Counting Points on the Jacobian Variety of a Hyperelliptic Curve defined by $y^2 = x^5 + ax$ over a Prime Field

E. Furukawa,* M. Kawazoe† and T. Takahashi‡

Abstract

Counting the order of the Jacobian group of a hyperelliptic curve over a finite field is very important for constructing a hyperelliptic curve cryptosystem (HECC), but known algorithms to compute the order of a Jacobian group over a given large prime field need very long running times. In this note, we propose a practical polynomial-time algorithm to compute the order of the Jacobian group for a hyperelliptic curve of type $y^2 = x^5 + ax$ over a given large prime field $\mathbb{F}_p$, e.g. an 80-bit field. We also investigate the order of the Jacobian group for such curve and determine the necessary condition to be suitable for HECC, that is, to satisfy that the order of the Jacobian group is of the form $l \cdot c$ where l is a prime number greater than about 2^{160} and c is a very small integer. Moreover we show some examples of a suitable curve for HECC obtained by using our algorithm.

1 Introduction

Let C be a hyperelliptic curve of genus 2 over $\mathbb{F}_q$. Let J_C be the Jacobian variety of C and $J_C(\mathbb{F}_q)$ the Jacobian group of C which is the set of $\mathbb{F}_q$-rational points of J_C. $J_C(\mathbb{F}_q)$ is a finite abelian group and we can construct a public-key-cryptosystem with it. The advantage of this system to an elliptic curve cryptosystem (ECC) is that we can construct a cryptosystem at the same security level as an elliptic one by using a defining field in a half size, that is, we need a 160-bit field to construct a secure ECC, but for a hyperelliptic curve cryptosystem (HECC) we only need an 80-bit field. The order of the Jacobian group of a hyperelliptic curve defined over an 80-bit field is about 160-bit. It is said that $\sharp J_C(\mathbb{F}_q) = c \cdot l$ where l is a prime number greater than about 2^{160} and c is a very small integer is suitable for HECC. We call a hyperelliptic curve "suitable for HECC" if its Jacobian group has such a suitable order.

As in the case of ECC, counting the order of the Jacobian group $J_C(\mathbb{F}_q)$ is very important for constructing HECC. But it is very difficult to count for a curve defined over an 80-bit field and there are very few results on it: Gaudry-Harley's algorithm [5] [9] can compute the order of a random hyperelliptic curve over an 80-bit field but their algorithm is useful

*Department of Mathematics and Information Sciences, Graduate School of Sciences, Osaka Prefecture University

†Department of Mathematics and Information Sciences, College of Integrated Arts and Sciences, Osaka Prefecture University; E-mail: kawazoe@mi.cias.osakafu-u.ac.jp

‡Department of Mathematics and Information Sciences, College of Integrated Arts and Sciences, Osaka Prefecture University; E-mail: takahasi@mi.cias.osakafu-u.ac.jp

only for an extension field of a small prime field. For a hyperelliptic curve with complex multiplication, there are known algorithms to construct a curve with its Jacobian group having a 160-bit prime factor. But these algorithms cannot be used to compute the order of a Jacobian group over a given defining field. Some other algorithms are known. But they need very long running times.

In this note, for a hyperelliptic curve C of type $y^2 = x^5 + ax$ over a large prime field $\mathbb{F}_p$, we propose a fast algorithm to compute the order of the Jacobian group $J_C(\mathbb{F}_p)$. In fact, the expected running time of our algorithm is $O(\ln^4 p)$. So our algorithm is practical for a curve over an 80-bit and much larger field. Moreover we investigate the order of the Jacobian group for the above curve and determine the necessary condition to be suitable for HECC. In the last section of this note, we show some examples of hyperelliptic curves suitable for HECC obtained by using our algorithm.

2 Basic facts on Jacobian varieties over a finite field

Here we recall basic facts on the order of Jacobian groups of hyperelliptic curves over a finite field. (cf. [5], [7])

2.1 General theory

Let p be a prime number, $\mathbb{F}_q$ is a finite field of order $q = p^l$ and C a hyperelliptic curve of genus g defined over $\mathbb{F}_q$. Then the defining equation of C is given as

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

where $f(x)$ is a polynomial in $\mathbb{F}_q[x]$ of degree $2g + 1$.

Let J_C be the Jacobian variety of a hyperelliptic curve C. We denote the group of $\mathbb{F}_q$-rational points on J_C by $J_C(\mathbb{F}_q)$. Let $\chi_q(t)$ be the characteristic polynomial of q-th power Frobenius endomorphism of C. Then, the order $\sharp J_C(\mathbb{F}_q)$ is given by

$$\sharp J_C(\mathbb{F}_q) = \chi_q(1).$$

The following "Hasse-Weil bound" is a famous inequality which bounds $\sharp J_C(\mathbb{F}_q)$.

$$\lceil (\sqrt{q} - 1)^{2g} \rceil \leq \sharp J(\mathbb{F}_q) \leq \lfloor (\sqrt{q} + 1)^{2g} \rfloor.$$

Due to Mumford [10], a point on $J_C(\mathbb{F}_q)$ can be represented by a pair $\langle u(x), v(x) \rangle$ where $u(x)$ and $v(x)$ are polynomials in $\mathbb{F}_q[x]$ with $\deg v(x) < \deg u(x) \leq 2$ such that $u(x)$ divides $f(x) - v(x)^2$. The identity element of the addition law is represented by $\langle 1, 0 \rangle$. We refer this representation as "Mumford representation" in the following. By using Mumford representation of a point on $J_C(\mathbb{F}_q)$, we obtain an algorithm for adding two points on $J_C(\mathbb{F}_q)$ (cf. Cantor's algorithm [2], Harley's algorithm [5]).

2.2 Hasse-Witt matrix and the order of $J_C(\mathbb{F}_q)$

There is a well-known method to calculate $\sharp J_C(\mathbb{F}_q) \pmod p$ by using the Hasse-Witt matrix. The method is based on the following two theorems.

Theorem 2.1 (Yui[12]). *Let $y^2 = f(x)$ with $\deg f = 2g + 1$ be the equation of a genus g hyperelliptic curve. Denote by c_i the coefficient of x^i in the polynomial $f(x)^{(p-1)/2}$. Then the Hasse-Witt matrix is given by*

$$A = (c_{ip-j})_{1 \leq i,j \leq g}.$$

For $A = (a_{ij})$, put $A^{(p^i)} = (a_{ij}^{p^i})$. Then we have the following theorem.

Theorem 2.2 (Manin[8]). *Let C be a curve of genus g defined over a finite field $\mathbb{F}_q$ where $q = p^l$. Let A be the Hasse-Witt matrix of C, and let $A_\phi = AA^{(p)}A^{(p)} \cdots A^{(p^{l-1})}$. Let $\kappa(t)$ be the characteristic polynomial of the matrix A_ϕ and χ_q the characteristic polynomial of the q-th power Frobenius endomorphism. Then*

$$\chi_q(t) \equiv (-1)^g t^g \kappa(t) \pmod{p}.$$

Due to the above two theorems, we can calculate $\sharp J_C(\mathbb{F}_q) \pmod{p}$ by the following formula.

$$\sharp J_C(\mathbb{F}_q) \equiv (-1)^g \kappa(1) \pmod{p}$$

But this method is not practical in general when p is very large.

3 Counting the number of points on Jacobian variety

We only consider the case of genus 2 in the following. Let $f(x)$ be a polynomial in $\mathbb{F}_q[x]$ of degree 5, C a hyperelliptic curve over $\mathbb{F}_q$ of genus 2 defined by the equation $y^2 = f(x)$. Then, the characteristic polynomial $\chi_q(t)$ of the q-th power Frobenius endomorphism of C is of the form:

$$\chi_q(t) = t^4 - s_1 t^3 + s_2 t^2 - s_1 q t + q^2, \quad s_i \in \mathbb{Z},$$
$$|s_1| \leq 4\sqrt{q}, \quad |s_2| \leq 6q.$$

Hence $J_C(\mathbb{F}_q)$ is given by the following formula:

$$\sharp J_C(\mathbb{F}_q) = q^2 + 1 - s_1(q+1) + s_2.$$

The following sharp bound is useful for calculating $\sharp J_C(\mathbb{F}_q)$.

Lemma 3.1 (cf. [9]). $\lceil 2\sqrt{q}|s_1| - 2q \rceil \leq s_2 \leq \lfloor s_1^2/4 + 2q \rfloor$

Here we consider how to calculate $\sharp J_C(\mathbb{F}_p) \pmod{p}$ when $q = p$.

Lemma 3.2. *Let c_i be the coefficient of x^i in $f(x)^{(p-1)/2}$. Then*

$$s_1 \equiv c_{p-1} + c_{2p-2} \pmod{p}$$
$$s_2 \equiv c_{p-1}c_{2p-2} + c_{p-2}c_{2p-1} \pmod{p}.$$

Proof. First of all, the matrix A in Theorem 2.1 is as follows.

$$A = \begin{pmatrix} c_{p-1} & c_{p-2} \\ c_{2p-1} & c_{2p-2} \end{pmatrix}.$$

Then we have

$$\kappa(t) = t^2 - (c_{p-1} + c_{2p-2})t + (c_{p-1}c_{2p-2} + c_{p-2}c_{2p-1})$$

and by Theorem 2.2 we have

$$t^4 - s_1 t^3 + s_2 t^2 \equiv t^4 - (c_{p-1} + c_{2p-2})t^3 + (c_{p-1}c_{2p-2} + c_{p-2}c_{2p-1})t^2 \pmod{p}.$$

Hence

$$s_1 \equiv c_{p-1} + c_{2p-2} \pmod{p}$$
$$s_2 \equiv c_{p-1}c_{2p-2} + c_{p-2}c_{2p-1} \pmod{p}$$

□

Remark 3.3. Since $|s_1| \leq 4\sqrt{p}$, if $p > 64$ then s_1 is uniquely determined by c_{p-1}, c_{2p-2}. Moreover, by Lemma 3.1, if $s_2 \pmod p$ is determined, then there are only at most five possibilities for the value of s_2.

When p is very large, it is difficult to calculate $s_i \pmod p$ in general even in the case of $g = 2$. But for hyperelliptic curves of special type, we can calculate them in a remarkably short time even when p is extremely large, e.g. 160-bit.

Now we show the following theorem which is essential to construct our algorithm.

Theorem 3.4. *Let a be an element of $\mathbb{F}_p$, C a hyperelliptic curve defined by the equation $y^2 = x^5 + ax$ and J_C the Jacobian variety of C. Then s_1, s_2 are given as follows.*

1. *if $p \equiv 1 \pmod 8$, then*

$$\begin{aligned} s_1 &\equiv (-1)^{(p-1)/8} 2c(a^{3(p-1)/8} + a^{(p-1)/8}) \pmod p, \\ s_2 &\equiv 4c^2 a^{(p-1)/2} \pmod p \end{aligned}$$

   where c is an integer satisfying $p = c^2 + 2d^2$, $c \equiv 1 \pmod 4$.

2. *if $p \equiv 3 \pmod 8$, then*

$$\begin{aligned} s_1 &\equiv 0 \pmod p, \\ s_2 &\equiv -4c^2 a^{(p-1)/2} \pmod p \end{aligned}$$

   where c is an integer such that $p = c^2 + 2d^2$.

3. *if otherwise, then $s_1 \equiv 0 \pmod p$, $s_2 \equiv 0 \pmod p$.*

Proof. Since

$$(x^5 + ax)^{(p-1)/2} = \sum_{i=0}^{(p-1)/2} \binom{(p-1)/2}{r} x^{4r+(p-1)/2} a^{(p-1)/2-r},$$

the necessary condition for an entry c_{ip-j} of the Hasse-Witt matrix $A = \begin{pmatrix} c_{p-1} & c_{p-2} \\ c_{2p-1} & c_{2p-2} \end{pmatrix}$ of C being non-zero is that there must be an integer r, $0 \leq r \leq (p-1)/2$ such that $4r + (p-1)/2 = ip - j$. Then there are the following three possibilities;

1. $p \equiv 1 \pmod 8 \Longrightarrow A = \begin{pmatrix} c_{p-1} & 0 \\ 0 & c_{2p-2} \end{pmatrix}$,
2. $p \equiv 3 \pmod 8 \Longrightarrow A = \begin{pmatrix} 0 & c_{p-2} \\ c_{2p-1} & 0 \end{pmatrix}$,
3. $p \not\equiv 1, 3 \pmod 8 \Longrightarrow A = O$.

Case (1). Put $f = (p-1)/8$. Then, since $4r + (p-1)/2 = p - 1$ for c_{p-1}, we have $r = (p-1)/8 = f$ and $c_{p-1} = \binom{4f}{f} a^{3f}$. For c_{2p-2}, since $4r + (p-1)/2 = 2p - 2$, we have $r = 3(p-1)/8 = 3f$ and $c_{2p-2} = \binom{4f}{3f} a^f$. Then from the result of Hudson-Williams [6, Theorem 11.2], we have

$$\binom{4f}{f} \equiv (-1)^f 2c \pmod p, \quad (p = c^2 + 2d^2,\ c \equiv 1 \pmod 4).$$

Since $\binom{4f}{f} = \binom{4f}{3f}$, we have the conclusion.

Case (2). By the condition, it is obvious that $s_1 \equiv 0 \pmod p$. Put $f = (p-3)/8$. Then, since $4r + (p-1)/2 = p-2$ for c_{p-2}, we have $r = (p-3)/8 = f$ and $c_{p-2} = \binom{4f+1}{f} a^{3f+1}$. For c_{2p-1}, since $4r + (p-1)/2 = 2p-1$, we have $r = (3p-1)/8 = 3f+1$ and $c_{2p-1} = \binom{4f+1}{3f+1} a^f$. From the result of Berndt-Evans-Williams [1, Theorem 12.9.7],

$$\binom{4f+1}{f} \equiv -2c \pmod p, \quad (p = c^2 + 2d^2,\ c \equiv (-1)^f \pmod 4).$$

Since $\binom{4f+1}{3f+1} = \binom{4f+1}{f}$, we have

$$\begin{aligned} s_2 &\equiv -\binom{4f+1}{f}^2 a^{4f+1} \pmod p \\ &\equiv -4c^2 a^{(p-1)/2} \pmod p \end{aligned}$$

Case (3). This is obvious. □

Remark 3.5. Note that the Jacobian variety of $y^2 = x^5 + ax$ has a point of order 2. Then the order of $J_C(\mathbb{F}_p)$ is always even. By Lemma 3.1, if $p > 64$, then there are only at most three possibilities for the value of s_2.

By using the above result, we can calculate (at most three) possibilities of $\sharp J_C(\mathbb{F}_p)$ in a very short time. Then to get $\sharp J_C(\mathbb{F}_p)$, we only have to multiply a random point on $J_C(\mathbb{F}_p)$ by each possible order.

The following remark is also important.

Remark 3.6. If $p > 16$ in (2) and (3), we have $s_1 = 0$.

4 Study on the order of Jacobian groups

Before considering about a counting-point algorithm, we study the order of the Jacobian group more precisely. Due to Theorem 3.4, we divide the situation into the following three cases: (1) $p \equiv 1 \pmod 8$, (2) $p \equiv 3 \pmod 8$, (3) $p \equiv 5, 7 \pmod 8$.

4.1 The case of $p \equiv 1 \pmod 8$

Lemma 4.1. *Let p be a prime number such that $p \equiv 1 \pmod 8$ and C a hyperelliptic curve over $\mathbb{F}_p$ defined by an equation $y^2 = x^5 + ax$. If $a^{(p-1)/2} = 1$, then 4 divides $\sharp J_C(\mathbb{F}_p)$. Moreover, if $a^{(p-1)/4} = 1$, then 16 divides $\sharp J_C(\mathbb{F}_p)$.*

Proof. First note that there is a primitive 8th root of unity, say ζ_8, in $\mathbb{F}_p$ because 8 divides $p-1$. If $a^{(p-1)/2} = 1$, then there exists an element $b \in \mathbb{F}_p$ such that $b^2 = a$. Then

$$x^5 + ax = x^5 + b^2 x = x(x^2 + \zeta_8^2 b)(x^2 - \zeta_8^2 b)$$

It is easy to see that $\langle x, 0\rangle$ and $\langle x^2 + \zeta_8^2 b, 0\rangle$, which are points on $J_C(\mathbb{F}_p)$ in the Mumford representation, generate a subgroup of order 4 in $J_C(\mathbb{F}_p)$. Hence 4 divides $\sharp J_C(\mathbb{F}_p)$.

If $a^{(p-1)/4} = 1$, there is an element u in $\mathbb{F}_p$ such that $a = u^4$. Then

$$x^5 + ax = x^5 + u^4 x = x(x + \zeta_8 u)(x - \zeta_8 u)(x + \zeta_8^3 u)(x - \zeta_8^3 u).$$

It is easy to see that $\langle x, 0\rangle$, $\langle x + \zeta_8 u, 0\rangle$, $\langle x - \zeta_8 u, 0\rangle$ and $\langle x + \zeta_8^3 u, 0\rangle$ generate a subgroup of order 16 in $J_C(\mathbb{F}_p)$. Hence 16 divides $\sharp J_C(\mathbb{F}_p)$. □

Theorem 4.2. *Let p be a prime number such that $p > 64$ and $p \equiv 1 \pmod 8$ and C a hyperelliptic curve over $\mathbb{F}_p$ defined by an equation $y^2 = x^5 + ax$. If $\left(\dfrac{a}{p}\right) = 1$, then the order of $J_C(\mathbb{F}_p)$ is as follows:*

1. *if $p \equiv 1 \pmod{16}$ and $a^{(p-1)/8} = 1$, then $\sharp J_C(\mathbb{F}_p) = (1 + p - 2c)^2$,*
2. *if $p \equiv 9 \pmod{16}$ and $a^{(p-1)/8} = 1$, then $\sharp J_C(\mathbb{F}_p) = (1 + p + 2c)^2$,*
3. *if $p \equiv 1 \pmod{16}$ and $a^{(p-1)/8} = -1$, then $\sharp J_C(\mathbb{F}_p) = (1 + p + 2c)^2$,*
4. *if $p \equiv 9 \pmod{16}$ and $a^{(p-1)/8} = -1$, then $\sharp J_C(\mathbb{F}_p) = (1 + p - 2c)^2$,*
5. *if otherwise, $\sharp J_C(\mathbb{F}_p) = (1 - p)^2 + 4c^2$*

where $p = c^2 + 2d^2$, $c, d \in \mathbb{Z}$ and $c \equiv 1 \pmod 4$.

Proof. First of all, from Theorem 3.4, we have that

$$s_1 \equiv (-1)^{(p-1)/8} 2c \left(a^{3(p-1)/8} + a^{(p-1)/8}\right) \pmod p \quad \text{and} \quad s_2 \equiv 4c^2 \pmod p$$

for all cases.

For the case (1), from Theorem 3.4 we have $s_1 \equiv 4c \pmod p$. By the definition of c, $c^2 < p$ and hence $0 < |4c| < 4\sqrt{p}$. Since $p > 64$ and Remark 3.3, we have that $s_1 = 4c$. Moreover since $|s_2| \leq 6p$ and $0 < 4c^2 < 4p$, s_2 is of the form $4c^2 + mp$, $-9 \leq m \leq 5$, $m \in \mathbb{Z}$. Then

$$\sharp J_C(Fp) = 1 + p^2 - 4c(1 + p) + 4c^2 + mp, \quad -9 \leq m \leq 5, \quad m \in \mathbb{Z}.$$

Since $\sharp J_C(\mathbb{F}_p) \equiv 0 \pmod{16}$ from Lemma 4.1, $1 + p^2 - 4c(1 + p) + 4c^2 + mp \equiv 0 \pmod{16}$. Since $p \equiv 1 \pmod 8$ and $c \equiv 1 \pmod 4$, we have $mp \equiv 2 \pmod{16}$ and then $m = 2$. Hence $\sharp J_C(\mathbb{F}_p) = 1 + p^2 - 4c(1 + p) + 4c^2 + 2p = (1 + p - 2c)^2$.

For the cases (2), (3), (4), we can show in the same way.

For the case (5), $a^{(p-1)/8}$ is a primitive 4th root of unity and $a^{3(p-1)/8} + a^{(p-1)/8} = 0$. So we have that $s_1 = 0$ by Theorem 3.4 and $p > 64$. Since $|s_2| \leq 2p$ in this case by Lemma 3.1 and $0 < 4c^2 < 4p$ by the definition of c, s_2 is of the form $4c^2 + mp$, $m \in \{-5, -4, -3, -2, -1, 0, 1\}$. On the other hand, since $1 + p^2 \equiv 2 \pmod 4$ and $\sharp J_C(\mathbb{F}_p) \equiv 0 \pmod 4$ by Lemma 4.1, we have that $s_2 \equiv 2 \pmod 4$. Hence we obtain $m = -2$ and $\sharp J_C(\mathbb{F}_p) = 1 + p^2 + 4c^2 - 2p = (1 - p)^2 + 4c^2$. □

Hence in particular if $p \equiv 1 \pmod 8$ and $\left(\dfrac{a}{p}\right) = 1$, then C with $a^{(p-1)/8} = \pm 1$ is not suitable for HECC.

4.2 The case of $p \equiv 3 \pmod 8$

In this case we first note that $\left(\dfrac{-1}{p}\right) = -1$.

Lemma 4.3. *For a hyperelliptic curve $C : y^2 = x^5 + ax$, $a \in \mathbb{F}_p$ where $p \equiv 3 \pmod 8$, the followings hold:*

1. *if $\left(\dfrac{a}{p}\right) = 1$, then 4 divides $\sharp J_C(\mathbb{F}_p)$,*

2. if $\left(\dfrac{a}{p}\right) = -1$*, then* 8 *divides* $\sharp J_C(\mathbb{F}_p)$*.*

Proof. If $\left(\dfrac{a}{p}\right) = 1$, then there exists an element $b \in \mathbb{F}_p$ such that $a = b^2$. Since $\left(\dfrac{-1}{p}\right) = -1$, either $2b$ or $-2b$ is a square. If $2b = u^2$, then

$$x^5 + ax = x\{(x^2 + b)^2 - 2bx^2\} = x(x^2 + ux + b)(x^2 - ux + b)$$

over $\mathbb{F}_p$ and $\langle x, 0\rangle$ and $\langle x^2 + ux + b, 0\rangle$ generate a subgroup of order 4 in $J_C(\mathbb{F}_p)$. If $-2b = u^2$,

$$x^5 + ax = x\{(x^2 - b)^2 - (-2b)x^2\} = x(x^2 + ux - b)(x^2 - ux - b)$$

over $\mathbb{F}_p$ and $\langle x, 0\rangle$ and $\langle x^2 + ux - b, 0\rangle$ generate a subgroup of order 4 in $J_C(\mathbb{F}_p)$.

If $\left(\dfrac{a}{p}\right) = -1$, then $x^5 + ax$ factors into a form $x(x+\beta)(x-\beta)(x^2+\gamma)$ over $\mathbb{F}_p$. It is easy to see that $\langle x, 0\rangle$, $\langle x + \beta, 0\rangle$ and $\langle x - \beta, 0\rangle$ generate a subgroup of order 8 in $J_C(\mathbb{F}_p)$. □

Theorem 4.4. *Let* p *be a prime number such that* $p > 16$ *and* $p \equiv 3 \pmod 8$ *and* C *a hyperelliptic curve over* $\mathbb{F}_p$ *defined by the equation* $y^2 = x^5 + ax$*. If* $\left(\dfrac{a}{p}\right) = 1$*, then the order of the Jacobian group* $J_C(\mathbb{F}_p)$ *is* $(1 + p + 2c)(1 + p - 2c)$ *where* $p = c^2 + 2d^2$*,* $c, d \in \mathbb{Z}$*.*

Proof. The order $J_C(\mathbb{F}_p)$ is given by $1+p^2+s_2$ because $s_1 = 0$. Moreover $s_2 \equiv -4c^2a^{(p-1)/2} \equiv -4c^2 \pmod p$. Since $|s_2| \leq 2p$, $s_2 = -4c^2 + mp$ where $m \in \mathbb{Z}$ such that $-2p \leq -4c^2 + mp \leq 2p$. By the definition of c, $0 < c^2 < p$ and $-4p < -4c^2 < 0$. Hence we have $-1 \leq m \leq 5$.

Since 4 divides $\sharp J_C(\mathbb{F}_p)$ by Lemma 4.3,

$$4|(1 + p^2 + mp - 4c^2), \quad -1 \leq m \leq 5.$$

By $p \equiv 3 \pmod 8$ and $c^2 \equiv 1 \pmod 4$, we have the condition

$$1 + p^2 + mp - 4c^2 \equiv 2 + 3m \equiv 0 \pmod 4.$$

and we obtain $m = 2$. Hence

$$\sharp J_C(\mathbb{F}_p) = 1 + p^2 + 2p - 4c^2 = (1 + p)^2 - 4c^2 = (1 + p + 2c)(1 + p - 2c).$$

□

Theorem 4.5. *Let* p *be a prime number such that* $p > 16$ *and* $p \equiv 3 \pmod 8$ *and* C *a hyperelliptic curve over* $\mathbb{F}_p$ *defined by the equation* $y^2 = x^5 + ax$*. If* $\left(\dfrac{a}{p}\right) = -1$*, then the order of the Jacobian group* $J_C(\mathbb{F}_p)$ *is* $(p - 1)^2 + 4c^2$ *where* $p = c^2 + 2d^2$*,* $c, d \in \mathbb{Z}$*.*

Proof. In this case,

$$\sharp J_C(\mathbb{F}_p) = 1 + p^2 + mp + 4c^2$$

where $-2p \leq mp + 4c^2 \leq 2p$ and $-5 \leq m \leq 1$. Since 8 divides $\sharp J_C(\mathbb{F}_p)$ by Lemma 4.3,

$$1 + p^2 + mp + 4c^2 \equiv 6 + 3m \equiv 0 \pmod 8$$

and we obtain $m = -2$. Hence

$$\sharp J_C(\mathbb{F}_p) = 1 + p^2 - 2p + 4c^2 = (1 - p)^2 + 4c^2.$$

□

Hence in this case, $\sharp J_C(\mathbb{F}_p)$ only depends on p and the value of the Jacobi symbol for a in $\mathbb{F}_p$. And in particular, C is not suitable for HECC if $\left(\dfrac{a}{p}\right) = 1$.

4.3 The case of $p \equiv 5, 7 \pmod 8$

This is the case that the Jacobian variety J_C is supersingular and the order of $J_C(\mathbb{F}_p)$ is $1 + p^2 \pm 2p = (1 \pm p)^2$ (cf. [3]). So in this case, C is not suitable for HECC.

4.4 Necessary condition to be suitable for HECC

From the results in this section, we have the following corollary.

Corollary 4.6. *Let p be a prime number and C a hyperelliptic curve defined by an equation $y^2 = x^5 + ax$ where $a \in \mathbb{F}_p$. Then C is not suitable for HECC if one of the followings holds:*

1. $p \equiv 1 \pmod 8$, $a^{(p-1)/4} = 1$,
2. $p \equiv 3 \pmod 8$, $\left(\dfrac{a}{p}\right) = 1$,
3. $p \equiv 5, 7 \pmod 8$.

5 Algorithm

We describe our algorithm based on Theorem 3.4. We only focus on the case (1) in Theorem 3.4 with the additional condition $a^{(p-1)/2} = -1$ because for other cases we gave the formula for the order of Jacobian groups in the previous section.

Input: $a \in \mathbb{F}_p$, $p(= 8f + 1 > 64)$
Output: $\sharp J_C(\mathbb{F}_p)$ (C : a hyperelliptic curve of genus 2 defined by $y^2 = x^5 + ax$)

1. Calculate an integer c such that $p = c^2 + 2d^2$, $c \equiv 1 \pmod 4$ (Cornacchia's Algorithm)
2. Determine s_1.
$$s \leftarrow (-1)^{(p-1)/8} 2c(a^{3(p-1)/8} + a^{(p-1)/8}) \pmod p \qquad (0 \le s \le p-1)$$
$$s_1 \leftarrow \begin{cases} s & (s < 4\sqrt{p}) \\ s - p & (s > 4\sqrt{p}) \end{cases}$$
3. Determine the list S of candidates of s_2.
$$t \leftarrow 4c^2 a^{(p-1)/2} \pmod p \qquad (0 \le t \le p-1)$$
$$S \leftarrow \begin{cases} \left\{t + 2mp \;\middle|\; 2\sqrt{p}|s_1| - 2p \le t + 2mp \le s_1^2/4 + 2p\right\} & (t\text{: even}) \\ \left\{t + (2m+1)p \;\middle|\; 2\sqrt{p}|s_1| - 2p \le t + (2m+1)p \le s_1^2/4 + 2p\right\} & (t\text{: odd}) \end{cases}$$
4. Calculate the list L of candidates of $\sharp J_C(\mathbb{F}_p)$.
$$L \leftarrow \left\{1 + p^2 - s_1(p+1) + s_2 \;\middle|\; s_2 \in S\right\}$$
5. If $\sharp L = 1$, return the unique element of L, else determine $\sharp J_C(\mathbb{F}_p)$ by multiplying a random point D (in the Mumford representation) on $J_C(\mathbb{F}_p)$ by each element of L.

It is easy to show that the expected running time of the above algorithm is $O(\ln^4 p)$. (For an estimation for Cornacchia's algorithm and so on, see Cohen's book [4].)

6 Searching Suitable Curves for HECC and Results

For hyperelliptic curves of type $C : y^2 = x^5 + ax$, $a \in \mathbb{F}_p$, we have searched hyperelliptic curves suitable for HECC. Since $J_C(\mathbb{F}_p)$ for such curve has a 2-torsion point (Remark 3.5), the best possible order of its Jacobian group is $2l$ where l is prime. The case of $p \equiv 1 \pmod 8$ and $\left(\dfrac{a}{p}\right) = -1$ is the only one such case due to the results in Section 4.

Our search is based on the algorithm which we proposed in the previous section. All computation below were done by *Mathematica* 4.1®[1] on Celeron 600MHz with less than 1GB memory (OS: FreeBSD 4.4).

Examples 6.1.

$$\begin{aligned} p &= 2417851639229258349419161 \text{(82-bit)},\ a = 16807, \\ J_C(\mathbb{F}_p) &= 5846006549324650191248125613942200572806220552962 \\ &= 2 \times 2923003274662325095624062806971100286403110276481 \\ &= 2 \times (\text{a 162-bit prime}) \end{aligned}$$

(The computation took 0.04s.)

$$\begin{aligned} p &= 4835703278458516698822641 \text{(82-bit)},\ a = 243, \\ J_C(\mathbb{F}_p) &= 23384026197286693734683162559398770155678059933602 \\ &= 2 \times 11692013098643346867341581279699385077839029966801 \\ &= 2 \times (\text{a 163-bit prime}) \end{aligned}$$

(The computation took 0.04s.)

$$\begin{aligned} p &= 2923003274661805836407369665432566039311865180529 \text{(162-bit)},\ a = 371293, \\ J_C(\mathbb{F}_p) &= 8543948143683640329580084318401338115672828124663448275867130387651937373152534160174163969676194 \\ &= 2 \times 4271974071841820164790042159200669057836414062331724137933565193825968686576267080087081984838097 \\ &= 2 \times (\text{a 321-bit prime}) \end{aligned}$$

(The computation took 0.07s.)

References

[1] B. C. Berndt, R. J. Evans and K. S. Williams, Gauss and Jacobi Sums, Canadian Mathematical Society Series of Monographs and Advanced Texts **21**, A Wiley-Interscience Publication, 1998,

[2] D. G. Cantor, *Computing in the Jacobian of hyperelliptic curve*, Math. Comp. **48** (1987), pp. 95–101,

[3] Y. Choie, E. Jeong and E. Lee, *Supersingular Hyperelliptic Curves of Genus 2 over Finite Fields*, Cryptology ePrint Archive: Report 2002/032 (2002), http://eprint.iacr.org/2002/032/,

[1] *Mathematica* is a trademark of Wolfram Research, Inc.

[4] H. Cohen, A Course in Computational Algebraic Number Theory, Graduate Texts in Mathematics **138**, Springer, 1996,

[5] P. Gaudry and R. Harley, *Counting Points on Hyperelliptic Curves over Finite Fields*, ANTS-IV, W. Bosma ed., Lecture Notes in Computer Science, No.1838, pp. 297–312, Springer-Verlag, 2000,

[6] R. H. Hudson and K. S. Williams, *Binomial Coefficients and Jacobi Sums*, Trans. Amer. Math. Soc. **281** (1984), pp. 431–505,

[7] N. Koblitz, Algebraic Aspects of Cryptography, Algorithms and Computation in Mathematics Vol. 3, Springer-Verlag, 1998,

[8] Ju. I. Manin, *The Hasse-Witt Matrix of an Algebraic Curves*, Amer. Math. Soc. Transl. Ser. **45** (1965), pp. 245–264

[9] K. Matsuo, J. Chao and S. Tsujii, *An improved baby step giant step algorithm for point counting of hyperelliptic curves over finite fields*, ANTS-V, Springer-Verlag LNCS 2369, 2002, pp. 461–474,

[10] D. Mumford, Tata Lectures on Theta II, Progress in Mathematics **43**, Birkhäuser, 1984,

[11] S. Wolfram, The Mathematica Book, 4th ed., Wolfram Media/Cambridge University Press, 1999,

[12] N. Yui, *On the Jacobian Varieties of Hyperelliptic Curves over Fields of Characteristic* $p > 2$, J. Alg. **52** (1978), pp. 378–410,