コンピュータセキュリティ　10－11
（2000.　7.　25）

超楕円曲線のヤコビ多様体の位数計算について

佐藤尚宜　　高橋昌史

(株) 日立製作所システム開発研究所

〒244-0817 横浜市戸塚区吉田町292番地
{hisato, takahasi}@sdl.hitachi.co.jp

あらまし
安全な超楕円曲線暗号を構成する上で超楕円曲線に付随するヤコビ多様体の位数計算は最も重要な課題の一つである。本稿では有限体上定義された種数2の超楕円曲線とそのヤコビ多様体の有理点の個数を計算する効率的な方法を提案する。超楕円曲線の有理点の個数はゼータ関数の分子の係数を用いて計算されるが、それを直接計算するのではなく、定義体の標数を法とした計算で係数の候補を算出することにより高速な位数計算を可能にした。また実装実験結果についても報告する。

キーワード
公開鍵暗号, 超楕円曲線, 離散対数問題, ヤコビ多様体

On Counting the Rational Points on Hyperelliptic Curves of genus 2 over Finite Fields

Hisayoshi SATO　　Masashi TAKAHASHI

Systems Developement Laboratory, Hitachi, Ltd.

292 Yoshida-cho, Tostuka-ku, Yokohama 244-0817, Japan
{hisato, takahasi}@sdl.hitachi.co.jp

Abstract.
When constructing secure hyperelliptic curve cryptosystems, counting the number of rational points on hyperelliptic curve and its jacobian variety defined over finite fields is one of the most important problem. In this paper we propose an effcient method of counting the number of rational points. In this method, we improved the formula for the coefficients (modulo characteristic of defined fields) of the numerator of congruent zeta function which are related to the number of rational points on the Jacobian varieties, in order to implement efficiently.Moreover we report on some experimental results.

Keywords.
Public key cryptography, Hyperelliptic curve, Discrete logarithm problem, Jacobian variety

1 Introduction

As a natural generalization of elliptic curve cryptosystems (ECC) [MIL85, KO87] , Koblitz [KO88, KO89] has proposed hyperelliptic curve cryptosystems (HECC) based on the discrete logarithm problem for the Jacobian varieties of the curves defined over finite fields. As in the case of ECC, the security of HECC depends on the number of of rational points on hyperelliptic curves and their Jacobian varieties. In theory the number of rational points can be computed in polynomial time using methods due to Adleman, Huang[AH96] and Pira[PI90]. These methods are generalralizations of the method of Schoof[Sc85], and some work on its implementation has been reported[GH00]. But these methods are not practical. At the moment, one of the problems to implement is that there is no known analogue of the improvements of Atkins and Elkies to the Schoof algorithm[Sc95]. Original Schoof algoritm[Sc85] is ineffcient even for elliptic curves.

In this paper, we propose an efficient method of counting the number of rational points on hyperelliptic curves of genus 2 and their Jacobian varieties over finite fields. In this method, we improved the formula for the coefficients (modulo prime p) of the numerator of congruent zeta function which are related to the number of rational points on the Jacobian varieties, in order to implement efficiently. In section 2, we recall some general facts regarding on the hyperelliptic curves and its Jacobian varietes. In section 3, we will describe a general strategy for point counting and derive an explicit formula for some special case. Finally we report on some experimental results in section 4.

2 General Facts

Here is a brief review of some general facts on hyperelliptic curves and jacobian varieties. (For more detail, see [Ko89, Ko98].)

Let p be an odd prime and $q = p^n$ be some power of p. Let $\mathbb{F}_q$ denote the finite field with q elements and $\hat{\mathbb{F}}_q^*$ be the character group (the group of homomorphisms from $\mathbb{F}_q^* = \mathbb{F}_q \setminus \{0\}$ to the multiplicative group of complex numbers). We consider an affine curve given by the equation

$$C : y^2 = f(x) = x^{2g+1} + a_1x^{2g} + a_2x^{2g-1} + \cdots + a_{2g}x + a_{2g+1} \quad (a_i \in \mathbb{F}_q),$$

where the discriminant of $f \neq 0$. Then C defines a smooth projective curve (in some projective space) which is called a **hyperelliptic curve**. (There exists only one point which is on the hyperelliptic curve, but not on the affine curve C. We call this "point at infinity" and denote ∞.) In an abuse of the notation, C also denotes the projective curve. The genus of C is equal to g, where the genus is defined as the dimension of the space of regular differential forms on the curve over the algebraic closure of $\mathbb{F}_q$. If $g = 1$, then C is called an **elliptic curve**.

For any finite extension $\mathbb{F}_{q^m}$ of $\mathbb{F}_q$, let $C(\mathbb{F}_{q^m})$ be the set of $\mathbb{F}_{q^m}$-rational points on C. For $a \in \mathbb{F}_{q^m}$, there exist $\mathbb{F}_{q^m}$-rational points on C that have an x-coordinate a if and only if $f(a)$ is a square in $\mathbb{F}_{q^m}$, and when that is the case, two such points will exist if $f(a) \neq 0$, and one point will exisit if $f(a) = 0$. Moreover, let $\chi_m(\neq 1) \in \hat{\mathbb{F}}_{q^m}^*$ be the unique character of order 2, then $f(a)(\neq 0)$ is a square in $\mathbb{F}_q$ if and only if $\chi_m(f(a)) = 1$ (we extend $\chi_m(0) = 0$). Thus the number of elements in $C(\mathbb{F}_{q^m})$ is given by

$$\#C(\mathbb{F}_{q^m}) = 1 + \sum_{x \in \mathbb{F}_{q^m}} (\chi_m(f(x)) + 1) = 1 + q^m + \sum_{x \in \mathbb{F}_{q^m}} \chi_m(f(x)).$$

Next, we will briefly review on the Jacobian varieties associated with hyerelliptic curves.

For a point $P = (x, y) \in C$, let $\tilde{P} := (x, -y)$ be the opposite of P.If $P = \tilde{P}$, then P is called special (otherwise P is said to be ordinary). For two divisors $D_1 = \sum m_P(P)$ and $D_2 = \sum n_P(P)$ on C (formal (finite) sums of points on C), the greatest common divisor of D_1, D_2 is defined by

$$\gcd(D_1, D_2) := \sum \min(m_P, n_P)(P) - \left(\sum \min(m_P, n_P)\right)(\infty).$$

A divisor D on the hyperelliptic curve C is called semi-reduced if $D = \sum m_P(P) - (\sum m_P)(\infty)$, $m_P \geq 0$, and for $P \in \mathrm{Supp}(D) = \{P | n_P \neq 0\}$, $\tilde{P} \notin \mathrm{Supp}(D)$ if P is ordinary, and $m_P = 1$ if special.

A semi-reduced divisor $D = \sum m_P(P) - (\sum m_P)(\infty)$ is called reduced if $\sum m_P \leq g$ (g : genus of C). Then for each divisor of degree 0, there exists a unique reduced divisor that is linearly equivalent to the given divisor. Moreover we have the following theorem.

Theorem 2.1 *Let $D = \sum m_i(P_i) - (\sum m_i)(\infty)$ be a semi-reduced divisor on the hyperelliptic curve C and $P_i = (\alpha_i, \beta_i)$. Let $a(x) = \prod(x - \alpha_i)^{m_i}$. Then there exists unique polynomial function $b(x)$ on C such that:*

(1) $\deg_x b < \deg_x a (\leq g)$,

(2) $b(\alpha_i) = \beta_i$ for any i (such that $m_i \neq 0$),

(3) $b^2 \equiv f \bmod a$.

Then, we have $D = \gcd(\mathrm{div}(a), \mathrm{div}(b - y))$.

The Jacobian variety $J/\mathbb{F}_q$ of C is a g-dimensional abelian variety (= projective group variety) which has the following properties:

For any point P on C, there exists an injective map $F^P : C \to J$ such that $F^P(P) = O_J$ and for any rational map ϕ from C to an abelian variety A, there exists unique homomorphism $\psi : J \to A$ such that $\phi = \psi \circ F^P$.

The set $J(\mathbb{F}_q)$ of $\mathbb{F}_q$-rational points on J is a finite abelian group (with respect to some group law). If $g = 1$ (that is, C is an elliptic curve), then C and J are isomorphic. Hence in this case, $C(\mathbb{F}_q)$ is itself an abelian group.

It is well-known that $J(\mathbb{F}_q)$ is isomorphic to the group $\mathrm{Pic}^0_{\mathbb{F}_q}(C)$ of linearly equivalent classes of $\mathbb{F}_q$-rational divisors that have degree 0. Hence we can treat a point on J as a pair of polynomials in x as in Theorem 2.1:

$$J(\mathbb{F}_q) = \left\{(a(x), b(x)) \mid a, b \in \mathbb{F}_q[x], a = \prod(x - \alpha_i)^{m_i} (\text{in } \bar{\mathbb{F}}_q), \text{and } (1),\ (3) \text{ in Theorem2.1}\right\}.$$

(Note that property (2) is not needed in above.)

From here, we will concentrate on the case of genus 2 (and prime fields). Then a hyperelliptic curve C of genus 2 has a defining equation of the form

$$C : y^2 = x^5 + ax^4 + bx^3 + cx^2 + dx + e.$$

Let us define a_i and M_i $(i = 1, 2)$ as integers which satisfy

$$\begin{cases} \#C(\mathbb{F}_p) = M_1 = 1 + p + a_1 = 1 + p + \sum_{x \in \mathbb{F}_p} \chi(f(x)), \\ \#C(\mathbb{F}_{p^2}) = M_2 = 1 + p^2 + 2a_2 - a_1^2 = 1 + p^2 + \sum_{x \in \mathbb{F}_{p^2}} \chi_2(f(x)), \end{cases}$$

where $\chi(\neq 1) \in \hat{\mathbb{F}}_p^*$, $\chi^2 = 1$ and $\chi_2(\neq 1) \in \hat{\mathbb{F}}_{p^2}^*$, $\chi_2^2 = 1$

Then the numerator $P(T)$ of the zeta function $Z(C/\mathbb{F}_p, T)$ of C is given by

$$\begin{aligned} P(T) &= p^2T^4 + a_1pT^3 + a_2T^2 + a_1T + 1 \\ &= (1 - \alpha T)(1 - \bar{\alpha}T)(1 - \beta T)(1 - \bar{\beta}T) \quad |\alpha| = |\beta| = \sqrt{p} \quad (\bar{\ } : \text{ complex conjugate}). \end{aligned}$$

Let $J/\mathbb{F}_p$ be the jacobian variety of C. Then it is known that the number of $\mathbb{F}_p$-rational points on J is given by

$$\#J(\mathbb{F}_p) = P(1) = 1 + a_1 + a_2 + pa_1 + p^2.$$

More generally, the facts described below are known (Weil conjecture):

Theorem 2.2 *Notation is as above.*

(1) (Functional equation) $P(T)$ is a polynomial with integer coefficients of the form

$$\begin{aligned} P(T) &= 1 + a_1T + a_2T^2 + \cdots + a_{g-1}T^{g-1} + a_gT^g \\ &\quad + qa_{g-1}T^{g+1} + q^2a_{g-2}T^{g+2} + \cdots + q^{g-1}a_1T^{2g-1} + q^gT^{2g}. \end{aligned}$$

(2) (The Riemann Hypothesis) $P(T)$ factors as

$$P(T) = \prod_{i=1}^{g}(1 - \alpha_iT)(1 - \bar{\alpha}_iT), \quad |\alpha_i| = \sqrt{q}, \quad \text{(where}\ \bar{\ }\ \text{means the complex conjugate)}$$

(3) The number of rational points on J is given by

$$\#J(\mathbb{F}_{q^m}) = \prod_{i=1}^{g}|1 - \alpha_i^m|^2 = \prod_{i=1}^{g}(1 - \alpha_i^m)(1 - \bar{\alpha}_i^m).$$

In particular, $\#J(\mathbb{F}_q) = P(1)$.

By the definition of the zeta function, it can easily be seen that

$$\frac{P'(T)}{P(T)} = \sum_{n\geq 0}(M_{n+1} - 1 - q^{n+1})T^n.$$

Hence, by comparing the coefficients of T^n on both sides, we have

$$\begin{array}{rcl} M_1 - 1 - q & = & a_1, \\ M_2 - 1 - q^2 & = & 2a_2 - a_1^2, \\ M_3 - 1 - q^3 & = & 3a_3 - 3a_1a_2 + a_1^3, \\ \vdots & & \end{array}$$

(3) of Theorem 2.2 and the relations between the roots and the coefficients of $P(T)$ gives rise to a bound $|a_i| \leq \binom{2g}{i}\sqrt{q}^i$. Therefore the following holds:

$$|\#C(\mathbb{F}_q) - 1 - q| \leq 2g\sqrt{q},$$
$$|\#J(\mathbb{F}_q) - 1 - q^g| \leq \sum_{i=1}^{g}\binom{2g}{i}\sqrt{q}^i(1 + q^{g-i}).$$

For example, if the case of $g = 2$, then we have $|\#J(\mathbb{F}_q) - 1 - q^2| \leq 4q^{\frac{3}{2}} + 6q + 4q^{\frac{1}{2}}$, and for the case of $g = 3$, $|\#J(\mathbb{F}_q) - 1 - q^3| \leq 6q^{\frac{5}{2}} + 15q^2 + 20q^{\frac{3}{2}} + 15q + 6q^{\frac{1}{2}}$.

3 A strategy for counting the number of rational points

As in the previous section, let $C : y = f(x)$ be a hyperelliptic curve of genus 2 defined over a prime field $\mathbb{F}_p$. In this section, we consider methods of counting the number of rational points on the Jacobian variety J of C. As mentioned in the previous section, if we have $M_1 = \#C(\mathbb{F}_p)$ and $M_2 = \#C(\mathbb{F}_{p^2})$, then $\#J(\mathbb{F}_p)$ is easily calculated. Moreover, by applying Theorem 2.2 (3), we can easily calculate $\#J(\mathbb{F}_{p^n})$.

If the characteristic p is small, then we can calculate M_1 and M_2 by using the formula in Section 2. To calculate the value of the character χ (resp. χ_2), we can use Euler's criterion: $\chi(a) = a^{\frac{p-1}{2}} (= \pm 1 \text{ in } \mathbb{F}_p)$ (resp. $\chi(a) = a^{\frac{p^2-1}{2}} (= \pm 1 \text{ in } \mathbb{F}_{p^2})$). However, in this calculation, in particular for M_2, we must sum over $\mathbb{F}_{p^2}$ which has p^2 elements. Hence this method requries at least $O(p^2)$ operations. Thus we need a more efficient method for big p. In the following, we consider a method which M_2 does not need to be calculated directly.

Remarks.

In general, for a hyperelliptic curve C of genus g, we must calculate $\#C(\mathbb{F}_p)$, $\#C(\mathbb{F}_{p^2})$, ..., $\#C(\mathbb{F}_{p^g})$.

We start with a simple lemma.

Lemma 3.1 *Let $\mathbb{F}_q$ be a finite field. Then we have $\sum_{x\in\mathbb{F}_q} x^i = -1$ if $q - 1|i > 0$, and 0 otherwise.*

Proof. For any $x \in \mathbb{F}_q \setminus 0$, we have $x^{q-1} = 1$. Hence if $q - 1|i$, then $\sum_{x\in\mathbb{F}_q} x^i = \sum_{x\in\mathbb{F}_q\setminus 0} 1 = q - 1 = -1$ (as an element in $\mathbb{F}_q$). On the other hand, if $q - 1 \not| i$, then there exists some $y \in \mathbb{F}_q$ such that $y^i \neq 1$. Then $y^i(\sum_{x\in\mathbb{F}_q} x^i) = \sum_{x\in\mathbb{F}_q}(yx)^i \sum_{x\in\mathbb{F}_q} x^i$, hence $(y^i - 1)\sum_{x\in\mathbb{F}_q} x^i = 0$ and $y^i - 1 \neq 0$. This gives the desired result. ∎

For a power $q = p^n$ $(n = 1, 2, \ldots)$ of p, let us define $A_i^{(n)} \in \mathbb{F}_p$ by the following relation:

$$f(x)^{\frac{q-1}{2}} =: \sum A_i^{(n)} x^i.$$

Then by the lemma gives us $\#C(\mathbb{F}_q) \equiv 1 - (A_{q-1}^{(n)} + A_{2(q-1)}^{(n)}) \pmod p$. Moreover, in the case of $q = p^2$, it can easily be seen that $f(x)^{\frac{p^2-1}{2}} = f(x)^{\frac{p-1}{2}}\left(f(x)^{\frac{p-1}{2}}\right)^p$ (in $\mathbb{F}_p[x]$).

Hence, as elements in $\mathbb{F}_p$, we have

$$\left\{\begin{array}{rcl} A^{(2)}_{p^2-1} & = & \left(A^{(1)}_{p-1}\right)^2 + A^{(1)}_{2p-1}A^{(1)}_{p-2} \\ A^{(2)}_{2(p^2-1)} & = & \left(A^{(1)}_{2(p-1)}\right)^2 + A^{(1)}_{2p-1}A^{(1)}_{p-2}. \end{array}\right. \qquad \text{(in } \mathbb{F}_p\text{)}$$

Therefore, by the definition of a_1, a_2, we have

$$\left\{\begin{array}{lcll} a_1 & \equiv & -(A^{(1)}_{p-1} + A^{(1)}_{2(p-1)}) \quad \bmod p \quad (|a_1| < 4\sqrt{p}) & (1) \\ a_2 & \equiv & A^{(1)}_{p-1}A^{(1)}_{2(p-1)} - A^{(1)}_{2p-1}A^{(1)}_{p-2} \quad \bmod p & (2). \end{array}\right.$$

Hence, a_1 mod p and a_2 mod p are calculated in terms of the coefficients of $f(x)^{\frac{p-1}{2}}$ mod p.

The Riemann Hypothesis (Theorem 2.2 (2) R-H) for the congruent zeta function of hyperelliptic curve $C/\mathbb{F}_p$ tells us that $|a_1| < 4\sqrt{p}$ (note that the genus of C is 2). Therefore, if $64 < p$, we can determine a_1 by the above relation (1).

Similarly, by using the R-H, we obtain $-2p + a_1^2/2 \leq a_2 \leq 2p + a_1^2/2$. Thus there are 4 or 5 possible values for a_2. More explicitly, let a_2' be an integer which satisfies (2) and $-2p + a_1^2/2 \leq a_2' < p + a_1^2/2$. Then all possible values of a_2 are $a_2' + ip$, $i = 0, 1, 2, 3$ (or 4). Since $1 + a_1 + a_1 p + p^2$ is even, we can obtain $\#J(\mathbb{F}_p) \equiv a_2$ mod 2 ($\#J(\mathbb{F}_p) = 1 + a_1 + a_1 p + p^2 + a_2$) and by the type of factorization of $f(x)$ mod p (see below), we can have $\#J(\mathbb{F}_p)$ mod 2. Thus we can restrict the possible values of a_2 to 2 or 3.

Finally, if we can determine $\#J(\mathbb{F}_p)$ mod ℓ for a (small) prime ℓ, then the value for a_2 is determined, because 0 and $2p$ (and $-2p$) modulo ℓ have different values.

By the type of factorization of $f(x)$, we can easily have $\#J(\mathbb{F}_q)$ mod 2.

Lemma 3.2 *Let* $f(x) = \prod_{i=1}^{5}(x - a_1)$ *(in* $\bar{\mathbb{F}}_q$*), and* $P_i := (a_i, 0)$. *Then we have*

$$\begin{array}{rcl} J(\bar{\mathbb{F}}_q)[2] & = & \langle (P_1) - (\infty)\rangle \times \langle (P_2) - (\infty)\rangle \times \langle (P_3) - (\infty)\rangle \times \langle (P_4) - (\infty)\rangle \\ & = & \{O, (P_i) - (\infty)\ (i = 1, \ldots, 5),\ (P_i) + (P_j) - 2(\infty)\ (1 \leq i < j \leq 5)\}. \end{array}$$

Proof. This follows from the uniqueness of the reduced divisor on the hyperelliptic curve in a linearly equivalent class, $\operatorname{div}(y) = \sum_{i=1}^{5}(P_i) - 5(\infty)$ and $\#J[2] = 2^4$. ∎

Proposition 3.1 $\#J(\mathbb{F}_q)$ *is even if and only if* $f(x)$ *has at least one factor of degree 1 or 2 (in* $\mathbb{F}_q[x]$*) or equivalently,* $\deg(\mathrm{GCD}(x^{p^2} - x, f(x))) \geq 1$.

Proof. The notations are as in Lemma 3.2. Divisor $(P_i) - (\infty)$ is $\mathbb{F}_q$-rational if and only if $a_i \in \mathbb{F}_q$, and $(P_i) + (P_j) - 2(\infty)$ is rational if and only if $a_i^q = a_j$, thus a_i and a_j are roots of a quadratic equation over $\mathbb{F}_q$ which divides $f(x)$. ∎

Next we will consider how $A_i^{(1)}$'s are calculated for a reasonably large characteristic p.

Let $f(x) = x^5 + ax^3 + bx^2 + cx + d$. Then the coefficients $A_n^{(1)}$ of x^n in $f(x)^{\frac{p-1}{2}}$ are given by

$$\sum \binom{\frac{p-1}{2}}{i}\binom{\frac{p-1}{2} - i}{j}\binom{\frac{p-1}{2} - i - j}{k}\binom{\frac{p-1}{2} - i - j - k}{l} a^j b^k c^l d^{\frac{p-1}{2} - i - j - k - l}$$

where the sum is taken over i, j, k, l such that $5i + 3j + 2k + l = n$, $0 \leq i \leq m$, $0 \leq j \leq m - i$, $0 \leq k \leq m - i - j$, $0 \leq l \leq m - i - j - k$.

As a simpler example, we will consider the case for the defining equation f is given by 3-terms:

$$f(x) = x^5 + ax^u + b \qquad (1 \leq u \leq 4).$$

Then $A_n := A_n^{(1)}$ is given by $A_n = \sum \binom{\frac{p-1}{2}}{i}\binom{\frac{p-1}{2} - i}{j} a^j b^{\frac{p-1}{2} - i - j}$ where the sum is taken over i, j such that $5i + uj = n$, $0 \leq i \leq \frac{p-1}{2}$, $0 \leq j \leq \frac{p-1}{2} - i$.

Let $s = 5^{-1}n \pmod{u}$, $0 \leq s \leq u-1$, then i which apears in the above sum must be congruent to s mod u, thus if we change the suffix so that $i = s + tu$, then there exist some integers M_1, M_2, and A_n can be written as

$$A_n = \sum_{t=M_1}^{M_2} \binom{\frac{p-1}{2}}{s+tu} \binom{\frac{p-1}{2} - (s+tu)}{K-5t} a^{K-5t} b^{\frac{p-1}{2}-s-K+(5-u)t},$$

where $K := (n-5s)/u \in \mathbb{Z}$. Since it holds that $i!(p-1-i)! \equiv (-1)^{i+1} \bmod p$, we have

$$A_n = \left(\frac{p-1}{2}\right)! a^K b^{\frac{p-1}{2}-s-K} \sum_{t=M_1}^{M_2} \frac{(-1)^{K-5t+1}(p-1-K+5t)!}{(s+tu)!\,(\frac{p-1}{2}-s-K+(5-u)t)!} \left(\frac{b^{5-u}}{a^5}\right)^t.$$

Let B_t be the t-th term of the above sum. Then there exists a multiplicative relation between B_t and B_{t-1}. Hence we can calculate A_n by repeating $B \leftarrow c(t)B$ and $A \leftarrow A + B$.

We will now sum up the above discussion and give explicit formulae:

Theorem 3.1 *For a given p and an equation $y^2 = f(x) = x^5 + ax^u + b$, we set:*

$$\begin{cases} s := 5^{-1}n \pmod{u} \ (0 \leq s \leq u-1), \\ K := \dfrac{n-5s}{u} \ (\in \mathbb{Z}), \\ M_1 := \text{ceiling of } \max\left\{-\dfrac{s}{u}, \dfrac{1}{5-u}\left(K + s - \dfrac{p-1}{2}\right)\right\}, \\ M_2 := \text{floor of } \dfrac{K}{5}. \end{cases}$$

Then A_n is given by

$$A_n = \left(\frac{p-1}{2}\right)! a^K b^{\frac{p-1}{2}-s-K} \sum_{t=M_1}^{M_2} B_t,$$

where

$$B_{M_1} := \frac{(-1)^{K-5M_1+1}(p-1-K+5M_1)!}{(s+M_1u)!(\frac{p-1}{2}-s-K+(5-u)M_1)!} \left(\frac{b^{5-u}}{a^5}\right)^{M_1},$$

$$B_t = B_{t-1} \frac{-f_5(p-1-K+5t)}{f_u(s+ut)f_{5-u}(\frac{p-1}{2}-s-K+(5-u)t)} \frac{b^{5-u}}{a^5} \qquad (M_1 < t \leq M_2).$$

where $f_m(x) := x(x-1)\cdots(x-i+1)$.

Remarks.

1. All of the above calculations must be done in $\mathbb{F}_p$.
2. Note that s, M and K depend on the given p, u and n (we must calculate A_n's for $n = p-2, p-1, 2(p-1)$ and $2p-1$), and independent on a and b. Hence for given p and u, we can calculate s, M, K and the factorials in B_M previously.
3. For higher genus, the formulae become quite complicated. The same method can, however, still applied.

4 Experimental results

In this section, we report some experimental results of implementation of our method. We used the MAPLE algebra program on a PC with Pentium III 500MHz CPU. In view of using optimal extention field[BP98], we used a 16-bit prime field.

We calculated the number of $\mathbb{F}_p$-rational points on the Jacobian varieties of hyperelliptic curves of genus 2 defined by equations in the following forms. For each example listed in Appendix, the order of the group $J(\mathbb{F}_{p^7})/J(\mathbb{F}_p)$ is about 192-bit prime number. The average time for calculation of a_1 and a_2 (determination) was 6.49 seconds. (excluding the calculation of the order $\#J(\mathbb{F}_{p^7})$ and prime factoring)

We have calculated $y^2 = x^5 + ax^3 + 1/\mathbb{F}_p$, $1 \leq a \leq 1000$ and $y^2 = x^5 + x^3 + b/\mathbb{F}_p$, $1 \leq b \leq 1000$ and found 55 curves which have prime order for $(J(\mathbb{F}_{p^7})/J(\mathbb{F}_p))$.

5 Conclusion

We proposed a method of counting points on the Jacobian varieties of hyperelliptic curves over finite fields. In this method, we improved the formula for the coefficients (mod p) of the numerator of congruent zeta function which are related to the number of rational points on the Jacobian varieties, in order to implement efficiently. The average time so as to calculate the main part of our method was 6.49 seconds.

References

[ADH94] L.M. Adleman, J. DeMarrais and M. Huang, "A Subexponential Algorithm for Discrete Logarithm over the Rational Subgroup of the Jacobians of Large Genus Hyperelliptic Curves over Finite Fields", *Algorithmic Number Theory I*, LNCS, **877** (1998), Springer-Verlag, 28–40.

[AH96] L.M. ADLEMAN and M. HUANG, "Counting Rational Points on Curves and Abelian Varieties over Finete Fields", *Algorithmitic Number Theory II,LNCS*,1122 (1996),Springer-Verlag,28-40.

[BP98] D.V. Bailey and C. Paar "Optimal Extension Fields for Fast Arithmetic in Public-Key Algorithms", *Advances in Cryptology – CRYPTO'98*, LNCS, **1462** (1998), Springer-Verlag, 472–485.

[FR94] 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), 865–874.

[GA00] P. Gaudry, "An Algorithm for Solving the Discrete Log Problem on Hyperelliptic Curves", *Advances in Cryptology - EUROCRYPT2000,LNCS*,1807,(2000), Springer-Verlag,19-43.

[GH00] P. Gaudry and R. Harley, "Counting Points on Hyperelliptic Curves over FiniteFields", preprint

[Ko87] N. Koblitz, "Elliptic curve cryptosystems", *Mathematics of Computation*, **48** (1987), 203–209.

[Ko88] N. Koblitz, "A Family of Jacobians Suitable for Discrete Log Cryptosystems", *Advances in Cryptology - CRYPTO'88*, LNCS, **403** (1988), Springer-Verlag, 94–99.

[Ko89] N. Koblitz, "Hyperelliptic Cryptosystems", *J. Cryptology*, **1** (1989), Springer-Verlag, 139–150.

[Ko98] N. Koblitz, "Algebraic Aspects of Cryptography", Springer-Verlag, (1998)

[Mil85] V. Miller, "Uses of elliptic curves in cryptography", *Advances in Cryptology – CRYPTO'85*, LNCS, **218** (1986), Springer-Verlag, 417–426.

[Pi90] J. Pila, "Frobenius maps of abelian varieties and finding roots of unity in finite fields", *Math. Comp*, **55**, No.206 (1990), 745-763.

[Ru99] H.G. Rück, "On the discrete logarithms in the divisor class group of curves", *Math. Comp.* **68**(226) (1999), 805–806.

[Sc85] R. Schoof, "Elliptic Curves over Finite Fields and the Computation of Square Roots mod p", *Math. Comp*, **44**(1985), 483-494.

[Sc95] R. Schoof, "Counting Points on Elliptic Curves over Finite Fields", *J. Théor Nombres Boadeaux* **7** (1995), 219-254.

[Sm99] N.P. Smart, "On the performance of hyperelliptic cryptosystems", *Advances in Cryptology – EUROCRYPT'99*, LNCS, **1592** (1999), Springer-Verlag, 165–175.

A Curve examples

$p = 65521 =$ largest prime less than 2^{16}
$(a, b, u) = \{C : y^2 = x^5 + ax^u + b/\mathbb{F}_p\}$
$J = J(C)$: the Jacobian variety of C.

$C : y^2 = x^5 + ax^3 + 1/\mathbb{F}_p$

$y^2 = x^5 + 20x^3 + 1$
$\#J(\mathbb{F}_p) = 4292069372 = (2^2) * (19) * (347) * (162751)$
$\#(J(\mathbb{F}_{p^7})/J(\mathbb{F}_p)) =$
$6261242248149854411491526925185309068882545646066170969601$

$y^2 = x^5 + 30x^3 + 1$
$\#J(\mathbb{F}_p) = 4283385114 = (2) * (3) * (713897519)$
$\#(J(\mathbb{F}_{p^7})/J(\mathbb{F}_p)) =$
$6273936470508174010741372129455062873918789656819030488481$

$y^2 = x^5 + 75x^3 + 1$
$\#J(\mathbb{F}_p) = 4291540462 = (2) * (11) * (195070021)$
$\#(J(\mathbb{F}_{p^7})/J(\mathbb{F}_p)) =$
$6262013913631466956030152270611851263819204142157300476369$

$y^2 = x^5 + 82x^3 + 1$
$\#J(\mathbb{F}_p) = 4271964544 = (2^7) * (17) * (1963219)$
$\#(J(\mathbb{F}_{p^7})/J(\mathbb{F}_p)) =$
$6290709065387883037427482065152628515560124077180084611601$

$C : y^2 = x^5 + x^3 + b/\mathbb{F}_p$

$y^2 = x^5 + x^3 + 62$
$\#J(\mathbb{F}_p) = 4309251388 = (2^2) * (13) * (23) * (3603053)$
$\#(J(\mathbb{F}_{p^7})/J(\mathbb{F}_p)) =$
$6236277177699992278686480666591981062513907089062982993161$

$y^2 = x^5 + x^3 + 75$
$\#J(\mathbb{F}_p) = 4285555915 = (5) * (61) * (151) * (93053)$
$\#(J(\mathbb{F}_{p^7})/J(\mathbb{F}_p)) =$
$6270758477306301290323521925241066596926028162900097596969$

$y^2 = x^5 + x^3 + 103$
$\#J(\mathbb{F}_p) = 4291596612 = (2^2) * (3^2) * (119211017)$
$\#(J(\mathbb{F}_{p^7})/J(\mathbb{F}_p)) =$
$6261931983265442616781851094698463546551985997709940226161$

$y^2 = x^5 + x^3 + 121$
$\#J(\mathbb{F}_p) = 4303436782 = (2) * (2151718391)$
$\#(J(\mathbb{F}_{p^7})/J(\mathbb{F}_p)) =$
$6244703348812064705456262466347507146579044296618771608521$