Bull. Korean Math. Soc. **46** (2009), No. 5, pp. 917–930
DOI 10.4134/BKMS.2009.46.5.917

ISOMORPHISM CLASSES OF GENUS-3 POINTED TRIGONAL CURVES OVER FINITE FIELDS OF CHARACTERISTIC 2

Pyung-Lyun Kang[1] and Sunmi Sun

Abstract. We find all distinct representatives of isomorphism classes of genus-3 pointed trigonal curves and compute the number of isomorphism classes of a special class of genus-3 pointed trigonal curves including that of Picard curves over a finite field F of characteristic 2.

1. Introduction

A $C_{a,b}$ curve C over a field F is defined by a nonsingular affine equation in the affine plane over F of the form

$$a_{b0}x^b + a_{0a}y^a + \sum_{ai+bj<ab} a_{ij}x^iy^j, \quad a_{b0},\, a_{0a} \in F^*, \; a_{ij} \in F \tag{1.1}$$

for $a < b$ and $(a, b) = 1$. It is introduced by S. Miura in [8]. Arita then studied an addition algorithm on the Jacobian of $C_{a,b}$ curves in [1]. These $C_{a,b}$ curves generalize hyperelliptic curves, Picard curves and superelliptic curves whose properties and the addition algorithms on which studied intensively by many people [5], [4].

On the other hand, Encinas-Menezes-Masqúe [3] and Choie-Yun [2] classified the isomorphism classes of hyperelliptic curves of genus 2 over a finite field of characteristic different from 2 and 5, and of characteristic 2 respectively, in order to know how many essentially different choices of curves there are. Along this line, Lee [6] computed the number of isomorphism classes of Picard curves over a finite field, but there is some error when the characteristic of the field is 2. In this paper we correct this error in Corollary 1.2. A Picard curve is a nonsingular curve of genus 3 whose affine equation is given by $y^3 = f(x)$.

Received July 24, 2008.

2000 *Mathematics Subject Classification.* 11G20.

Key words and phrases. isomorphism classes, genus-3 trigonal curves, Picard curve, finite fields of characteristic 2.

[1] This study was financially supported by research fund of Chungnam National University in 2007.

In this paper we study the isomorphism classes of $C_{3,4}$ curves over a finite field of characteristic 2. The moduli space of $C_{3,4}$ curves over a field F has codimension 1 in the moduli of curves of genus 3. Note that every non-hyperelliptic curve of genus 3 can be realized as a nonsingular plane quartic, and the study of nonsingular quartics has a long history. More general result for the number of isomorphism classes of smooth plane quartics over a finite field of characteristic 2 was studied in [9] by Nart and Ritzenthaler and others.

In Section 2, we give all distinct representatives of isomorphism classes of $C_{3,4}$ curves that are pointed genus-3 trigonal curves over a finite field F of characteristic 2. In Section 3, we prove Theorem 1.1 in which we compute the number of isomorphism classes of codimension 1 subfamily of $C_{3,4}$ curves.

Theorem 1.1. *Let F be a field of order $q = 2^m$. Then the number of isomorphism classes of genus-3 trigonal curves that are represented by nonsingular equations*

$$y^3 + (b_2x^2 + b_8)y = x^4 + c_3x^3 + c_6x^2 + c_9x + c_{12}$$

is

$$\begin{cases} q(q^3+q-1) & \textit{if } m \textit{ is odd};\\ q^4+3q^2+q-2 & \textit{if } m \textit{ is even and } m \not\equiv 0 \pmod 6;\\ q^4+3q^2+q+4 & \textit{if } m \equiv 0 \pmod 6.\end{cases}$$

From the proof of Theorem 1.1, we obtain Corollary 1.2 that corrects the error in Theorem 4.5 of [6].

Corollary 1.2. *The number of isomorphism classes of Picard curves over a field of order $q = 2^m$ is*

$$\begin{cases} q^2+q-1 & \textit{if } m \textit{ is odd};\\ 3(q^2+q-1) & \textit{if } m \textit{ is even and } m \not\equiv 0 \pmod 6;\\ 3q^2+3q+3 & \textit{if } m \equiv 0 \pmod 6.\end{cases}$$

Notations. For the remainder of this paper, we fix notations.

- $F = F_q$, a field of order q with $q = 2^m$.
- g is a generator of the multiplicative cyclic group $F^* = F - \{0\}$.
- $\rho \in F$ is a fixed primitive cubic root of unity when m is even. So, ρ satisfies $\rho^2+\rho+1 = 0$. Note that such ρ does not exist if m is odd since $\rho^3 = 1$. See Lemma 2.2.

2. Isomorphism classes of $C_{3,4}$ curves

Let a and b be positive integers such that $a < b$ and $(a, b) = 1$. A $C_{a,b}$ curve C in (1.1) over a field F is a pointed a-gonal curve, i.e., there exists a point $P \in C$ with $\dim L(aP) = 2$, $L(\infty P) = \langle x, y\rangle$ where $x, y \in \bar{F}(C)$ with $a = -\mathrm{ord}_P(x), b = -\mathrm{ord}_P(y)$ and $g(C) = (a-1)(b-1)/2$. Furthermore, it can be written

$$y^a = x^b + \sum_{ai+bj<ab} a_{ij}x^iy^j \tag{2.1}$$

unique up to a change of coordinates of the form

$$x = u^a\hat{x} + r,\ \ y = u^b\hat{y} + t(\hat{x}), \tag{2.2}$$

where $u \in F^*$, $r \in F$ and t is a polynomial over F of degree not greater than $\frac{2g}{a(a-1)}$. In fact, we can $a_{0a} = -1$ by dividing the equation (1.1) through $-a_{0a}$. Since there exist integers δ and ϵ with $a\delta + b\epsilon = 1$, we obtain $a_{b0} = 1$ from the F-rational transformation $\hat{x} = a_{b0}^{\epsilon}x$, $\hat{y} = a_{b0}^{-\delta}y$. The final claim comes from the direct computations. Note that $L(D)$ consists of rational functions f with poles no worse than D when D is effective and $L(\infty P)$ is a ring of functions on C which are holomorphic away from P.

From now on, we restrict our study on $C_{3,4}$ curves

$$T(x,y) : y^3 + a(x)y^2 + b(x)y = x^4 + c_3x^3 + c_6x^2 + c_9x + c_{12} \tag{2.3}$$

that are the simplest cases of $C_{a,b}$ curves besides hyperelliptic ones. We may assume $a(x) = 0$ by replacing y with $y - \frac{a(x)}{3}$ if $\mathrm{char}(F) \neq 3$.

The next lemma gives the condition for our curves to be nonsingular. Note that Resultant$(f,g) \neq 0$ if and only f and g in $F[x]$ have no common zeroes in $\overline{F}$. So, the discriminant $D(f) = \mathrm{Resultant}(f,f') \neq 0$ if and only if f is *separable*, i.e., f has no multiple zeroes in $\overline{F}$.

Lemma 2.1. *Let F be a field of characteristic* 2.

(1) *Assume that $b_5 \neq 0$. Then*

$$T(x,y) : y^3 + (b_2x^2 + b_5x + b_8)y = x^4 + c_3x^3 + c_6x^2 + c_9x + c_{12}$$

is nonsingular if and only if

$$\mathrm{Resultant}(c_3^2x^4 + b_2b_5^2x^2 + b_5^3x + c_9^2 + b_5^2b_8, x^4 + c_3x^3 + c_6x^2 + c_9x + c_{12}) \neq 0.$$

(2) *Let $b_5 = 0$. Then $y^3 + (b_2x^2 + b_8)y = f(x) = x^4 + c_3x^3 + c_6x^2 + c_9x + c_{12}$ is nonsingular if and only if $c_9^2 + c_3c_6c_9 + c_3^2c_{12} \neq 0$ if and only if $f(x)$ has no multiple zeroes in $\overline{F}$.*

Proof. The partial derivatives with respect to x and y are, respectively,

$$b_5y = c_3x^2 + c_9, \qquad y^2 + b_2x^2 + b_5x + b_8 = 0.$$

So, if singular, the above partial derivatives must have a common solution with $f(x) = x^4 + c_3x^3 + c_6x^2 + c_9x + c_{12} = 0$. Since $b_5 \neq 0$, by substituting y in the first equation into $f(x)$ and by multiplying b_5^2, we see that two polynomials in resultant have a common zero. Now suppose that two polynomials in resultant have a common zero x_0. Then (x_0, y_0) becomes a singular point of $T(x,y)$ if we let $y_0 = b_5^{-1}(c_3x^2 + c_9)$. Assume $b_5 = 0$. Then, from the similar computation as in the proof of (1), $y^3 + (b_2x^2 + b_8)y = x^4 + c_3x^3 + c_6x^2 + c_9x + c_{12}$ is singular if and only if Resultant$(c_3x^2 + c_9, x^4 + c_3x^3 + c_6x^2 + c_9x + c_{12}) = D(f) = 0$, since $f'(x) = c_3x^2 + c_9$. Since $D(f) = (c_9^2 + c_3c_6c_9 + c_3^2c_{12})^2$ when char$F = 2$, we are done. □

Let

(2.4)
$\tilde{\mathfrak{T}} = \{T(x,y) : y^3+(b_2x^2+b_5x+b_8)y = x^4+c_3x^3+c_6x^2+c_9x+c_{12} \mid \text{nonsingular}\}.$

Then the group

$$G = \{A_{u,\gamma} : (x,y) \mapsto (u^3x+\gamma, u^4y) \mid u \in F^*, \gamma \in F\} \tag{2.5}$$

of all possible changes of coordinates of curves in $\tilde{\mathfrak{T}}$ acts on $\tilde{\mathfrak{T}}$ in the obvious way: $A_{u,\gamma} \cdot T(x,y) = T(u^3x+\gamma, u^4y)$. We say two curves

$$T(x,y) : y^3 + (b_2x^2 + b_5x + b_8)y = x^4 + c_3x^3 + c_6x^2 + c_9x + c_{12},$$
$$\overline{T}(x,y) : y^3 + (\bar{b}_2x^2 + \bar{b}_5x + \bar{b}_8)y = x^4 + \bar{c}_3x^3 + \bar{c}_6x^2 + \bar{c}_9x + \bar{c}_{12}$$

in $\tilde{\mathfrak{T}}$ are isomorphic over F if they satisfy $A_{u,\gamma} \cdot T = \overline{T}(x,y)$ for some $u \in F^*$ and $\gamma \in F$. If this happens, we have the following relations when the characteristic of F is 2:

$$\begin{cases} u^2\bar{b}_2 = b_2, \\ u^5\bar{b}_5 = b_5, \\ u^8\bar{b}_8 = b_2\gamma^2 + b_5\gamma + b_8, \\ u^3\bar{c}_3 = c_3, \\ u^6\bar{c}_6 = c_3\gamma + c_6, \\ u^9\bar{c}_9 = c_3\gamma^2 + c_9, \\ u^{12}\bar{c}_{12} = \gamma^4 + c_3\gamma^3 + c_6\gamma^2 + c_9\gamma + c_{12}. \end{cases} \tag{2.6}$$

The following observation on a finite field of characteristic 2 is useful.

Lemma 2.2. *Let F be a finite field of order 2^m.*

(1) *F^* has an element of order r if and only if r divides $2^m - 1$.*
(2) *A homomorphism $e_r : F^* \to F^*$ defined by $e_r(\alpha) = \alpha^r$ is an automorphism of the multiplicative group F^* if and only if $(r, 2^m-1) = 1$. In this case, for any $\beta \in F^*$, there exists a unique $\alpha \in F^*$ such that $\alpha^r = \beta$.*
(3) *$m \equiv 0 \pmod 2$ if and only if $2^m - 1 \equiv 0 \pmod 3$.*
(4) *$m \equiv 0 \pmod 6$ if and only if $2^m - 1 \equiv 0 \pmod 9$.*
(5) *Suppose $m \equiv 0 \pmod 6$. If F^* is generated by g, there exists no element $u \in F$ with $u^9 = g^l$ for $1 \le l \le 8$.*
(6) *ρ is a cube in F if and only if $m \equiv 0 \pmod 6$.*

Proof. (1) Since F^* is a cyclic group of order 2^m-1 with respect to the multiplication, it is well known fact from group theory. (2) Since e_r is a homomorphism of finite group F^*, it is enough to show that e_r is injective. But $\operatorname{Ker} e_r = \{1\}$ if and only if $(r, 2^m-1) = 1$ by (1). The proofs of (3) and (4) are similar. We here do (4). Note that $2^m - 1 \equiv 0 \pmod 9$ for $m = 0$ and 6. Now suppose

$m = 6k$ for $k \geq 2$. Then $2^{6k} - 1 = (2^6 - 1)(2^{6(k-1)} + 2^{6(k-2)} + \cdots + 2^6 + 1) \equiv 0 \pmod 9$. To show the converse, assume $m = 6k + l$ for $1 \leq l \leq 5$. Then $2^m - 1 = 2^{6k} 2^l - 1 \equiv 2^l - 1 \not\equiv 0 \pmod 9$ for $1 \leq l \leq 5$. For (5), suppose there exists an element $u \in F$ such that $u^9 = g^l$ for some $1 \leq l \leq 8$. Then $g^{l(2^m-1)/9} = 1$, which implies that $\operatorname{ord}(g) < 2^m - 1$. (6) If m is odd, there is no solution ρ in F of $x^2 + x + 1 = 0$ by (3). Otherwise, $\rho = g^{(2^m-1)/3}$ or $\rho = g^{2(2^m-1)/3}$ where $F^* = \langle g \rangle$. So, ρ is a cube only if 9 divides $2^m - 1$, i.e., $m \equiv 0 \pmod 6$. □

Proposition 2.3. *If* $b_5 \neq 0$*, then every curve in* $\tilde{\mathcal{T}}$ *is isomorphic to one of following three types of nonsingular equations*:

(1) $y^3 + x^2 y + b_5 xy + f_i y = x^4 + c_3 x^3 + c_6 x^2 + c_9 x + c_{12}, i = 1, 2,$ *where* $f_1 = 0$ *and* $f_2 \in F - \{\gamma^2 + b_5 \gamma \mid \gamma \in F\}$;

(2) $y^3 + b_5 xy = x^4 + c_3 x^3 + c_6 x^2 + b_5 x + c_{12}$;

(3) $y^3 + b_5 xy = x^4 + c_3 x^3 + c_6 x^2 + b_5^2$.

Proof. Suppose $b_5 \neq 0$ and $b_2 \neq 0$. Then taking $u^2 = b_2$, we get (1). The existence of such $u \in F^*$ is guaranteed by Lemma 2.2(2). If $b_5 \neq 0$ and $b_2 = 0$, we may assume that $b_8 = 0$ by replacing x with $x + b_5^{-1} b_8$. In this case we must have $c_9 \neq 0$ or $c_{12} \neq 0$ for such curves to be nonsingular due to Lemma 2.1. If two curves in this type are isomorphic, then, by (2.6), we have either $u^4 \frac{\bar{c}_9}{b_5} = \frac{c_9}{b_5}$ or $u^2 \frac{\bar{c}_{12}}{b_5^2} = \frac{c_{12}}{b_5^2}$ and $\gamma = 0$. So, by taking either $u^4 = \frac{c_9}{b_5}$ or $u^2 = \frac{c_{12}}{b_5^2}$, we have (2) or (3). □

We remark that no two in (2) and (3) of Proposition 2.3 are isomorphic. For, if $A_{u,\gamma} \cdot T = \bar{T}$ for $T, \bar{T}$ in (2) (or in (3), resp.), we have $\gamma = 0$ and $u^4 = 1$ ($u^2 = 1$, resp.), and $u^4 = 1$ or $u^2 = 1$ implies $u = 1$ if the characteristic of F is 2 (Lemma 2.2(1)). But the special two curves in (1) are possibly isomorphic. For example, $y^3 + x^2 y + xy = x^4 + x^2 + x + 1$ and $y^3 + x^2 y + xy = x^4 + x^2 + x$ are isomorphic over F_2. In fact, there are 18 distinct isomorphism classes over F_2 when $b_5 \neq 0$. See Example 2.11.

From now on we concentrate on curves with $b_5 = 0$. Let

$$\mathcal{T} = \{T(x,y) \in \tilde{\mathcal{T}} : y^3 + (b_2 x^2 + b_8) y = x^4 + c_3 x^3 + c_6 x^2 + c_9 x + c_{12}\}. \tag{2.7}$$

Lemma 2.1(2) tells that the nonsingular condition of $T(x,y) \in \mathcal{T}$ depends on the terms only in x. We start by dividing $\mathcal{T}$ into the following G-invariant subsets. Let

$$\begin{aligned} \mathcal{A}_1 &= \{T(x,y) \in \mathcal{T} \mid b_2 = 0 = b_8, c_3 \neq 0\}, \\ \mathcal{A}_2 &= \{T(x,y) \in \mathcal{T} \mid b_2 = 0 = b_8, c_3 = 0, c_6 \neq 0\}, \\ \mathcal{A}_3 &= \{T(x,y) \in \mathcal{T} \mid b_2 = 0 = b_8, c_3 = 0, c_6 = 0\}, \\ \mathcal{B} &= \{T(x,y) \in \mathcal{T} \mid b_2 \neq 0\}, \end{aligned} \tag{2.8}$$

$$\mathcal{C}_1 = \{T(x,y) \in \mathcal{T} \mid b_2 = 0, b_8 \neq 0, c_3 \neq 0\},$$
$$\mathcal{C}_2 = \{T(x,y) \in \mathcal{T} \mid b_2 = 0, b_8 \neq 0, c_3 = 0, c_6 \neq 0\},$$
$$\mathcal{C}_3 = \{T(x,y) \in \mathcal{T} \mid b_2 = 0, b_8 \neq 0, c_3 = 0, c_6 = 0\}.$$

Let $h(x) = x^4 + ax^2 + bx \in F[x]$. Define

$$\Psi_h : F \to F, \ \Psi_h(\alpha) = h(\alpha).$$

Then Ψ_h is an additive homomorphism if $\mathrm{char}(F) = 2$. Moreover, $|F/\mathrm{Im}\Psi_h| = |\mathrm{Ker}\Psi_h|$ since F is finite.

Theorem 2.4. *Let F be a field of order 2^m and let $h(x) = x^4 + ax^2 + bx$ with $b \neq 0$. Then $T_1 : y^3 = h(x) + e_1$ and $T_2 : y^3 = h(x) + e_2$ are isomorphic if and only if*

$$e_1 + u^3 e_2 \in \mathrm{Im}\Psi_h$$

for some $u \in F^*$ satisfying $u^9 = 1$. In particular, if $m \not\equiv 0 \pmod 6$, then T_1 and T_2 are isomorphic if and only if $e_1 + \mathrm{Im}\Psi_h = e_2 + \mathrm{Im}\Psi_h$. That is,

$$\{y^3 = h(x) + e_j \mid 1 \leq j \leq n = |\mathrm{Ker}\ \Psi_h|\}$$

are all distinct representatives of the class given by $y^3 = h(x) + e$ where $\{e_j + \mathrm{Im}\Psi_h\} = F/\mathrm{Im}\Psi_h$.

Proof. Suppose $A_{u,\gamma}(T_1) = T_2$. Then, from (2.6), we have $u^9 = 1$, $u^3 e_2 = \gamma^4 + a\gamma^2 + b\gamma + e_1$. So, $e_1 + u^3 e_2 \in \mathrm{Im}\Psi_h$. Conversely, if there exist u and γ satisfying $e_1 + u^3 e_2 = h(\gamma)$ and $u^9 = 1$, then $A_{u,\gamma}(T_1) = T_2$. If $m \not\equiv 0 \pmod 6$, then $u^9 = 1$ implies either $u = 1$ when m is odd or $u^3 = 1$ otherwise, since 9 does not divide $2^m - 1$ by Lemma 2.2(4). Now the last statement follows from that Ψ_h is a homomorphism. □

Proposition 2.5. Curves in $\mathcal{A}_1$

(1) *If m is odd, then every curve in $\mathcal{A}_1$ is isomorphic to only one curve in*

$$\{y^3 = x^4 + x^3 + c_9 x + c_{12} \mid c_9^2 + c_{12} \neq 0\}.$$

(2) *If m is even, then every curve in $\mathcal{A}_1$ is isomorphic to only one curve in*

$$\{y^3 = x^4 + g^i x^3 + c_9 x + c_{12} \mid i = 0, 1, 2, \ c_9^2 + g^{2i} c_{12} \neq 0\}$$

where $F^* = \langle g \rangle$. If $m \not\equiv 0 \pmod 6$, we can take ρ instead of g in (2).

Proof. By letting $x \mapsto x + c_3^{-1} c_6$, we may assume that $c_6 = 0$. If m is odd, then $c_3 = d^3$ for some $d \in F^*$. Then (1) follows if we let $x \mapsto d^3 x$, $y \mapsto d^4 y$. If m is even, write $c_3 = g^{3k+i}$, $0 \leq i \leq 2$. Then letting $x \mapsto u^3 x, y \mapsto u^4 y$ where $u = g^k$, we can make $c_3 = g^i$ for $i = 0, 1, 2$. Since $y^3 = x^4 + \rho^i x^3 + c_9 x + c_{12}$ are all distinct for $i = 0, 1, 2$ if ρ is not a cube, we can replace g with ρ if m is even and $m \not\equiv 0 \pmod 6$. □

Proposition 2.6. Curves in $\mathcal{A}_2$

(1) *If m is odd, then every curve in $\mathcal{A}_2$ is isomorphic to only one curve in*

$$\{y^3 = x^4 + x^2 + c_9 x + e_j \mid 1 \le j \le |\mathrm{Ker}\Psi_h|,\ c_9 \ne 0\},$$

where $\{e_j + \mathrm{Im}\Psi_h\} = F/\mathrm{Im}\Psi_h$ and $h(x) = x^4 + x^2 + c_9 x$.

(2) *If m is even, then every curve in $\mathcal{A}_2$ is isomorphic to only one curve in*

$$\{y^3 = x^4 + g^i x^2 + c_9 x + e_{ij} \mid i = 0, 1, 2,\ c_9 \ne 0\},$$

where $h_i(x) = x^4 + g^i x^2 + c_9 x$ and $\{e_{ij} + \mathrm{Im}\Psi_{h_i}\} = F/\mathrm{Im}\Psi_{h_i}$ for each $0 \le i \le 2$. We can take $g = \rho$ if $m \not\equiv 0 \pmod 6$.

Proof. If m is odd, we may assume that $c_6 = 1$. For, $c_6 = u^6$ for some $u \in F^*$ since $(6,\ 2^m - 1) = 1$ (Lemma 2.2). If m is even, write $c_6 = g^{3k+i}$ for $0 \le i \le 2$. Choosing $u \in F^*$ with $u^2 = g^k$, we may assume $c_6 = g^i$ since $c_6/u^6 = g^i$ for $0 \le i \le 2$. Now refer Theorem 2.4. For the last statement, see the proof of Proposition 2.5. □

Proposition 2.7. Curves in $\mathcal{A}_3$

(1) *If m is odd, every element in $\mathcal{A}_3$ is isomorphic to either $y^3 = x^4 + x$ or $y^3 = x^4 + x + 1$.*

(2) *If $m \equiv 2$ or $4 \pmod 6$, every curve in $\mathcal{A}_3$ is isomorphic to either*

$$y^3 = x^4 + \rho x, \quad y^3 = x^4 + \rho^2 x,$$

or

$$y^3 = x^4 + x + e_j,$$

where $\{e_j + \mathrm{Im}\Psi_h\} = F/\mathrm{Im}\Psi_h$ with $h(x) = x^4 + x$.

(3) *If $m \equiv 0 \pmod 6$, every curve in $\mathcal{A}_3$ is isomorphic to either*

$$y^3 = x^4 + g^i x, \quad i = 1, 2, 4, 5, 7, 8,$$

or

$$y^3 = x^4 + g^i x,\ y^3 = x^4 + g^i x + e$$

with $e \notin \mathrm{Im}\Psi_h$, where $h = x^4 + g^i x$ for each $i = 0, 3, 6$.

Proof. (1) If m is odd, we may assume that $c_9 = 1$. For, $c_9 = u^9$ for some $u \in F^*$ since $(9,\ 2^m - 1) = 1$ (Lemma 2.2). Since there is no γ satisfying $\gamma^4 + \gamma + 1 = 0$ when m is odd, two curves in (1) are not isomorphic. The fact $|\,\mathrm{Ker}\,\Psi_h| = 2$ for $b = x^4 + x$ implies that they are all. Note that, if there is an element $\gamma \in F$ satisfying $\gamma^4 + \gamma + 1 = 0$, F contains $\mathbb{Z}_2(\gamma)$ as a subfield and $4|m$, since $x^4 + x + 1$ is an irreducible polynomial over $\mathbb{Z}_2$. (2) Suppose $m \equiv 2$ or $4 \pmod 6$. Then ρ is not a cube. Therefore any two curves in (2) are not isomorphic and give 6 different isomorphism classes since $|\,\mathrm{Ker}\,\Psi_{x^2+x}| = 4$. From Proposition 3.7, these are all. For (3), from the proof of Proposition 3.7 for the case $m \equiv 0 \pmod 6$, we know that we can choose only one class when c_9 is not a cube and two when c_9 is a cube: one from $c_{12} \in \mathrm{Im}\Psi_h$ and the other from $c_{12} \notin \mathrm{Im}\Psi_h$. Note that no curves in the list are isomorphic by Lemma 2.2(5) and Theorem 2.4. □

Proposition 2.8. Curves in $\mathcal{B}$
Every curve in $\mathcal{B}$ is isomorphic to only one in

$$\{y^3 + x^2y = x^4 + c_3x^3 + c_6x^2 + c_9x + c_{12} \mid c_9^2 + c_3c_6c_9 + c_3^2c_{12} \neq 0\}.$$

Proof. Take u, γ such that $u^2 = b_2, \gamma^2 = b_2^{-1}b_8$. □

Note that every curve in $\mathcal{C}_i$ can be transformed to $y^3 + y = x^4 + c_3x^3 + c_6x^2 + c_9x + c_{12}$ by taking $A_{u,0}$ in (2.5) such that $u^8 = b_8$. If $c_3 \neq 0$ we can make $c_6 = 0$. Now together with Theorem 2.4, we have:

Proposition 2.9. Curves in $\mathcal{C}_i$

(1) *Every curve in $\mathcal{C}_1$ is isomorphic to only one of $\{y^3 + y = x^4 + c_3x^3 + c_9x + c_{12} \mid c_9^2 + c_3^2c_{12} \neq 0\}$.*

(2) *Every curve in $\mathcal{C}_2$ and $\mathcal{C}_3$ is isomorphic to only one of the following curves given by*

$$y^3 + y = x^4 + c_6x^2 + c_9x + e_j \ (c_9 \neq 0),$$

where $e_j + \mathrm{Im}\Psi_h$ are distinct elements of $F/\mathrm{Im}\Psi_h$ for each $h(x) = x^4 + c_6x^2 + c_9x$.

Example 2.10. The representatives of the isomorphism classes of $\mathcal{T}$ over F_2.

types	representatives
$\mathcal{A}_1$	$y^3 = x^4 + x^3 + x, \quad y^3 = x^4 + x^3 + 1.$
$\mathcal{A}_2$	$y^3 = x^4 + x^2 + x.$
$\mathcal{A}_3$	$y^3 = x^4 + x, \quad y^3 = x^4 + x + 1.$
$\mathcal{B}$	$y^3 + x^2y = x^4 + x^3 + x^2 + x, \quad y^3 + x^2y = x^4 + x^3 + x^2 + 1,$ $y^3 + x^2y = x^4 + x^3 + x, \quad y^3 + x^2y = x^4 + x^3 + 1,$ $y^3 + x^2y = x^4 + x^2 + x, \quad y^3 + x^2y = x^4 + x^3 + x^2 + x + 1,$ $y^3 + x^2y = x^4 + x, \quad y^3 + x^2y = x^4 + x + 1.$
$\mathcal{C}_1$	$y^3 + y = x^4 + x^3 + 1, \quad y^3 + y = x^4 + x^3 + x.$
$\mathcal{C}_2$	$y^3 + y = x^4 + x^2 + x.$
$\mathcal{C}_3$	$y^3 + y = x^4 + x, \quad y^3 + y = x^4 + x + 1.$

Example 2.11. The representatives of the isomorphism classes of $\tilde{\mathcal{T}}$ over F_2 when $b_5 \neq 0$. See Proposition 2.3.

types	representatives
$b_2 \neq 0,\ b_5 \neq 0$	$y^3 + x^2y + xy = x^4 + x^3 + 1, \quad y^3 + x^2y + xy = x^4 + x^2 + 1,$ $y^3 + x^2y + xy = x^4 + x^2 + x, \quad y^3 + x^2y + xy = x^4 + x + 1,$ $y^3 + x^2y + xy + y = x^4, \quad y^3 + x^2y + xy + y = x^4 + x^2,$ $y^3 + x^2y + xy + y = x^4 + x^3 + x^2, \quad y^3 + x^2y + xy + y = x^4 + x^3 + 1,$ $y^3 + x^2y + xy + y = x^4 + x + 1.$
$b_2 = 0,\ b_5 \neq 0$	$y^3 + xy = x^4 + x^2 + x, \quad y^3 + xy = x^4 + x + 1,$ $y^3 + xy = x^4 + x^3 + x, \quad y^3 + xy = x^4 + x^3 + x^2 + x,$ $y^3 + xy = x^4 + x^3 + x + 1, \quad y^3 + x^2y = x^4 + x^3 + x^2 + x + 1,$ $y^3 + xy = x^4 + 1, \quad y^3 + xy = x^4 + x^3 + 1,$ $y^3 + xy = x^4 + x^2 + 1.$

Example 2.12. The representatives of the isomorphism classes of $\mathcal{T}$ over F_4. Note that we get all representatives for $\mathcal{C}_i$ by inserting y in each representative of $\mathcal{A}_i$.

types	representatives	cardinality
$\mathcal{A}_1$	$y^3 = x^4 + x^3 + c_9x + c_{12},\ y^3 = x^4 + \rho x^3 + c_9x + c_{12},$ $y^3 = x^4 + \rho^2x^3 + c_9x + c_{12}.$	36
$\mathcal{A}_2$	$y^3 = x^4 + x^2 + x,\ y^3 = x^4 + x^2 + \rho x,\ y^3 = x^4 + x^2 + \rho x + 1,$ $y^3 = x^4 + x^2 + \rho^2x,\ y^3 = x^4 + x^2 + \rho^2x + 1,$ $y^3 = x^4 + \rho x^2 + x,\ y^3 = x^4 + \rho x^2 + \rho x,\ y^3 = x^4 + \rho x^2 + \rho x + \rho,$ $y^3 = x^4 + \rho x^2 + \rho^2x,\ y^3 = x^4 + \rho x^2 + \rho^2x + 1,$ $y^3 = x^4 + \rho^2x^2 + x,\ y^3 = x^4 + \rho^2x^2 + \rho x,\ y^3 = x^4 + \rho^2x^2 + \rho x + \rho,$ $y^3 = x^4 + \rho^2x^2 + \rho^2x,\ y^3 = x^4 + \rho^2x^2 + \rho^2x + \rho.$	15
$\mathcal{A}_3$	$y^3 = x^4 + x,\ y^3 = x^4 + x + 1,\ y^3 = x^4 + x + \rho,$ $y^3 = x^4 + x + \rho^2,\ y^3 = x^4 + \rho x,\ y^3 = x^4 + \rho^2x.$	6
$\mathcal{B}$	$y^3 + x^2y = x^4 + c_3x^3 + c_6x^2 + c_9x + c_{12}.$	192

Corollary 2.13. *The number of isomorphism classes of C_{34} curves over F_2 is 36.*

3. Proof of Theorem 1.1

In this section, we count the number of isomorphism classes in $\mathcal{T}$.

Proposition 3.1. *We have $|\mathcal{A}_1| = (q-1)^2q^2$, $|\mathcal{A}_2| = (q-1)^2q$, $|\mathcal{A}_3| = (q-1)q$, $|\mathcal{B}| = (q-1)^2q^4$, $|\mathcal{C}_1| = (q-1)^3q^2$, $|\mathcal{C}_2| = (q-1)^3q$, $|\mathcal{C}_3| = (q-1)^2q$, and $|\mathcal{T}| = q^5(q-1)$.*

Recall that the group $G = \{A_{u,\gamma} : (x,y) \mapsto (u^3x + \gamma, u^4y),\ u \in F^*, \gamma \in F\}$ acts on $\mathcal{T}$ as $A_{u,\gamma} \cdot T = T(u^3x + \gamma, u^4y)$. Suppose that $\mathcal{S}$ is a G-invariant subset of $\mathcal{T}$. Then the number of isomorphism classes in $\mathcal{S}$ is $|\mathcal{S}/G|$ where $\mathcal{S}/G$ is the set of all distinct G-orbits in $\mathcal{S}$. Note that

$$|\mathcal{S}/G| = \frac{|\mathcal{S}|}{|G \cdot T|} = \frac{|\mathcal{S}||G_T|}{|G|} \tag{3.1}$$

if $|G_T|$ is constant for any $T \in \mathcal{S}$. Here $G \cdot T$ is a G-orbit containing T and G_T is the isotropy group of T.

From (2.6), the isotropy group of a curve in each set in (2.8) is given as follows:

(3.2)

$$G_T = \begin{cases} \{(u,\gamma) \in F^* \times F \mid u^3 = 1,\ \gamma = 0\} \text{ for } T \in \mathcal{A}_1, \\ \{(u,\gamma) \in F^* \times F \mid u^3 = 1,\ \gamma^4 + c_6\gamma^2 + c_9\gamma = 0\} \text{ for } T \in \mathcal{A}_2, \\ \{(u,\gamma) \in F^* \times F \mid u^9 = 1,\ \gamma^4 + c_9\gamma + c_{12}(1 + u^3) = 0\} \text{ for } T \in \mathcal{A}_3, \\ \{(u,\gamma) \in F^* \times F \mid u = 1,\ \gamma = 0\} \text{ for } T \in \mathcal{B}, \text{ or } T \in \mathcal{C}_1, \\ \{(u,\gamma) \in F^* \times F \mid u = 1,\ \gamma^4 + c_6\gamma^2 + c_9\gamma = 0\} \text{ for } T \in \mathcal{C}_2, \\ \{(u,\gamma) \in F^* \times F \mid u = 1,\ \gamma^4 + c_9\gamma = 0\} \text{ for } T \in \mathcal{C}_3. \end{cases}$$

We now count the number of isomorphism classes of sets in (2.8). Easily, $|G_T| = 1$ when $T \in \mathcal{B}$ or $\mathcal{C}_1$. If $T \in \mathcal{A}_1$, $|G_T| = 1$ for an odd number m and $|G_T| = 3$ for even m by Lemma 2.2. Now (3.1) gives:

Proposition 3.2. *The number of isomorphism classes of curves in $\mathcal{A}_1$, $\mathcal{B}$ and $\mathcal{C}_1$.*

1. *The number of isomorphism classes of curves in $\mathcal{A}_1$ is $(q-1)q$ if m is odd, and $3(q-1)q$ if m is even.*
2. *The number of isomorphism classes of curves in $\mathcal{B}$ is $(q-1)q^3$.*
3. *The number of isomorphism classes of curves in $\mathcal{C}_1$ is $(q-1)^2q$.*

For $\mathcal{A}_2, \mathcal{A}_3, \mathcal{C}_2$, and $\mathcal{C}_3$, we need to count the number of zeroes of some polynomials $\in F[x]$ according to their coefficients.

Lemma 3.3. *Let*

$$\begin{aligned}
\mathcal{R}_0 &= \{(a,b) \in F \times F^* |\ x^3 + ax + b \text{ has no zero in } F\},\\
\mathcal{R}_1 &= \{(a,b) \in F \times F^* |\ x^3 + ax + b \text{ has only one zero in } F\},\\
\mathcal{R}_3 &= \{(a,b) \in F \times F^* |\ x^3 + ax + b \text{ has three distinct zeroes in } F\},\\
\mathcal{R}_{00} &= \{b \in F^* |\ x^3 + b \text{ has no zero in } F\},\\
\mathcal{R}_{10} &= \{b \in F^* |\ x^3 + b \text{ has only one zero in } F\},\\
\mathcal{R}_{30} &= \{b \in F^* |\ x^3 + b \text{ has three distinct zeroes in } F\}.
\end{aligned}$$

Then we have

$$|\mathcal{R}_0| = \frac{1}{3}(q-1)(q+1),\ |\mathcal{R}_1| = \frac{1}{2}q(q-1),\ |\mathcal{R}_3| = \frac{1}{6}(q-1)(q-2);$$

$$\begin{cases} |\mathcal{R}_{00}| = 0 \\ |\mathcal{R}_{10}| = q-1 \\ |\mathcal{R}_{30}| = 0 \end{cases} \text{if } m \text{ is odd;} \qquad \begin{cases} |\mathcal{R}_{00}| = \frac{2}{3}(q-1) \\ |\mathcal{R}_{10}| = 0 \\ |\mathcal{R}_{30}| = \frac{1}{3}(q-1) \end{cases} \text{if } m \text{ is even.}$$

Proof. One can check that $x^3 + ax + b$ has no multiple zeroes since $b \neq 0$. Assume that $f(x) = x^3 + ax + b$ has three distinct zeroes. Then

$$\begin{aligned}
x^3 + ax + b &= (x+\alpha)(x+\beta)(x+\gamma)\\
&= x^3 + (\alpha+\beta+\gamma)x^2 + (\alpha\beta+\beta\gamma+\gamma\alpha)x + \alpha\beta\gamma
\end{aligned}$$

with $\alpha\beta\gamma \neq 0$. Then $\gamma = \alpha + \beta$, γ is determined from α, β. If we choose any two elements of α, β, γ, we have the same equation. Hence

$$|\mathcal{R}_3| = \frac{(q-1)(q-2)}{3!}.$$

Suppose $f(x)$ has one zero. Then $f(x) = (x+\alpha)(x^2+\alpha x+\beta)$ with $x^2+\alpha x+\beta$ is irreducible. Note that if $x^2 + \alpha x + \beta$ is irreducible over F_{2^m} then $\alpha \neq 0, \beta \neq 0$. So $|\mathcal{R}_1| = \frac{1}{2}q(q-1)$ and $|\mathcal{R}_0| = \frac{1}{3}(q-1)(q+1)$. For $|\mathcal{R}_{i0}|$, it is enough to observe the following. Note that the map $e_3 : F^* \to F^*$ sending $x \mapsto x^3$ is one to one if and only if $x^3 = 1$ has only one solution 1 if and only if 3 does not divide $2^m - 1$ if and only if m is odd (Lemma 2.2(3)). Otherwise e_3 is a 3 to 1 map. □

Note that $|\mathcal{R}_0 - \mathcal{R}_{00}| = \frac{1}{3}(q-1)(q+1)$, $|\mathcal{R}_1 - \mathcal{R}_{10}| = \frac{1}{2}(q-1)(q-2)$, $|\mathcal{R}_3 - \mathcal{R}_{30}| = \frac{1}{6}(q-1)(q-2)$ if m is odd; $|\mathcal{R}_0 - \mathcal{R}_{00}| = \frac{1}{3}(q-1)^2$, $|\mathcal{R}_1 - \mathcal{R}_{10}| = \frac{1}{2}q(q-1)$, $|\mathcal{R}_3 - \mathcal{R}_{30}| = \frac{1}{6}(q-1)(q-4)$ if m is even.

Proposition 3.4. *The number of isomorphism classes of curves in $\mathcal{A}_2$ is*

$$\begin{cases} 2q-3 & \textit{if } \ m \textit{ is odd} \\ 6q-9 & \textit{if } \ m \textit{ is even.} \end{cases}$$

Proof. Note that

$$G_{A_2} = \{(u,\gamma) \in F^* \times F| \ \ u = 1, \ \gamma^4 + c_6\gamma^2 + c_9\gamma = 0\}$$

if m is odd, and

$$G_{A_2} = \{(u,\gamma) \in F^* \times F| \ \ u^3 = 1, \ \gamma^4 + c_6\gamma^2 + c_9\gamma = 0\}$$

if m is even. Then, from Lemma 3.3

$$|G_{A_2}| = \begin{cases} 1 \text{ if } m \text{ is odd and } x^3 + c_6x + c_9 \in \mathcal{R}_0 - \mathcal{R}_{00}, \\ 2 \text{ if } m \text{ is odd and } x^3 + c_6x + c_9 \in \mathcal{R}_1 - \mathcal{R}_{10}, \\ 4 \text{ if } m \text{ is odd and } x^3 + c_6x + c_9 \in \mathcal{R}_3 - \mathcal{R}_{30}, \\ 3 \text{ if } m \text{ is even and } x^3 + c_6x + c_9 \in \mathcal{R}_0 - \mathcal{R}_{00}, \\ 6 \text{ if } m \text{ is even and } x^3 + c_6x + c_9 \in \mathcal{R}_1 - \mathcal{R}_{10}, \\ 12 \text{ if } m \text{ is even and } x^3 + c_6x + c_9 \in \mathcal{R}_3 - \mathcal{R}_{30}. \end{cases}$$

Therefore,

$$\begin{aligned} |\mathcal{A}_2/G| &= \frac{\frac{1}{3}(q-1)(q+1)q}{(q-1)q} + \frac{\{\frac{1}{2}(q-1)q - (q-1)\}q \cdot 2}{(q-1)q} + \frac{\frac{1}{6}(q-2)(q-1)q \cdot 4}{(q-1)q} \\ &= \frac{q+1}{3} + (q-2) + \frac{2}{3}(q-2) = 2q-3 \quad \text{if } m \text{ is odd,} \\ |\mathcal{A}_2/G| &= \frac{\{\frac{1}{3}(q-1)(q+1) - \frac{2}{3}(q-1)\}q \cdot 3}{(q-1)q} \\ &\quad + \frac{\{\frac{1}{2}(q-1)q\}q \cdot 6}{(q-1)q} + \frac{\{\frac{1}{6}(q-2)(q-1) - \frac{1}{3}(q-1)\}q \cdot 12}{(q-1)q} \\ &= (q-1) + 3q + (2q-8) = 6q-9 \quad \text{if } m \text{ is even.} \end{aligned}$$

□

We inserted the intermediate calculations because we need similar computations in following propositions and it is helpful when we try to find representatives of isomorphism classes in each type. Similar computation as in the proof of Proposition 3.4 gives:

Proposition 3.5. *The numbers of isomorphism classes of curves in $\mathcal{C}_2$ and in $\mathcal{C}_3$ are $(q-1)(2q-3)$ and $2(q-1)$, respectively.*

Proof. We divide $\mathcal{C}_2$ as we have done for $\mathcal{A}_2$. For $\mathcal{C}_3$, we divide it into two subsets according that c_9 is a cube or not. Then Lemma 3.3 gives the answer. For even m, we get $\frac{4}{3}(q-1)$ isomorphism classes if c_9 is a cube and $\frac{2}{3}(q-1)$ isomorphism classes if c_9 is not a cube. □

Lemma 3.6. *Let F be a finite field of order 2^m and let $h(x) = x^4 + bx$, $b \neq 0$.*

(1) *If b is not a cube, then x^4+bx+c has only one zero in F for any $c \in F$.* ([7, Theorem 3.83])

(2) *If b is a non-zero cube in F, then either $x^4 + bx + c$ has no zeroes or it has 4 (2, resp.) distinct zeroes if m is even (m is odd, resp.). Moreover it has 4 (or 2, resp.) distinct zeroes if and only if $c \in \mathrm{Im}\Psi_h$.*

(3) *Suppose $u^9 = 1$. Then $c \in \mathrm{Im}\Psi_h$ if and only if $u^3c \in \mathrm{Im}\Psi_h$ if and only if $u^6c \in \mathrm{Im}\Psi_h$.*

(4) *Suppose* $\mathrm{ord}(\alpha) = 9$*. Then $c \in Im\ \Psi_h$ if and only if $c(1 + \alpha^{3i}) \in \mathrm{Im}\Psi_h$ for $i = 1, 2$.*

Proof. Since Ψ_h is a homomorphism, the number $|\Psi_h^{-1}(c)|$ of zeroes of x^4+bx+c is equal to $|\operatorname{Ker}\Psi_h|$. (1) follows since $\operatorname{Ker}\Psi_h = \{0\}$ when b is not a cube. (2) Let $b = A^3$. Then $\operatorname{Ker}\Psi_h = \{0, A, A\rho, A\rho^2\}$ if m is even and $\operatorname{Ker}\Psi_h = \{0, A\}$ if m is odd. (3) follows from $u^3(\gamma^4 + b\gamma) = (u^3\gamma)^4 + b(u^3\gamma)$ and $c = u^3(u^3(u^3c))$. (4) Since $\alpha^3 \neq 1$, $\alpha^9 = 1$ implies $\alpha^6 + \alpha^3 + 1 = 0$. So, $\alpha^6c + \alpha^3c + c = 0$. Thus, $c + \alpha^3c = \alpha^6c$ or $c + \alpha^6c = \alpha^3c$. Now apply (3). □

Proposition 3.7. *The number of isomorphism classes of curves in $\mathcal{A}_3$ is*

$$\begin{cases} 2 \text{ if } m \text{ is odd,} \\ 6 \text{ if } m \equiv 2, 4 \pmod 6, \\ 12 \text{ if } m \equiv 0 \pmod 6. \end{cases}$$

Proof. If m is odd, $u^9 = 1$ implies $u = 1$. Since every element is a cube, we have $|G_{\mathcal{A}_3}| = 2$ and $|\mathcal{A}_3/G| = 2$.

If $m \equiv 2$ or $4 \pmod 6$, $u^9 = 1$ implies $u^3 = 1$. Then for $T \in \mathcal{A}_3$,

$$|G_T| = |\{(u,\gamma) \in F^* \times F \mid u^3 = 1,\ \gamma^4 + c_9\gamma = 0\}| = \begin{cases} 12 & \text{if } c_9 \text{ is a cube,} \\ 3 & \text{if } c_9 \text{ is not a cube.} \end{cases}$$

Therefore, $|\mathcal{A}_3/G| = 6$: two from curves where c_9 is not a cube, two from curves where c_9 is a cube. In fact, if c_9 is not a cube, then $y^3 = x^4 + c_9x + c_{12}$ is isomorphic either $y^3 = x^4 + \rho x$ or $y^3 = x^4 + \rho^2 x$; if c_9 is a cube, isomorphic to $y^3 = x^4 + x + e_i$ for some e_i in Theorem 2.4.

Now assume that $m \equiv 0 \pmod 6$. Write $\{u \in F \mid u^9 = 1\} = \langle\alpha\rangle$. Then the isotropy group G_T of $T \in \mathcal{A}_3$ is

$$\begin{aligned} G_T &= \{(u,\gamma) \in F^* \times F \mid\ u^9 = 1,\ \gamma^4 + c_9\gamma + c_{12}(1 + u^3)\} \\ &= \{(u,\gamma) \in F^* \times F \mid\ u = 1, \alpha^3, \alpha^6,\ \gamma^4 + c_9\gamma = 0\} \end{aligned}$$

$$\cup \{(u, \gamma) \in F^* \times F \mid \ u = \alpha^j \text{ with } j \not\equiv 0 \pmod 3, \\ \gamma^4 + c_9\gamma + c_{12}(1 + \alpha^{3j}) = 0\}.$$

Now the number of zeroes in the equations in G_T for $T \in \mathcal{A}_3$ depends on whether c_9 is cubic and $c_{12} \in \mathrm{Im}\Psi_h$ or not, where $h(x) = x^4 + c_9x$ as in Lemma 3.6. Divide $\mathcal{A}_3$ into three subsets:

$$\mathcal{D}_1 = \{T \in \mathcal{A}_3 \mid c_9 : \text{non-cubic}\}, \quad |\mathcal{D}_1| = \frac{2(q-1)q}{3};$$

$$\mathcal{D}_2 = \{T \in \mathcal{A}_3 \mid c_9 : \text{cubic}, \ c_{12} \in \mathrm{Im}\Psi_h\}, \quad |\mathcal{D}_2| = \frac{(q-1)q}{12};$$

$$\mathcal{D}_3 = \{T \in \mathcal{A}_3 \mid c_9 : \text{cubic}, \ c_{12} \notin \mathrm{Im}\Psi_h\}, \quad |\mathcal{D}_3| = \frac{(q-1)q}{4}.$$

Note that G acts on each $\mathcal{D}_i$ since $A_{u,\gamma} \cdot C : y^3 = x^4 + c_9x + (\gamma^4 + g^i\gamma + c_{12})/u^3$ due to Lemma 3.6. We also have $c_{12} \in \mathrm{Im}\Psi_h$ if and only if $c_{12}(1+u^3) \in \mathrm{Im}\Psi_h$. So,

$$|G_T| = \begin{cases} 9 & \text{if } \ T \in \mathcal{D}_1, \\ 36 & \text{if } \ T \in \mathcal{D}_2, \\ 12 & \text{if } \ T \in \mathcal{D}_3. \end{cases}$$

Therefore we get 6 isomorphism classes from $\mathcal{D}_1$, 3 from $\mathcal{D}_2$ and 3 from $\mathcal{D}_3$. □

Proof of Theorem 1.1. By combining all the results of Propositions 4.1-4.7, we prove Theorem 1.1. □

Proof of Corollary 1.2. It follows from that $\mathcal{A}_1 \cup \mathcal{A}_2 \cup \mathcal{A}_3$ consists of all Picard curves. □

We finally remark that the number of all isomorphic classes of $C_{3,4}$ curves in characteristic 2 other than F_2 as well as in other characteristic is still unknown.

Acknowledgement. The first author acknowledges the hospitality of KIAS during her visit in the year 2006.

References

[1] S. Arita, *Algorithms for computations in Jacobian group of C_{ab} curve and their application to discrete-log based public key cryptosystems*, IEICE Transactions **J82-A** (1999), no. 8, 1291–1299.

[2] Y. Choie and D. Yun, *Isomorphism classes of hyperelliptic curves of genus 2 over $\mathbb{F}_q$*, In: Information Security and Privacy, ACISP 2002. LNCS, vol. 2384, pp. 190–202, Springer, Heidelberg, 2002.

[3] I. H. Encinas, A. J. Menezes, and J. M. Masqué, *Isomorphism classes of genus-2 hyperelliptic curves over finite fields*, AAECC **13** (2002), 57–65.

[4] S. D. Galbraith, S. M. Paulus, and N. P. Smart, *Arithmetic on superelliptic curves*, Math. Comp. **71** (2002), no. 237, 393–405.

[5] N. Koblitz, *Hyperelliptic cryptosystems*, J. Cryptology **1** (1989), no. 3, 139–150.

[6] J. Lee, *Isomorphism classes of Picard curves over finite fields*, Appl. Algebra Engrg. Comm. Comput. **16** (2005), no. 1, 33–44.

[7] R. Lidl and H. Niederreiter, *Introduction to Finite Fields and Their Applications*, Revision of the 1986 first edition. Cambridge University Press, Cambridge, 1994.

[8] S. Miura, *Algebraic geometric codes on certain plane curves*, Trans. IEICE **J75-A** (1992), no. 11, 1735–1745.

[9] E. Nart and C. Ritzenthaler, *Non-hyperelliptic curves of genus three over finite fields of characteristic two*, J. Number Theory **116** (2006), no. 2, 443–473.

Pyung-Lyun Kang
Department of Mathematics
Chungnam National University
Daejeon 305-764, Korea
E-mail address: plkang@cnu.ac.kr

Sunmi Sun
Daejeon Gwanjeo High School
Gwanjeo-dong Seo-gu
Daejeon 301-243, Korea
E-mail address: ssm1096@hanmail.net