(H):
 - (u(x), 0)
 - deg $u(x) \leq g$
 - *f*(*x*) is divisible by *u*(*x*)

・ロト ・ 理 ト ・ ヨ ト ・

What is a hyperelliptic curve The Jacobian Factoring f(x)

- f(x) is square-free and reducible in k[x]
- 2 $\deg f(x) = 2g + 1$
- **3** $H: y^2 = f(x)$ over *k*
- 2-torsion points of Jac(H):
 - (u(x), 0)
 - deg $u(x) \leq g$
 - *f*(*x*) is divisible by *u*(*x*)

・ロ・ ・ 同・ ・ ヨ・ ・ ヨ・

What is a hyperelliptic curve The Jacobian Factoring f(x)

- f(x) is square-free and reducible in k[x]
- 2 degf(x) = 2g + 1
- 3 $H: y^2 = f(x)$ over *k*
- 2-torsion points of Jac(H):
 - (*u*(*x*), 0)
 - deg $u(x) \leq g$
 - *f*(*x*) is divisible by *u*(*x*)

ヘロト 人間 とくほとく ほとう

What is a hyperelliptic curve The Jacobian Factoring f(x)

- f(x) is square-free and reducible in k[x]
- 2 degf(x) = 2g + 1
- 3 $H: y^2 = f(x)$ over *k*
- 2-torsion points of Jac(H):
 - (u(x), 0)
 - deg $u(x) \leq g$
 - f(x) is divisible by u(x)

ヘロン 人間 とくほ とくほ とう

What is a hyperelliptic curve The Jacobian Factoring f(x)

Finding a 2-torsion point in Jac(H)

Find a random D in Jac(H)

- 2 Find #Jac(H) = 2^em, (m, 2) = 1
- 3 $2^{i}m(D)$ is a 2-torsion point for some i < e if # D is even

Two big problems:

- Finding a random divisor class *D* in Jac(*H*)
- Finding the order of Jac(*H*)

くロト (過) (目) (日)

What is a hyperelliptic curve The Jacobian Factoring f(x)

Finding a 2-torsion point in Jac(H)

- Find a random D in Jac(H)
- 2 Find #Jac(H) = 2^em, (m, 2) = 1
 - 3 $2^{i}m(D)$ is a 2-torsion point for some i < e if # D is even
- Two big problems:
 - Finding a random divisor class *D* in Jac(*H*)
 - Finding the order of Jac(*H*)

くロト (過) (目) (日)

What is a hyperelliptic curve The Jacobian Factoring f(x)

Finding a 2-torsion point in Jac(H)

- **()** Find a random D in Jac(H)
- 2 Find #Jac(H) = 2^em, (m, 2) = 1
- 3 $2^{i}m(D)$ is a 2-torsion point for some i < e if # D is even
 - Two big problems:
 - Finding a random divisor class *D* in Jac(*H*)
 - Finding the order of Jac(*H*)

ヘロト 人間 ト ヘヨト ヘヨト

What is a hyperelliptic curve The Jacobian Factoring f(x)

Finding a 2-torsion point in Jac(H)

- **()** Find a random D in Jac(H)
- 2 Find #Jac(H) = 2^em, (m, 2) = 1
- **3** $2^i m(D)$ is a 2-torsion point for some i < e if # D is even
- Two big problems:
 - Finding a random divisor class D in Jac(H)
 - Finding the order of Jac(*H*)

くロト (過) (目) (日)

The Mumford Representation for Singular Hyperelliptic Curves

ヘロン ヘアン ヘビン ヘビン

1

• $H: y^2 = f(x), f(x)$ has repeated roots and $\deg f(x) = 2g + 1$

- Singular points: (a, 0) where a is a root of f(x) with multiplicity> 1
- 3 the Mumford Representation: any D ∈ Jac(H) is uniquely represented by a pair of polynomials (u(x), v(x)) satisfying the followings:
 - u(x) is monic
 - $\deg v(x) < \deg u(x) \le g$
 - $f(x) v(x)^2$ is divisible by u(x)
 - if both u(x) and v(x) are divisible by (x − a) for a singular point (a, 0) then (f − v(x)²)/u(x) is not divisible by (x − a)

The Mumford Representation for Singular Hyperelliptic Curves

・ロト ・ 理 ト ・ ヨ ト ・

- $H: y^2 = f(x), f(x)$ has repeated roots and $\deg f(x) = 2g + 1$
- Singular points: (a, 0) where *a* is a root of f(x) with multiplicity > 1
- Ithe Mumford Representation: any D ∈ Jac(H) is uniquely represented by a pair of polynomials (u(x), v(x)) satisfying the followings:
 - u(x) is monic
 - $\deg v(x) < \deg u(x) \le g$
 - $f(x) v(x)^2$ is divisible by u(x)
 - if both u(x) and v(x) are divisible by (x − a) for a singular point (a, 0) then (f − v(x)²)/u(x) is not divisible by (x − a)

The Mumford Representation for Singular Hyperelliptic Curves

- $H: y^2 = f(x), f(x)$ has repeated roots and $\deg f(x) = 2g + 1$
- Singular points: (a, 0) where a is a root of f(x) with multiplicity> 1
- So the Mumford Representation: any D ∈ Jac(H) is uniquely represented by a pair of polynomials (u(x), v(x)) satisfying the followings:
 - u(x) is monic
 - $\deg v(x) < \deg u(x) \le g$
 - $f(x) v(x)^2$ is divisible by u(x)
 - if both u(x) and v(x) are divisible by (x − a) for a singular point (a, 0) then (f − v(x)²)/u(x) is not divisible by (x − a)

The Mumford Representation for Singular Hyperelliptic Curves

- $H: y^2 = f(x), f(x)$ has repeated roots and $\deg f(x) = 2g + 1$
- Singular points: (a, 0) where a is a root of f(x) with multiplicity> 1
- So the Mumford Representation: any D ∈ Jac(H) is uniquely represented by a pair of polynomials (u(x), v(x)) satisfying the followings:
 - u(x) is monic
 - $\deg v(x) < \deg u(x) \le g$
 - $f(x) v(x)^2$ is divisible by u(x)
 - if both u(x) and v(x) are divisible by (x − a) for a singular point (a, 0) then (f − v(x)²)/u(x) is not divisible by (x − a)

The Mumford Representation for Singular Hyperelliptic Curves

ヘロン 人間 とくほ とくほ とう

- $H: y^2 = f(x), f(x)$ has repeated roots and $\deg f(x) = 2g + 1$
- Singular points: (a, 0) where a is a root of f(x) with multiplicity> 1
- So the Mumford Representation: any D ∈ Jac(H) is uniquely represented by a pair of polynomials (u(x), v(x)) satisfying the followings:
 - u(x) is monic
 - $\deg v(x) < \deg u(x) \le g$
 - $f(x) v(x)^2$ is divisible by u(x)
 - if both u(x) and v(x) are divisible by (x − a) for a singular point (a, 0) then (f − v(x)²)/u(x) is not divisible by (x − a)

The Mumford Representation for Singular Hyperelliptic Curves

ヘロン 人間 とくほ とくほ とう

- $H: y^2 = f(x), f(x)$ has repeated roots and $\deg f(x) = 2g + 1$
- Singular points: (a, 0) where a is a root of f(x) with multiplicity> 1
- So the Mumford Representation: any D ∈ Jac(H) is uniquely represented by a pair of polynomials (u(x), v(x)) satisfying the followings:
 - u(x) is monic
 - $\deg v(x) < \deg u(x) \le g$
 - $f(x) v(x)^2$ is divisible by u(x)
 - if both u(x) and v(x) are divisible by (x − a) for a singular point (a, 0) then (f − v(x)²)/u(x) is not divisible by (x − a)

The Algorithm for factoring f(x)

k = F_p, p f(x) = f₁(x) ··· f_n(x), degf_i(x) = d_i H : y² = xf(x)² Jac(H) = G₁ ⊕ ··· ⊕ G_n

◆□ ▶ ◆□ ▶ ◆ □ ▶ ◆ □ ▶ ● □ ● ● ● ●

The Algorithm for factoring f(x)

• $k = \mathbb{F}_p, p$ • $f(x) = f_1(x) \cdots f_n(x), \deg f_i(x) = d_i$ • $H : y^2 = xf(x)^2$ • $\operatorname{Jac}(H) = \mathbb{G}_1 \oplus \cdots \oplus \mathbb{G}_n$

Enver, Ozdemir Factoring Polynomials over Finite Fields

◆□ ▶ ◆□ ▶ ◆ □ ▶ ◆ □ ▶ ● □ ● ● ● ●

The Algorithm for factoring f(x)

•
$$k = \mathbb{F}_p, p$$

• $f(x) = f_1(x) \cdots f_n(x), \deg f_i(x) = d_i$
• $H : y^2 = xf(x)^2$
• $\operatorname{Jac}(H) = \mathbb{G}_1 \oplus \cdots \oplus \mathbb{G}_n$

Enver, Ozdemir Factoring Polynomials over Finite Fields

The Algorithm for factoring f(x)

•
$$k = \mathbb{F}_p, p$$

• $f(x) = f_1(x) \cdots f_n(x), \deg f_i(x) = d_i$
• $H : y^2 = xf(x)^2$
• $\operatorname{Jac}(H) = \mathbb{G}_1 \bigoplus \cdots \bigoplus \mathbb{G}_n$

- Any D
 ∈ Jac(H) is uniquely represented by a pair of the form [f(x)², h(x)f(x)] such that deg(h(x)) < deg(f(x)) and f(x) divides f(x)</p>
- $\bigcirc \#D_i$ divides either $p^{d_i} + 1$ or $p^{d_i} 1$
- $D = [f(x)^2, h(x)f(x)] = D_1 + \cdots + D_n$ such that $D_i \in \mathbb{G}_i$
- if a power D annihilates some of D_i we get a non-trivial factor of f(x)
- $D = D_1 + \dots + D_s \dots + D_r =$ $[f_1^2, h_1g_1] + \dots + [f_s^2 + h_sf_s] + \dots + [f_r^2, h_rf_r]$
- $mD_s = 0,$ $mD = [f_1^2, \tilde{h}_1 g_1] + \dots + 0 + \dots + [f_r^2, \tilde{h}_r f_r] = [f_1^2 f_2^2 \cdots f_r^2, \dots]$
- (a) $(p^{j} \pm 1)D$ for $j = 1, ..., \tilde{d} = \max\{d_{i}\}$, gives a non-trivial factor or [1, 0]
- Ithe probability of getting a non-trivial factor is at least 1/2

- Any D
 ∈ Jac(H) is uniquely represented by a pair of the form [f(x)², h(x)f(x)] such that deg(h(x)) < deg(f(x)) and f(x) divides f(x)
- - 3 $\#D_i$ divides either $p^{d_i} + 1$ or $p^{d_i} 1$
- $D = [f(x)^2, h(x)f(x)] = D_1 + \cdots + D_n$ such that $D_i \in \mathbb{G}_i$
- if a power D annihilates some of D_i we get a non-trivial factor of f(x)
- $D = D_1 + \dots + D_s \dots + D_r =$ $[f_1^2, h_1g_1] + \dots + [f_s^2 + h_sf_s] + \dots + [f_r^2, h_rf_s] + \dots + [f_r^2, h_r$
- $mD_s = 0,$ $mD = [f_1^2, \tilde{h}_1 g_1] + \dots + 0 + \dots + [f_r^2, \tilde{h}_r f_r] = [f_1^2 f_2^2 \cdots f_r^2, \dots]$
- ($p^{j} \pm 1$)D for $j = 1, ..., \tilde{d} = \max\{d_{i}\}$, gives a non-trivial factor or [1,0]
- Ithe probability of getting a non-trivial factor is at least 1/2

- Any D
 ∈ Jac(H) is uniquely represented by a pair of the form [f(x)², h(x)f(x)] such that deg(h(x)) < deg(f(x)) and f(x) divides f(x)
- 3 $\#D_i$ divides either $p^{d_i} + 1$ or $p^{d_i} 1$
- $\bigcirc D = [f(x)^2, h(x)f(x)] = D_1 + \dots + D_n$ such that $D_i \in \mathbb{G}_i$
- if a power D annihilates some of D_i we get a non-trivial factor of f(x)
- $D = D_1 + \dots + D_s \dots + D_r = [f_1^2, h_1g_1] + \dots + [f_s^2 + h_sf_s] + \dots + [f_r^2, h_r]$
- $mD_s = 0,$ $mD = [f_1^2, \tilde{h}_1 g_1] + \dots + 0 + \dots + [f_r^2, \tilde{h}_r f_r] = [f_1^2 f_2^2 \cdots f_r^2, \dots]$
- (a) $(p^{j} \pm 1)D$ for $j = 1, ..., \tilde{d} = \max\{d_{i}\}$, gives a non-trivial factor or [1, 0]
- Ithe probability of getting a non-trivial factor is at least 1/2

- Any D
 ∈ Jac(H) is uniquely represented by a pair of the form [f(x)², h(x)f(x)] such that deg(h(x)) < deg(f(x)) and f(x) divides f(x)</p>
- $\#D_i$ divides either $p^{d_i} + 1$ or $p^{d_i} 1$
- $D = [f(x)^2, h(x)f(x)] = D_1 + \cdots + D_n$ such that $D_i \in \mathbb{G}_i$
- if a power D annihilates some of D_i we get a non-trivial factor of f(x)
- ⁽⁵⁾ $D = D_1 + \dots + D_s \dots + D_r = [f_1^2, h_1g_1] + \dots + [f_s^2 + h_sf_s] + \dots + [f_r^2, h_rf_s]$
- $mD_s = 0,$ $mD = [f_1^2, \tilde{h}_1 g_1] + \dots + 0 + \dots + [f_r^2, \tilde{h}_r f_r] = [f_1^2 f_2^2 \cdots f_r^2, \dots]$
- (a) $(p^{j} \pm 1)D$ for $j = 1, ..., \tilde{d} = \max\{d_{i}\}$, gives a non-trivial factor or [1, 0]
- Ithe probability of getting a non-trivial factor is at least 1/2

- Any D
 ∈ Jac(H) is uniquely represented by a pair of the form [f(x)², h(x)f(x)] such that deg(h(x)) < deg(f(x)) and f(x) divides f(x)</p>
- 3 $\#D_i$ divides either $p^{d_i} + 1$ or $p^{d_i} 1$
- $D = [f(x)^2, h(x)f(x)] = D_1 + \cdots + D_n$ such that $D_i \in \mathbb{G}_i$
- if a power D annihilates some of D_i we get a non-trivial factor of f(x)
- $D = D_1 + \dots + D_s \dots + D_r = [f_1^2, h_1g_1] + \dots + [f_s^2 + h_sf_s] + \dots + [f_r^2, h_r]$
- $O mD_s = 0,$
 - $mD = [f_1^2, \tilde{h}_1 g_1] + \dots + 0 + \dots + [f_r^2, \tilde{h}_r f_r] = [f_1^2 f_2^2 \cdots f_r^2, \cdots]$
- ($p^{j} \pm 1$)D for $j = 1, ..., \tilde{d} = \max\{d_{i}\}$, gives a non-trivial factor or [1,0]
- Ithe probability of getting a non-trivial factor is at least 1/2

- Any D
 ∈ Jac(H) is uniquely represented by a pair of the form [f(x)², h(x)f(x)] such that deg(h(x)) < deg(f(x)) and f(x) divides f(x)</p>
- $D_i = [f_i(x)^2, h_i(x)f_i(x)] \in \mathbb{G}_i, \deg h_i(x) < \deg(d_i)$
- 3 $\#D_i$ divides either $p^{d_i} + 1$ or $p^{d_i} 1$
- $D = [f(x)^2, h(x)f(x)] = D_1 + \cdots + D_n$ such that $D_i \in \mathbb{G}_i$
- if a power D annihilates some of D_i we get a non-trivial factor of f(x)
- $D = D_1 + \dots + D_s \dots + D_r = [f_1^2, h_1g_1] + \dots + [f_s^2 + h_sf_s] + \dots + [f_r^2, h_rf_r]$
- () $mD_s = 0,$
 - $mD = [f_1^2, \tilde{h}_1g_1] + \dots + \underbrace{0}_{\sim} + \dots + [f_r^2, \tilde{h}_rf_r] = [f_1^2f_2^2 \cdots f_r^2, \cdots]$
- (a) $(p^{j} \pm 1)D$ for $j = 1, ..., d = \max\{d_{i}\}$, gives a non-trivial factor or [1, 0]
- Ithe probability of getting a non-trivial factor is at least 1/2

- Any D
 ∈ Jac(H) is uniquely represented by a pair of the form [f(x)², h(x)f(x)] such that deg(h(x)) < deg(f(x)) and f(x) divides f(x)</p>
- 3 $\#D_i$ divides either $p^{d_i} + 1$ or $p^{d_i} 1$
- $D = [f(x)^2, h(x)f(x)] = D_1 + \cdots + D_n$ such that $D_i \in \mathbb{G}_i$
- if a power D annihilates some of D_i we get a non-trivial factor of f(x)
- $D = D_1 + \dots + D_s \dots + D_r = [f_1^2, h_1g_1] + \dots + [f_s^2 + h_sf_s] + \dots + [f_r^2, h_rf_r]$
- $mD_s = 0,$ $mD = [f_1^2, \tilde{h}_1g_1] + \dots + 0 + \dots + [f_r^2, \tilde{h}_rf_r] = [f_1^2f_2^2 \cdots f_r^2, \dots]$
- (i) $(p^{j} \pm 1)D$ for $j = 1, ..., \tilde{d} = \max\{d_{i}\}$, gives a non-trivial factor or [1, 0]
- the probability of getting a non-trivial factor is at least 1/2

- Any D
 ∈ Jac(H) is uniquely represented by a pair of the form [f(x)², h(x)f(x)] such that deg(h(x)) < deg(f(x)) and f(x) divides f(x)</p>
- 3 $\#D_i$ divides either $p^{d_i} + 1$ or $p^{d_i} 1$
- $D = [f(x)^2, h(x)f(x)] = D_1 + \cdots + D_n$ such that $D_i \in \mathbb{G}_i$
- if a power D annihilates some of D_i we get a non-trivial factor of f(x)
- $D = D_1 + \dots + D_s \dots + D_r = [f_1^2, h_1g_1] + \dots + [f_s^2 + h_sf_s] + \dots + [f_r^2, h_rf_r]$
- $mD_{s} = 0,$ $mD = [f_{1}^{2}, \tilde{h}_{1}g_{1}] + \dots + 0 + \dots + [f_{r}^{2}, \tilde{h}_{r}f_{r}] = [f_{1}^{2}f_{2}^{2} \cdots f_{r}^{2}, \dots]$
- ($p^{j} \pm 1$)*D* for $j = 1, ..., \tilde{d} = \max\{d_{i}\}$, gives a non-trivial factor or [1,0]
 -) the probability of getting a non-trivial factor is at least 1/2

- Any D
 ∈ Jac(H) is uniquely represented by a pair of the form [f(x)², h(x)f(x)] such that deg(h(x)) < deg(f(x)) and f(x) divides f(x)</p>
- 3 $\#D_i$ divides either $p^{d_i} + 1$ or $p^{d_i} 1$
- $D = [f(x)^2, h(x)f(x)] = D_1 + \cdots + D_n$ such that $D_i \in \mathbb{G}_i$
- if a power D annihilates some of D_i we get a non-trivial factor of f(x)
- $D = D_1 + \dots + D_s \dots + D_r = [f_1^2, h_1g_1] + \dots + [f_s^2 + h_sf_s] + \dots + [f_r^2, h_rf_r]$
- $mD_{s} = 0,$ $mD = [f_{1}^{2}, \tilde{h}_{1}g_{1}] + \dots + 0 + \dots + [f_{r}^{2}, \tilde{h}_{r}f_{r}] = [f_{1}^{2}f_{2}^{2} \cdots f_{r}^{2}, \dots]$
- $(p^{j} \pm 1)D$ for $j = 1, ..., \tilde{d} = \max\{d_{i}\}$, gives a non-trivial factor or [1, 0]
- the probability of getting a non-trivial factor is at least 1/2

The Algorithm for factoring f(x)

Suppose $(p^r \pm 1)D = [1, 0]$ and $p^r \pm 1 = 2^e m$, (m, 2) = 1

- if #D is even then 2^sm(D) must be a 2-torsion point for s = 0,..., e
- **2**-torsion points [x, 0], $[x\tilde{f}(x)^2, 0]$, $[\tilde{f}(x)^2, 0]$ such that $\tilde{f}(x)$ is a non-trivial factor of f(x)
- the probability of finding a non-trivial factor of f(x) in a single trial is at least 3/4
- this probability is close to 1/2 for C-Z and Berlekamp's algorithms

ヘロト 人間 ト ヘヨト ヘヨト

The Algorithm for factoring f(x)

- Suppose $(p^r \pm 1)D = [1, 0]$ and $p^r \pm 1 = 2^e m$, (m, 2) = 1
- if #D is even then 2^sm(D) must be a 2-torsion point for s = 0, ..., e
- Solution 2-torsion points [x, 0], $[x\tilde{f}(x)^2, 0]$, $[\tilde{f}(x)^2, 0]$ such that $\tilde{f}(x)$ is a non-trivial factor of f(x)
- the probability of finding a non-trivial factor of f(x) in a single trial is at least 3/4
- this probability is close to 1/2 for C-Z and Berlekamp's algorithms

ヘロト ヘアト ヘビト ヘビト

The Algorithm for factoring f(x)

- Suppose $(p^r \pm 1)D = [1, 0]$ and $p^r \pm 1 = 2^e m$, (m, 2) = 1
- if #D is even then 2^sm(D) must be a 2-torsion point for s = 0, ..., e
- Solution 2-torsion points [x, 0], $[x\tilde{f}(x)^2, 0]$, $[\tilde{f}(x)^2, 0]$ such that $\tilde{f}(x)$ is a non-trivial factor of f(x)
- the probability of finding a non-trivial factor of f(x) in a single trial is at least 3/4
- this probability is close to 1/2 for C-Z and Berlekamp's algorithms

ヘロン 人間 とくほ とくほ とう

- Suppose $(p^r \pm 1)D = [1, 0]$ and $p^r \pm 1 = 2^e m$, (m, 2) = 1
- if #D is even then 2^sm(D) must be a 2-torsion point for s = 0, ..., e
- Solution 2-torsion points [x, 0], $[x\tilde{f}(x)^2, 0]$, $[\tilde{f}(x)^2, 0]$ such that $\tilde{f}(x)$ is a non-trivial factor of f(x)
- the probability of finding a non-trivial factor of f(x) in a single trial is at least 3/4
- this probability is close to 1/2 for C-Z and Berlekamp's algorithms

<ロ> (四) (四) (三) (三) (三)

The Algorithm for factoring f(x)

- Suppose $(p^r \pm 1)D = [1, 0]$ and $p^r \pm 1 = 2^e m$, (m, 2) = 1
- if #D is even then 2^sm(D) must be a 2-torsion point for s = 0, ..., e
- Solution 2-torsion points [x, 0], $[x\tilde{f}(x)^2, 0]$, $[\tilde{f}(x)^2, 0]$ such that $\tilde{f}(x)$ is a non-trivial factor of f(x)
- the probability of finding a non-trivial factor of f(x) in a single trial is at least 3/4
- this probability is close to 1/2 for C-Z and Berlekamp's algorithms

The Algorithm for factoring f(x)

- Suppose $(p^r \pm 1)D = [1, 0]$ and $p^r \pm 1 = 2^e m$, (m, 2) = 1
- if #D is even then 2^sm(D) must be a 2-torsion point for s = 0, ..., e
- Solution 2-torsion points [x, 0], $[x\tilde{f}(x)^2, 0]$, $[\tilde{f}(x)^2, 0]$ such that $\tilde{f}(x)$ is a non-trivial factor of f(x)
- the probability of finding a non-trivial factor of f(x) in a single trial is at least 3/4
- this probability is close to 1/2 for C-Z and Berlekamp's algorithms

ヘロン 人間 とくほ とくほ とう