Memoirs of the Faculty of Engineering, Okayama University, Vol. 42, pp. 110-114, January 2008

A Method for Checking the Parity of $(\#J_C - 1)/2$ *of Genus* 2 *and* 3 *Hyperelliptic Curves*

Yasuyuki NOGAMI
Graduate School of Natural Science
and Technology, Okayama University
3-1-1, Tsushima-naka, Okayama, Japan

Yoshitaka MORIKAWA
Graduate School of Natural Science
and Technology, Okayama University
3-1-1, Tsushima-naka, Okayama, Japan

(Received December 4, 2007)

This paper shows a method for checking the parity of $(\#J_C - 1)/2$ without calculating the order $\#J_C$, where $\#J_C$ is the order of genus 2 or 3 hyperelliptic curve.

1 INTRODUCTION

This paper especially deals with genus 2 and 3 *no two–torsion* hyperelliptic curves over prime field F_p, where a genus one curve is an elliptic curve. *No two–torsion* means that the curve has *no two–torsion* points, in other words, $\#J_C$ is not divisible by 2, where $\#J_C$ denotes the order over F_p. For no two–torsion curves, this paper shows a method for checking the parity of $(\#J_C - 1)/2$ without calculating the order $\#J_C$. This paper is the extended version of our previous work[1].

Throughout this paper, characteristic p is a prime number larger than 5. $F_{p^m} - F_p$ denotes the set of elements which belong to F_{p^m} but not F_p.

2 PRELIMINARY

In this section, we briefly go over the fundamentals of quadratic residue/non-residue, shift product–based polynomial transform (SPPT), and genus 2 and 3 hyperelliptic curves defined over prime field F_p.

2.1 Quadratic residue/non-residue

For a non-zero element $c \in F_q$, we can check whether c is a quadratic residue (QR) or quadratic non-residue (QNR) in F_q as follows:

$$c^{(q-1)/2} = \begin{cases} 1 & \text{when } c \text{ is a QR} \\ -1 & \text{when } c \text{ is a QNR} \end{cases}. \quad (1)$$

The product of two non-zero QRs and that of two QNRs become QRs in F_q. On the other hand, the product of a QR and a QNR becomes a QNR in F_q. In this paper, we use the fact that all elements in F_p are QRs in F_{p^2} , in addition, whether or not a non-zero element $a \in F_p$ is a QR in F_p is equivalent to that in F_{p^3}.

2.2 Shift product–based polynomial transform

Shift product–based polynomial transform (SPPT) is defined as follows[1]. Let $f(x)$ be an irreducible polynomial of degree m over F_p. According to SPPT[1], when $m < p$ and $\gcd(k, m) = 1$, we can uniquely determine another irreducible polynomial $f_k(x)$ of degree m over F_p from the given irreducible polynomial $f(x)$ such that

$$F_k(x) = f_k(x^{p^k} - x) \quad = \quad f(x) \prod_{j=1}^{p^k-1} f(x + s^j), \quad (2)$$

where s is a generator of $F^*_{p^k}$ (*see* **App**.A). Let ω be a zero of $f(x)$, a zero τ of $f_k(x)$ is given by $\tau = \omega^{p^k} - \omega$. In other words, $f_k(x)$ is the minimal polynomial of $\omega^{p^k} - \omega$. In what follows, we call the transformation from $f(x)$

to $f_k(x)$ *SPPT over* F_{p^k}. SPPT is just the minimal polynomial determination for $\tau = \omega^{p^k} - \omega$.

2.3 Hyperelliptic curve

In this paper, let the definition field be the prime field F_p, we particularly deal with genus $g = 2$ and 3 hyperelliptic curves in the following form :

$$H(x, y) = f(x) - y^2 = 0,\ f(x) = H(x, 0), \tag{3}$$

where $f(x)$ is an irreducible polynomial of degree $2g+1$ over F_p. Let $\#J_C$ be the order over F_p, it is given by[2]

$$\begin{aligned} g = 2 : \quad \#J_C &= p^2 + 1 + s_1(p+1) + s_2, && \text{(4a)} \\ s_1 &= M_1 - 1 - p, && \text{(4b)} \\ s_2 &= (M_2 - 1 - p^2 + s_1^2)/2, && \text{(4c)} \end{aligned}$$

$$\begin{aligned} g = 3 : \quad \#J_C &= p^3 + 1 + s_1(p^2+1) + s_2(p+1) + s_3, && \text{(5a)} \\ s_1 &= M_1 - 1 - p, && \text{(5b)} \\ s_2 &= (M_2 - 1 - p^2 + s_1^2)/2, && \text{(5c)} \\ s_3 &= (M_3 - 1 - p^3 - s_1^3 + 3s_1 s_2)/3, && \text{(5d)} \end{aligned}$$

where M_1, M_2, and M_3 are the numbers of the rational points of the hyperelliptic curve $H(x, y) = 0$ over F_p, F_{p^2}, and F_{p^3}, respectively[2]. Since $H(x, 0)$ of degree $2g + 1$ is irreducible over F_p in this paper, it is also irreducible over the concerned extension field. In addition, s_1, s_2, and s_3 are odd numbers.

2.4 The number of rational points over F_p

Noting that the definition field of hyperelliptic curve Eq.(3) is prime field F_p and let the number of QRs in the following set be N_1 :

$$\{H(0, 0), H(1, 0), H(2, 0), \cdots, H(p-1, 0)\}. \tag{6}$$

The number of rational points on $H(x, y) = 0$ over F_p, that is M_1, is given by

$$M_1 = 2N_1 + 1, \tag{7}$$

where we should note that $H(i, 0), i \in F_p$ does not become 0 because $H(x, 0)$ is irreducible over F_p in this paper. The number of QNRs is given by $p - N_1$. From Eq.(4b) and Eq.(7), we find that s_1 becomes an odd number when $H(x, 0)$ is irreducible.

2.5 The number of rational points over F_{p^2}

Noting that the coefficients of $H(x, y)$ are in F_p, as introduced in **Sec**.2.1, every element in the set Eq.(6) become QRs in F_{p^2}. In other words, substituting each element in F_p for x, we have the following $2p$ rational points over F_{p^2} :

$$\left(i, \pm\sqrt{H(i, 0)}\right),\ 0 \le i \le p - 1. \tag{8}$$

On the other hand, for an arbitrary element α in $F_{p^2} - F_p$, we can consider its conjugate α^p in $F_{p^2} - F_p$ and these conjugates satisfy

$$H(\alpha^p, 0) = H(\alpha, 0)^p. \tag{9}$$

Therefore, $H(\alpha^p, 0)$ is a QR in F_{p^2} if and only if $H(\alpha, 0)$ is a QR in F_{p^2}. For example, if $H(\alpha, 0)$ is a QR in F_{p^2}, we have the following four rational points :

$$\left(\alpha^{p^i}, \pm\sqrt{H(\alpha^{p^i}, 0)}\right),\ i = 0, 1. \tag{10}$$

In $F_{p^2} - F_p$, there exist $(p^2 - p)/2$ conjugate pairs. Among them, let N_2' be the number of conjugate pairs such that $H(\alpha, 0)$ and $H(\alpha^p, 0)$ become QRs in F_{p^2},

$$M_2 = 2p + 4N_2' + 1 = 2(p + 2N_2') + 1. \tag{11}$$

The number of conjugate pairs such that $H(\alpha, 0)$ and $H(\alpha^p, 0)$ become QNRs in F_{p^2} is given by $(p^2-p)/2-N_2'$. From Eq.(4b), Eq.(4c) and Eq.(11), we find that s_2 becomes an odd number in this paper.

2.6 The number of rational points over F_{p^3}

In the same way of N_2', for an arbitrary element α in $F_{p^3} - F_p$, we can consider its conjugates α^p and α^{p^2} and these conjugates satisfy

$$H(\alpha^p, 0) = H(\alpha, 0)^p,\ H(\alpha^{p^2}, 0) = H(\alpha, 0)^{p^2}. \tag{12}$$

Therefore, $H(\alpha^p, 0)$ and $H(\alpha^{p^2}, 0)$ are QRs in F_{p^3} if and only if $H(\alpha, 0)$ is a QR in F_{p^3}. For example, if $H(\alpha, 0)$ is a QR in F_{p^3}, we have the following 6 rational points:

$$\left(\alpha^{p^i}, \pm\sqrt{H(\alpha^{p^i}, 0)}\right),\ i = 0, 1, 2. \tag{13}$$

In $F_{p^3} - F_p$, there exist $(p^3 - p)/3$ conjugate pairs. Thus, let N_3' be the number of conjugate pairs such

that $H(\alpha,0)$, $H(\alpha^p,0)$, and $H(\alpha^{p^2},0)$ become QRs in F_{p^3}, using N_1 that denotes the number of QRs in the set Eq.(6), we have

$$M_3 = 2N_1 + 6N_3' + 1 = 2(N_1 + 3N_3') + 1. \quad (14)$$

In this case, s_3 becomes odd. The number of conjugate pairs such that $H(\alpha,0)$, $H(\alpha^p,0)$, and $H(\alpha^{p^2},0)$ become QNRs in F_{p^3} is given by $(p^3-p)/3 - N_3'$.

3 MAIN RESULT

Corresponding to genus g, this paper shows a method for checking the parity of $(\#J_C-1)/2$. We use the following notations :

$$P(n) = (-1)^n = \begin{cases} 1 & \text{when } n \text{ is even} \\ -1 & \text{when } n \text{ is odd} \end{cases}, \quad (15a)$$

$$n_l(x) = \prod_{i=0}^{l-1} x^{p^i} = x \cdot x^p \cdot x^{p^2} \cdots x^{p^{l-1}}, \quad (15b)$$

$$H_j(x^{p^j} - x, 0) = H(x,0) \prod_{i=1}^{p^j-1} H(x + s^i, 0), \quad (15c)$$

where $j = 1,2,3$ and s is a generator of $F_{p^j}^*$. According to our previous work[1], when $g=1$, we have

$$P\left(\frac{\#J_C-1}{2}\right) = P(N_1) = -\left(-n_3(\omega^p - \omega)\right)^{(p-1)/2}, \quad (16a)$$

$$H_1(0,0) = \prod_{i=0}^{p-1} H(i,0) = -n_3(\omega^p - \omega), \quad (16b)$$

$$P(N_1) = (-1)^{N_1} = -H_1(0,0)^{(p-1)/2}. \quad (16c)$$

3.1 The parity of $(\#J_C-1)/2$ when the genus $g=2$

From Eqs.(4), by substituting Eq.(4b) into Eq.(4a) we have the following equation :

$$\#J_C = M_1(p+1) - 2p + s_2. \quad (17)$$

Then, noting that M_1 and p are odd numbers,

$$P\left(\frac{\#J_C-1}{2}\right) = P\left(\frac{p-1}{2}\right) P\left(\frac{s_2-1}{2}\right). \quad (18)$$

From Eq.(4c), Eq.(11), and noting that s_1 is odd,

$$P\left(\frac{s_2-1}{2}\right) = P\left(\frac{p-1}{2}\right) P(N_2'). \quad (19)$$

Thus, from Eq.(18) and Eq.(19), we have

$$P\left(\frac{\#J_C-1}{2}\right) = P(N_2'). \quad (20)$$

In what follows, we consider how to determine $P(N_2')$.

3.1.1 How to determine $P(N_2')$

According to SPPT over F_{p^2}, we can uniquely determine $H_2(x,0)$ from $H(x,0)$ and Eq.(15c). Since $H(x,0)$ is an irreducible polynomial of degree $2g+1=5$ over F_p, $H_2(x,0)$ is also irreducible as introduced in **Sec**.2.2. Substituting $x=0$, we have

$$H_2(0,0) = H(0,0) \prod_{i=1}^{p^2-1} H(s^i, 0). \quad (21)$$

The right hand side of the above equation is the product of the values that is given by substituting each element in F_{p^2} into $H(x,0)$. Since $F_{p^2} = F_p \cup (F_{p^2} - F_p)$ and $F_p \cap (F_{p^2} - F_p) = \phi$, we can rewrite Eq.(21) as

$$H_2(0,0) = \prod_{i=0}^{p-1} H(i,0) \prod_{\forall \alpha \in F_{p^2} - F_p} H(\alpha, 0). \quad (22)$$

For α in $F_{p^2} - F_p$, let us consider the following pair :

$$\{H(\alpha,0), H(\alpha^p,0)\} \quad (23)$$

that corresponds to the conjugate pair $\{\alpha, \alpha^p\}$, where $H(\alpha^p,0) = H(\alpha,0)^p$ as shown in **Sec**.2.5. For the pair Eq.(23), we have the following relation :

$$H(\alpha,0)^{(p^2-1)/2} = \{H(\alpha,0)H(\alpha,0)^p\}^{(p-1)/2}, \quad (24)$$

where we note that $H(\alpha,0)H(\alpha^p,0) = H(\alpha,0)H(\alpha,0)^p$ becomes a certain non-zero element in F_p. The left hand side of Eq.(24) is the check whether or not $H(\alpha,0)$ is a QR in F_{p^2}. From Eq.(24), consider the following calculation :

$$H_2(0,0)^{(p-1)/2} = \left\{\prod_{i=0}^{p-1} H(i,0)^{(p-1)/2}\right\} \times \left\{\prod_{\forall \alpha \in F_{p^2} - F_p} H(\alpha,0)^{(p-1)/2}\right\}. \quad (25)$$

From **Sec**.2.5, Eq.(16c), and Eq.(24), we have

$$H_2(0,0)^{(p-1)/2} = -P\left(\frac{p^2-p}{2} - N_2'\right) P(N_1), \quad (26)$$

where N_1 and N'_2 are defined in **Sec**.2.4 and **Sec**.2.5, respectively. Thus, we have

$$\begin{aligned} P\left(N'_2\right) &= -P\left(\frac{p^2-p}{2}\right) P\left(N_1\right) H_2(0,0)^{(p-1)/2} \\ &= P\left(\frac{p-1}{2}\right) \left\{H_1(0,0)H_2(0,0)\right\}^{(p-1)/2} \\ &= \left\{-H_1(0,0)H_2(0,0)\right\}^{(p-1)/2}. \end{aligned} \tag{27}$$

3.1.2 How to calculate $H_1(0,0)H_2(0,0)$

As introduced in **Sec**.2.2, let ω be a zero of $H(x,0)$, $H_1(x,0)$ and $H_2(x,0)$ are the minimal polynomials of $\omega^p-\omega$ and $\omega^{p^2}-\omega$, respectively. Noting that $H_1(0,0)$ and $H_2(0,0)$ are their constant terms, we have

$$H_1(0,0)H_2(0,0) = n_5\left((\omega^p-\omega)(\omega^{p^2}-\omega)\right). \tag{28}$$

Finally, from Eq.(20), Eq.(27), and Eq.(28),

$$\begin{aligned} &P\left(\frac{\#J_C-1}{2}\right) \\ &\quad = \left(-n_5\left((\omega^p-\omega)(\omega^{p^2}-\omega)\right)\right)^{(p-1)/2}. \end{aligned} \tag{29}$$

3.2 The parity of $(\#J_C-1)/2$ when the genus $g=3$

From Eq.(5a), we have the following equation :

$$\begin{aligned} \frac{\#J_C-1}{2} &= \frac{(p+1)(p^2+p+1+s_2)}{2} \\ &\quad + \frac{s_1(p^2+1)}{2} + \frac{s_3-1}{2}. \end{aligned} \tag{30}$$

Noting that s_1, s_2, s_3, and p are odd numbers, we have

$$P\left(\frac{\#J_C-1}{2}\right) = -P\left(\frac{s_3-1}{2}\right). \tag{31}$$

From Eq.(5d), we have

$$\begin{aligned} \frac{3(s_3-1)}{2} &= \frac{M_3-1}{2} - \frac{p^3+s_1^3}{2} + \frac{3(s_1s_2-1)}{2} \\ &= N_1 + 3N'_3 - \frac{(p+1)(p^2-p+1)}{2} \\ &\quad - \frac{(s_1-1)(s_1^2+s_1+1)-3(s_1s_2-1)}{2}, \end{aligned} \tag{32}$$

$$\frac{s_1s_2-1}{2} = \frac{s_1(s_2-1)}{2} + \frac{s_1-1}{2}. \tag{33}$$

Therefore, from Eq.(19),

$$P\left(\frac{s_3-1}{2}\right) = -P\left(N_1\right) P\left(N'_2\right) P\left(N'_3\right). \tag{34}$$

3.2.1 How to determine $P\left(N'_3\right)$

According to SPPT over F_{p^3}, we can uniquely determine $H_3(x,0)$ from $H(x,0)$ and Eq.(15c). Since $H(x,0)$ is an irreducible polynomial of degree $2g+1=7$ over F_p, $H_3(x,0)$ is also irreducible as introduced in **Sec**.2.2. In the same of $H_2(0,0)$, we have

$$H_3(0,0) = \prod_{i=0}^{p-1} H(i,0) \prod_{\forall\alpha\in F_{p^3}-F_p} H(\alpha,0). \tag{35}$$

For α in $F_{p^3}-F_p$, let us consider the following set :

$$\left\{H(\alpha,0), H(\alpha^p,0), H(\alpha^{p^2},0)\right\} \tag{36}$$

that corresponds to the conjugates set $\{\alpha, \alpha^p, \alpha^{p^2}\}$, where $H(\alpha^p,0) = H(\alpha,0)^p$ and $H(\alpha^{p^2},0) = H(\alpha,0)^{p^2}$ as shown in **Sec**.2.6. For the set Eq.(36), we have

$$H(\alpha,0)^{(p^3-1)/2} = \left(\prod_{i=0}^{2} H(\alpha,0)^{p^i}\right)^{(p-1)/2}. \tag{37}$$

In the same of Eq.(25), consider

$$\begin{aligned} H_3(0,0)^{(p-1)/2} &= \prod_{i=0}^{p-1} H(i,0)^{(p-1)/2} \\ &\quad \times \prod_{\forall\alpha\in F_{p^3}-F_p} H(\alpha,0)^{(p-1)/2}. \end{aligned} \tag{38}$$

From **Sec**.2.6, Eq.(16c), and Eq.(37), we have

$$H_3(0,0)^{(p-1)/2} = -P\left(\frac{p^3-p}{3} - N'_3\right) P\left(N_1\right), \tag{39}$$

where N_1 and N'_3 are defined in **Sec**.2.4 and **Sec**.2.6, respectively. Thus, we have

$$\begin{aligned} P\left(N'_3\right) &= -P\left(N_1\right) H_3(0,0)^{(p-1)/2} \\ &= \left\{H_1(0,0)H_3(0,0)\right\}^{(p-1)/2} \end{aligned} \tag{40}$$

3.2.2 How to calculate $H_1(0,0)H_3(0,0)$

As introduced in **Sec**.2.2, let ω be a zero of $H(x,0)$, $H_1(x,0)$ and $H_3(x,0)$ are the minimal polynomials of $\omega^p-\omega$ and $\omega^{p^3}-\omega$, respectively. Noting that $H_1(0,0)$ and $H_3(0,0)$ are their constant terms, we have

$$H_1(0,0)H_3(0,0) = n_7\left((\omega^p-\omega)(\omega^{p^3}-\omega)\right). \tag{41}$$

Finally, from Eq.(16c), Eq.(27), Eq.(31), Eq.(34), Eq.(40), and Eq.(41), $P\left(\frac{\#J_C-1}{2}\right)$ is given by

$$-\left(-n_7\left((\omega^p-\omega)(\omega^{p^2}-\omega)(\omega^{p^3}-\omega)\right)\right)^{(p-1)/2}. \tag{42}$$

Using $H(x, 0)$ as the modular polynomial, Eq.(29) and Eq.(42) are calculated by arithmetic operations in F_{p^5} and F_{p^7}, respectively.

4 CONCLUSION

This paper has shown a method for checking the parity of $(\#J_C - 1)/2$ of genus 2 and 3 hyperelliptic curves without calculating the order $\#J_C$.

References

[1] Y.Nogami, M.Obara, and Y.Morikawa, "A Method for Distinguishing the Two Candidate Elliptic Curves in the Complex Multiplication Method," ETRI Journal, vol.28, no.6, pp.745-760, 2006.

[2] I.Blake, G.Seroussi, and N.Smart, *Elliptic Curves in Cryptography*, LNS 265, Cambridge University Press, 1999.

A SPPT OVER F_{p^k}

Let $f(x)$ be an irreducible polynomial of degree m over F_p and let its zero be ω in F_{p^m}. Then, for Eq.(2), noting that s is a generator of $F^*_{p^k}$, we have

$$F_k(x) = \prod_{i=0}^{m-1} \left\{ (x - \omega^{p^i}) \prod_{j=1}^{p^k-1} (x - \omega^{p^i} + s^j) \right\}, \quad (43)$$

using the relation $x \prod_{j=1}^{p^k-1} (x + s^j) = x^{p^k} - x$, we have

$$= \prod_{i=0}^{m-1} \left\{ (x^{p^k} - x) - (\omega^{p^k} - \omega)^{p^i} \right\}. \quad (44)$$

Let $\tau = \omega^{p^k} - \omega$ and let $f_k(x)$ be the minimal polynomial of τ, we have

$$f(x) \prod_{j=1}^{p^k-1} f(x + s^j) = f_k(x^{p^k} - x), \quad (45)$$

where $\tau \in F_{p^m}$ does not belong to any proper subfield in F_{p^m} as shown below.

Suppose that $\tau = \omega^{p^k} - \omega$ belongs to a proper subfield F_{p^r}, $m = m'r$, $m' \neq 1$, then we show a contradiction. Using τ and ω, we have

$$\sum_{i=0}^{r-1} \tau^{p^i} = \sum_{i=0}^{r-1} \left(\omega^{p^i}\right)^{p^k} - \sum_{i=0}^{r-1} \omega^{p^i} = c, \quad (46)$$

where $c \in F_p$ because τ belongs to F_{p^r} and the sum of all conjugates of τ becomes an element in F_p. Let $\gamma = \sum_{i=0}^{r-1} \omega^{p^i}$, we have $\gamma^{p^{ik}} = \gamma + ic$, $1 \leq i \leq p$. Since ω is a non-zero element in F_{p^m} and does not belong to any proper subfields of F_{p^m}, c must be 0 because p does not divide m as introduced in **Sec**.1. Then, γ belongs to F_{p^k}, accordingly γ belongs to F_p because $\gcd(m, k) = 1$ in this paper. Since ω belongs to F_{p^m} but not to its proper subfields, it contradicts that γ is an element in F_p as

$$\begin{aligned} 0 &= \gamma^p - \gamma = \left(\sum_{i=0}^{r-1} \omega^{p^i} \right)^p - \sum_{i=0}^{r-1} \omega^{p^i} \\ &= \omega^{p^r} - \omega \neq 0. \end{aligned} \quad (47)$$