J. Appl. Math. & Informatics Vol. **32***(2014), No. 1 - 2, pp. 17 - 26*
http://dx.doi.org/10.14317/jami.2014.017

COMPUTING THE NUMBER OF POINTS ON GENUS 3 HYPERELLIPTIC CURVES OF TYPE $Y^2 = X^7 + aX$ OVER FINITE PRIME FIELDS[†]

GYOYONG SOHN

Abstract. In this paper, we present an algorithm for computing the number of points on the Jacobian varieties of genus 3 hyperelliptic curves of type $y^2 = x^7 + ax$ over finite prime fields. The problem of determining the group order of the Jacobian varieties of algebraic curves defined over finite fields is important not only arithmetic geometry but also curve-based cryptosystems in order to find a secure curve. Based on this, we provide the explicit formula of the characteristic polynomial of the Frobenius endomorphism of the Jacobian variety of hyperelliptic curve $y^2 = x^7 + ax$ over a finite field $\mathbb{F}_p$ with $p \equiv 1$ modulo 12. Moreover, we also introduce some implementation results by using our algorithm.

AMS Mathematics Subject Classification : 14H45. 14G50. 94A60.
Key words and phrases : Counting points, Characteristic polynomial, Hyperelliptic curve.

1. Introduction

In recent years, computing the number of points on algebraic curves over finite fields is an important task for public key cryptography. In order to generate curves suitable for cryptosystems, we must determine the order of Jacobian of a curve over a finite field. It is required that the order of Jacobian is a prime or a small cofactor times a prime.

For elliptic curves, Schoof gave a polynomial time algorithm [7] and there are its improved algorithm for the time and space complexity [1, 5, 12]. Gaudry and Harley extended its algorithm to genus 2 curve [4]. For higher genus curves, there are several efficient counting points algorithms of Jacobian varieties [13, 14, 15]. In [9], authors suggest a fast point counting algorithm for genus 2 hyperelliptic curves of type $y^2 = x^5 + ax$ over finite prime fields. Also, there are many efficient

Received June 14, 2013. Revised August 23, 2013. Accepted August 26, 2013.
[†]This work was supported by the research grant of Daegu National University of Education.

algorithms for algebraic varieties over finite fields of small characteristic, which is so called p-adic method [16, 17, 18]. Our approach follows l-adic method which is more useful for algebraic curve over large field characteristic.

In this paper, we provide an algorithm for computing the orders of the Jacobians on genus 3 hyperelliptic curves of type $y^2 = x^7 + ax$ over finite prime fields. In particular, by using baby-step giant-step algorithm, we determine the order of the Jacobian of a curve defined over finite prime field with characteristic greater than the 54-bit. We also provide the explicit formula of the characteristic polynomial of the Frobenius endomorphism of the Jacobian of the hyperelliptic curves $y^2 = x^7 + ax$ over $\mathbb{F}_p$ with $p \equiv 1$ modulo 12. Furthermore, we present additional computational results using our algorithm.

2. Basic Facts on Hyperelliptic Curves

Let $\mathbb{F}_q$ be a finite field of $q = p^n$ elements, where p is an odd prime. The hyperelliptic curve C of genus g over $\mathbb{F}_q$ is given by

$$C \ : \ y^2 = f(x),$$

where $f(x)$ is a polynomial in $\mathbb{F}_q[x]$ of degree $2g + 1$ without singular points. We denote the Jacobian variety of a hyperelliptic curve C by J_C. Then, $J_C(\mathbb{F}_q)$ is the group of $\mathbb{F}_q$-rational points on J_C. A semi-reduced divisor is a divisor with k points and no two points in the opposite side. A reduced divisor is a semi-reduced divisor of $k \leq g$.

In [11], every semi-reduced divisor on $J_C(\mathbb{F}_q)$ can be uniquely represented by a pair of polynomials $\langle u(x), v(x)\rangle$, where $u(x) = \prod_i (x - x_i)$ is monic and $v(x)$ is unique polynomial such that $\deg v(x) < \deg u(x)$, $v(x_P) = y_P$ for all $P = (x_P, y_P) \in C(\mathbb{F}_q)$ and $u(x)$ divides $f(x) - v(x)^2$. $\langle 1, 0\rangle$ is the identity element of the addition law. Cantor's algorithm can be used to compute the sum of two reduced divisors in $J_C(\mathbb{F}_q)$.

We consider the hyperelliptic curves of genus 3 defined over finite fields $\mathbb{F}_q$. The characteristic polynomial $\chi_q(t)$ of the q-th power Frobenius endomorphism of J_C is given as follows:

$$\chi_q(t) = t^6 - s_1 t^5 + s_2 t^4 - s_3 t^3 + q s_2 t^2 - q^2 s_1 t + q^3,$$

where $s_i \in \mathbb{Z}$. We also know that $\sharp J_C(\mathbb{F}_q) = \chi_q(1)$. i.e.,

$$\sharp J_C(\mathbb{F}_q) = 1 + q^3 - s_1(1 + q^2) + s_2(1 + q) - s_3. \tag{1}$$

Let $M_r = (q^r + 1) - N_r$, where N_r is the number of $\mathbb{F}_{q^r}$-rational points on C for $r = 1, 2, 3$. Then, we have

$$s_1 = M_1, \ s_2 = \frac{1}{2}(M_1^2 - M_2), \text{ and } s_3 = \frac{1}{3}(M_3 - \frac{3}{2}M_2 M_1 + \frac{1}{2}M_1^3) \tag{2}$$

The following is a well-known inequality, the Hasse-Weil bound, that bounds $\sharp J_C(\mathbb{F}_q)$:

$$\lceil (\sqrt{q} - 1)^6 \rceil \leq \sharp J_C(\mathbb{F}_q) \leq \lfloor (\sqrt{q} + 1)^6 \rfloor.$$

Then, we have

$$|s_1| \leq 6\sqrt{q},\ |s_2| \leq 15q,\ |s_3| \leq 20q\sqrt{q}. \tag{3}$$

S. Haloui [19] presented the efficient bounds of the coefficients of characteristic polynomial of genus 3 abelian varieties over finite fields.

Theorem 2.1 ([19]). *Let $\chi(t) = t^6 - s_1t^5 + s_2t^4 - s_3t^3 + qs_2t^2 - q^2s_1t + q^3$ be a polynomial with integer coefficients. Then $\chi(t)$ is a Weil polynomial if and only if the following conditions hold*

(1) $|s_1| \leq 6\sqrt{q}$,
(2) $4\sqrt{q}|s_1| - 9q \leq s_2 \leq \frac{s_1^2}{3} + 3q$,
(3) $-\frac{2s_1^3}{27} + \frac{s_1s_2}{3} + qs_1 - \frac{2}{27}(s_1^2 - 3s_2 + 9q)^{3/2} \leq s_3 \leq -\frac{2s_1^3}{27} + \frac{s_1s_2}{3} + qs_1 + \frac{2}{27}(s_1^2 - 3s_2 + 9q)^{3/2}$,
(4) $-2qs_1 - 2\sqrt{q}s_2 - 2q\sqrt{q} \leq s_3 \leq -2qs_1 + 2\sqrt{q}s_2 + 2q\sqrt{q}$.

3. Hasse-Witt matrix

In this section, we recall the definition of the Hasse-Witt matrix in the case of hyperelliptic curves. It is a useful tool to compute the modulo characteristic p of $\sharp J_C(\mathbb{F}_p)$. Yui's made the following theorem [6].

Theorem 3.1. *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*

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

In [8], Manin showed that this matrix is related to the characteristic polynomial of the Frobenius endomorphism modulo p. For a matrix $H = (a_{ij})$, let $H^{(p)}$ denote the elements raised to the power p, i.e., (a_{ij}^p). Then, we have the following theorem.

Theorem 3.2. *Let C be a curve of genus g defined over a finite field $\mathbb{F}_{p^n}$. Let H be the Hasse-Witt matrix of C and let $H_\pi = H \cdot H^p \cdot H^{p^2} \cdots H^{p^{n-1}}$. Let $\kappa(t)$ be the characteristic polynomial of the matrix H_π and $\chi(t)$ the characteristic polynomial of the Frobenius endomorphism of the Jacobian of C. Then,*

$$\chi(t) \equiv (-1)^g t^g \kappa(t)\ (mod\ p).$$

4. The Characteristic Polynomial of C

In this section, we present the explicit formula of the characteristic polynomial of the Frobenius endomorphism on hyperelliptic curves of type $C : y^2 = x^7 + ax$ over finite fields $\mathbb{F}_p$ with $p \equiv 1 \pmod{12}$, and show how to efficiently compute the Hasse-Witt matrix of C. The below theorem is a tool used to compute the Hasse-Witt matrix of C.

Corollary 4.1 ([3]). *If $p = 12f + 1 = A^2 + B^2$ ($A \equiv 1 \pmod 4$, $B \equiv 0 \pmod 2$) is prime then*

$$\binom{6f}{f} \equiv \begin{cases} \binom{6f}{3f} & (\text{mod } p) \text{ if } B \equiv 0 \ (\text{mod } 3), \\ -\binom{6f}{3f} & (\text{mod } p) \text{ if } A \equiv 0 \ (\text{mod } 3). \end{cases}$$

Proof. See Corollary 4.2.2 in [3]. □

Theorem 4.2 ([3]). *Let $p = 12f + 1 = A^2 + B^2 = x^2 + 3y^2$ be a prime with $A \equiv 1 \pmod 4$, $x \equiv 1 \pmod 3$. Then we have the following congruences modulo p:*

$$\binom{6f}{f} \equiv 2\theta^2 A,$$

where

$$\theta^2 = \begin{cases} 1 & \text{if } A \equiv 1, 2 \ (\text{mod } 3),\ B \equiv 0 \ (\text{mod } 3), \\ B^2/A^2 & \text{if } A \equiv 0 \ (\text{mod } 3),\ B \equiv 1, 2 \ (\text{mod } 3). \end{cases}$$

Proof. See Theorem 15.1 in [3]. □

Theorem 4.3. *Let C be a hyperelliptic curve defined by the equation $y^2 = x^7 + ax$ over $\mathbb{F}_p$ with $p \equiv 1 \pmod{12}$ such that $p = A^2 + B^2$ ($A \equiv 1 \pmod 4$, $B \equiv 0 \pmod 2$) and $\chi(t)$ the characteristic polynomial of the p-th power Frobenius endomorphism of C. Then s_1, s_2 and s_3 in $\chi(t)$ are given as follows:*

1. *if $A \equiv 1,\ 2 \pmod 3$ and $B \equiv 0 \pmod 3$, then*

$$s_1 \equiv 2Aa^{(p-1)/12}(a^{(p-1)/3} + a^{(p-1)/6} + 1) \ (\text{mod } p),$$
$$s_2 \equiv 4A^2a^{(p-1)/3}(a^{(p-1)/3} + a^{(p-1)/6} + 1) \ (\text{mod } p),$$
$$s_3 \equiv 8A^3a^{(9p-9)/12} \ (\text{mod } p).$$

2. *if $A \equiv 0 \pmod 3$ and $B \equiv 1,\ 2 \pmod 3$, then*

$$s_1 \equiv 2\frac{B^2}{A}a^{(p-1)/12}(a^{(p-1)/3} - a^{(p-1)/6} + 1) \ (\text{mod } p),$$
$$s_2 \equiv 4\frac{B^4}{A^2}a^{(p-1)/3}(a^{(p-1)/3} - a^{(p-1)/6} - 1) \ (\text{mod } p),$$
$$s_3 \equiv -8\frac{B^6}{A^3}a^{(9p-9)/12} \ (\text{mod } p).$$

Proof. First, we compute the entities c_{ip-j} of the Hasse-Witt matrix H of the curve C. From Theorem 3.1, the entities c_{ip-j} are computed by an integer k, $0 \le k \le (p-1)/2$, for $ip - j = p - 1 + 3k$ from $(x^7 + ax)^{(p-1)/2} = \sum_{k=0}^{(p-1)/2} \binom{\frac{p-1}{2}}{k} a^{(p-1)/2-k} x^{(p-1)/2+6k}$. Since the characteristic p with $p \equiv 1 \pmod{12}$, the Hasse-Witt matrix is

$$H = \begin{pmatrix} c_{p-1} & 0 & 0 \\ 0 & c_{2p-2} & 0 \\ 0 & 0 & c_{3p-3} \end{pmatrix}. \tag{4}$$

Then we have that $c_{p-1} = \binom{\frac{p-1}{2}}{\frac{p-1}{12}} a^{(5p-5)/12}$, $c_{2p-2} = \binom{\frac{p-1}{2}}{\frac{3p-3}{12}} a^{(3p-3)/12}$, and $c_{3p-3} = \binom{\frac{p-1}{2}}{\frac{5p-5}{12}} a^{(p-1)/12}$. On the other hand, the each s_i of $\chi(t)$ has the following congruence modulo p;

$$\begin{aligned} s_1 &\equiv c_{p-1} + c_{2p-2} + c_{3p-3} \pmod{p}, \\ s_2 &\equiv c_{p-1}c_{2p-2} + c_{2p-2}c_{3p-3} + c_{p-1}c_{3p-3} \pmod{p}, \\ s_3 &\equiv c_{p-1}c_{2p-2}c_{3p-3} \pmod{p}. \end{aligned}$$

Let $p = 12f + 1$ be a prime. Then, since $(p-1)/2 + 6k = p - 1$ for c_{p-1}, we have $k = (p-1)/12 = f$ and $c_{p-1} = \binom{6f}{f} a^{5f}$. For c_{2p-2}, since $(p-1)/2 + 6k = 2p - 2$, we have $k = (3p-3)/12 = 3f$ and $c_{2p-2} = \binom{6f}{3f} a^{3f}$. For c_{3p-3}, since $(p-1)/2 + 6k = 3p - 3$, we have $k = (5p-5)/12 = 5f$ and $c_{3p-3} = \binom{6f}{5f} a^{5f}$. Hence, since $\binom{6f}{5f} = \binom{6f}{f}$, Theorem 4.2 and Corollary 4.1, we have the congruence values modulo p for s_1, s_2 and s_3. □

The equation of given curve gives us to some information about 2^k-torsion subgroups of the Jacobian variety.

Lemma 4.4. *Let p be a prime number such that $p \equiv 1$ (mod 12) and $C : y^2 = f(x)$ be a hyperelliptic curve over $\mathbb{F}_p$ where $f(x) = x^7 + ax$. If $f(x)$ splits completely over $\mathbb{F}_p$ (i.e.,$a^{(p-1)/6} = 1$), then 64 divide $\sharp J_C(\mathbb{F}_p)$. If $f(x)$ splits into four factors over $\mathbb{F}_p$ (i.e, $a^{(p-1)/3} = 1$), then 8 divide $\sharp J_C(\mathbb{F}_p)$. Otherwise, if $f(x)$ splits into two factors of degree 3 and a factor of degree 1, or into two factors of degree 6 and 1, then 2 divide $\sharp J_C(\mathbb{F}_p)$.*

Proof. Since 12 divide $p-1$, there are exists a primitive 12-th root of unity, ζ_{12}, in $\mathbb{F}_p$. The points on C with vanishing y-coordinates correspond to $(1-\zeta_{12})$-torsion points of the Jacobian. If $f(x)$ splits completely over $\mathbb{F}_p$ (i.e., $a^{(p-1)/6} = 1$), then $J_C[1-\zeta_{12}]$ is defined over $\mathbb{F}_p$. Hence, $(\mathbb{Z}/2\mathbb{Z})^6$ is a subgroup in $J_C(\mathbb{F}_p)$ and 64 divide $\sharp J_C(\mathbb{F}_p)$. Moreover precisely, in this case, there exists an element $b \in \mathbb{F}_p$ such that $a = b^6$. Then we have

$$\begin{aligned} y^2 = x^7 + ax &= x(x^6 + b^6) \\ &= x(x - \zeta_{12}^3 b)(x + \zeta_{12}^3 b)(x - \zeta_{12}^5 b)(x + \zeta_{12}^5 b)(x - \zeta_{12}^7 b)(x + \zeta_{12}^7 b). \end{aligned}$$

If $f(x)$ splits four factors over $\mathbb{F}_p$ (i.e., $a^{(p-1)/3} = 1$), then the three $(1-\zeta_{12})$-torsion points arising from the roots of $f(x)$ are linearly independent. Hence $(\mathbb{Z}/2\mathbb{Z})^3 \leq J_C(\mathbb{F}_p)$ and 8 divides $\sharp J_C(\mathbb{F}_p)$. Moreover, in this case, there exists an element $b \in \mathbb{F}_p$ such that $a = b^3$. Then we have

$$y^2 = x^7 + ax = x(x^6 + b^3) = x(x^2 + b)(x^2 + \zeta_{12}^5 b)(x^2 + \zeta_{12}^9 b).$$

Otherwise, $J_C(\mathbb{F}_p)$ contains one non-trivial $(1-\zeta_{12})$-torsion point. Moreover, in this case, there exists an element $b \in \mathbb{F}_p$ such that $a = b^2$. Then we have that

$$y^2 = x^7 + ax = x(x^6 + b^2) = x(x^3 + b)(x^3 - b), \text{ and } y^2 = x(x^6 + a).$$

□

Throughout this paper, we consider the case of the prime $p = A^2 + B^2$ with $A \equiv 1 \pmod 4$ and $B \equiv 0 \pmod 2$.

Theorem 4.5. *Let C be a hyperelliptic curve of the form $y^2 = x^7 + ax$ defined over a finite field $\mathbb{F}_p$ with $p \equiv 1$ (mod 12), $p = A^2 + B^2$. Then the characteristic polynomial $\chi(t)$ is as follows:*

1. *If $a^{(p-1)/12} = 1$, then $\chi(t) = (t^2 - 2At + p)^3$.*
2. *If $a^{(p-1)/12} = -1$ and $\chi(t) = (t^2 + 2At + p)^3$.*

where $A \equiv 1,\ 2$ (mod 3) and $B \equiv 0$ (mod 3).

3. *If $a^{(p-1)/12} = 1$, then $\chi(t) = (t^2 - 2\frac{B^2}{A}t + p)(t^2 + 2\frac{B^2}{A}t + p)^2$.*
4. *If $a^{(p-1)/12} = -1$, then $\chi(t) = (t^2 + 2\frac{B^2}{A}t + p)(t^2 - 2\frac{B^2}{A}t + p)^2$.*

where $A \equiv 0$ (mod 3) and $B \equiv 1, 2$ (mod 3).

Proof. For the case (1), from $a^{(p-1)/12} = 1$ and Theorem 4.3, we have $s_1 \equiv 6A \pmod p$, $s_2 \equiv 12A^2 \pmod p$, and $s_3 \equiv 8A^3 \pmod p$. By the Definition of A, $A^2 < p$ and hence $0 < |6A| < 6\sqrt{p}$. If $p > 37$, then s_1 is uniquely determined by Hasse-Witt matrix. Hence we have that $s_1 = 6A$.

Denote $s_2 = mp + 12A^2$ for $m \in \mathbb{Z}$. Since $0 < 12A^2 < 12p$ and $\lceil 4\sqrt{p}|s_1| - 9p \rceil \le s_2 \le \lfloor s_1^2/3 + 3p \rfloor$, m is satisfied in $-9 \le m \le 3$. Now we determine the value m. We know that $\chi(t)$ splits into three factors $h_i(x)$ of degree 2, for $i = 1, 2, 3$. In particular, let π_i be a complex roots of $\chi(t)$ in $\mathbb{Z}[t]$ for $i = 1, 2, 3$, and $\overline{\pi_i}$ its complex conjugate. We denote $\lambda_i = \pi_i + \overline{\pi_i}$ for $i = 1, 2, 3$. Then we have that $s_1 = \lambda_1 + \lambda_2 + \lambda_3$, $s_2 = 3p + \lambda_1\lambda_2 + \lambda_2\lambda_3 + \lambda_3\lambda_1$, and $s_3 = 2ps_1 + \lambda_1\lambda_2\lambda_3$. Since $\lambda_i < 2\sqrt{p}$ and $A < \sqrt{p}$, we thus have $m = 3$.

We denote $s_3 = \widetilde{m}p + 8A^3$ for $\widetilde{m} \in Z$. Since $\prod \lambda_i < 8p\sqrt{p}$, we have $m' = 12A$. Then the characteristic polynomial $\chi(t)$ is

$$\begin{aligned}\chi(t) &= t^6 - 6At^5 + (12A^2 + 3p)t^4 - (12Ap + 8A^3)t^3 + p(3p + 12A^2)t^2 - p^2(6A)t + p^3, \\ &= (t^2 - 2At + p)^3.\end{aligned}$$

For the case (3), we have that $s_1 \equiv 2B^2/A \pmod p$, $s_2 = -4B^4/A^2 \pmod p$, and $s_3 \equiv -8B^6/A^3 \pmod p$. Following as the above way, the characteristic polynomial $\chi(t)$ is

$$\begin{aligned}\chi(t) &= t^6 + 2\frac{B^2}{A}t^5 + (3p - 4\frac{B^4}{A^2})t^4 + (4p\frac{B^2}{A} - 8\frac{B^6}{A^3})t^3 + p(3p - 4\frac{B^4}{A^2})t^2 - 2p^2\frac{B^2}{A}t - p^3 \\ &= (t^2 - 2\frac{B^2}{A}t + p)(t^2 - \frac{B^2}{A}t + p)^2.\end{aligned}$$

For the case (2),(4), we can derive the $\chi(t)$ in the same way. □

Theorem 4.6. *Let C be a hyperelliptic curve of the form $y^2 = x^7 + ax$ defined over a finite field $\mathbb{F}_p$. If $a^{(p-1)/6} = -1$ (i.e, $a^{(p-1)/3} = 1$) and $A \equiv 1, 2$ (mod 3)*

and $B \equiv 0$ (mod 3), then the characteristic polynomial $\chi(t)$ has the form of the following as

$$\chi(t) = t^6 - c_1 t^5 + c_2 t^4 - c_3 t^3 + p c_2 t^2 - p^2 c_1 t + p^3.$$

where c_1 is $2Aa^{(p-1)/12}$ or $-p + 2Aa^{(p-1)/12}$, $c_2 = mp + 4A^2$ for $-1 \leq m \leq 2$, and c_3 is an integer with $c_3 \equiv 0$ (mod 2) for $|c_3| \leq 20p\sqrt{p}$.

Proof. From $a^{(p-1)/6} = -1$ and Theorem 4.3, we have that $s_1 \equiv 2Aa^{(p-1)/12} \pmod{p}$, $s_2 \equiv 4A^2 \pmod{p}$ and $s_3 \equiv 8A^3 a^{9(p-1)/12} \pmod{p}$. Since Hasse-Weil bound of s_1 and $A < \sqrt{p}$, the coefficient s_1 only have $2Aa^{(p-1)/12}$ or $-p + 2Aa^{(p-1)/12}$.

Let $s_2 = mp + 4A^2$ for $m \in \mathbb{Z}$. From the sharp bound of s_2 in Theorem 2.1, $-1 \leq m \leq 2$. For $s_3 = m'p + 8A^3 a^{9(p-1)/12}$, $m' \in \mathbb{Z}$, we have $s_3 \equiv 0 \pmod{2}$ since $s_1 \equiv 0 \pmod{2}$ and $\sharp J_C(\mathbb{F}_p) \equiv 0 \pmod{2}$. □

Theorem 4.7. *Let C be a hyperelliptic curve of the form $y^2 = x^7 + ax$ defined over a finite field $\mathbb{F}_p$ with $p \equiv 1$ (mod 12). Assume that $A \equiv 1$ (mod 4) and $A \equiv 1, 2$ (mod 3). If $a^{(p-1)/3} \neq 1$ and $f(x)$ splits three factors, then the $\chi(t)$ has the following form*

$$\chi(t) = t^6 - c_3 t^3 + p^3.$$

where c_3 is an integer for $|c_3| \leq 2p\sqrt{p}$ and $c_3 \equiv 0$ (mod 2).

Proof. In this case, the prime satisfies $p = A^2 + B^2$ where $A \equiv 1, 5 \pmod{12}$ and $B \equiv 0 \pmod{6}$. We have $a^{(p-1)/3} + a^{(p-1)/6} + 1 = 0$. Then $s_1 \equiv 0 \pmod{p}$ and $N_1 = \sharp C(\mathbb{F}_p) = p + 1$. Hence $s_1 = 0$. Since $N_2 = \sharp C(\mathbb{F}_{p^2}) = p^2 + 1$, we have $s_2 = 0$.

For the value s_3, we denote $s_3 = mp + 8A^3 a^{9(p-1)/12}$. From the bounds of s_3 in theorem 2.1, we have $|m| \leq 2\sqrt{q}$. Since $\sharp J_C(\mathbb{F}_p) \equiv 0 \pmod{2}$,

$$\chi(1) = 1 + p^3 - c_3 \equiv 0 - c_3 \equiv 0 \pmod{2}.$$

Then we have $c_3 \equiv 0 \pmod{2}$ for $|c_3| \leq [2p\sqrt{p}]$ from Theorem 2.1 . Hence we have conclusion. □

5. Implementation details

5.1. BSGS algorithm. Now, we show how to determine the order of the Jacobian of a hyperelliptic curve using the BSGS algorithm. We denote by L_i (U_i) the lower (upper) bound of s_i for $i = 1, 2, 3$ in (3). According to Theorem 3.2, we denote that for $i = 1, 2, 3$

$$s_i = s_i' + t_i p, \tag{2}$$

with $s_i', t_i \in \mathbb{Z}$ $(0 \leq s_i' < p)$. Then each t_i is bounded by

$$\lceil L_i/p \rceil \leq t_i \leq \lfloor U_i/p \rfloor.$$

We substitute (2) into (1) and denote $M = 1 + p^3 - s_1'(1+p^2) + s_2'(1+p) - s_3'$. Then, the order of the Jacobian follows the equation

$$\sharp J_C(\mathbb{F}_p) = M - t_1 p(1+p^2) + t_2 p(1+p) - t_3 p. \tag{3}$$

We should determine the values (t_1, t_2, t_3) in order to get $\sharp J_C(\mathbb{F}_p)$. Assume that N is a positive integer(to be specified). Let u and v be integers such that

$$t_3 = u + vN,\ 0 \le u < N. \tag{4}$$

Then, the boundary for v is

$$\lceil L_3/pN \rceil \le v \le \lfloor U_3/pN \rfloor.$$

By substituting (4) into (3), we have

$$\sharp J_C(\mathbb{F}_p) = M - t_1 p(1+p^2) + t_2 p(1+p) - up - vNp.$$

Hence, $\sharp J_C(\mathbb{F}_p)$ can be computed by finding the 4-tuple (t_1, t_2, u, v) such that

$$(M - t_1 p(1+p^2) + t_2 p(1+p) - up)D = (vNp)D, \tag{5}$$

for all $D \in J_C(\mathbb{F}_p)$ for the above each ranges. We search for a collision between the lhs and the rhs of (5) in the corresponding ranges. Moreover, we choose

$$N = \sqrt{2^3 U_1 U_2 U_3 / p^3}.$$

Thus the algorithm require the computation of $O(N)$ point multiples.

5.2. Speeding up algorithm. In this section, we discuss the some technique to speed up the algorithm during its implementation. First, we use the Cornacchia's algorithm in order to compute the coefficients s_i' in (2) (see [10]). Then we can be easily calculated the binomial coefficients. Moreover, since $|s_1| \le 6\sqrt{p}$, if $p > 37$, then s_1 is uniquely determined by sum of c_{p-1}, c_{2p-2} and c_{3p-3}.

In [2], Gonda et. al. provide the efficient arithmetic on Jacobian of genus 3 hyperelliptic curves over a finite field. Using this method, the addition operation in a Jacobian can be computed by performing 70 multiplications and 1 inversions and 113 additions. The doubling can be obtained as 71 multiplications, 1 inversion and 107 additions.

In (5) of section 5.1, the precomputation of p and the addition of a divisor pN times are needed, and an double-and-add method is used for these operations. When we search for a collision between them, the same divisors are repeatedly computed. So, we store them at first and subsequently execute the comparison test. Two divisors identical and therefore, their chord are the same. Hence, we can limit the boundary to $0 \le k \le \lfloor U_3/N \rfloor$ and then avoid the computation for the inversion of a divisor.

Now, we consider an efficient value N for the case of Theorem 4.7. We let $c_3 = u + vN$ with $0 \le u < N$ and $|v| \le (2\sqrt{p})/N$. For the v, there are $4\sqrt{p}/N$ choices, and for u there are N choices. We also set the N as $N = \sqrt{2\sqrt{p}}$. In (2) of Theorem 4.6, the s_1 and s_2 are easily determined. We similarly set the N as $N = \sqrt{20\sqrt{p}}$. Therefore, the expected running time of our algorithm is $O(p^{\frac{1}{4}})$.

6. Computational results

In this section, we present our experimental results. We implemented our algorithm on a Pentium 2.13 GHz computer with less than 2 GB memory using Shoup's NTL library.

Example 6.1. Let $p = 12970096625951449$ be a 54-bit prime and let curve C over $\mathbb{F}_p$ be defined by

$$C \ : \ y^2 = x^7 + 12345601677x.$$

We compute the group order of the Jacobian:

$$218187385537053616784533048812278635860428785889 0$$

The number of the Jacobian is of 160 bits and the total time is 1882 s.

Example 6.2. Let $p = 26144785074025909$ be a 55-bit prime and let C be the curve defined by $C : y^2 = x^7 + 4857394849x$. The group order of the Jacobian is given by:

$$178712622571907053989539231112397193490170498152 84$$

The number of the Jacobian is of 163 bits and the total time is 259 s.

Table 1 has the implementation results for Jacobians with a quasiprime factor greater than 160 bits.

7. Conclusions

In this paper, we have presented an algorithm for computing the orders of the Jacobian varieties of genus 3 hyperelliptic curves defined by $y^2 = x^7 + ax$ over a finite prime field. By using the baby-step giant-step method, we determined the order of the Jacobian of a curve defined over a finite prime field bigger than 55 bit. Moreover, we also provided the explicit formula of the characteristic polynomial of the Frobenius endomorphism of the Jacobian of the hyperelliptic curves $y^2 = x^7 + ax$ over $\mathbb{F}_p$ with $p \equiv 1$ modulo 12. Finally, we verified usefulness of the our algorithm by the simple examples.

References

1. N. Elkies, *Elliptic and modular curves over finite fields and related computational issues*, Computational perspectives on number theory, AMS/IP Stud. Adv. Math. **7** (1998), Math. Soc., 21–76.
2. M. Gonda, K. Matsuo, K. Aoki, and J. Chao, *Improvements of Addition Algorithm on Genus 3 Hyperelliptic Curves and Their Implementation*, IEICE TRANS. FUNDAMENTALS **E88-A**(1) (2005), 89–96.
3. R. H. Hudson and K. S. Williams, *Binomial Coefficients and Jacobi Sums*, Trans. Amer. Math. Soc. **281** (1984), 431–505.
4. P. Gaudry and R. Harley, *Counting points on hyperelliptic curves over finite fields*, ANTS-IV, W. Bosma ed., LNCS **1838** (2000), Springer-Verlag, 297–312.
5. I. Blake, G. Seroussi and N. Smart, *Elliptic curves in cryptography*, London Math. Soc. Lecture Note Series **265** (1999).

TABLE 1. Implementation results

Prime p	704589887337525130270500 1 (83 bits)
Curve a	3212003
$\sharp J_C(\mathbb{F}_p)$	3497914719197398278272766865425949079451 39\ 5041564076403929229054455749821 00 (247 bits)
Prime p	4341919238864522015180317 (82 bits)
Curve a	21374924713
$\sharp J_C(\mathbb{F}_p)$	8185500201262045096903572127582712936724\ 1220270192088842798034439911824260 (245 bits)
Prime p	1468779960393313157311762 9 (84 bits)
Curve a	2633412312194
$\sharp J_C(\mathbb{F}_p)$	3168620411698486271822633774958808942474 7\ 1161048103901141942794842027849570 (250 bits)

6. H. Yui. *On the jacobian varieties of hyperelliptic curves over fields of characteristic $p \geq 2$*, J. Algebra **52** (1987), 378–410.
7. R. Schoof, *Elliptic curves over finite fields and the computation of square roots mod p*, Math. Comp. **44** (1985), 483–494.
8. Yu. I. Manin, *The Hasse-Witt matrix of an algebraic curve*, AMS Trans. Ser. 2 **45** (1965), 245–264.
9. E. Furukawa, M. Kawazoe, and T.Takahashi, *Counting Points for Hyperelliptic Curves of Type $y^2 = x^5 + ax$ over Finite Prime Fields*, LNCS **2004**, 26–41.
10. J. Buhler and N. Koblitz, *Lattics Basis Reduction, Jacobi Sums and Hyperelliptic Cryptosystems*, Bull. Austral. Math. Soc. **58** (1998), 147–154.
11. D. Mumford, *Tata Lectures on Theta II*, Progress in Mathematics **43**, Birkhäuser, 1984.
12. R. Lercier, *Algorithmique des courbes elliptiques dans les corps finis*. Thése, École polytechnique, June 1997.
13. L. Adleman and M. D. Huang, *Counting points on curves and abelian varieties over finite fields*, J. Symb. Comp. 32(3) (2001) pp. 171–189.
14. M. D. Huang and D. Ierardi, *Counting points on curves over finite fields*, J. Symb. Comp. 25(1), pp. 1-21 (1998)
15. J. Pila, *Frobenius maps of abelian varieites and finding roots of unity in finite fields*, Math. Comp. 55(192), pp. 745–763 (1990)
16. K.S. Kedlaya, *Counting points on hyperelliptic curves using Monsky-Washnitzer cohomology*, J. Ramanujan Math. Soc. **16** (2001), 323–338.
17. T. Satoh, *The canonical lift of an ordinary elliptic curve over a finite field and its point counting*, J. Ramanujan Math. Soc. **15** (2000), 247–270.
18. J. Denef and F. Vercauteren, *An Extension of Kedlaya's Algorithm to Hyperelliptic Curves in Characteristic 2*, J. Cryptology **19** (2006), 1–25.
19. S. Haloui, *The characteristic polynomials of abelain varieites of dimensions 3 over finite fields*, J. number theory, 2011.

Gyoyong Sohn received the Ph.D degree in Mathematics from Kyungpook National University in 2008. He has been an assistant professor in Department of Mathematics Education at Daegu National University since 2012. His research interests include computational algebraic geometry and cryptography.

Department of Mathematics Education, Daegu National University of Education, Daegu National University of Education, Daegu 705-715, Korea.
e-mail: gysohn@dnue.ac.kr