Counting Points for Hyperelliptic Curves of Type $y^2 = x^5 + ax$ over Finite Prime Fields

Eisaku Furukawa[1], Mitsuru Kawazoe[2], and Tetsuya Takahashi[2]

[1] Fujitsu Kansai-Chubu Net-Tech Limited
[2] Department of Mathematics and Information Sciences
College of Integrated Arts and Sciences
Osaka Prefecture University
1-1 Gakuen-cho Sakai Osaka 599-8531 Japan
{kawazoe,takahasi}@mi.cias.osakafu-u.ac.jp

Abstract. Counting rational points on Jacobian varieties of hyperelliptic curves over finite fields is very important for constructing hyperelliptic curve cryptosystems (HCC), but known algorithms for general curves over given large prime fields need very long running time. In this article, we propose an extremely fast point counting algorithm for hyperelliptic curves of type $y^2 = x^5 + ax$ over given large prime fields $\mathbb{F}_p$, e.g. 80-bit fields. For these curves, we also determine the necessary condition to be suitable for HCC, 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. We show some examples of suitable curves for HCC obtained by using our algorithm. We also treat curves of type $y^2 = x^5 + a$ where a is not square in $\mathbb{F}_p$.

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 group of $\mathbb{F}_q$-rational points of J_C. We call the group $J_C(\mathbb{F}_q)$ the Jacobian group of C. Since $J_C(\mathbb{F}_q)$ is a finite abelian group, we can construct a public-key-cryptosystem with it. This cryptosystem is called a "hyperelliptic curve cryptosystem (HCC)". The advantage of HCC 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. More precisely, we need a 160-bit field to construct a secure ECC, but for HCC 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 needed for a secure HCC. We call a hyperelliptic curve "suitable for HCC" if its Jacobian group has such a suitable order.

As in the case of ECC, computing the order of the Jacobian group $J_C(\mathbb{F}_q)$ is very important for constructing HCC. But it is very difficult for hyperelliptic curves defined over 80-bit fields and there are very few results on it: Gaudry-Harley's algorithm [9, 15] can compute the order for random hyperelliptic curves

M. Matsui and R. Zuccherato (Eds.): SAC 2003, LNCS 3006, pp. 26–41, 2004.

over 80-bit fields but their algorithm needs very long running time, e.g. 1 week or longer. For a hyperelliptic curve with complex multiplication, there are known efficient algorithms (we call them “CM-methods”) to construct a curve with its Jacobian group having a 160-bit prime factor. But CM-methods also need rather long time and do not give an algorithm to compute the order of the Jacobian group over a given defining field. There is another way. For special curves, it is possible to obtain a fast point counting algorithm for given defining fields. Buhler-Koblitz [2] obtained such algorithm for special curves of type $y^2 + y = x^n$ over prime fields $\mathbb{F}_p$ where n is an odd prime such that $p \equiv 1 \pmod{n}$.

In this article, we propose an extremely fast algorithm to compute the order of the Jacobian group $J_C(\mathbb{F}_p)$ for hyperelliptic curves C defined by the equation $y^2 = x^5 + ax$ over large prime fields $\mathbb{F}_p$. Curves of this type are different from Buhler-Koblitz’s curves [2]. Though the curves of this type have complex multiplication, by using our algorithm we can obtain suitable curves for HCC much faster than by using CM-methods. The expected running time of our algorithm is $O(\ln^4 p)$. The program based on our algorithm runs instantaneously on a system with Celeron 600MHz CPU and less than 1GB memory. It only takes less than 0.1 seconds even for 160-bit prime fields. Moreover we study on the reducibility of the Jacobian variety over extension fields and the order of the Jacobian group for the above curves. After these studies, we determine the necessary condition to be suitable for HCC. In Section 5, we describe our algorithm and give some examples of hyperelliptic curves suitable for HCC obtained by using it. In the last section of this article, we treat another hyperelliptic curves of type $y^2 = x^5 + a$, $a \in \mathbb{F}_p$. When a is square in $\mathbb{F}_p$, it is a kind of Buhler-Koblitz’s curves [2]. Here we consider the case that a is not square. It is not appeared in Buhler-Koblitz’s curves. We describe our point counting algorithm for this type and show the result of search for suitable curves for HCC. In fact, Jacobian groups with prime order are obtained in a very short time over 80-bit prime fields.

2 Basic Facts on Jacobian Varieties over Finite Fields

Here we recall basic facts on the order of Jacobian groups of hyperelliptic curves over finite fields. (cf. [9, 11])

2.1 General Theory

Let p be an odd 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 [16], every point on $J_C(\mathbb{F}_q)$ can be represented uniquely 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 [3], Harley's algorithm [9]).

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 ([14, 22]).

Theorem 1. *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. *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 $A_\phi = AA^{(p)}A^{(p^2)}\cdots A^{(p^{l-1})}$. Let $\kappa(t)$ be the polynomial given by $\det(I_g - tA_\phi)$ where I_g is the $(g\times g)$ identity matrix 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 Basic Idea for Our Algorithm

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 with no multiple root, 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:

$$\chi_q(t) = t^4 - s_1t^3 + s_2t^2 - s_1qt + q^2, \quad s_i \in \mathbb{Z}, \quad |s_1| \leq 4\sqrt{q}, \quad |s_2| \leq 6q.$$

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

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

We also note on the well-known fact that s_i are given by

$$s_1 = 1 + q - M_1 \quad \text{and} \quad s_2 = (M_2 - 1 - q^2 + s_1^2)/2$$

where M_i is the number of $\mathbb{F}_{q^i}$-rational points on C (cf. [11]).

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

Lemma 1 (cf. [17, 15]). $\lceil 2\sqrt{q}|s_1| - 2q \rceil \le s_2 \le \lfloor s_1^2/4 + 2q \rfloor$.

In the following we consider the case of $q = p$. When $q = p$, we obtain the following lemma as a collorary of Theorem 1 and 2.

Lemma 2. *Let $f(x)$, s_i, p be as above and c_i the coefficient of x^i in $f(x)^{(p-1)/2}$. Then $s_1 \equiv c_{p-1} + c_{2p-2} \pmod p$ and $s_2 \equiv c_{p-1}c_{2p-2} - c_{p-2}c_{2p-1} \pmod p$.*

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

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

Here we consider hyperelliptic curves of type $y^2 = x^5 + ax$, $a \in \mathbb{F}_p$. We show the following theorem which is essential to construct our algorithm.

Theorem 3. *Let a be an element of $\mathbb{F}_p$, C a hyperelliptic curve defined by the equation $y^2 = x^5 + ax$ and $\chi_p(t)$ the characteristic polynomial of the p-th power Frobenius endomorphism of C. Then s_1, s_2 in $\chi_p(t)$ are given as follows.*

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

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

   where c is an integer such that $p = c^2 + 2d^2$, $c \equiv 1 \pmod 4$ and $d \in \mathbb{Z}$.
2. *if $p \equiv 3 \pmod 8$, then $s_1 \equiv 0 \pmod p$ and $s_2 \equiv -4c^2 a^{(p-1)/2} \pmod p$ where c is an integer such that $p = c^2 + 2d^2$ and $d \in \mathbb{Z}$.*
3. *Otherwise, $s_1 \equiv 0 \pmod p$ and $s_2 \equiv 0 \pmod p$.*

Proof. Since $(x^5 + ax)^{\frac{p-1}{2}} = \sum_{r=0}^{(p-1)/2} \binom{\frac{p-1}{2}}{r} x^{4r+(p-1)/2} a^{(p-1)/2-r}$, 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, $0 \le r \le (p-1)/2$ such that $4r + (p-1)/2 = ip - j$. Then there are the following three possibilities: (i) $A = \begin{pmatrix} c_{p-1} & 0 \\ 0 & c_{2p-2} \end{pmatrix}$ if $p \equiv 1 \pmod 8$, (ii) $A = \begin{pmatrix} 0 & c_{p-2} \\ c_{2p-1} & 0 \end{pmatrix}$ if $p \equiv 3 \pmod 8$, (iii) $A = O$ if $p \not\equiv 1, 3 \pmod 8$.

Case (i). 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 $c_{2p-2} = \binom{4f}{3f}a^{f}$. From the result of Hudson-Williams [10, Theorem 11.2], we have $\binom{4f}{f} \equiv (-1)^f 2c \pmod{p}$ where $p = c^2+2d^2$ and $c \equiv 1 \pmod{4}$. Since $\binom{4f}{f} = \binom{4f}{3f}$, we have the case (1).

Case (ii). 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], $\binom{4f+1}{f} \equiv -2c \pmod{p}$ where $p = c^2+2d^2$ and $c \equiv (-1)^f \pmod{4}$. Since $\binom{4f+1}{3f+1} = \binom{4f+1}{f}$, we have $s_2 \equiv -\binom{4f+1}{f}^2 a^{4f+1} \equiv -4c^2a^{(p-1)/2} \pmod{p}$. Thus we obtain the case (2).

Case (iii). This is obvious and we obtain the case (3). □

Remark 2. Note that the order of $J_C(\mathbb{F}_p)$ for a curve of type $y^2 = x^5 + ax$ is always even because $J_C(\mathbb{F}_p)$ has a point of order 2. By Lemma 1, if $p > 64$, then there are only at most three possibilities for the value of s_2.

By using Theorem 3 and Remark 2, we can calculate (at most three) possibilities of $\sharp J_C(\mathbb{F}_p)$ in a very short time. Then to determine $\sharp J_C(\mathbb{F}_p)$, 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. If $p > 16$ for the case (2) and (3) in Theorem 3, we have $s_1 = 0$.

4 Study on the Structure of the Jacobian Group

Before describing our point counting algorithm, we study the structure of the Jacobian group for $y^2 = x^5 + ax$ more precisely. First, we study the reducibility of the Jacobian variety over extension fields of the defining field $\mathbb{F}_p$. Second, we determine the characteristic polynomial of the p-th power Frobenius endomorphism for many cases and give a necessary condition to be suitable for HCC explicitly.

4.1 Reducibility of the Jacobian Variety

We recall a few basic facts on the relation between the reducibility of the Jacobian variety and the characteristic polynomial of the Frobenius endomorphism. The following famous result was proved by Tate [18]:

Theorem 4. *Let A_1, A_2 be abelian varieties over $\mathbb{F}_q$ and $\chi_1(t)$, $\chi_2(t)$ characteristic polynomials of q-th power Frobenius endomorphisms of A_1, A_2, respectively. Then, A_1 is isogenous to A_2 over $\mathbb{F}_q$ if and only if $\chi_1(t) = \chi_2(t)$.*

The characteristic polynomial of the q-th power Frobenius endomorphism for a simple abelian variety of dimension two over $\mathbb{F}_q$ is determined as follows:

Theorem 5 ([21], cf. [17, 19]). *All possible characteristic polynomials $\chi_q(t)$ of q-th power Frobenius endomorphisms for simple abelian varieties of dimension two over $\mathbb{F}_q = \mathbb{F}_{p^r}$ are the followings:*

1. *$\chi_q(t) = t^4 - s_1t^3 + s_2t^2 - qs_1t + q^2$ is irreducible in $\mathbb{Z}[t]$, where s_1, s_2 satisfy some basic conditions,*
2. *$\chi_q(t) = (t^2 - q)^2$, r is odd,*
3. *$\chi_q(t) = (t^2 + q)^2$, r is even and $p \equiv 1 \pmod 4$,*
4. *$\chi_q(t) = (t^2 \pm q^{1/2}t + q)^2$, r is even and $p \equiv 1 \pmod 3$.*

For the reducibility of $\chi_{q^2}(t)$, the following lemma holds:

Lemma 3. *Let C be a hyperelliptic curve over $\mathbb{F}_q$ and $\chi_q(t) = t^4 - s_1t^3 + s_2t^2 - qs_1t + q^2$ the characteristic polynomial of q-th power Frobenius endomorphism of C, $\chi_{q^2}(t)$ the one of q^2-th power Frobenius endomorphism. Assume that $\chi_q(t)$ is irreducible in $\mathbb{Z}[t]$. Then $\chi_{q^2}(t)$ is reducible in $\mathbb{Z}[t]$ if and only if $s_1 = 0$.*

Proof. Let α, $\bar{\alpha}$, β, $\bar{\beta}$ be four roots of $\chi_q(t)$ where $\bar{}$ means complex conjugate. Then it is a well-known fact that $\chi_{q^2}(t) = (t-\alpha^2)(t-\bar{\alpha}^2)(t-\beta^2)(t-\bar{\beta}^2)$.

Assume that $s_1 = 0$. Put $\omega_1 = \alpha + \bar{\alpha}$ and $\omega_2 = \beta + \bar{\beta}$. Then from $s_1 = 0$ and $s_2 \in \mathbb{Z}$, we have $\omega_1 + \omega_2 = 0$ and $\omega_1\omega_2 + 2q \in \mathbb{Z}$. Put $m = \omega_1\omega_2 + 2q$. Then $\alpha^2 + \bar{\alpha}^2 = \omega_1^2 - 2q = -m$. We also have $\beta^2 + \bar{\beta}^2 = -m$. Hence we have $\chi_{q^2}(t) = (t^2 + mt + q^2)^2$.

Assume that $\chi_{q^2}(t)$ is not irreducible over $\mathbb{Z}$. First we consider the case $\chi_{q^2}(t)$ factors into a product of two polynomials of degree 2 over $\mathbb{Z}$. In this case, there are two possibilities: (a) $(t-\alpha^2)(t-\bar{\alpha}^2)$, $(t-\beta^2)(t-\bar{\beta}^2) \in \mathbb{Z}[t]$, (b) $(t-\alpha^2)(t-\beta^2)$, $(t-\bar{\alpha}^2)(t-\bar{\beta}^2) \in \mathbb{Z}[t]$. In case (a), $(\alpha+\bar{\alpha})^2 = \alpha^2 + \bar{\alpha}^2 + 2q \in \mathbb{Z}$. We also have $(\beta+\bar{\beta})^2 \in \mathbb{Z}$. Since $\chi_q(t)$ is irreducible over $\mathbb{Z}$, $\alpha+\bar{\alpha}$ and $\beta+\bar{\beta}$ are irrational numbers and we obtain that $s_1 = (\alpha+\bar{\alpha}) + (\beta+\bar{\beta})$ must be zero. In case (b), since $\alpha^2+\beta^2$, $\bar{\alpha}^2+\bar{\beta}^2$, $\alpha^2\beta^2$, $\bar{\alpha}^2\bar{\beta}^2$ are all in $\mathbb{Z}$, we have $\alpha^2+\beta^2 = \bar{\alpha}^2+\bar{\beta}^2$ and $\alpha^2\beta^2 = \bar{\alpha}^2\bar{\beta}^2$. Then $\alpha^2 = \bar{\alpha}^2$ or $\alpha^2 = \bar{\beta}^2$. Since $\chi_q(t)$ is irreducible, it cannot have a double root. So we have $\alpha = -\bar{\alpha}$ or $\alpha = -\bar{\beta}$. Moreover $\alpha = -\bar{\alpha}$ does not occur because if $\alpha = -\bar{\alpha}$ then $\chi_q(t)$ has a factor $(t-\alpha)(t-\bar{\alpha}) = t^2 + q$ over $\mathbb{Z}$. Hence we obtain $\alpha = -\bar{\beta}$. Then $\alpha+\bar{\beta} = 0$ and we have $s_1 = (\alpha+\bar{\beta})+(\bar{\alpha}+\beta) = 0$. Finally, we consider the case that $\chi_{q^2}(t)$ has a factor of degree 1 over $\mathbb{Z}$. But if $t - \alpha^2 \in \mathbb{Z}[t]$ then we obtain $\alpha^2 = \bar{\alpha}^2$. As we showed in case (b), it does not occur. □

Now we consider the reducibility for the Jacobian variety of our curve $y^2 = x^5 + ax$.

Lemma 4. *Let p be an odd prime and C a hyperelliptic curve defined by $y^2 = x^5 + ax$, $a \in \mathbb{F}_p^\times$ and $\mathbb{F}_q = \mathbb{F}_{p^r}$, $r \geq 1$. If $a^{1/4} \in \mathbb{F}_q$, then J_C is isogenous to the product of the following two elliptic curves E_1 and E_2 over $\mathbb{F}_q$:*

$$E_1 : \ Y^2 = X(X^2 + 4a^{1/4}X - 2a^{1/2}),$$
$$E_2 : \ Y^2 = X(X^2 - 4a^{1/4}X - 2a^{1/2}).$$

Proof. Let α be an element of $\mathbb{F}_q$ such that $\alpha^4 = a$. We can construct maps $\varphi_i : C \rightarrow E_i$ explicitly as follows: $\varphi_i^*(X) = (x - (-1)^i\alpha)^2/x, \varphi_i^*(Y) = (x - (-1)^i\alpha)y/x^2$, $i = 1,\ 2$. Since pull-backs of regular 1-forms dX/Y on E_i's generate the space of regular 1-forms on C, $\varphi_1 \times \varphi_2$ induces an isogeny from J_C to $E_1 \times E_2$ (cf. [13, 12]). □

The Jacobian variety for curves of type $y^2 = x^5 + ax$ is reducible over $\mathbb{F}_{p^4}$ by the above lemma. From a cryptographic point of view, if the Jacobian variety splits over an extension field of degree two, HCC for these curves might lose its advantage to ECC. Hence in the following, it is important to see whether the Jacobian splits over an extension field $\mathbb{F}_{p^r}$ of lower degree, i.e. $r = 1, 2$.

Remark 4. If $\mathbb{F}_q$ includes a 4-th primitive root of unity, E_1 and E_2 in Lemma 4 are isomorphic to each other by the following transformation: $X \rightarrow -X$, $Y \rightarrow \zeta_4 Y$ where ζ_4 is a 4-th primitive root of unity in $\mathbb{F}_q$.

4.2 Determining the Characteristic Polynomial of the p-th Power Frobenius Endomorphism

Due to Theorem 3, we divide the situation into the following three cases: (1) $p \equiv 1 \pmod 8$, (2) $p \equiv 3 \pmod 8$, (3) $p \equiv 5, 7 \pmod 8$.

The Case of $p \equiv 1 \pmod 8$.

Lemma 5. *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 8-th root of unity, 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

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

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

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

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 6. *Let p be a prime number such that $p > 64$, $p \equiv 1 \pmod 8$ and C a hyperelliptic curve over $\mathbb{F}_p$ defined by an equation $y^2 = x^5 + ax$. If $\left(\frac{a}{p}\right) = 1$, then $\chi_p(t)$ are as follows:*

1. *if* $p \equiv 1 \pmod{16}$ *and* $a^{(p-1)/8} = 1$*, then* $\chi_p(t) = (t^2 - 2ct + p)^2$*,*
2. *if* $p \equiv 9 \pmod{16}$ *and* $a^{(p-1)/8} = 1$*, then* $\chi_p(t) = (t^2 + 2ct + p)^2$*,*
3. *if* $p \equiv 1 \pmod{16}$ *and* $a^{(p-1)/8} = -1$*, then* $\chi_p(t) = (t^2 + 2ct + p)^2$*,*
4. *if* $p \equiv 9 \pmod{16}$ *and* $a^{(p-1)/8} = -1$*, then* $\chi_p(t) = (t^2 - 2ct + p)^2$*,*
5. *otherwise,* $\chi_p(t) = t^4 + (4c^2 - 2p)t^2 + p^2$*,*

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

Proof. First of all, from Theorem 3, $s_1 \equiv (-1)^{(p-1)/8} 2c \left(a^{3(p-1)/8} + a^{(p-1)/8}\right) \pmod p$ and $s_2 \equiv 4c^2 \pmod p$ for all cases.

For the case (1), from Theorem 3 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 1, we have that $s_1 = 4c$. Moreover since $\lceil 2\sqrt{p}|s_1| - 2p \rceil \le s_2 \le \lfloor s_1^2/4 + 2p \rfloor$ and $0 < 4c^2 < 4p$, s_2 is of the form $4c^2 + mp$, $-5 \le m \le 2$, $m \in \mathbb{Z}$. Then $\sharp J_C(\mathbb{F}_p) = 1 + p^2 - 4c(1+p) + 4c^2 + mp$ where m is an integer such that $-5 \le m \le 2$. Since $\sharp J_C(\mathbb{F}_p) \equiv 0 \pmod{16}$ from Lemma 5, $1 + p^2 - 4c(1+p) + 4c^2 + mp \equiv 0 \pmod{16}$. Since $p \equiv 1 \pmod{16}$ and $c \equiv 1 \pmod 4$, we have $mp \equiv 2 \pmod{16}$ and then $m = 2$. Hence we obtain $\chi_p(t) = t^4 - 4ct^3 + (4c^2 + 2p)t^2 - 4cpt + p^2 = (t^2 - 2ct + p)^2$.

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

For the case (5), $a^{(p-1)/8}$ is a primitive 4-th root of unity and $a^{3(p-1)/8} + a^{(p-1)/8} = 0$. So we have that $s_1 = 0$ by Theorem 3 and $p > 64$. Since $|s_2| \le 2p$ in this case by Lemma 1 and $0 < 4c^2 < 4p$ by the definition of c, s_2 is of the form $4c^2 + mp$, $-5 \le m \le 1$, $m \in \mathbb{Z}$. 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 5, we have that $m = -2$. Hence we obtain $\chi_q(t) = t^4 + (4c^2 - 2p)t^2 + p^2$. □

Hence in particular if $p \equiv 1 \pmod 8$ and $\left(\frac{a}{p}\right) = 1$, then C with $a^{(p-1)/4} = 1$ is not suitable for HCC because $\sharp J_C(\mathbb{F}_p) = (p \pm 2c + 1)^2$ and $|c| < \sqrt{p}$. In addition, J_C in case (5) is isogenous to the product of two elliptic curves over $\mathbb{F}_{p^2}$ because $a^{1/4} \in \mathbb{F}_{p^2}$.

The Case of $p \equiv 3 \pmod 8$.

Lemma 6. *For a hyperelliptic curve* $C : y^2 = x^5 + ax$*,* $a \in \mathbb{F}_p$ *where* $p \equiv 3 \pmod 4$*, the followings hold:*

1. *if* $\left(\frac{a}{p}\right) = 1$*, then* $\sharp J_C(\mathbb{F}_p) \equiv 0 \pmod 4$*,*
2. *if* $\left(\frac{a}{p}\right) = -1$*, then* $\sharp J_C(\mathbb{F}_p) \equiv 0 \pmod 8$*.*

Proof. If $\left(\frac{a}{p}\right) = 1$, then there exists an element $b \in \mathbb{F}_p$ such that $a = b^2$. Since $\left(\frac{-1}{p}\right) = -1$ by $p \equiv 3 \pmod 4$, 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 $\left(\frac{a}{p}\right) = -1$, 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 7. *Let p be a prime number such that $p > 16$, $p \equiv 3 \pmod 8$ and C a hyperelliptic curve over $\mathbb{F}_p$ defined by the equation $y^2 = x^5 + ax$. If $\left(\frac{a}{p}\right) = 1$, then $\chi_p(t) = (t^2 + 2ct + p)(t^2 - 2ct + p)$ where $p = c^2 + 2d^2$, $c, d \in \mathbb{Z}$.*

Proof. The order of $J_C(\mathbb{F}_p)$ 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 $-1 \leq m \leq 5$.

On the other hand, since 4 divides $\sharp J_C(\mathbb{F}_p)$ by Lemma 6, we have $(1 + p^2 + mp - 4c^2) \equiv 0 \pmod 4$. 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 $\chi_p(t) = t^4 + (2p - 4c^2)t^2 + p^2 = (t^2 + 2ct + p)(t^2 - 2ct + p)$. □

Theorem 8. *Let p be a prime number such that $p > 16$, $p \equiv 3 \pmod 8$ and C a hyperelliptic curve over $\mathbb{F}_p$ defined by the equation $y^2 = x^5 + ax$. If $\left(\frac{a}{p}\right) = -1$, then $\chi_p(t) = t^4 + (4c^2 - 2p)t^2 + p^2$ 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 6, $1 + p^2 + mp + 4c^2 \equiv 6 + 3m \equiv 0 \pmod 8$ and we obtain $m = -2$. Hence $\chi_p(t) = t^4 + (4c^2 - 2p)t^2 + p^2$. □

Hence in this case, $\sharp J_C(\mathbb{F}_p)$ only depends on p and the value of the Legendre symbol for $\left(\frac{a}{p}\right)$. And in particular, C is not suitable for HCC if $\left(\frac{a}{p}\right) = 1$ because $\sharp J_C(\mathbb{F}_p) = (p + 2c + 1)(p - 2c + 1)$ and $|c| < \sqrt{p}$. In addition, J_C for the case of $\left(\frac{a}{p}\right) = -1$ is isogenous to the product of two elliptic curves over $\mathbb{F}_{p^2}$ because $a^{1/4} \in \mathbb{F}_{p^2}$.

The Case of $p \equiv 5, 7 \pmod 8$. This is the case that the Jacobian variety J_C is supersingular because $s_1 \equiv s_2 \equiv 0 \pmod p$ (cf. [21]).

Lemma 7. *Let p be a prime number such that $p > 16$ and $p \equiv 5 \pmod 8$. For a hyperelliptic curve $C : y^2 = x^5 + ax$, $a \in \mathbb{F}_p$, the followings hold:*

1. *if $a^{(p-1)/4} = 1$, then $\sharp J_C(\mathbb{F}_p) \equiv 0 \pmod 4$,*
2. *if $a^{(p-1)/4} = -1$, then $\sharp J_C(\mathbb{F}_p) \equiv 0 \pmod 8$.*

Proof. Note that $\mathbb{F}_p$ has a 4-th primitive root of unity, ζ_4, because $p - 1 \equiv 0 \pmod 4$. Since $\left(\frac{a}{p}\right) = 1$ in both cases, there exists an element $b \in \mathbb{F}_p$ such that $a = b^2$ and $x^5 + ax = x(x^2 + \zeta_4 b)(x^2 - \zeta_4 b)$. Hence $\langle x, 0\rangle$, $\langle x^2 + \zeta_4 b, 0\rangle$ generates a subgroup of order 4 in $J_C(\mathbb{F}_p)$.

If $a^{(p-1)/4} = -1$, $\left(\frac{b}{p}\right) = -1$ and then $x^2 - \zeta_4 b$ factors into the form $(x + \beta)(x - \beta)$ because $\left(\frac{\zeta_4}{p}\right) = -1$. Hence in case (2), $\langle x, 0\rangle$, $\langle x + \beta, 0\rangle$, $\langle x - \beta, 0\rangle$ generate a subgroup of order 8 in $J_C(\mathbb{F}_p)$. □

Using the above lemma and Lemma 6, we obtain the following theorem.

Theorem 9. *Let p be a prime number such that $p > 16$, $p \equiv 5, 7 \pmod 8$ and C a hyperelliptic curve over $\mathbb{F}_p$ defined by the equation $y^2 = x^5 + ax$. Then,*

1. *if $p \equiv 5 \pmod 8$ and $a^{(p-1)/4} = 1$, then $\chi_p(t) = (t^2 + p)^2$,*
2. *if $p \equiv 5 \pmod 8$ and $a^{(p-1)/4} = -1$, then $\chi_p(t) = (t^2 - p)^2$,*
3. *if $p \equiv 5 \pmod 8$ and $\left(\frac{a}{p}\right) = -1$, then $\chi_p(t) = t^4 + p^2$,*
4. *if $p \equiv 7 \pmod 8$, then $\chi_p(t) = (t^2 + p)^2$.*

Proof. The order of $J_C(\mathbb{F}_p)$ is given by $1 + p^2 + s_2$ because $s_1 = 0$. Moreover, $s_2 = 0$ or $\pm 2p$ by Lemma 1 and Remark 2. Note that $1 + p^2 \equiv 2 \pmod 8$.

In case (1), $a^{1/4} \in \mathbb{F}_p$. Then J_C is isogenous to the product of two elliptic curves over $\mathbb{F}_p$ by Lemma 4. Hence by the list of Theorem 5, $\chi_p(t)$ must be $(t^2 + p)^2$.

In case (2), $\sharp J_C(\mathbb{F}_p) \equiv 0 \pmod 8$ by Lemma 7. Then we obtain $s_2 = -2p$ and the result.

In case (3), we use the relation $s_2 = (M_2 - 1 - p^2 + s_1^2)/2$ where $M_2 = \sharp C(\mathbb{F}_{p^2})$. Since $s_1 = 0$, $s_2 = (M_2 - 1 - p^2)/2$ and M_2 is given by $1 + \sharp R + 2\sharp S$ where $R = \{x \in \mathbb{F}_{p^2} | x^5 + ax = 0\}$ and $S = \{x \in \mathbb{F}_{p^2} | x^5 + ax$ is a non-zero square $\}$. Since $\mathbb{F}_{p^2}$ has a primitive 8-th root of unity, ζ_8, we easily see that if $u \in S$ then $\zeta_8^2 u \in S$. Hence we have that 4 divides $\sharp S$. In the case of $p \equiv 5 \pmod 8$ and $\left(\frac{a}{p}\right) = -1$, $\sharp R = 1$ and we have $M_2 \equiv 2 \pmod 8$. Hence in this case, $s_2 \equiv 0 \pmod 4$ and we have that $s_2 = 0$.

In case (4), we divide the situation by the value of the Legendre symbol $\left(\frac{a}{p}\right)$. If $\left(\frac{a}{p}\right) = 1$ then $a^{1/4} \in \mathbb{F}_p$ because $\left(\frac{-1}{p}\right) = -1$. By this fact, if $\left(\frac{a}{p}\right) = 1$ then J_C is isogenous to the product of two elliptic curves over $\mathbb{F}_p$ and we obtain the result as in case (1). For the case of $\left(\frac{a}{p}\right) = -1$, we have $s_2 = 2p$ by Lemma 6. □

So in this case, C is not suitable for HCC if $p \equiv 5 \pmod 8$ with $\left(\frac{a}{p}\right) = 1$ or $p \equiv 7 \pmod 8$, because $\sharp J_C(\mathbb{F}_p) = (p \pm 1)^2$. If $p \equiv 5 \pmod 8$ and $\left(\frac{a}{p}\right) = -1$, $\chi_{p^2}(t)$ is split because $s_1 = 0$ but J_C is simple over $\mathbb{F}_{p^2}$ by Theorem 5.

4.3 Necessary Condition to be Suitable for HCC

From the results in 4.2, we have the following corollary.

Corollary 1. *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 HCC if one of the followings holds: (1) $p \equiv 1 \pmod 8$, $a^{(p-1)/4} = 1$, (2) $p \equiv 3 \pmod 8$, $\left(\frac{a}{p}\right) = 1$, (3) $p \equiv 5 \pmod 8$, $\left(\frac{a}{p}\right) = 1$, (4) $p \equiv 7 \pmod 8$.*

In addition to the above cases, if $p \equiv 1 \pmod 8$ with $a^{(p-1)/4} = -1$ or $p \equiv 3 \pmod 8$ with $\left(\frac{a}{p}\right) = -1$, J_C is isogenous to the product of two elliptic curves over $\mathbb{F}_{p^2}$.

5 Point Counting Algorithm and Searching Suitable Curves

In this section we search suitable curves for HCC among hyperelliptic curves of type $y^2 = x^5 + ax$, $a \in \mathbb{F}_p$. From the result of the previous section, all the cases which can have suitable orders are the followings: (1) $p \equiv 1 \pmod 8$ with $\left(\frac{a}{p}\right) = -1$, (2) $p \equiv 1 \pmod 8$ with $a^{(p-1)/4} = -1$, (3) $p \equiv 3 \pmod 8$ with $\left(\frac{a}{p}\right) = -1$, (4) $p \equiv 5 \pmod 8$ with $\left(\frac{a}{p}\right) = -1$. But as we remarked in 4.2 and 4.3, J_C's are reducible over $\mathbb{F}_{p^2}$ in the case (2) and (3). Moreover J_C is supersingular in the case (4) as we remarked in 4.2. Hence we exclude these cases and only focus on the remaining case (1): $p \equiv 1 \pmod 8$ with $\left(\frac{a}{p}\right) = -1$.

On the other hand, the Jacobian group $J_C(\mathbb{F}_p)$ for our curve has a 2-torsion point (Remark 2), the best possible order of $J_C(\mathbb{F}_p)$ is $2l$ where l is prime. The case (1) in the above is the case that we can obtain the best possible order.

For the case (1) we cannot determine the characteristic polynomial of the p-th power Frobenius endomorphism by using the same method in 4.2. So we need a point counting algorithm for $J_C(\mathbb{F}_p)$. First we describe our algorithm and next we show the result of the search based on our algorithm.

5.1 Point Counting Algorithm for $p \equiv 1 \pmod 8$ and $\left(\frac{a}{p}\right) = -1$

We describe our algorithm based on Theorem 3. The algorithm is as follows:

Algorithm 1

`Input`*:* $a \in \mathbb{F}_p$ *where* $p \equiv 1 \pmod 8$ *and* $p > 64$

`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* $p = c^2 + 2d^2$, $c \equiv 1 \pmod 4$, $d \in \mathbb{Z}$ *by using Cornacchia's Algorithm.*

```
2. Determine $s_1$:
   $s \leftarrow (-1)^{(p-1)/8} 2c(a^{3(p-1)/8} + a^{(p-1)/8}) \pmod p \qquad (0 \le s \le p-1)$
   If $s < 4\sqrt{p}$, then $s_1 \leftarrow s$, else $s_1 \leftarrow s - p$.
3. Determine the list $S$ of candidates for $s_2$:
   $t \leftarrow 4c^2 a^{(p-1)/2} \pmod p \qquad (0 \le t \le p-1)$
   If $t$: even, then $S \leftarrow \left\{ t + 2mp \;\middle|\; 2\sqrt{p}|s_1| - 2p \le t + 2mp \le s_1^2/4 + 2p \right\}$,
   else $S \leftarrow \left\{ t + (2m+1)p \;\middle|\; 2\sqrt{p}|s_1| - 2p \le t + (2m+1)p \le s_1^2/4 + 2p \right\}$.
4. Determine the list $L$ of candidates for $\sharp J_C(\mathbb{F}_p)$:
   $L \leftarrow \left\{ 1 + p^2 - s_1(p+1) + s_2 \;\middle|\; s_2 \in S \right\}$.   ($\sharp L \le 3$ by Remark 2.)
5. If $\sharp L = 1$, then return the unique element of $L$,
   else determine $\sharp J_C(\mathbb{F}_p)$ by multiplying a random point $D$ 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 [5] for example.)

5.2 Searching Suitable Curves for HCC and Results

Here we show the result that we have searched hyperelliptic curves suitable for HCC among hyperelliptic curves of type $y^2 = x^5 + ax$, $a \in \mathbb{F}_p$.

Our search is based on the algorithm which we proposed in 5.1. All computation below were done by *Mathematica* 4.1 on Celeron 600MHz.

Example 1. The followings are examples of curves such that the orders of their Jacobian groups are in the form 2·(prime).

$$p = 1208925819614629175095961(\text{81-bit}), a = 3,$$
$$J_C(\mathbb{F}_p) = 2 \cdot 730750818666480869498570026461293846666412451841(\text{160-bit})$$

(The computation for counting points took 0.04s.)

$$p{=}2923003274661805836407369665432566039311865180529(\text{162-bit}), a{=}371293,$$
$$J_C(\mathbb{F}_p){=}2{\cdot}42719740718418201647900421592006690578364140623317241379335\backslash$$
$$65193825968686576267080087081984838097(\text{321-bit})$$

(The computation for counting points took 0.07s.)

In the above examples, J_C's are simple over $\mathbb{F}_{p^2}$. Since $\sharp J_C(\mathbb{F}_p)$ has a large prime factor, the characteristic polynomial of the p-th power Frobenius endomorphism must be irreducible. Moreover since $s_1 \neq 0$ over $\mathbb{F}_p$, the characteristic polynomial of p^2-th power Frobenius endomorphism cannot split by Lemma 3.

Furthermore, one can easily check that large prime factors of the above $\sharp J_C(\mathbb{F}_p)$ do not divide $p^r - 1$, $r = 1, 2, \ldots, 2^3\lfloor \log^2 p \rfloor$. Hence these curves are not weak against the Frey-Rück attack [7].

Example 2. The following table shows the result of search in many p's. We can find the following number of suitable curves for each search range.

search range (r, s)	num. of primes	num. of curves s.t.	time
for p, $r < p < s$	$p \equiv 1 \pmod 8$	$\sharp J_C(\mathbb{F}_p) = 2\times(\text{prime})$	(seconds)
$2^{80}, 2^{80} + 10^6$	4441	366	416.67
$2^{81}, 2^{81} + 10^6$	4309	352	409.72
$2^{161}, 2^{161} + 10^6$	2276	93	497.49
$2^{325}, 2^{325} + 10^6$	1100	30	731.52

Remark 5. From the result of Duursma, Gaudry and Morain [6], an automorphism of large order can be exploited to accelerate the Pollard's rho algorithm. If there is an automorphism of order m, we can get a speed up of $\sqrt{m}$. The order of any automorphism of $y^2 = x^5 + ax$ is at most 8. So the Pollard's rho algorithm for these curves can be improved only by a factor $\sqrt{8}$.

6 Point Counting Algorithm for another Curve: $y^2 = x^5 + a$

In this section, we consider another curve $y^2 = x^5 + a$, $a \in \mathbb{F}_p$. For the case a is square in $\mathbb{F}_p$, it is a kind of Buhler-Koblitz's curves [2]. Hence we consider the case a is non-square.

Theorem 10. *Let p be an odd prime number such that $p \equiv 1 \pmod 5$. C a hyperelliptic curve defined by the equation $y^2 = x^5 + a$ where $a \in \mathbb{F}_p$. Moreover let $J_5(\chi, \chi) = \sum_{s=0}^{p-1} \chi(s)\chi(1-s)$ be the Jacobi sum for a character χ of $\mathbb{F}_p$ which maps a fixed non-quintic element in $\mathbb{F}_p$ to $\zeta = e^{2\pi i/5}$ and c_1, c_2, c_3, c_4 be coefficients of ζ^i in the expression $J_5(\chi, \chi) = c_1\zeta + c_2\zeta^2 + c_3\zeta^3 + c_4\zeta^4$. Then for the characteristic polynomial $t^4 - s_1t^3 + s_2t^2 - s_1pt + p^2$ of the p-th power Frobenius endomorphism of C, s_1, s_2 are given as follows:*

$$s_1 \equiv \frac{1}{2}\alpha^3 \left(-z + \beta\right) a^{3(p-1)/10} + \frac{1}{2}\alpha \left(-z - \beta\right) a^{(p-1)/10} \pmod p$$

$$s_2 \equiv \frac{1}{4}\alpha^4 \left(z^2 - \beta^2\right) a^{2(p-1)/5} \pmod p$$

where $\alpha = 2^{(p-1)/5} \pmod p$, $\beta = \frac{w(z^2-125w^2)}{4(zw+uv)}$ and z, u, v, w are given by $z = -(c_1 + c_2 + c_3 + c_4)$, $5u = c_1 + 2c_2 - 2c_3 - c_4$, $5v = 2c_1 - c_2 + c_3 - 2c_4$, $5w = c_1 - c_2 - c_3 + c_4$.

Proof. Since $(x^5 + a)^{(p-1)/2} = \sum_{r=0}^{(p-1)/2} \binom{\frac{p-1}{2}}{r} x^{5r} a^{(p-1)/2-r}$ and $p \equiv 1 \pmod 5$, the Hasse-Witt matrix of C is of the form $\begin{pmatrix} c_{p-1} & 0 \\ 0 & c_{2p-2} \end{pmatrix}$. Put $f = (p-1)/10$. Then $s_1 \equiv \binom{5f}{2f}a^{3f} + \binom{5f}{4f}a^f \pmod p$ and $s_2 \equiv \binom{5f}{2f}\binom{5f}{4f}a^{4f} \pmod p$. From the result of [10, Theorem 13.1], $\binom{5f}{2f} = \frac{1}{2}\alpha^3 \left(-z + \frac{w(z^2-125w^2)}{4(zw+uv)}\right)$ and $\binom{5f}{f} = \frac{1}{2}\alpha \left(-z - \frac{w(z^2-125w^2)}{4(zw+uv)}\right)$. Hence we obtain the result. □

Remark 6. If $p \not\equiv 1 \pmod 5$, then the Hasse-Witt matrix is of the form $\begin{pmatrix} 0 & c_{p-2} \\ 0 & 0 \end{pmatrix}$ or $\begin{pmatrix} 0 & 0 \\ c_{2p-1} & 0 \end{pmatrix}$. Hence $s_1 \equiv s_2 \equiv 0 \pmod p$ and J_C is supersingular [21].

From the above theorem, we obtain a point counting algorithm for curves of type $y^2 = x^5 + a$ over $\mathbb{F}_p$ when $p \equiv 1 \pmod 5$. The algorithm is as follows:

Algorithm 2
`Input`*:* $a \in \mathbb{F}_p$ *where* $p \equiv 1 \pmod 5$ *and* $p > 64$.
`Output`*:* $\sharp J_C(\mathbb{F}_p)$ *(*C*: a hyperelliptic curve of genus 2 defined by* $y^2 = x^5 + a$*).*

1. *Calculate coefficients* c_1, c_2, c_3, c_4 *in* $J_5(\chi, \chi) = \sum_{i=1}^{4} c_i \zeta^i$ *in Theorem 10 by using the LLL algorithm. (See [2] for details.)*
2. *Determine* s_1 *by Theorem 10 and the bound* $|s_1| < 4\sqrt{p}$*.*
3. *Determine the list of candidates for* s_2 *by Theorem 10 and Lemma 1.*
4. *Determine the list* L *of candidates for* $\sharp J_C(\mathbb{F}_p)$ *from results of Step 2 and 3. (*$\sharp L \leq 5$ *by Remark 1.)*
5. `If` $\sharp L = 1$, `then` *return the unique element of* L*,* `else` *determine* $\sharp J_C(\mathbb{F}_p)$ *by multiplying a random point* D *on* $J_C(\mathbb{F}_p)$ *by each element of* L*.*

We show the result that we have searched suitable curves for HCC among hyperelliptic curves of type $y^2 = x^5 + a$, $a \in \mathbb{F}_p$ where a is non-square. All computation below were done by *Mathematica* 4.1 on Celeron 600MHz.

Example 3. The followings are examples of curves whose Jacobian groups have prime orders.

$$p = 1208925819614629174708801(81\text{-bit}), a = 1331,$$
$$J_C(\mathbb{F}_p) = 1461501637326815988079848163961117521046955445901(160\text{-bit})$$
(The computation for counting points took 0.18s.)

$$p = 1208925819614629174709941(81\text{-bit}), a = 2,$$
$$J_C(\mathbb{F}_p) = 1461501637331762771847359428275278989652932675771(161\text{-bit})$$
(The computation for counting points took 24.58s.)

In these examples, J_C's are simple over $\mathbb{F}_{p^2}$ by Lemma 3 and not weak against the Frey-Rück attack.

Example 4. The following table shows the result of search in many p's. We can find the following number of suitable curves for each search range.

search range (r, s)	num. of primes	num. of curves s.t.	time
for p, $r < p < s$	$p \equiv 1 \pmod 5$	$\sharp J_C(\mathbb{F}_p)$ =prime	(seconds)
2^{80}, $2^{80} + 10^4$	50	7	237.67
2^{81}, $2^{81} + 10^4$	40	7	224.16
2^{82}, $2^{82} + 10^4$	39	5	297.13
2^{100}, $2^{100} + 10^4$	33	5	335.76

Remark 7. The order of any automorphism of $y^2 = x^5 + a$ is at most 10. So as same as we remarked in Remark 5, the Pollard's rho algorithm for these curves can be improved only by a factor $\sqrt{10}$.

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, 30

[2] J. Buhler and N. Koblitz, *Lattice Basis Reduction, Jacobi Sums and Hyperelliptic Cryptosystems*, Bull. Austral. Math. Soc. **58** (1998), pp. 147–154, 27, 38, 39

[3] D. G. Cantor, *Computing in the Jacobian of hyperelliptic curve*, Math. Comp. **48** (1987), pp. 95–101, 28

[4] 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/,

[5] H. Cohen, A Course in Computational Algebraic Number Theory, Graduate Texts in Mathematics **138**, Springer, 1996, 37

[6] I. Duursma, P. Gaudry and F. Morain, *Speeding up the Discrete Log Computation on Curves with Automorphisms*, Advances in Cryptology – ASIA CRYPT '99, Springer-Verlag LNCS 1716, 1999, pp. 103–121, 38

[7] G. Frey and H.-G. Rück, *A Remark Concerning m-divisibility and the Discrete Logarithm in the Divisor Class Group of Curves*, Math. Comp. **62**, No.206 (1994) pp. 865–874, 37

[8] S. G. Galbraith, *Supersingular Curves in Cryptography*, Advances in Cryptology – ASIACRYPT 2001, Springer-Verlag LNCS 2248, 2001, pp. 495–513,

[9] P. Gaudry and R. Harley, *Counting Points on Hyperelliptic Curves over Finite Fields*, ANTS-IV, Springer-Verlag LNCS 1838, 2000, pp. 297–312, 26, 27, 28

[10] R. H. Hudson and K. S. Williams, *Binomial Coefficients and Jacobi Sums*, Trans. Amer. Math. Soc. **281** (1984), pp. 431–505, 30, 38

[11] N. Koblitz, Algebraic Aspects of Cryptography, Algorithms and Computation in Mathematics Vol. 3, Springer-Verlag, 1998, 27, 29

[12] S. Lang, Abelian Varieties, Springer-Verlag, 1983, 32

[13] F. Leprévost and F. Morain, *Revêtements de courbes elliptiques à multiplication complexe par des courbes hyperelliptiques et sommes de caractères*, J. Number Theory **64** (1997), pp. 165–182, 32

[14] Ju. I. Manin, *The Hasse-Witt Matrix of an Algebraic Curve*, Amer. Math. Soc. Transl. Ser. **45** (1965), pp. 245–264, 28

[15] 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, 26, 29

[16] D. Mumford, Tata Lectures on Theta II, Progress in Mathematics **43**, Birkhäuser, 1984, 28

[17] H-G. Rück, *Abelian surfaces and Jacobian varieties over finite fields*, Compositio Math. **76** (1990), pp. 351–366, 29, 31

[18] J. Tate, *Endomorphisms of abelian varieties over finite fields*, Invent. Math. **2** (1996), pp. 134–144, 30

[19] W. C. Waterhouse, *Abelian varieties over finite fields*, Ann. Sci. École Nor. Sup. (4) **2** (1969), pp. 521–560, 31

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

[21] C. Xing, *On supersingular abelian varieties of dimension two over finite fields*, Finite Fields and Their Appl. **2** (1996), pp. 407–421, 31, 34, 39

[22] N. Yui, *On the Jacobian Varieties of Hyperelliptic Curves over Fields of Characteristic* $p > 2$, J. Alg. **52** (1978), pp. 378–410. 28