Bull. Korean Math. Soc. **56** (2019), No. 2, pp. 333–349
https://doi.org/10.4134/BKMS.b180167
pISSN: 1015-8634 / eISSN: 2234-3016

AVERAGE VALUES ON THE JACOBIAN VARIETY OF A HYPERELLIPTIC CURVE

Jiman Chung and Bo-Hae Im

Abstract. We give explicitly an average value formula under the multiplication-by-2 map for the x-coordinates of the 2-division points D on the Jacobian variety $J(C)$ of a hyperelliptic curve C with genus g if $2D \equiv 2P - 2\infty \pmod{\mathrm{Pic}(C)}$ for $P = (x_P, y_P) \in C$ with $y_P \neq 0$. Moreover, if $g = 2$, we give a more explicit formula for D such that $2D \equiv P - \infty \pmod{\mathrm{Pic}(C)}$.

1. Introduction

In [3], Feng and Wu have given a mean value formula for the n-division points on elliptic curves. We recall the definition of an n-division point of an elliptic curve E of $Q \in E$ by a point $P \in E$ such that $Q = nP$. More precisely, they have shown in [3, Theorem 1] that if $P = (x_P, y_P)$ is a point on an elliptic curve E over $\overline{K}$ and $[n] : E \to E$ is the multiplication-by-n map which is an isogeny of E and defined by $P \longmapsto nP$, then for a point $Q = (x_Q, y_Q) \neq O$ on E, where O is the identity element of E,

$$\frac{1}{n^2} \sum_{P \in [n]^{-1}(Q)} x_P = x_Q$$

and

$$\frac{1}{n^3} \sum_{P \in [n]^{-1}(Q)} y_P = y_Q.$$

An application of this result is to get some information on the Discrete Logarithm Problem in the group of an elliptic curve.

Received February 22, 2018; Revised July 29, 2018; Accepted October 25, 2018.
2010 *Mathematics Subject Classification.* Primary 11G05.
Key words and phrases. Jacobian variety, hyperelliptic curve.
Bo-Hae Im was supported by Basic Science Research Program through the National Research Foundation of Korea(NRF) funded by the Ministry of Science, ICT & Future Planning(NRF-2017R1A2B4002619). Jiman Chung was supported by the Chung-Ang University Graduate Research Scholarship.

In general it is not easy to compute the coordinates of the images under the multiplication-by-n map on the Jacobian variety even though there are some known algorithms of computing and reducing them (see [1]).

In this paper we generalize this result for the Jacobian variety of a hyperelliptic curve with positive genus and give an explicit formula for the average values of coordinates of points on the Jacobian variety under the multiplication-by-2 map. First, we reduce the divisors into reduced ones (see Definition 1) and give a simpler average formula for the coordinates of the 2-division points.

This also gives some relation between the points under the multiplication-by-2 map and simpler results for computational use. Especially, we would like to emphasize that our result can give an explicit average value formula of the 2-division points in terms of simple algebraic equations of a polynomial and its derivatives. Also, we note that we can proceed the same argument if we can specify coordinates of n-torsion points for higher n by using [2], but it is very complicated to write in literature. So our result motivates us to try for any $[n]$-map when we have coordinates of n-torsion points concretely.

2. For general genera

Let K be a number field and let $\overline{K}$ be the algebraic closure of K. We will consider hyperelliptic curves of genus g (including $g = 1$) defined by

$$C : y^2 = f(x) := x^{2g+1} + a_{2g}x^{2g} + \cdots + a_1x + a_0,$$

where $f(x) \in K[x]$ is factored into $f(x) = \prod_{i=1}^{2g+1} (x - x_i)$ for distinct $x_i \in \overline{K}$.

Denote the group of divisors of C and divisors with degree zero by $div(C)$ and $div^0(C)$, respectively. Denote the principal divisor group of C by $\mathrm{Pic}(C)$. Then the Jacobian $J(C)$ of C is $J(C) = div^0(C)/\mathrm{Pic}(C)$. If the context is clear, we may omit $(\mathrm{mod}\ \mathrm{Pic}(C))$. Denote the identity of $J(C)$ by O. For $f(u) \in \overline{K}(C)^*$, let $div(f(u)) = \sum m_iP_i - \sum n_jQ_j$, where P_i are zeros of $f(u)$ and Q_j are poles of $f(u)$.

Let $P = (x, y)$ and $Q = (x, -y)$ be points on C and let ∞ be the point at infinity. Then P and Q are the zeros of the function $f(u) = u - x \in \overline{K}(C)^*$ which has a double pole at ∞. Then $div(f(u)) = P + Q - 2\infty$ so that for any $D = -nP \in div(C), -nP \equiv n(Q - 2\infty) \pmod{\mathrm{Pic}(C)}$, where n is a positive integer.

Define $inv(P) := Q - 2\infty$. Further define $inv(O) = O$ and $inv(\infty) = -\infty$ so that inv is an automorphism of the divisor class group of C. It follows that $inv(P - \infty) = P - \infty$ if and only if $P = (x, 0)$ (i.e., $P - \infty$ is a 2-torsion point of $J(C)$ if $P = (x, 0)$).

Definition 1. A divisor $D \in div^0(C)$ is called a *semireduced divisor* if D is of the form $D = \sum_{k=1}^{n} m_k(P_k - \infty)$ with $m_k > 0$ for all k, where P_i are points of C such that $P_i \neq P_j$ and $P_i + P_j - 2\infty \neq O$ for all $i \neq j$.

For any semireduced divisor $D = \sum_{k=1}^{n} m_k(P_k - \infty) \in div(C)$, define

$$N(D) = \sum_{k=1}^{n} m_k.$$

A semireduced divisor D is called a *reduced divisor* if $N(D) \leq g$.

Let $D = \sum_{P \in C} m_p P$ and $D' = \sum_{P \in C} n_p P$. Define

$$\gcd(D, D') := \sum_{P \in C} \min(m_p, n_p) P.$$

Let $D = \sum_{k=1}^{n} m_k(P_k - \infty)$ be a semireduced divisor for some $P_k = (x_{P_k}, y_{P_k}) \in C$, $1 \leq k \leq n$. Then it can be represented by a pair of polynomials $a(u)$ and $b(u)$ over K where $a(u) = \prod_{k=1}^{n} (u - x_{P_k})^{m_k}$ and $b(u)$ is the unique polynomial of degree $< \deg(a(u))$ with $b(x_{P_k}) = y_{P_k}$ for all $1 \leq k \leq n$. It can be verified that $a(u) \mid f(u) - (b(u))^2$ and $D = \gcd(div(a(u)), div(b(u) - v))$ where $v^2 = f(u)$. Define

$$div(a(u), b(u)) = \gcd(div(a(u)), div(b(u) - v)).$$

For any $P = (x_P, y_P) \in C$, let $x : C \to \overline{K}$ be the x-coordinate map such that $x(P) = x_P$. From now on, we will denote $x(P) = x_P$, $x(Q) = x_Q$ and so on when the context is clear.

Define a function $\phi : J(C) \to \overline{K}$ as follows. For any $D \in J(C)$, there exists a unique reduced divisor $\tilde{D} = \sum_{k=1}^{n} m_k(P_k - \infty)$ such that $D \equiv \tilde{D} \pmod{\operatorname{Pic}(C)}$ by the Riemann-Roch Theorem [4, Ch.4. Theorem 1.3]. Define

$$\phi(D) = \sum_{k=1}^{n} m_k x(P_k).$$

Let $\tilde{D} = div(a(u), b(u))$ for some polynomials $a(u)$ and $b(u)$. Let $m = \deg(a(u))$. Suppose $m \leq g$ and $a(u) = a_0 + \cdots + a_{m-1}u^{m-1} + u^m$. Then, $\phi(D) = -a_{m-1}$.

We recall the algorithm to reduce a semireduced divisor to a reduced form as follows.

Algorithm 2 ([1]). An algorithm for reducing a semireduced divisor to a reduced form.

Let $D = div(a(u), b(u))$ for some polynomials $a(u)$ and $b(u)$. Assume $\deg(a(u)) > g$. Let

$$\begin{cases} E = D - div(b(u) - v), \\ \hat{a}(u) = \dfrac{f(u) - (b(u))^2}{a(u)}, \\ \hat{b}(u) \equiv -b(u) \pmod{\hat{a}(u)} \end{cases}$$

with $\deg(\hat{b}(u)) < \deg(\hat{a}(u))$. Then, $E = div(\hat{a}(u), \hat{b}(u)) \equiv D \pmod{\text{Pic}(C)}$. It is easy to see that $\deg(\hat{a}(u)) < \deg(a(u))$. We repeat this process until the degree is g or less.

Lemma 3. *Let $D' \pmod{\text{Pic}(C)} \in J(C)$. If $D \pmod{\text{Pic}(C)} \in J(C)$ satisfies $nD = D'$ for some positive integer n, then $D + [n]^{-1}(O) := \{D + \tilde{D} \mid \tilde{D} \in [n]^{-1}(O)\}$ is equivalent to $[n]^{-1}(D')$.*

Proof. It is easy to check that $n(D+\tilde{D}) = D'$ for any $\tilde{D} \in [n]^{-1}(O)$. Conversely for any $E \in [n]^{-1}(D')$,

$$n(E + inv(D)) = nE + inv(nD) = D' + inv(D') = O.$$

Thus $E = D + \tilde{D}$ for some $\tilde{D} \in [n]^{-1}(O)$. □

Lemma 4. *Let $P_j = (x_{P_j}, 0)$ be distinct points on C for $j = 1, \ldots, 2g+1$. Let $A_0 = \{O\}$ and $A_m = \{P_{j_1} + \cdots + P_{j_m} - m\infty \mid j_k \neq j_\ell \text{ for all } k \text{ and } \ell\}$ for $m = 1, \ldots, g$. Then $[2]^{-1}(O) = \bigcup_{k=0}^{g} A_k$ and in particular, $|[2]^{-1}(O)| = 2^{2g} = \sum_{k=0}^{g} |A_k|$.*

Proof. Since each element of the form $P_{j_1} + \cdots + P_{j_m} - m\infty$ is reduced, they represent distinct elements of $J(C)$. Thus $A_n \cap A_m = \emptyset$ for $n \neq m$. Moreover any $D \in \bigcup_{k=0}^{g} A_k$ is just a sum of 2-torsion points, $P_j - \infty$. Therefore $D \in [2]^{-1}(O)$. Hence it is enough to check that $\left|[2]^{-1}(O)\right| = \sum_{k=0}^{g} |A_k|$. It is well known that $[n]^{-1}(O)$ is isomorphic to $(\mathbb{Z}/n\mathbb{Z})^{2g}$ as groups so that $\left|[2]^{-1}(O)\right| = 2^{2g}$. By counting the number of elements, $|A_0| = 1$ and $|A_k| = \binom{2g+1}{k}$ for $k = 1, \ldots, g$. Then $\sum_{k=0}^{g} |A_k| = \sum_{k=0}^{g} \binom{2g+1}{k} = \frac{1}{2} \sum_{k=0}^{2g+1} \binom{2g+1}{k} = 2^{2g} = \left|[2]^{-1}(O)\right|$. □

Hence in order to find the average value formula $\frac{1}{2^{2g}} \sum_{D \in [2]^{-1}(D_P)} \phi(D)$ for the x-coordinates of 2-division points, it is enough to compute $\sum_{D \in [2]^{-1}(D_P)} \phi(D)$.

Theorem 5. *Let $D_P = 2P - 2\infty$ be a (reduced) divisor of $J(C)$ for some $P = (x_P, y_P) \in C$ with $y_P \neq 0$.*

Then,

$$\sum_{D \in [2]^{-1}(D_P)} \phi(D) = \Delta(g, P) + \left(\binom{2g-1}{g-2} - 2^{2g-1} \right) a_{2g} + \left(2^{2g} - 2\binom{2g+1}{g} \right) x_P,$$

where $\Delta(g, P) = \sum_{D \in A_g} \frac{f(x_P)}{\prod_{k=1}^{g} (x_P - x_{j_k})^2}$.

Proof. By Lemma 3 and Lemma 4,

$$\sum_{D\in[2]^{-1}(D_P)}\phi(D)=\sum_{D\in[2]^{-1}(O)}\phi(P-\infty+D)=\sum_{k=0}^{g}\sum_{D\in A_k}\phi(P-\infty+D).$$

For each $m\le g-1$, $N(P-\infty+D)\le g$ where $D\in A_m$. Thus $\phi(P-\infty+D)=x_P+x_{P_{j_1}}+\cdots+x_{P_{j_m}}$. However, $N(P-\infty+D)>g$ for $D\in A_g$. Hence we need to reduce $P-\infty+D$ into a reduced divisor D'. Let $P+P_{j_1}+\cdots+P_{j_g}-(g+1)\infty=div(a(u),b(u))$. Then

$$a(u)=(u-x_P)\prod_{k=1}^{g}(u-x_{j_k})\text{ and }b(u)=y_P\frac{\prod_{k=1}^{g}(u-x_{j_k})}{\prod_{k=1}^{g}(x_P-x_{j_k})}.$$

Let $\hat{a}(u)=\frac{f(u)-(b(u))^2}{a(u)}$ and let $\hat{b}(u)$ be the polynomial satisfying $\deg(\hat{b}(u))\le\deg(\hat{a}(u))$ and $\hat{b}(u)\equiv -b(u)\pmod{\hat{a}(u)}$. Let $D'=div(\hat{a}(u),\hat{b}(u))$. Since

$$\begin{aligned}\deg(\hat{a}(u))&=\max\{\deg(f(u)),2\deg(b(u))\}-\deg(a(u))\\&=\max\{2g+1,2g\}-(g+1)=g,\end{aligned}$$

D' is indeed a reduced divisor such that $D'\equiv P-\infty+D\pmod{\mathrm{Pic}(C)}$. By letting $\hat{a}(u)=\frac{f(u)-(b(u))^2}{a(u)}=\prod_{k=1}^{g}(u-c_k)$ for some $c_k\in\overline{K}$, we have

$$\phi(P-\infty+D)=\sum_{k=1}^{g}c_k=\frac{f(x_P)}{\prod_{k=1}^{g}(x_P-x_{j_k})^2}-\left(\sum_{k=1}^{g}x_{j_k}\right)-x_P-a_{2g},$$

by comparing the coefficients of $\frac{f(u)-(b(u))^2}{a(u)}$ and $\prod_{k=1}^{g}(u-c_k)$.

Define

$$\Delta(g,P):=\sum_{D\in A_g}\frac{f(x_P)}{\prod_{k=1}^{g}(x_P-x_{j_k})^2}.$$

Then,

$$\begin{aligned}\sum_{D\in A_g}\phi(P-\infty+D)&=\Delta(g,P)-\binom{2g}{g-1}\sum_{j=1}^{2g+1}x_j-\binom{2g+1}{g}(x_P+a_{2g})\\&=\Delta(g,P)+\left(\binom{2g}{g-1}-\binom{2g+1}{g}\right)a_{2g}-\binom{2g+1}{g}x_P.\end{aligned}$$

Similarly for $0<m<g$,

$$\sum_{D\in A_m}\phi(P-\infty+D)=\binom{2g}{m-1}\sum_{j=1}^{2g+1}x_j+\binom{2g+1}{m}x_P.$$

By adding them up,

$$\begin{aligned}
&\sum_{k=0}^{g}\sum_{D\in A_k}\phi(P-\infty+D)\\
&=x_P+\sum_{k=1}^{g-1}\sum_{D\in A_k}\phi(P-\infty+D)+\sum_{D\in A_g}\phi(P-\infty+D)\\
&=\Delta(g,P)+\left(\binom{2g}{g-1}-\binom{2g+1}{g}-\sum_{m=1}^{g-1}\binom{2g}{m-1}\right)a_{2g}\\
&\quad+\left(\left(\sum_{m=0}^{g-1}\binom{2g+1}{m}\right)-\binom{2g+1}{g}\right)x_P\\
&=\Delta(g,P)+\left(\binom{2g-1}{g-2}-2^{2g-1}\right)a_{2g}+\left(2^{2g}-2\binom{2g+1}{g}\right)x_P.
\end{aligned}$$

□

3. For genus 2 with arbitrary divisors

Throughout this section, we consider a hyperelliptic curve $C : y^2 = f(x)$ of genus 2 and we let $P_j = (x_j, 0)$ for $j = 1, \ldots, 5$ be five points on C.

Lemma 6. *Let $g = 2$. Let $D = 2P - 2\infty$ and let $D_Q = Q - \infty$ be divisors of $J(C)$ for some $P = (x_P, y_P)$ and $Q = (x_Q, y_Q) \in C$. Let $\frac{dy}{dx}$ be the usual implicit differentiation of $y^2 = f(x)$. Then, $2D \equiv D_Q \pmod{\mathrm{Pic}(C)}$ implies $D \not\equiv O \pmod{\mathrm{Pic}(C)}$ and we have that*

$$2D \equiv D_Q \pmod{\mathrm{Pic}(C)}$$

if and only if

$$\left.\frac{d^3y}{dx^3}\right|_P = 0 \tag{1}$$

or equivalently,

$$4(f(x_P))^2 f^{(3)}(x_P) - 6f(x_P)f'(x_P)f''(x_P) + 3(f'(x_P))^3 = 0 \tag{2}$$

and

$$x_Q = x_P + \frac{\left(2f(x_P)f''(x_P) - (f'(x_P))^2\right)^2}{64(f(x_P))^3} - \frac{f^{(4)}(x_P)}{4!}. \tag{3}$$

Proof. Since $D_Q \neq O$, the condition that $2D \equiv D_Q \pmod{\mathrm{Pic}(C)}$ implies $D \not\equiv O \pmod{\mathrm{Pic}(C)}$. Let $2D = 4(P - \infty) = div(a(u), b(u))$ be a semireduced divisor such that $2D \equiv D_Q \pmod{\mathrm{Pic}(C)}$ where $a(u) = (u - x_P)^4$ and

$\deg(b(u)) \leq 3$. Take

$$\hat{a}(u) = \frac{f(u) - (b(u))^2}{a(u)} \text{ and}$$
$$\hat{b}(u) \equiv -b(u) \pmod{\hat{a}(u)} \text{ with } \deg(\hat{b}(u)) \leq \deg(\hat{a}(u)).$$

Then, $\deg(\hat{a}(u)) = \max\{5, 2\deg(b(u))\} - 4$. Let $D' = div(\hat{a}(u), \hat{b}(u))$. If $\deg(b(u)) = 3$, then D' is a reduced divisor with $N(D') = 2$ but $N(D_Q) = 1$. This is a contradiction to $D' \equiv 2D \equiv D_Q \pmod{\mathrm{Pic}(C)}$. Thus we must have that $\deg(b(u)) < 3$. Let $h(u) = f(u) - (b(u))^2$. Since $a(u) \mid h(u)$, we have $h(x_P) = h'(x_P) = h''(x_P) = h^{(3)}(x_P) = 0$. Equivalently, $b^{(k)}(x_P) = \frac{d^k y}{dx^k}\Big|_P$ for $0 \leq k \leq 3$. Let $z_k := \frac{1}{k!}\frac{d^k y}{dx^k}\Big|_P$ and $f_k := \frac{f^{(k)}(x_P)}{k!}$. Then we can easily check that

$$f_0 = {z_0}^2 \text{ and } f_k = \sum_{i+j=k} z_i z_j,$$

where $0 \leq i, j \leq k$. Since $\deg(b(u)) < 3$ and $b(u) = \sum_{k=0}^{3} \frac{b^{(k)}(x_P)}{k!}(u - x_P)^k = \sum_{k=0}^{3} z_k (u - x_P)^k$, we must have $z_3 = 0$ or equivalently

$$\frac{8f_0^2 f_3 - 4f_0 f_1 f_2 + f_1^3}{16 y_0^5} = 0.$$

Thus,

$$4(f(x_P))^2 f^{(3)}(x_P) - 6f(x_P)f'(x_P)f''(x_P) + 3(f'(x_P))^3 = 0.$$

Now, we have that $D' = D_Q$ since D' and D_Q are both reduced and $D' \equiv D_Q$ $(\mathrm{mod}\ \mathrm{Pic}(C))$. Then,

$$\hat{a}(u) = \frac{f(u) - (b(u))^2}{a(u)} = u - x_P + f_4 - y_2^2 = u - x_Q.$$

Hence,

$$x_Q = x_P + \frac{\left(2f(x_P)f''(x_P) - (f'(x_P))^2\right)^2}{64(f(x_P))^3} - \frac{f^{(4)}(x_P)}{4!}. \qquad \square$$

Theorem 7. *Let $g = 2$, and $D_Q = Q - \infty$ be a divisor in $J(C)$. Assume there exists $D \in [2]^{-1}(D_Q)$ of the form $D = 2P - 2\infty$ with $P = (x_P, y_P)$ and for each pair (j, k) such that $1 \leq j < k \leq 5$, let $b_2(j, k)$ and $b_3(j, k)$ be solutions for the system of equations*

$$\begin{cases} b_0 + b_1 x_j + b_2 x_j^2 + b_3 x_j^3 = 0, \\ b_0 + b_1 x_k + b_2 x_k^2 + b_3 x_k^3 = 0, \\ b_0 + b_1 x_P + b_2 x_P^2 + b_3 x_P^3 = y_P, \\ b_1 + 2b_2 x_P + 3b_3 x_P^2 = \frac{f'(x_P)}{2y_P}. \end{cases}$$

Let

$$\Delta = \sum_{1\le j<k\le 5} \frac{1-2b_2(j,k)b_3(j,k)}{(b_3(j,k))^2}.$$

Then

$$\sum_{D\in[2]^{-1}(D_Q)} \phi(D) = \Delta - \sum_{j=1}^{5} \frac{(2f(x_P)+f'(x_P)(x_j-x_P))^2}{4f(x_P)(x_j-x_P)^4} - 28x_P.$$

Proof. Recalling the definition of A_i in Lemma 3 and Lemma 4 for $i=1,2$, we let

$$D + A_i := \{D + D' : D' \in A_i\}.$$

Case 1. Let $D + P_j - \infty = div(a(u), b(u)) \in D + A_1$ for some $a(u)$ and $b(u)$. Then $a(u) = (u-x_j)(u-x_P)^2$ and $b(u)$ is the unique polynomial with the properties $\deg(b(u)) < \deg(a(u)) = 3$ and $a(u) \mid f(u) - (b(u))^2$. Moreover, by letting $b(u) = b_0 + b_1 u + b_2 u^2$ we have the following system of equations:

$$\begin{cases} b_0 + b_1 x_j + b_2 x_j^2 = b(x_j) = 0, \\ b_0 + b_1 x_P + b_2 x_P^2 = b(x_P) = y_P, \\ b_1 + 2b_2 x_P = b'(x_P) = \frac{f'(x_P)}{2y_P}. \end{cases}$$

Then, we solve the system for b_0, b_1, and b_2 to obtain

$$b_2 = -\frac{y_P + \frac{f'(x_P)}{2y_P}(x_j - x_P)}{(x_j-x_P)^2}.$$

Let $\hat{a}(u) = \frac{f(u)-(b(u))^2}{a(u)}$ and $\hat{b}(u) \equiv -b(u) \pmod{\hat{a}(u)}$ with $\deg(\hat{b}(u)) < \deg(\hat{a}(u))$. Let $D' = div(\hat{a}(u), \hat{b}(u))$. Then, $D + P_j - \infty \equiv D' \pmod{\operatorname{Pic}(C)}$. It is easy to check that $\deg(\hat{a}(u)) \le 2$. Thus D' is indeed a reduced divisor. Let $a(u) = c_0 + c_1 u + c_2 u^2 + u^3$ and $\hat{a}(u) = c_0' + c_1' u + u^2$. Then,

$$\begin{aligned} \phi(D + P_j - \infty) = -c_1' &= -(a_4 - b_2^2 - c_2) \\ &= -a_4 + \frac{\left(y_P + \frac{f'(x_P)}{2y_P}(x_j - x_P)\right)^2}{(x_j-x_P)^4} - x_j - 2x_P \end{aligned}$$

and

$$\sum_{j=1}^{5} \phi(D + P_j - \infty) = \sum_{j=1}^{5} \frac{(2f(x_P)+f'(x_P)(x_j-x_P))^2}{4f(x_P)(x_j-x_P)^4} - 10x_P - 4a_4.$$

Case 2. Similarly let $D + P_j + P_k - 2\infty = div(a(u), b(u)) \in D + A_2$ for some $a(u)$ and $b(u)$. Then $a(u) = (u-x_j)(u-x_k)(u-x_P)^2$ and $b(u)$ is the unique polynomial with the properties $\deg(b(u)) < \deg(a(u)) = 4$ and

$a(u) \mid f(u) - (b(u))^2$. Let $b(u) = b_0 + b_1 u + b_2 u^2 + b_3 u^3$. Then we have the following system of equations:

$$\begin{cases} b_0 + b_1 x_j + b_2 x_j^2 + b_3 x_j^3 = b(x_j) = 0, \\ b_0 + b_1 x_k + b_2 x_k^2 + b_3 x_k^3 = b(x_k) = 0, \\ b_0 + b_1 x_P + b_2 x_P^2 + b_3 x_P^3 = b(x_P) = y_P, \\ b_1 + 2b_2 x_P + 3b_3 x_P^2 = b'(x_P) = \frac{f'(x_P)}{2y_P}. \end{cases}$$

Then,

$$b_2 = \frac{y_P((x_j - x_P)(x_k - x_P) - (x_j + x_k - 2x_P)(x_j + x_k + x_P)) - \frac{f'(x_P)}{2y_P}(x_j - x_P)(x_k - x_P)(x_j + x_k + x_P)}{(x_j - x_P)^2 (x_k - x_P)^2},$$

and

$$b_3 = \frac{\frac{f'(x_P)}{2y_P}(x_j - x_P)(x_k - x_P) + y_P(x_j - x_P) + y_P(x_k - x_P)}{(x_j - x_P)^2 (x_k - x_P)^2}.$$

If we take $\hat{a}(u) = \frac{f(u) - (b(u))^2}{a(u)}$, let $\hat{b}(u) \equiv -b(u) \pmod{\hat{a}(u)}$ with $\deg(\hat{b}(u)) < \deg(\hat{a}(u))$ and let $D' = div(\hat{a}(u), \hat{b}(u))$ so that $D + P_j + P_k - 2\infty \equiv D'$ (mod Pic(C)). Suppose $b_3 = 0$. Then $\deg(\hat{a}(u)) = 1$ which implies $D' = R - \infty$ for some $R \in C$. Since $P_j - \infty$ and $P_k - \infty$ are 2-torsion elements of $J(C)$ and by the previous lemma, we have that

$$Q - \infty \equiv 2D \equiv 2(D + P_j + P_k - 2\infty) \equiv 2D' = 2R - 2\infty \pmod{\mathrm{Pic}(C)}.$$

This is clearly impossible. Thus, $\deg(b(u)) = 3$ and $\hat{a}(u)$ is not a monic polynomial of degree 2. We may take $\hat{a}(u) = \frac{f(u) - (b(u))^2}{-b_3^2 a(u)}$ because $div(h(u)) = div(kh(u))$ for all $k \in K$ and any $h(u) \in K[u]$. Then, $\hat{a}(u)$ is a monic polynomial of degree 2. By using the same argument from Case 1,

$$\phi(D + P_j + P_k - 2\infty) = \frac{1}{b_3^2} - \frac{2b_2}{b_3} - 2x_P - x_j - x_k.$$

Let $\Delta = \sum_{1 \le j < k \le 5} \frac{1 - 2b_2(j,k) b_3(j,k)}{(b_3(j,k))^2}$. Then,

$$\sum_{1 \le j < k \le 5} \phi(D + P_j + P_k - 2\infty) = \Delta - 20x_P + 4a_4.$$

Since

$$\sum_{D \in [2]^{-1}(D_Q)} \phi(D) = \phi(2P - 2\infty) + \sum_{j=1}^{5} \phi(2P + P_j - 3\infty) + \sum_{1 \le j < k \le 5} \phi(2P + P_j + P_k - 4\infty),$$

finally we have that

$$\sum_{D\in[2]^{-1}(D_Q)} \phi(D) = \Delta + \sum_{j=1}^{5} \frac{(2f(x_P)+f'(x_P)(x_j-x_P))^2}{4f(x_P)(x_j-x_P)^4} - 28x_P.$$

□

Remark 8. Each of the linear systems in Theorem 7 has a unique solution. In fact, if we let A and B be the matrix of the systems in Theorem 7, respectively (i.e., $A\vec{x}=\vec{y}$, and $B\vec{u}=\vec{v}$). Then,

$$\det(A) = (x_j - x_p)^2,$$
$$\det(B) = (x_k - x_j)(x_j - x_P)^2(x_k - x_P)^2.$$

Since $2P - 2\infty \neq O$, we have $x_P \neq x_j$ and $x_P \neq x_k$ for all $1 \leq j,k \leq 5$. Therefore, both systems have a unique solution.

Lemma 9. *Let $g = 2$. Let $D_R = R - \infty$ be a divisor in $J(C)$ for some $R = (x_R, y_R) \in C$ and let $D = P + Q - 2\infty \in J(C)$ for some P and $Q \in C$ with $x(P) \neq x(Q)$. Then, $2D \equiv D_R \pmod{\mathrm{Pic}(C)}$ implies $P, Q \notin [2]^{-1}(O)$ and*

$$2D \equiv D_R \pmod{\mathrm{Pic}(C)}$$

if and only if

$$\frac{y_P - y_Q}{x_P - x_Q} = \frac{1}{2}\left(\left.\frac{dy}{dx}\right|_P + \left.\frac{dy}{dx}\right|_Q\right) \tag{4}$$

and

$$x_R = \frac{1}{2}\left(x_P + x_Q - \left(\frac{f^{(4)}(x_P)}{4!} + \frac{f^{(4)}(x_Q)}{4!}\right)\right) + \frac{\left(\left.\frac{dy}{dx}\right|_P - \left.\frac{dy}{dx}\right|_Q\right)^2}{4(x_P - x_Q)^2}, \tag{5}$$

where $\frac{dy}{dx}$ is the usual implicit differentiation of $y^2 = f(x)$.

Proof. If $P - \infty$ or $Q - \infty$ is a 2-torsion divisor, we have $N(2D) = 0$ or 2 but $N(D_R) = 1$. Thus, we assume $x_P \neq x_k$ and $x_Q \neq x_k$ for $1 \leq k \leq 5$. Let $2D = 2(P + Q - 2\infty) = div(a(u), b(u))$ be a semireduced divisor such that $2D \equiv D_R \pmod{\mathrm{Pic}(C)}$, where $a(u) = (u - x_P)^2(u - x_Q)^2$ and $\deg(b(u)) \leq 3$. The polynomial $b(u)$ must satisfy the following system of equations;

$$\begin{cases} b(x_P) = y_P, \\ b'(x_P) = \frac{f'(x_P)}{2y_P}, \\ b(x_Q) = y_Q, \\ b'(x_Q) = \frac{f'(x_Q)}{2y_Q}, \end{cases}$$

with determinant $(x_P - x_Q)^4 \neq 0$. Let $b(u) = b_0 + b_1u + b_2u^2 + b_3u^3$. Then

$$b_2 = \frac{3(x_P+x_Q)(y_P-y_Q) - \left(\frac{f'(x_P)}{2y_P} + \frac{f'(x_Q)}{2y_Q}\right)(x_P^2 - x_Q^2) - (x_P - x_Q)\left(\frac{f'(x_Q)}{2y_Q}x_P + \frac{f'(x_P)}{2y_P}x_Q\right)}{(x_P - x_Q)^3}$$

and

$$b_3 = \frac{(x_P - x_Q)\left(\frac{f'(x_P)}{2y_P} + \frac{f'(x_Q)}{2y_Q}\right) - 2(y_P - y_Q)}{(x_P - x_Q)^3}$$

by using the Cramer's rule. Take

$$\hat{a}(u) = \frac{f(u) - (b(u))^2}{a(u)} \text{ and}$$

$$\hat{b}(u) \equiv -b(u) \pmod{\hat{a}(u)} \text{ with } \deg(\hat{b}(u)) \le \deg(\hat{a}(u)).$$

Then, $\deg(\hat{a}(u)) = \max\{5, 2\deg(b(u))\} - 4$. Let $D' = div(\hat{a}(u), \hat{b}(u))$. If $\deg(b(u)) = 3$, then D' is a reduced divisor with $N(D') = 2$ but $N(D_Q) = 1$. This is a contradiction to $D' \equiv 2D \equiv D_Q \pmod{\mathrm{Pic}(C)}$. Thus we must have $\deg(b(u)) < 3$ which results in

$$0 = \frac{(x_P - x_Q)^2}{2} b_3 = \frac{1}{2}\Big(\frac{f'(x_P)}{2y_P} + \frac{f'(x_Q)}{2y_Q}\Big) - \frac{(y_P - y_Q)}{(x_P - x_Q)}.$$

Now, $D' = D_R$ since D' and D_R are both reduced and $D' \equiv D_R \pmod{\mathrm{Pic}(C)}$. Then,

$$\hat{a}(u) = \frac{f(u) - (b(u))^2}{a(u)} = u - x_R.$$

Since the constant term of $\frac{f(u)-(b(u))^2}{a(u)}$ must be $-x_R$,

$$x_R = b_2^2 - a_4 - 2(x_P + x_Q).$$

By substituting

$$a_4 = \frac{1}{2}\left(\frac{f^{(4)}(x_P)}{4!} + \frac{f^{(4)}(x_Q)}{4!} - 5(x_P + x_Q)\right)$$

into the above equation, we get

$$x_R = \frac{1}{2}\left(x_P + x_Q - \left(\frac{f^{(4)}(x_P)}{4!} + \frac{f^{(4)}(x_Q)}{4!}\right)\right) + \left(\frac{(x_P + x_Q)(y_Q - y_Q)}{(x_P - x_Q)^3} - \frac{\frac{f'(x_Q)}{2y_Q}x_P + \frac{f'(x_P)}{2y_P}x_Q}{(x_P - x_Q)^2}\right)^2.$$

Finally, we substitute

$$\frac{y_P - y_Q}{x_P - x_Q} = \frac{1}{2}\left(\frac{f'(x_P)}{2y_P} + \frac{f'(x_Q)}{2y_Q}\right)$$

to get the result. □

In particular, if $g = 2$, for $D' \in J(C)$, there exits $D \in [2]^{-1}(D')$ of the form $D = P + Q - 2\infty$ for some $P, Q \in C$. If $P = Q$, then Theorem 7 can be applied. Therefore, we prove the following theorem when $P \neq Q$.

Theorem 10. *Let* $g = 2$ *and let* $D_R = R - \infty$ *be a divisor in* $J(C)$. *Let* $D \in [2]^{-1}(D_R)$ *be of the form* $D = P + Q - 2\infty$ *with* $x_P \neq x_Q$. *For each pair* (j, k) *such that* $0 \leq j < k \leq 5$, *let* $b_2(j, k)$ *and* $b_3(j, k)$ *be solutions to the system of equations*

$$\begin{cases} b_0 + b_1 x_j + b_2 x_j^2 + b_3 x_j^3 = 0, \\ b_0 + b_1 x_k + b_2 x_k^2 + b_3 x_k^3 = 0, \\ b_0 + b_1 x_P + b_2 x_P^2 + b_3 x_P^3 = y_P, \\ b_0 + b_1 x_Q + b_2 x_Q^2 + b_3 x_Q^3 = y_Q, \end{cases}$$

and let

$$\Delta = \sum_{1 \leq j < k \leq 5} \frac{1 - 2b_2(j,k) b_3(j,k)}{(b_3(j,k))^2}.$$

Then

$$\sum_{D \in [2]^{-1}(D_Q)} \phi(D) = \Delta + \sum_{j=1}^{5} \frac{(x_Q y_P - x_P y_Q + x_j(y_Q - y_P))^2}{(x_P - x_Q)^2 (x_P - x_j)^2 (x_Q - x_j)^2} - 14 x_P - 14 x_Q.$$

Proof. Again, we will consider two cases in terms of two sets $D + A_1$ and $D + A_2$.

Case 1. Let $D + P_j - \infty = div(a(u), b(u)) \in D + A_1$ with $a(u) = (u - x_j)(u - x_P)(u - x_Q)$ and $b(u) = b_0 + b_1 u + b_2 u^2$ for some b_0, b_1, and b_2. Then, we get the system of equations,

$$\begin{cases} b_0 + b_1 x_j + b_2 x_j^2 = b(x_j) = 0, \\ b_0 + b_1 x_P + b_2 x_P^2 = b(x_P) = y_P, \\ b_0 + b_1 x_Q + b_2 x_Q^2 = b(x_Q) = y_Q \end{cases}$$

with determinant $(x_P - x_j)(x_Q - x_j)(x_Q - x_P) \neq 0$. Then,

$$b_2 = \frac{x_Q y_P - x_P y_Q + x_j(y_Q - y_P)}{(x_P - x_Q)(x_P - x_j)(x_Q - x_j)}$$

by solving the system.

Let

$$D' = div(\hat{a}(u), \hat{b}(u)) \text{ with } \hat{a}(u) = \frac{f(u) - (b(u))^2}{a(u)} \text{ and}$$
$$\hat{b}(u) \equiv -b(u) \pmod{\hat{a}(u)} \text{ with } \deg(\hat{b}(u)) < \deg(\hat{a}(u)) = 2.$$

Then D' is a reduced divisor such that $D + P_j - \infty \equiv D' \pmod{\mathrm{Pic}(C)}$. Then,

$$\begin{aligned} \phi(D + P_j - \infty) &= -(a_4 - b_2^2 + (x_j + x_P + x_Q)) \\ &= \frac{(x_Q y_P - x_P y_Q + x_j(y_Q - y_P))^2}{(x_P - x_Q)^2 (x_P - x_j)^2 (x_Q - x_j)^2} - a_4 - (x_j + x_P + x_Q). \end{aligned}$$

Thus,

$$\sum_{j=1}^{5}\phi(D+P_j-\infty)=\sum_{j=1}^{5}\frac{(x_Qy_P-x_Py_Q+x_j(y_Q-y_P))^2}{(x_P-x_Q)^2(x_P-x_j)^2(x_Q-x_j)^2}-4a_4-5x_P-5x_Q.$$

Case 2. Let $D+P_j+P_k-2\infty=div(a(u),b(u))\in D+A_2$, where $a(u)=(u-x_j)(u-x_k)(u-x_P)(u-x_Q)$ and $b(u)=b_0+b_1u+b_2u^2+b_3u^3$ for some b_j $(j=0,1,2,3)$. Then we have the following system of equations:

$$\begin{cases} b_0+b_1x_j+b_2x_j^2+b_3x_j^3=b(x_j)=0,\\ b_0+b_1x_k+b_2x_k^2+b_3x_k^3=b(x_k)=0,\\ b_0+b_1x_P+b_2x_P^2+b_3x_P^3=b(x_P)=y_P,\\ b_0+b_1x_Q+b_2x_Q^2+b_3x_Q^3=b(x_Q)=y_Q,\end{cases}$$

with determinant $(x_P-x_j)(x_Q-x_j)(x_P-x_k)(x_Q-x_k)(x_P-x_Q)\neq 0$.

Then,

$$\begin{aligned} b_2=&\frac{x_Py_Q(x_P-x_j+x_k)(x_P+x_j-x_k)-x_Qy_P(x_Q-x_j+x_k)(x_Q+x_j-x_k)}{(x_P-x_Q)(x_P-x_j)(x_P-x_k)(x_Q-x_j)(x_Q-x_k)}\\ &+\frac{y_Qx_jx_k(x_P+x_j+x_k)-y_Px_jx_k(x_Q+x_j+x_k)}{(x_P-x_Q)(x_P-x_j)(x_P-x_k)(x_Q-x_j)(x_Q-x_k)},\ \text{and}\\ b_3=&\frac{y_P(x_Q-x_j)(x_Q-x_k)-y_Q(x_P-x_j)(x_P-x_k)}{(x_P-x_Q)(x_P-x_j)(x_P-x_k)(x_Q-x_j)(x_Q-x_k)}.\end{aligned}$$

Let

$$\hat{a}(u)=\frac{f(u)-(b(u))^2}{a(u)}\ \text{and}$$
$$\hat{b}(u)\equiv -b(u) \pmod{\hat{a}(u)} \text{ with } \deg(\hat{b}(u))<\deg(\hat{a}(u)).$$

Let $D'=div(\hat{a}(u),\hat{b}(u))$ so that $D+P_j+P_k-2\infty\equiv D' \pmod{\mathrm{Pic}(C)}$. Using the same argument from Theorem 7, we have $b_3\neq 0$ and

$$\phi(D+P_j+P_k-2\infty)=\frac{1}{b_3^2}-\frac{2b_2}{b_3}-x_P-x_Q-x_j-x_k.$$

Let $\Delta=\sum_{1\le j<k\le 5}\frac{1-2b_2(j,k)b_3(j,k)}{(b_3(j,k))^2}$. Then,

$$\sum_{1\le j<k\le 5}\phi(D+P_j+P_k-2\infty)=\Delta-10x_P-10x_Q+4a_4.$$

Since

$$\begin{aligned}\sum_{D\in[2]^{-1}(D_Q)}\phi(D)=&\ \phi(P+Q-2\infty)+\sum_{j=1}^{5}\phi(P+Q+P_j-3\infty)\\ &+\sum_{1\le j<k\le 5}\phi(P+Q+P_j+P_k-4\infty),\end{aligned}$$

we get

$$\sum_{D\in[2]^{-1}(D_Q)} \phi(D) = \Delta + \sum_{j=1}^{5} \frac{(x_Q y_P - x_P y_Q + x_j(y_Q - y_P))^2}{(x_P - x_Q)^2(x_P - x_j)^2(x_Q - x_j)^2} - 14x_P - 14x_Q.$$

□

Lemma 11. *Let $C : y^2 = f(x)$ be a hyperelliptic curve of genus $g \geq 1$ defined over K and let $D' \in J(C)$ be a divisor. Then*

$$\sum_{D\in[n]^{-1}(D')} D = n^{2g-1}D'.$$

Proof. Let E be any divisor satisfying $nE = D'$. Then,

$$\sum_{D\in[n]^{-1}(D')} D = \sum_{D\in[n]^{-1}(O)} (E + D) = n^{2g}E + \sum_{D\in[n]^{-1}(O)} D = n^{2g}E = n^{2g-1}D'$$

by Lemma 3 and the fact that $\sum_{h\in G} h = 0$, where $G = \mathbb{Z}/n_1\mathbb{Z} \times \cdots \times \mathbb{Z}/n_k\mathbb{Z}$ with $k > 1$. □

Corollary 12. *Let $g = 2$ and let $P \in C$ satisfy* (1)*. Then,*

$$\phi\left(\sum_{D\in[2]^{-1}(P-\infty)} D\right) = 2x_P + \frac{\left(2f(x_P)f''(x_P) - (f'(x_P))^2\right)^2}{32(f(x_P))^3} - \frac{f^{(4)}(x_P)}{12}.$$

Proof. By using Lemma 11, it is easy to see that

$$\sum_{D\in[2]^{-1}(P-\infty)} D = 8(P - \infty).$$

If the point P satisfies (1), then $4(P - \infty) \equiv Q - \infty$ for some $Q \in C$ from Lemma 6. Moreover,

$$x_Q = x_P + \frac{\left(2f(x_P)f''(x_P) - (f'(x_P))^2\right)^2}{64(f(x_P))^3} - \frac{f^{(4)}(x_P)}{4!}.$$

Hence,

$$\begin{aligned}\phi\left(\sum_{D\in[2]^{-1}(P-\infty)} D\right) &= \phi(2(Q - \infty)) = 2x_Q \\ &= 2x_P + \frac{\left(2f(x_P)f''(x_P) - (f'(x_P))^2\right)^2}{32(f(x_P))^3} - \frac{f^{(4)}(x_P)}{12}.\end{aligned}$$

□

Remark 13. We note that it is possible to compute

$$\phi\left(\sum_{D\in[n]^{-1}(P-\infty)} D\right) = \phi(n^{2g-1}(P - \infty))$$

for any genus g and any integer n but it is very hard to find explicit value when n and g is larger. Corollary 12 is a special case of [2, Theorem 8.35], where $n = 2$ and $g = 2$ and the computation result of $\phi\left(\sum_{D\in[2]^{-1}(P-\infty)} D\right)$ is given explicitly.

4. An example

In this section, we give an example which can apply our formula given in the previous sections.

Example 14. In this example, we consider the case when $D_Q = inv(P) - \infty$ for $D_P = P - \infty$ defined in Lemma 6. In this case, such divisors $P - \infty$ are 5-torsion points.

For a fixed $k \in K - \{0\}$, let

$$C : y^2 = f(x) := x^5 + k.$$

We apply Lemma 6 to the curve C. Then we get the equation

$$15x^2 - 120kx^7 + 240k^2x^2 = 0$$

which is equivalent to the equation

$$x^2(x^5 - 4k)^2 = 0.$$

Thus, we have exactly 12 points satisfying Lemma 6. Denote them by

$$\begin{cases} P_{0+} = (0, k^{1/2}), \\ P_{0-} = (0, -k^{1/2}), \\ P_{\xi_j+} = ((4k)^{1/5}\xi^j, (5k)^{1/2}) \quad \text{for} \quad j = 1, \ldots, 5, \\ P_{\xi_j-} = ((4k)^{1/5}\xi^j, -(5k)^{1/2}) \quad \text{for} \quad j = 1, \ldots, 5, \end{cases}$$

where $\xi = e^{\frac{2\pi i}{5}}$ is a primitive 5th root of unity. Let

$$\begin{cases} D_{0+} = 2(P_{0+} - \infty), \\ D_{0-} = 2(P_{0-} - \infty), \\ D_{\xi^j+} = 2(P_{\xi^j+} - \infty) \quad \text{for} \quad j = 1, \ldots, 5, \\ D_{\xi^j-} = 2(P_{\xi^j-} - \infty) \quad \text{for} \quad j = 1, \ldots, 5. \end{cases}$$

For the divisor D_{0+}, it is easy to see that $\phi(2D_{0+}) = 0$ so that

$$2D_{0+} \equiv P_{0+} - \infty \quad \text{or} \quad 2D_{0+} \equiv P_{0-} - \infty \pmod{\operatorname{Pic}(C)}.$$

Equivalently,

$$3(P_{0+} - \infty) \equiv 0 \quad \text{or} \quad 5(P_{0+} - \infty) \equiv 0 \pmod{\operatorname{Pic}(C)}.$$

If $3(P_{0+}-\infty) \equiv 0 \pmod{\mathrm{Pic}(C)}$, then $2(P_{0+}-\infty) \equiv (P_{0-}-\infty) \pmod{\mathrm{Pic}(C)}$. This is impossible because $N(2(P_{0+}-\infty)) \neq N(P_{0-}-\infty)$. Thus P_{0+} is a 5-torsion point and similarly P_{0-} is also a 5-torsion point. As a result, we have the subgroup of order 5

$$S = \{O, P_{0+}-\infty, 2(P_{0+}-\infty), P_{0-}-\infty, 2(P_{0-}-\infty)\}.$$

Again, we can verify that

$$x_P = x_P + \frac{\left(2f(x_P)f''(x_P) - (f'(x_P))^2\right)^2}{64(f(x_P))^3} - \frac{f^{(4)}(x_P)}{4!}$$

for $x_P = (4k)^{1/5}\xi^j$ for any $j = 1, \ldots, 5$. Thus,

$$5(P_{\xi^j+}-\infty) \equiv 0 \pmod{\mathrm{Pic}(C)},$$

by using the same argument and

$$T_j = \{O, P_{\xi^j+}-\infty, 2(P_{\xi^j+}-\infty), P_{\xi^j-}-\infty, 2(P_{\xi^j-}-\infty)\}$$

are other subgroups of order 5.

For $P = P_{0+} = (0, k^{1/2})$, we apply Theorem 7 to get the average value of 2-division points. Since $x^5 + k = \prod_{j=1}^{5}(x + k^{\frac{1}{5}}\xi^j)$, we have that

$$b_3(j,\ell) = \frac{-k^{\frac{-1}{10}}(\xi^j + \xi^\ell)}{\xi^{2j}\xi^{2\ell}}$$

and

$$b_2(j,\ell) = \frac{k^{\frac{1}{10}}}{\xi^j\xi^\ell} - \frac{k^{\frac{1}{10}}(\xi^j + \xi^\ell)^2}{\xi^{2j}\xi^{2\ell}}.$$

Then,

$$\Delta(P) = k^{\frac{1}{5}} \sum_{1\le j<\ell\le 5} \frac{\xi^{4j}\xi^{4\ell} - (\xi^{2j} + \xi^{2\ell} + 1)(\xi^j + \xi^\ell)}{(\xi^j + \xi^\ell)^2},$$

and also

$$\sum_{j=1}^{5} \frac{(2f(x_P) + f'(x_P)(x_j - x_P))^2}{4f(x_P)(x_j - x_P)^4} = \sum_{j=1}^{5} k^{\frac{1}{5}}\xi^j = 0,$$

where $x_j = -k^{\frac{1}{5}}\xi^j$ in this case. We can represent $\Delta(P) = \frac{A}{(\xi+1)^2} + \frac{B}{(\xi^2+1)^2}$ for some appropriate A and B $\in \mathbb{C}$. Then, we can show that $A = B = 0$ by the direct elementary calculations.

Thus, the average value of the x-coordinates of 2-division points on $J(C)$ is

$$\frac{1}{16} \sum_{D\in[2]^{-1}(P_{0-}-\infty)} \phi(D) = 0.$$

References

[1] D. G. Cantor, *Computing in the Jacobian of a hyperelliptic curve*, Math. Comp. **48** (1987), no. 177, 95–101.
[2] ———, *On the analogue of the division polynomials for hyperelliptic curves*, J. Reine Angew. Math. **447** (1994), 91–145.
[3] R. Feng and H. Wu, *A mean value formula for elliptic curves*, Journal of Numbers, Vol. **2014** (2014), Article ID 298632, 5 pages, http://dx.doi.org/10.1155/2014/298632, Cryptology ePrint Archive, Report 2009/586 (2009), http://eprint.iacr.org/.
[4] R. Hartshorne, *Algebraic Geometry*, Springer-Verlag, New York, 1977.

Jiman Chung
Department of Mathematics
Chung-Ang University
Seoul 06974, Korea

Bo-Hae Im
Department of Mathematical Sciences
KAIST
Daejeon 34141, Korea
Email address: bhim@kaist.ac.kr