Factoring Polynomials over Finite Fields

Enver Ozdemir

1. $\mathbb{F}_p$, p 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.

1. $\mathbb{F}_p$, p 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.

1. $\mathbb{F}_p$, p 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.

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

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

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

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

1. k is a finite field of characteristic different from 2.
2. $H : y^2 = f(x)$
3. $f(x)$ is a monic polynomial with simple roots and $\deg(f(x)) = 2g + 1$

1. k is a finite field of characteristic different from 2.
2. $H : y^2 = f(x)$
3. $f(x)$ is a monic polynomial with simple roots and $\deg(f(x)) = 2g + 1$

1. k is a finite field of characteristic different from 2.
2. $H : y^2 = f(x)$
3. $f(x)$ is a monic polynomial with simple roots and $\deg(f(x)) = 2g + 1$

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

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

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

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

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

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

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

1. $f(x)$ is square-free and reducible in $k[x]$
2. $\deg f(x) = 2g + 1$
3. $H : y^2 = f(x)$ over k
4. 2-torsion points of Jac(H):
   - $(u(x), 0)$
   - $\deg u(x) \leq g$
   - $f(x)$ is divisible by $u(x)$

1. $f(x)$ is square-free and reducible in $k[x]$
2. $\deg f(x) = 2g + 1$
3. $H : y^2 = f(x)$ over k
4. 2-torsion points of Jac(H):
   - $(u(x), 0)$
   - $\deg u(x) \leq g$
   - $f(x)$ is divisible by $u(x)$

1. $f(x)$ is square-free and reducible in $k[x]$
2. $\deg f(x) = 2g + 1$
3. $H : y^2 = f(x)$ over k
4. 2-torsion points of Jac(H):
   - $(u(x), 0)$
   - $\deg u(x) \leq g$
   - $f(x)$ is divisible by $u(x)$

1. $f(x)$ is square-free and reducible in $k[x]$
2. $\deg f(x) = 2g + 1$
3. $H : y^2 = f(x)$ over k
4. 2-torsion points of Jac(H):
    - $(u(x), 0)$
    - $\deg u(x) \leq g$
    - $f(x)$ is divisible by $u(x)$

1. $f(x)$ is square-free and reducible in $k[x]$
2. $\deg f(x) = 2g + 1$
3. $H : y^2 = f(x)$ over k
4. 2-torsion points of Jac(H):
   - $(u(x), 0)$
   - deg $u(x) \leq g$
   - $f(x)$ is divisible by $u(x)$

Finding a 2-torsion point in Jac(H)

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

Finding a 2-torsion point in Jac(H)

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

Finding a 2-torsion point in Jac(H)

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

Finding a 2-torsion point in Jac(H)

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

1. $H : y^2 = f(x)$, $f(x)$ has repeated roots and $\deg f(x) = 2g + 1$
2. Singular points: $(a, 0)$ where a is a root of $f(x)$ with multiplicity > 1
3. the Mumford Representation: any $D \in \mathrm{Jac}(H)$ is uniquely represented by a pair of polynomials $(u(x), v(x))$ satisfying the followings:
    - $u(x)$ is monic
    - $\deg v(x) < \deg u(x) \leq g$
    - $f(x) - v(x)^2$ 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 $(x - a)$

1. $H : y^2 = f(x)$, $f(x)$ has repeated roots and $\deg f(x) = 2g + 1$
2. Singular points: $(a, 0)$ where a is a root of $f(x)$ with multiplicity > 1
3. the Mumford Representation: any $D \in \text{Jac}(H)$ is uniquely represented by a pair of polynomials $(u(x), v(x))$ satisfying the followings:
   - $u(x)$ is monic
   - $\deg v(x) < \deg u(x) \leq g$
   - $f(x) - v(x)^2$ 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 $(x - a)$

1. $H : y^2 = f(x)$, $f(x)$ has repeated roots and $\deg f(x) = 2g + 1$
2. Singular points: $(a, 0)$ where a is a root of $f(x)$ with multiplicity > 1
3. the Mumford Representation: any $D \in \mathrm{Jac}(H)$ is uniquely represented by a pair of polynomials $(u(x), v(x))$ satisfying the followings:
   - $u(x)$ is monic
   - $\deg v(x) < \deg u(x) \leq g$
   - $f(x) - v(x)^2$ 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 $(x - a)$

1. $H : y^2 = f(x)$, $f(x)$ has repeated roots and $\deg f(x) = 2g + 1$
2. Singular points: $(a, 0)$ where a is a root of $f(x)$ with multiplicity > 1
3. the Mumford Representation: any $D \in \mathrm{Jac}(H)$ is uniquely represented by a pair of polynomials $(u(x), v(x))$ satisfying the followings:
   - $u(x)$ is monic
   - $\deg v(x) < \deg u(x) \leq g$
   - $f(x) - v(x)^2$ 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 $(x - a)$

1. $H : y^2 = f(x)$, $f(x)$ has repeated roots and $\deg f(x) = 2g + 1$
2. Singular points: $(a, 0)$ where a is a root of $f(x)$ with multiplicity > 1
3. the Mumford Representation: any $D \in \mathrm{Jac}(H)$ is uniquely represented by a pair of polynomials $(u(x), v(x))$ satisfying the followings:
    - $u(x)$ is monic
    - $\deg v(x) < \deg u(x) \leq g$
    - $f(x) - v(x)^2$ 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 $(x - a)$

1. $H: y^2 = f(x)$, $f(x)$ has repeated roots and $\deg f(x) = 2g + 1$
2. Singular points: $(a, 0)$ where a is a root of $f(x)$ with multiplicity > 1
3. the Mumford Representation: any $D \in \mathrm{Jac}(H)$ is uniquely represented by a pair of polynomials $(u(x), v(x))$ satisfying the followings:
   - $u(x)$ is monic
   - $\deg v(x) < \deg u(x) \leq g$
   - $f(x) - v(x)^2$ 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 $(x - a)$

1. $k = \mathbb{F}_p$, p
2. $f(x) = f_1(x) \cdots f_n(x)$, $\deg f_i(x) = d_i$
3. $H : y^2 = xf(x)^2$
4. $\mathrm{Jac}(H) = \mathbb{G}_1 \bigoplus \cdots \bigoplus \mathbb{G}_n$

1. $k = \mathbb{F}_p$, p
2. $f(x) = f_1(x) \cdots f_n(x)$, $\deg f_i(x) = d_i$
3. $H : y^2 = xf(x)^2$
4. $\mathrm{Jac}(H) = \mathbb{G}_1 \bigoplus \cdots \bigoplus \mathbb{G}_n$

1. $k = \mathbb{F}_p$, p
2. $f(x) = f_1(x) \cdots f_n(x)$, $\deg f_i(x) = d_i$
3. $H : y^2 = xf(x)^2$
4. $\mathrm{Jac}(H) = \mathbb{G}_1 \bigoplus \cdots \bigoplus \mathbb{G}_n$

1. $k = \mathbb{F}_p$, p
2. $f(x) = f_1(x) \cdots f_n(x)$, $\deg f_i(x) = d_i$
3. $H : y^2 = xf(x)^2$
4. $\mathrm{Jac}(H) = \mathbb{G}_1 \bigoplus \cdots \bigoplus \mathbb{G}_n$

1. Any $\widetilde{D} \in \mathrm{Jac}(H)$ is uniquely represented by a pair of the form $[\widetilde{f}(x)^2, \widetilde{h}(x)\widetilde{f}(x)]$ such that $\deg(\widetilde{h}(x)) < \deg(\widetilde{f}(x))$ and $\widetilde{f}(x)$ divides $f(x)$
2. $D_i = [f_i(x)^2, h_i(x)f_i(x)] \in \mathbb{G}_i$, $\deg h_i(x) < \deg(d_i)$
3. $\#D_i$ divides either $p^{d_i} + 1$ or $p^{d_i} - 1$
4. $D = [f(x)^2, h(x)f(x)] = D_1 + \cdots + D_n$ such that $D_i \in \mathbb{G}_i$
5. if a power D annihilates some of D_i we get a non-trivial factor of $f(x)$
6. $D = D_1 + \cdots + D_s \cdots + D_r = [f_1^2, h_1 g_1] + \cdots + [f_s^2 + h_s f_s] + \cdots + [f_r^2, h_r f_r]$
7. $mD_s = 0$, $mD = [f_1^2, \widetilde{h}_1 g_1] + \cdots + 0 + \cdots + [f_r^2, \widetilde{h}_r f_r] = [f_1^2 f_2^2 \cdots f_r^2, \cdots]$
8. $(p^j \pm 1)D$ for $j = 1, \ldots, \widetilde{d} = \max\{d_i\}$, gives a non-trivial factor or $[1, 0]$
9. the probability of getting a non-trivial factor is at least 1/2

1. Any $\widetilde{D} \in \text{Jac}(H)$ is uniquely represented by a pair of the form $[\widetilde{f}(x)^2, \widetilde{h}(x)\widetilde{f}(x)]$ such that $\deg(\widetilde{h}(x)) < \deg(\widetilde{f}(x))$ and $\widetilde{f}(x)$ divides $f(x)$
2. $D_i = [f_i(x)^2, h_i(x)f_i(x)] \in \mathbb{G}_i$, $\deg h_i(x) < \deg(d_i)$
3. $\#D_i$ divides either $p^{d_i} + 1$ or $p^{d_i} - 1$
4. $D = [f(x)^2, h(x)f(x)] = D_1 + \cdots + D_n$ such that $D_i \in \mathbb{G}_i$
5. if a power D annihilates some of D_i we get a non-trivial factor of $f(x)$
6. $D = D_1 + \cdots + D_s \cdots + D_r = [f_1^2, h_1 g_1] + \cdots + [f_s^2 + h_s f_s] + \cdots + [f_r^2, h_r f_r]$
7. $mD_s = 0$, $mD = [f_1^2, \widetilde{h}_1 g_1] + \cdots + 0 + \cdots + [f_r^2, \widetilde{h}_r f_r] = [f_1^2 f_2^2 \cdots f_r^2, \cdots]$
8. $(p^j \pm 1)D$ for $j = 1, \ldots, \widetilde{d} = \max\{d_i\}$, gives a non-trivial factor or $[1, 0]$
9. the probability of getting a non-trivial factor is at least 1/2

1. Any $\widetilde{D} \in \text{Jac}(H)$ is uniquely represented by a pair of the form $[\widetilde{f}(x)^2, \widetilde{h}(x)\widetilde{f}(x)]$ such that $\deg(\widetilde{h}(x)) < \deg(\widetilde{f}(x))$ and $\widetilde{f}(x)$ divides $f(x)$
2. $D_i = [f_i(x)^2, h_i(x)f_i(x)] \in \mathbb{G}_i$, $\deg h_i(x) < \deg(d_i)$
3. $\# D_i$ divides either $p^{d_i} + 1$ or $p^{d_i} - 1$
4. $D = [f(x)^2, h(x)f(x)] = D_1 + \cdots + D_n$ such that $D_i \in \mathbb{G}_i$
5. if a power D annihilates some of D_i we get a non-trivial factor of $f(x)$
6. $D = D_1 + \cdots + D_s \cdots + D_r =$ $[f_1^2, h_1 g_1] + \cdots + [f_s^2 + h_s f_s] + \cdots + [f_r^2, h_r f_r]$
7. $mD_s = 0$, $mD = [f_1^2, \widetilde{h}_1 g_1] + \cdots + 0 + \cdots + [f_r^2, \widetilde{h}_r f_r] = [f_1^2 f_2^2 \cdots f_r^2, \cdots]$
8. $(p^j \pm 1)D$ for $j = 1, \ldots, \widetilde{d} = \max\{d_i\}$, gives a non-trivial factor or $[1, 0]$
9. the probability of getting a non-trivial factor is at least 1/2

1. Any $\widetilde{D} \in \mathrm{Jac}(H)$ is uniquely represented by a pair of the form $[\widetilde{f}(x)^2, \widetilde{h}(x)\widetilde{f}(x)]$ such that $\deg(\widetilde{h}(x)) <\deg(\widetilde{f}(x))$ and $\widetilde{f}(x)$ divides $f(x)$
2. $D_i = [f_i(x)^2, h_i(x)f_i(x)] \in \mathbb{G}_i$, $\deg h_i(x) <\deg(d_i)$
3. $\#D_i$ divides either $p^{d_i} + 1$ or $p^{d_i} - 1$
4. $D = [f(x)^2, h(x)f(x)] = D_1 + \cdots + D_n$ such that $D_i \in \mathbb{G}_i$
5. if a power D annihilates some of D_i we get a non-trivial factor of $f(x)$
6. $D = D_1 + \cdots + D_s \cdots + D_r =$ $[f_1^2, h_1 g_1] + \cdots + [f_s^2 + h_s f_s] + \cdots + [f_r^2, h_r f_r]$
7. $mD_s = 0$, $mD = [f_1^2, \widetilde{h}_1 g_1] + \cdots + 0 + \cdots + [f_r^2, \widetilde{h}_r f_r] = [f_1^2 f_2^2 \cdots f_r^2, \cdots]$
8. $(p^j \pm 1)D$ for $j = 1, \ldots, \widetilde{d} =\max\{d_i\}$, gives a non-trivial factor or $[1, 0]$
9. the probability of getting a non-trivial factor is at least 1/2

1. Any $\widetilde{D} \in \mathrm{Jac}(H)$ is uniquely represented by a pair of the form $[\widetilde{f}(x)^2, \widetilde{h}(x)\widetilde{f}(x)]$ such that $\deg(\widetilde{h}(x)) <\deg(\widetilde{f}(x))$ and $\widetilde{f}(x)$ divides $f(x)$
2. $D_i = [f_i(x)^2, h_i(x)f_i(x)] \in \mathbb{G}_i$, deg $h_i(x)$ $<\deg(d_i)$
3. $\#D_i$ divides either $p^{d_i} + 1$ or $p^{d_i} - 1$
4. $D = [f(x)^2, h(x)f(x)] = D_1 + \cdots + D_n$ such that $D_i \in \mathbb{G}_i$
5. if a power D annihilates some of D_i we get a non-trivial factor of $f(x)$
6. $D = D_1 + \cdots + D_s \cdots + D_r = [f_1^2, h_1 g_1] + \cdots + [f_s^2 + h_s f_s] + \cdots + [f_r^2, h_r f_r]$
7. $mD_s = 0$, $mD = [f_1^2, \widetilde{h}_1 g_1] + \cdots + 0 + \cdots + [f_r^2, \widetilde{h}_r f_r] = [f_1^2 f_2^2 \cdots f_r^2, \cdots]$
8. $(p^j \pm 1)D$ for $j = 1, \ldots, \widetilde{d} =\max\{d_i\}$, gives a non-trivial factor or $[1, 0]$
9. the probability of getting a non-trivial factor is at least 1/2

1. Any $\widetilde{D} \in \mathrm{Jac}(H)$ is uniquely represented by a pair of the form $[\widetilde{f}(x)^2, \widetilde{h}(x)\widetilde{f}(x)]$ such that $\deg(\widetilde{h}(x)) <\deg(\widetilde{f}(x))$ and $\widetilde{f}(x)$ divides $f(x)$
2. $D_i = [f_i(x)^2, h_i(x)f_i(x)] \in \mathbb{G}_i$, $\deg h_i(x) <\deg(d_i)$
3. $\#D_i$ divides either $p^{d_i} + 1$ or $p^{d_i} - 1$
4. $D = [f(x)^2, h(x)f(x)] = D_1 + \cdots + D_n$ such that $D_i \in \mathbb{G}_i$
5. if a power D annihilates some of D_i we get a non-trivial factor of $f(x)$
6. $D = D_1 + \cdots + D_s \cdots + D_r =$ $[f_1^2, h_1 g_1] + \cdots + [f_s^2 + h_s f_s] + \cdots + [f_r^2, h_r f_r]$
7. $mD_s = 0$, $mD = [f_1^2, \widetilde{h}_1 g_1] + \cdots + 0 + \cdots + [f_r^2, \widetilde{h}_r f_r] = [f_1^2 f_2^2 \cdots f_r^2, \cdots]$
8. $(p^j \pm 1)D$ for $j = 1, \ldots, \widetilde{d} = \max\{d_i\}$, gives a non-trivial factor or $[1, 0]$
9. the probability of getting a non-trivial factor is at least 1/2

1. Any $\widetilde{D} \in \mathrm{Jac}(H)$ is uniquely represented by a pair of the form $[\widetilde{f}(x)^2, \widetilde{h}(x)\widetilde{f}(x)]$ such that $\deg(\widetilde{h}(x)) < \deg(\widetilde{f}(x))$ and $\widetilde{f}(x)$ divides $f(x)$
2. $D_i = [f_i(x)^2, h_i(x)f_i(x)] \in \mathbb{G}_i$, deg $h_i(x) <$deg(d_i)
3. $\#D_i$ divides either $p^{d_i} + 1$ or $p^{d_i} - 1$
4. $D = [f(x)^2, h(x)f(x)] = D_1 + \cdots + D_n$ such that $D_i \in \mathbb{G}_i$
5. if a power D annihilates some of D_i we get a non-trivial factor of $f(x)$
6. $D = D_1 + \cdots + D_s \cdots + D_r =$ $[f_1^2, h_1 g_1] + \cdots + [f_s^2 + h_s f_s] + \cdots + [f_r^2, h_r f_r]$
7. $mD_s = 0$, $mD = [f_1^2, \widetilde{h}_1 g_1] + \cdots + 0 + \cdots + [f_r^2, \widetilde{h}_r f_r] = [f_1^2 f_2^2 \cdots f_r^2, \cdots]$
8. $(p^j \pm 1)D$ for $j = 1, \ldots, \widetilde{d} =max\{d_i\}$, gives a non-trivial factor or $[1, 0]$
9. the probability of getting a non-trivial factor is at least 1/2

1. Any $\widetilde{D} \in \mathrm{Jac}(H)$ is uniquely represented by a pair of the form $[\widetilde{f}(x)^2, \widetilde{h}(x)\widetilde{f}(x)]$ such that $\deg(\widetilde{h}(x)) <\deg(\widetilde{f}(x))$ and $\widetilde{f}(x)$ divides $f(x)$
2. $D_i = [f_i(x)^2, h_i(x)f_i(x)] \in \mathbb{G}_i$, deg $h_i(x) <\deg(d_i)$
3. $\#D_i$ divides either $p^{d_i} + 1$ or $p^{d_i} - 1$
4. $D = [f(x)^2, h(x)f(x)] = D_1 + \cdots + D_n$ such that $D_i \in \mathbb{G}_i$
5. if a power D annihilates some of D_i we get a non-trivial factor of $f(x)$
6. $D = D_1 + \cdots + D_s \cdots + D_r =$ $[f_1^2, h_1 g_1] + \cdots + [f_s^2 + h_s f_s] + \cdots + [f_r^2, h_r f_r]$
7. $mD_s = 0$, $mD = [f_1^2, \widetilde{h}_1 g_1] + \cdots + 0 + \cdots + [f_r^2, \widetilde{h}_r f_r] = [f_1^2 f_2^2 \cdots f_r^2, \cdots]$
8. $(p^j \pm 1)D$ for $j = 1, \ldots, \widetilde{d} =\max\{d_i\}$, gives a non-trivial factor or $[1, 0]$
9. the probability of getting a non-trivial factor is at least 1/2

1. Any $\widetilde{D} \in \mathrm{Jac}(H)$ is uniquely represented by a pair of the form $[\widetilde{f}(x)^2, \widetilde{h}(x)\widetilde{f}(x)]$ such that $\deg(\widetilde{h}(x)) < \deg(\widetilde{f}(x))$ and $\widetilde{f}(x)$ divides $f(x)$
2. $D_i = [f_i(x)^2, h_i(x)f_i(x)] \in \mathbb{G}_i$, $\deg h_i(x) < \deg(d_i)$
3. $\# D_i$ divides either $p^{d_i} + 1$ or $p^{d_i} - 1$
4. $D = [f(x)^2, h(x)f(x)] = D_1 + \cdots + D_n$ such that $D_i \in \mathbb{G}_i$
5. if a power D annihilates some of D_i we get a non-trivial factor of $f(x)$
6. $D = D_1 + \cdots + D_s \cdots + D_r =$ $[f_1^2, h_1 g_1] + \cdots + [f_s^2 + h_s f_s] + \cdots + [f_r^2, h_r f_r]$
7. $mD_s = 0$, $mD = [f_1^2, \widetilde{h}_1 g_1] + \cdots + 0 + \cdots + [f_r^2, \widetilde{h}_r f_r] = [f_1^2 f_2^2 \cdots f_r^2, \cdots]$
8. $(p^j \pm 1)D$ for $j = 1, \ldots, \widetilde{d} = \max\{d_i\}$, gives a non-trivial factor or $[1, 0]$
9. the probability of getting a non-trivial factor is at least 1/2

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

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

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

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

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

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