Commun. Korean Math. Soc. **28** (2013), No. 3, pp. 433–447
http://dx.doi.org/10.4134/CKMS.2013.28.3.433

THE NUMBER OF POINTS ON ELLIPTIC CURVES $y^2 = x^3 + Ax$ AND $y^2 = x^3 + B^3$ MOD 24

Wonju Jeon and Daeyeoul Kim

Abstract. In this paper, we calculate the number of points on elliptic curves $y^2 = x^3 + Ax$ over F_{p^r} modulo 24. This is a generalization of [8], [9] and [16].

1. Introduction

Let $p > 3$ be a prime, and let $\mathbb{F}_p$ be the finite field of p elements. From now on we let E_A^B denote the elliptic curve $y^2 = x^3 + Ax + B$ over $\mathbb{F}_p$ where $A, B \in \mathbb{F}_p$. The set of points $(x, y) \in \mathbb{F}_p \times \mathbb{F}_p$ together with a point O at infinity is called the set of points of E_A^B in $\mathbb{F}_p$ and is denoted by $E_A^B(\mathbb{F}_p)$. And let $\#E_A^B(\mathbb{F}_p)$ be the cardinality of the set $E_A^B(\mathbb{F}_p)$. For a more detailed information about elliptic curves in general, see [12]. It has been always interesting to look for the number of points over a given field $\mathbb{F}_p$. In [11], three algorithms to find the number of points on an elliptic curve over a finite field are given. Also in [3], [4] the number of rational points on Frey elliptic curves $E : y^2 = x^3 - n^2x$ and $E : y^2 = x^3 + a^3$ are found.

The purpose of this paper is to give a straightforward proof of the number of points mod 24 on elliptic curves over finite fields. One found the number of points on $E : y^2 = x^3 + Ax$ over $\mathbb{F}_p$ ([2], [3], [6], [8], [10]).

In 2003, H. Park, D. Kim and H. Lee, calculated the number of points on elliptic curves $E_A^0 : y^2 = x^3 + Ax$ over $\mathbb{F}_p$ mod 8 ([5], [8]). The purpose of this paper is to give a straightforward calculation of the number of points on elliptic curves over a finite fields mod 24.

Throughout the article we adopt the following notations:

- q_4: a quartic residue in F_p
- q_2: a quadratic residue but quartic non-residue in F_p
- q_1: a quadratic non-residue in F_p
- $p = a^2 + b^2$ with a odd and b even number in $\mathbb{Z}$

Received September 11, 2012.
2010 *Mathematics Subject Classification.* 11A07.
Key words and phrases. congruence, elliptic curve.

In this paper, without employing the advanced theory of elliptic curves, we compute the number of points mod 24 on elliptic curves. We prove the following:

Theorem 1.1. *Let $E_A^0 : y^2 = x^3 + Ax$ be an elliptic curve modulo p with $p > 3$, and $t \in \mathbb{Z}$ such that $3t^2 \equiv 1 \pmod{p}$.*

(1) *Let $p = a^2 + b^2 \equiv 1 \pmod{24}$ be a prime with $6 \mid b$. If $-1 + 2t = q_4$, then*

$$\#E_A^0(F_p) \equiv \begin{cases} 0 \pmod{24} & \text{if } A = q_4 \\ 4 \pmod{24} & \text{if } A = q_2 \\ 2 \pmod{24} & \text{if } A = q_1, \end{cases}$$

and if $-1 + 2t = q_2$, then

$$\#E_A^0(F_p) \equiv \begin{cases} 16 \pmod{24} & \text{if } A = q_4 \\ 12 \pmod{24} & \text{if } A = q_2 \\ 2 \pmod{24} & \text{if } A = q_1. \end{cases}$$

(2) *If $p = a^2 + b^2 \equiv 1 \pmod{24}$ is a prime with $2 \mid b$ and $3 \nmid b$, then*

$$\#E_A^0(F_p) \equiv \begin{cases} 8 \pmod{24} & \text{if } A = q_4 \\ 20 \pmod{24} & \text{if } A = q_2 \\ 18 \pmod{24} & \text{if } A = q_1 \\ 10 \pmod{24} & \text{if } A = q_1'. \end{cases}$$

(3) *Let $p = a^2 + b^2 \equiv 13 \pmod{24}$ be a prime with $6 \mid b$. If $-1 + 2t = q_4$, then*

$$\#E_A^0(F_p) \equiv \begin{cases} 12 \pmod{24} & \text{if } A = q_4 \\ 16 \pmod{24} & \text{if } A = q_2 \\ 2 \pmod{24} & \text{if } A = q_1, \end{cases}$$

and if $-1 + 2t = q_2$, then

$$\#E_A^0(F_p) \equiv \begin{cases} 4 \pmod{24} & \text{if } A = q_4 \\ 0 \pmod{24} & \text{if } A = q_2 \\ 2 \pmod{24} & \text{if } A = q_1. \end{cases}$$

(4) *If $p = a^2 + b^2 \equiv 13 \pmod{24}$ is a prime with $2 \mid b$ and $3 \nmid b$, then*

$$\#E_A^0(F_p) \equiv \begin{cases} 20 \pmod{24} & \text{if } A = q_4 \\ 8 \pmod{24} & \text{if } A = q_2 \\ 10 \pmod{24} & \text{if } A(-1 + 2t) = q_2 \\ 18 \pmod{24} & \text{if } A(-1 + 2t) = q_4. \end{cases}$$

(5) *If $p \equiv 5 \pmod{24}$ is a prime, then*

$$\#E_A^0(F_p) \equiv \begin{cases} 4 \pmod{24} & \text{if } A = q_4 \\ 8 \pmod{24} & \text{if } A = q_2 \\ 2 \pmod{24} & \text{if } A = q_1 \\ 10 \pmod{24} & \text{if } A = q_1' \end{cases}$$

or

$$\#E_A^0(F_p) \equiv \begin{cases} 20 \pmod{24} & \text{if } A = q_4 \\ 16 \pmod{24} & \text{if } A = q_2 \\ 2 \pmod{24} & \text{if } A = q_1 \\ 10 \pmod{24} & \text{if } A = q_1'. \end{cases}$$

(6) *If* $p \equiv 17 \pmod{24}$ *is a prime, then*

$$\#E_A^0(F_p) \equiv \begin{cases} 8 \pmod{24} & \text{if } A = q_4 \\ 4 \pmod{24} & \text{if } A = q_2 \\ 2 \pmod{24} & \text{if } A = q_1 \\ 10 \pmod{24} & \text{if } A = q_1' \end{cases}$$

or

$$\#E_A^0(F_p) \equiv \begin{cases} 16 \pmod{24} & \text{if } A = q_4 \\ 20 \pmod{24} & \text{if } A = q_2 \\ 2 \pmod{24} & \text{if } A = q_1 \\ 10 \pmod{24} & \text{if } A = q_1'. \end{cases}$$

2. Elliptic curves over finite fields

We denote E_a^b be an elliptic curve $y^2 = x^3 + ax + b$ over F_p where $a, b \in F_p$. The elliptic curves $E_a^b/F_p : y^2 = x^3 + ax + b$ and $E_{a'}^{b'}/F_p : y^2 = x^3 + a'x + b'$ are isomorphic over F_p if and only if there exists $u \in F_p^*$ such that $u^4a' = a$ and $u^6b' = b$ ([12]). If $E_a^b \cong E_{a'}^{b'}$ over F_p, then the isomorphism is given by

$$\phi : E_a^b \to E_{a'}^{b'}, \quad \phi : (x, y) \mapsto (u^{-2}x, u^{-3}y), \tag{2.1}$$

or equivalently,

$$\psi : E_{a'}^{b'} \to E_a^b, \quad \psi : (x, y) \mapsto (u^2x, u^3y).$$

Using (2.1), we get the following proposition.

Proposition 2.1. (1) *Let* $B = \{E_0^b : y^2 = x^3 + b,\ 1 \le b \le p-1\}$. *If* $p \equiv 1 \pmod 6$ *is prime, then there are six isomorphism classes of elliptic curves in* B, *i.e.,* E_0^1, E_0^g, $E_0^{g^2}$, $E_0^{g^3}$, $E_0^{g^4}$ *and* $E_0^{g^5}$.

(2) *Let* $B = \{E_a^0 : y^2 = x^3 + ax,\ 1 \le a \le p-1\}$. *If* $p \equiv 1 \pmod 4$ *is prime, then there are four isomorphism classes of elliptic curves in* B, *i.e.,* E_0^1, E_0^g, $E_0^{g^2}$, $E_0^{g^3} : y^2 = x^3 + g^3$.

A twist of a curve given in short Weierstrass form E_a^b is given by $E_{a'}^{b'}$ where $a' = v^2a$, $b' = v^3b$ for some quadratic non-residue $v \in F_p$. Let $p > 3$ be a prime, and let F_p be the finite field of p elements. The set of points $(x, y) \in F_p \times F_p$ together with a point O at infinity is called the set of F_p-rational points of E_a^b on F_p and is denoted by $E_a^b(F_p)$. The cardinality of the set $E_a^b(F_p)$ is denoted by $\#E_a^b(F_p)$.

Proposition 2.2 ([1], p. 153)**.** *Suppose* E *and* E' *have the same* j*-invariant but are not isomorphic over the field* F_p. *If* $j \neq 0$ *and* $j \neq 1728$, *then* E' *is the quadratic twist of* E, *and if* $\#E(F_p) = p + 1 - v$, *then* $\#E'(F_p) = p + 1 + v$.

Proposition 2.3 ([3], Theorem 9)**.** *Let $p \equiv 1 \pmod 6$ be prime. Then*

$$\sum_{a=1}^{p-1} \#E_0^{a^3}(F_p) = p^2 - 1.$$

Using the theory of a quadratic twist of elliptic curve (Proposition 2.2), we can reprove Proposition 2.3 and similar results on $E_a^0(F_p)$.

Theorem 2.4. *Let $p > 3$ be a prime. Then the followings are satisfied.*

(1) $\displaystyle\sum_{a=1}^{p-1} \#E_0^{a}(F_p) = \sum_{a=1}^{p-1} \#E_0^{a^3}(F_p) = p^2 - 1.$

(2) $\displaystyle\sum_{a=1}^{p-1} \#E_a^{0}(F_p) = \sum_{a=1}^{p-1} \#E_{a^2}^{0}(F_p) = p^2 - 1.$

Proof. (1) Let g be a primitive root of p. Then, $\{1, 2, \ldots, p-1\} = \{g^k \mid 1 \le k \le p-1\}$ and

$$\begin{aligned}\sum_{a=1}^{p-1} \#E_0^{a}(F_p) &= \sum_{k=1}^{p-1} \#E_0^{g^k}(F_p) \\ &= \frac{1}{2}\sum_{k=1}^{p-1} \left(\#E_0^{g^k(F_p)} + \#E_0^{g^{k+3}}(F_p)\right).\end{aligned}$$

Since $E_0^{u^3 g^k} : y^2 = x^3 + u^3 g^k$ is the quadratic twist of $E_0^{g^k} : y^2 = x^3 + g^k$ for a quadratic non-residue $u = g$, $\#E_0^{g^k}(F_p) + \#E_0^{g^{k+3}}(F_p) = (p+1-v)+(p+1+v) = 2(p+1)$. Therefore,

$$\begin{aligned}\sum_{a=1}^{p-1} \#E_0^{a}(F_p) &= \frac{1}{2}\sum_{k=1}^{p-1} \left(\#E_0^{g^k}(F_p) + \#E_0^{g^{k+3}}(F_p)\right) \frac{p-1}{2} \cdot 2 \cdot (p+1) \\ &= p^2 - 1.\end{aligned}$$

Likewise, $\{1^3, 2^3, \ldots, (p-1)^3\} = \{g^{3k} \mid 1 \le k \le p-1\}$ and

$$\begin{aligned}\sum_{a=1}^{p-1} \#E_0^{a^3}(F_p) &= \sum_{k=1}^{p-1} \#E_0^{g^{3k}}(F_p) \\ &= \frac{1}{2}\sum_{k=1}^{p-1} \left(\#E_0^{g^{3k}}(F_p) + \#E_0^{g^{3(k+1)}}(F_p)\right).\end{aligned}$$

Since $E_0^{u^3 g^{3k}} : y^2 = x^3 + u^3 g^{3k}$ is the quadratic twist of $E_0^{g^{3k}} : y^2 = x^3 + g^{3k}$ for a quadratic non-residue $u = g$, $\#E_0^{g^{3k}}(F_p) + \#E_0^{g^{3k+3}}(F_p) = 2(p+1)$ by Proposition 2.2. Therefore,

$$\sum_{a=1}^{p-1} \#E_0^{a^3}(F_p) = \frac{1}{2}\sum_{k=1}^{p-1} \left(\#E_0^{g^{3k}}(F_p) + \#E_0^{g^{3k+3}}(F_p)\right)$$

$$= \frac{p-1}{2} \cdot 2 \cdot (p+1) = p^2 - 1.$$

(2) Let g be a primitive root of p. Then, $\{1, 2, \ldots, p-1\} = \{g^k \mid 1 \leq k \leq p-1\}$ and

$$\sum_{a=1}^{p-1} \#E_a^0(F_p) = \sum_{k=1}^{p-1} \#E_{g^k}^0(F_p) = \frac{1}{2} \sum_{k=1}^{p-1} \left(\#E_{g^k}^0(F_p) + \#E_{g^{k+2}}^0(F_p) \right).$$

Since $E_{u^2 g^k}^0 : y^2 = x^3 + u^2 g^k x$ is the quadratic twist of $E_{g^k}^0 : y^2 = x^3 + g^k x$ for a quadratic non-residue $u = g$, $\#E_{g^k}^0(F_p) + \#E_{g^{k+2}}^0(F_p) = (p+1-v)+(p+1+v) = 2(p+1)$ by Proposition 2.2. Therefore,

$$\begin{aligned} \sum_{a=1}^{p-1} \#E_a^0(F_p) &= \frac{1}{2} \sum_{k=1}^{p-1} \left(\#E_{g^k}^0(F_p) + \#E_{g^{k+2}}^0(F_p) \right) \\ &= \frac{p-1}{2} \cdot 2 \cdot (p+1) = p^2 - 1. \end{aligned}$$

Likewise, $\{1^2, 2^2, \ldots, (p-1)^2\} = \{g^{2k} \mid 1 \leq k \leq p-1\}$ and

$$\begin{aligned} \sum_{a=1}^{p-1} \#E_{a^2}^0(F_p) &= \sum_{k=1}^{p-1} \#E_{g^{2k}}^0(F_p) \\ &= \frac{1}{2} \sum_{k=1}^{p-1} \left(\#E_{g^{2k}}^0(F_p) + \#E_{g^{2(k+1)}}^0(F_p) \right). \end{aligned}$$

Since $E_{u^2 g^{2k}}^0 : y^2 = x^3 + u^2 g^{2k} x$ is the quadratic twist of $E_{g^{2k}}^0 : y^2 = x^3 + g^{2k}$ for a quadratic non-residue $u = g$, $\#E_{g^{2k}}^0(F_p) + \#E_{g^{2k+2}}^0(F_p) = 2(p+1)$ by Proposition 2.2. Therefore,

$$\begin{aligned} \sum_{a=1}^{p-1} \#E_{a^2}^0(F_p) &= \frac{1}{2} \sum_{k=1}^{p-1} \left(\#E_{g^{2k}}^0(F_p) + \#E_{g^{2k+2}}^0(F_p) \right) \\ &= \frac{p-1}{2} \cdot 2 \cdot (p+1) = p^2 - 1. \end{aligned}$$

□

In the nineteenth century Dirichlet (see [14]) showed:

Proposition 2.5 ([13])**.** *Let p and q be distinct primes such that $p \equiv 1 \pmod 4$, $p = a^2 + b^2$, $2 \mid b$, and let $q^* = (-1)^{(q-1)/2} q$. Then q^* is a quartic residue of p if and only if there is an integer m such that $m^2 \equiv p \pmod q$ and $\left(\frac{m(m+b)}{q}\right) = 1$.*

In [9], we considered the following:

Let $p \equiv 1 \pmod{12}$ be a prime and let $3t^2 \equiv 1 \pmod p$ with $t \in \mathbb{F}_p^*$. Then $\#E_A^0 : y^2 = x^3 + Ax \equiv 0 \pmod 3$ if and only if $-A \pm 2tA$ are quartic residues in $\mathbb{F}_p$.

Using this property, the quadratic reciprocity law and elementary several calculations, we calculated the number of rational points mod 12 on elliptic curve over finite fields according to the case by case. We wrote the following theorem.

Proposition 2.6 ([9], [16]). *Let p be a rational prime, and let t be an element of $F_p^* = F_p - \{0\}$ such that $3t^2 \equiv 1 \pmod{p}$.*

(1) *If $p \equiv 1, 11 \pmod{12}$ is a prime and $3t^2 \equiv 1 \pmod{p}$, then we get the following table.*

p	A	$-1 \pm 2t$	$A(-1 \pm 2t)$	$\#E_A^0(\mathbb{F}_p)$
1 (mod 24)	q_4	q_4	q_4	0 (mod 24)
	q_4	q_2	q_2	8 *or* 16 (mod 24)
	q_4	q_1	q_1	8 *or* 16 (mod 24)
	q_2	q_2	q_4	12 (mod 24)
	q_2	q_4	q_2	4 *or* 20 (mod 24)
	q_2	q_1	q_1	4 *or* 20 (mod 24)
	q_1	q_1	q_4	18 (mod 24)
	q_1	q_1	q_2	2 *or* 10 (mod 24)
	q_1	q_4	q_1	2 *or* 10 (mod 24)
	q_1	q_2	q_1	2 *or* 10 (mod 24)
11 (mod 24)			*all*	12 (mod 24)
13 (mod 24)	q_4	q_4	q_4	12 (mod 24)
	q_4	q_2	q_2	4 *or* 20 (mod 24)
	q_4	q_1	q_1	4 *or* 20 (mod 24)
	q_2	q_2	q_4	0 (mod 24)
	q_2	q_4	q_2	8 *or* 16 (mod 24)
	q_2	q_1	q_1	8 *or* 16 (mod 24)
	q_1	q_1	q_4	18 (mod 24)
	q_1	q_1	q_2	2 *or* 10 (mod 24)
	q_1	q_4	q_1	2 *or* 10 (mod 24)
	q_1	q_2	q_1	2 *or* 10 (mod 24)
23 (mod 24)			*all*	0 (mod 24)

(2) *If $p \equiv 5, 7 \pmod{12}$ is a prime, then we get the following table.*

p	A	$\#E_A^0(\mathbb{F}_p)$
5 (mod 24)	q_4	4 *or* 20 (mod 24)
	q_2	8 *or* 16 (mod 24)
	q_1	2 *or* 10 (mod 24)
7 (mod 24)	*all*	8 (mod 24)
17 (mod 24)	q_4	8 *or* 16 (mod 24)
	q_2	4 *or* 20 (mod 24)
	q_1	2 *or* 10 (mod 24)
19 (mod 24)	*all*	20 (mod 24)

(3) *Let $p > 3$ be an odd prime. Then we get the following table.*

p	$(\frac{B}{p})$	$(\frac{3B(2t-1)}{p})$	$\#E_0^{B^3}(\mathbb{F}_p)$
$1 \pmod{12}$	1	1	$0 \pmod{24}$
	1	-1	$12 \pmod{24}$
	-1	1	8 *or* $16 \pmod{24}$
	-1	-1	4 *or* $20 \pmod{24}$
$5 \pmod{12}$	1 *or* -1		$6 \pmod{12}$
$7 \pmod{12}$	1		$12 \pmod{24}$
	-1		4 *or* $20 \pmod{24}$
$11 \pmod{12}$	1 *or* -1	1 *or* -1	$0 \pmod{12}$

In this proposition, we found a relation between a quadratic equation and a family of elliptic curves over a finite field. Let $p \equiv 1 \pmod{12}$ be a prime and let $3t^2 \equiv 1 \pmod{p}$ with $t \in F_p^*$. Then $\#E_A^0 : y^2 = x^3 + Ax \equiv 0 \pmod{3}$ if and only if $-A \pm 2tA$ are quartic residues in F_p ([9]). Under this condition, we obtain a following motivation:

Given a quadratic equation $At^2 + Bt + C \equiv 0 \pmod{p}$ and $E_{f(k)}^{g(k)} : y^2 = x^3 + g(k)x + f(k)$.

(1) Can one find $f(k)$ and $g(k)$ satisfying $\#E_{f(k)}^{g(k)}(F_p) \equiv \alpha \pmod{n}$ for a fixed n and for almost all primes p?
Moreover, we may consider partial conditions for some primes, for example $p \equiv 1 \pmod{4}$.

(2) Can one classify $f(k)$ and $g(k)$ satisfying $\#E(F_p) \equiv \alpha \pmod{n}$ for a fixed n in F_p?

We think that this sort of problems do not seem to be easy to handle in general. In this paper, we consider the case $A = 3$, $B = 0$ and $C = -1$.

3. The number of solutions for elliptic curves with $3t^2 \equiv 1 \pmod{p}$

Using Proposition 2.2, we obtain the proof of Theorem 1.1.

Proof. Note that $(\frac{3}{p}) = 1$ if and only if $p \equiv 1, 11 \pmod{12}$ by Proposition 2.5. Put $3^* = (-1)^{\frac{3-1}{2}} \cdot 3 = -3$ in Proposition 2.5. Then -3 is a quartic residue modulo p if and only if $m^2 \equiv p \pmod{3}$ and $(\frac{m(m+b)}{3}) = 1$. Thus we derive that -3 is a quartic residue modulo $p = a^2 + b^2$ with $6 \mid b$. If $p \equiv 1 \pmod{24}$, then -3 is a quartic residue modulo p if and only if $3 = q_4$. If $p = a^2 + b^2$ is a prime with $6 \mid b$, then $(\frac{t}{p}) = 1$. This leads us to the fact that

$$\left(\frac{3t-2}{p}\right)\left(\frac{t}{p}\right) = \left(\frac{3t^2-2t}{p}\right) = \left(\frac{2t-1}{p}\right)\left(\frac{-1}{p}\right) = 1.$$

So, we consider $2t - 1 = q_4$ or q_2. In the case of $-1 + 2t = q_4$, we find that $\#E_{q_4}^0(F_p) + \#E_{q_2}^0(F_p) \equiv 2p + 2 \equiv 2 + 2 \equiv 0 + 4 \pmod{24}$ and $\#E_{q_4}^0(F_p) + \#E_{q_2}^0(F_p) \equiv 2p+2 \equiv 2+2 \equiv 0+4 \pmod{24}$ by Proposition 2.2 and Proposition 2.6. Hence $\#E_{q_2}^0(F_p) \equiv 4 \pmod{24}$.

Let $-1+2t=q_2$. By Proposition 2.6, $\#E^0_{q_1}(F_p)\equiv 2$ or $10 \pmod{24}$. We can derive that $\#E^0_{q_1}(F_p)+\#E^0_{q_1'}(F_p)\equiv 2p+2\equiv 2+2\equiv 2+2 \pmod{24}$. So, this case, $\#E^0_{q_1}(F_p)\equiv 2 \pmod{24}$. Other cases are similar. □

Theorem 3.1. *Let $E_0^{B^3}: y^2=x^3+B^3$ be an elliptic curve modulo p with $p\equiv 1 \pmod 6$, and $t\in\mathbb{Z}$ such that $3t^2\equiv 1 \pmod p$.*

(1) *Let $p=a^2+b^2\equiv 1 \pmod{12}$ be a prime with $6\mid b$. Then*

$$\#E_0^{B^3}(F_p)\equiv\begin{cases} 0 \pmod{24} & \text{if } \left(\frac{B}{p}\right)=1\\ 4 \pmod{24} & \text{if } \left(\frac{B}{p}\right)=-1.\end{cases}$$

(2) *If $p=a^2+b^2\equiv 1 \pmod{12}$ is a prime with $2\mid b$ and $3\nmid b$, then*

$$\#E_0^{B^3}(F_p)\equiv\begin{cases} 12 \pmod{24} & \text{if } \left(\frac{B}{p}\right)=1\\ 16 \pmod{24} & \text{if } \left(\frac{B}{p}\right)=-1.\end{cases}$$

(3) *If $p\equiv 7 \pmod{12}$ is a prime, then*

$$\#E_0^{B^3}(F_p)\equiv\begin{cases} 12 \pmod{24} & \text{if } \left(\frac{B}{p}\right)=1\\ 4 \pmod{24} & \text{if } \left(\frac{B}{p}\right)=-1.\end{cases}$$

Proof. It is well-known that $(t+1)^2=t^2+2t+1=\frac{2}{3}(3t+2)$ and $(t-1)^2=-\frac{2}{3}(3t-2)$. Thus, we have

$$\left(\tfrac{3t+2}{p}\right)=\left(\tfrac{3t-2}{p}\right)=1,\ \text{if}\ \ p\equiv 1 \pmod{24}, \tag{3.1}$$

$$\left(\tfrac{3t+2}{p}\right)=\left(\tfrac{3t-2}{p}\right)=-1,\ \text{if}\ \ p\equiv 13 \pmod{24}, \tag{3.2}$$

$$\left(\tfrac{3t+2}{p}\right)=-1,\ \left(\tfrac{3t-2}{p}\right)=1,\ \text{if}\ \ p\equiv 11 \pmod{24}, \tag{3.3}$$

$$\left(\tfrac{3t+2}{p}\right)=1,\ \left(\tfrac{3t-2}{p}\right)=-1,\ \text{if}\ \ p\equiv 23 \pmod{24}. \tag{3.4}$$

On the other hand, we readily check that

$$t(2t-1)\equiv -\frac{1}{3}(3t-2) \pmod p \text{ and } t(2t+1)\equiv\frac{1}{3}(3t+2) \pmod p. \tag{3.5}$$

If $p=a^2+b^2\equiv 1 \pmod{24}$ with $6\mid b$, -3 is a quartic residue modulo p by Proposition 2.5. By (3.1) and (3.5), we derive that

$$\left(\frac{t}{p}\right)=\left(\frac{2t-1}{p}\right)=\left(\frac{2t+1}{p}\right)=1.$$

Put $(\frac{B}{p})=1$. Then, we derive from Proposition 2.6 and Proposition 2.2 that $\#E_0^{B^3}\equiv 0 \pmod{24}$, $\#E_0^{B^3}+\#E_0^{g^3}=2p+2\equiv 4 \pmod{24}$ and $\#E_0^{g^3}\equiv 4 \pmod{24}$. Other results are similar. □

The zeta function of a curve C is defined to be the exponential generating function

$$Z(C,T) = \exp\left(\sum_{k\geq 1} N_k \frac{T^k}{k}\right),$$

where N_k equals the number of points on C over F_{p^k}. A result due to Weil [15] is that the zeta function of an elliptic curve, in fact any curve, $Z(C,T)$ is rational, and moreover can be expressed as

$$Z(C,T) = \frac{(1-\alpha T)(1-\beta T)}{(1-T)(1-qT)} = \frac{1-(\alpha+\beta)T+\alpha\beta T^2}{(1-T)(1-qT)}.$$

The inverse roots α and β satisfy a functional equation which reduces to $\alpha\beta = p$ in the elliptic curve case. The value $v = \alpha + \beta$ is related to $N_1 = p + 1 - v$. In addition, the discriminant of the quadratic polynomial in the numerator is negative, and so the quadratic has two conjugate roots $\frac{1}{\alpha}$ and $\frac{1}{\beta}$ with absolute value $\frac{1}{\sqrt{p}}$. Writing the numerator in the form $1 - vT + pT^2 = (1-\alpha T)(1-\beta T)$ and taking the derivatives of logarithms of both sides, one can obtain the number of F_{p^k}-points on E, denoted by N_k, as follows:

$$N_k = p^k + 1 - \alpha^k - \beta^k, \quad k = 1, 2, \ldots. \tag{3.6}$$

All the results concerning the number of points on $F_p \pmod{24}$ obtained here for prime $p > 3$ can be generalized to F_{p^k}, for a natural number $k > 1$, using (3.6) and Theorem 1.1, Theorem 3.1.

Theorem 3.2. *Let $E_A^0 : y^2 = x^3 + Ax$ be an elliptic curve modulo p with $p > 3$, and l and $t \in \mathbb{Z}$ such that $3t^2 \equiv 1 \pmod{p}$ and let q_1' be a quadratic non-residue modulo p with $q_1' q_1 = q_4$.*

(1) *Let $p = a^2 + b^2 \equiv 1 \pmod{24}$ be a prime with $6 \mid b$. If $-1 + 2t = q_4$, then*

$$\#E_A^0(F_{p^r}) \equiv \begin{cases} 0 \pmod{24} & \text{if } A = q_4 \\ 4 \pmod{24} & \text{if } A = q_2 \text{ and } r \equiv 1 \pmod{2} \\ 0 \pmod{24} & \text{if } A = q_2 \text{ and } r \equiv 0 \pmod{2} \\ 2 \pmod{24} & \text{if } A = q_1 \text{ and } r \equiv 1 \pmod{2} \\ 4 \pmod{24} & \text{if } A = q_1 \text{ and } r \equiv 2 \pmod{4} \\ 0 \pmod{24} & \text{if } A = q_1 \text{ and } r \equiv 0 \pmod{4} \end{cases}$$

and if $-1 + 2t = q_2$, then

$$\#E_A^0(F_{p^r}) \equiv \begin{cases} 16 \pmod{24} & \text{if } A = q_4 \text{ and } r \equiv 1 \pmod{2} \\ 0 \pmod{24} & \text{if } A = q_4 \text{ and } r \equiv 0 \pmod{2} \\ 12 \pmod{24} & \text{if } A = q_2 \text{ and } r \equiv 1 \pmod{2} \\ 0 \pmod{24} & \text{if } A = q_2 \text{ and } r \equiv 0 \pmod{2} \\ 2 \pmod{24} & \text{if } A = q_1 \text{ and } r \equiv 1 \pmod{2} \\ 4 \pmod{24} & \text{if } A = q_1 \text{ and } r \equiv 2 \pmod{4} \\ 0 \pmod{24} & \text{if } A = q_1 \text{ and } r \equiv 0 \pmod{4}. \end{cases}$$

(2) *If* $p = a^2 + b^2 \equiv 1 \pmod{24}$ *is a prime with* $2 \mid b$ *and* $3 \nmid b$, *then*

$$\#E_A^0(F_{p^r}) \equiv \begin{cases} 8 \pmod{24} & \text{if } A = q_4 \text{ and } r \equiv 1 \pmod 2 \\ 16 \pmod{24} & \text{if } A = q_4 \text{ and } r \equiv 2 \pmod 4 \\ 0 \pmod{24} & \text{if } A = q_4 \text{ and } r \equiv 0 \pmod 4 \\ 20 \pmod{24} & \text{if } A = q_2 \text{ and } r \equiv 1 \pmod 2 \\ 16 \pmod{24} & \text{if } A = q_2 \text{ and } r \equiv 2 \pmod 4 \\ 0 \pmod{24} & \text{if } A = q_2 \text{ and } r \equiv 0 \pmod 4 \\ 18 \pmod{24} & \text{if } A = q_1 \text{ and } r \equiv 1 \pmod 2 \\ 12 \pmod{24} & \text{if } A = q_1 \text{ and } r \equiv 2 \pmod 4 \\ 0 \pmod{24} & \text{if } A = q_1 \text{ and } r \equiv 0 \pmod 4 \\ 10 \pmod{24} & \text{if } A = q_1' \text{ and } r \equiv 1 \pmod 2 \\ 12 \pmod{24} & \text{if } A = q_1' \text{ and } r \equiv 2 \pmod 4 \\ 0 \pmod{24} & \text{if } A = q_1' \text{ and } r \equiv 0 \pmod 4. \end{cases}$$

(3) *Let* $p = a^2 + b^2 \equiv 13 \pmod{24}$ *be a prime with* $6 \mid b$. *If* $-1 + 2t = q_4$, *then*

$$\#E_A^0(F_{p^r}) \equiv \begin{cases} 12 \pmod{24} & \text{if } A = q_4 \text{ and } r \equiv 1 \pmod 2 \\ 0 \pmod{24} & \text{if } A = q_4 \text{ and } r \equiv 0 \pmod 2 \\ 16 \pmod{24} & \text{if } A = q_2 \text{ and } r \equiv 1 \pmod 2 \\ 0 \pmod{24} & \text{if } A = q_2 \text{ and } r \equiv 0 \pmod 2 \\ 2 \pmod{24} & \text{if } A = q_1 \text{ and } r \equiv 1 \pmod 2 \\ 4 \pmod{24} & \text{if } A = q_1 \text{ and } r \equiv 2 \pmod 4 \\ 0 \pmod{24} & \text{if } A = q_1 \text{ and } r \equiv 0 \pmod 4 \end{cases}$$

and if $-1 + 2t = q_2$, *then*

$$\#E_A^0(F_{p^r}) \equiv \begin{cases} 4 \pmod{24} & \text{if } A = q_4 \text{ and } r \equiv 1 \pmod 2 \\ 0 \pmod{24} & \text{if } A = q_4 \text{ and } r \equiv 0 \pmod 2 \\ 0 \pmod{24} & \text{if } A = q_2 \\ 2 \pmod{24} & \text{if } A = q_1 \text{ and } r \equiv 1 \pmod 2 \\ 4 \pmod{24} & \text{if } A = q_1 \text{ and } r \equiv 2 \pmod 4 \\ 0 \pmod{24} & \text{if } A = q_1 \text{ and } r \equiv 0 \pmod 4. \end{cases}$$

(4) *If* $p = a^2 + b^2 \equiv 13 \pmod{24}$ *is a prime with* $2 \mid b$ *and* $3 \nmid b$, *then*

$$\#E_A^0(F_{p^r}) \equiv \begin{cases} 20 \pmod{24} & \text{if } A = q_4 \text{ and } r \equiv 1 \pmod 2 \\ 16 \pmod{24} & \text{if } A = q_4 \text{ and } r \equiv 2 \pmod 4 \\ 0 \pmod{24} & \text{if } A = q_4 \text{ and } r \equiv 0 \pmod 4 \\ 8 \pmod{24} & \text{if } A = q_2 \text{ and } r \equiv 1 \pmod 2 \\ 16 \pmod{24} & \text{if } A = q_2 \text{ and } r \equiv 2 \pmod 4 \\ 0 \pmod{24} & \text{if } A = q_2 \text{ and } r \equiv 0 \pmod 4 \\ 10 \pmod{24} & \text{if } A(-1+2t) = q_2 \text{ and } r \equiv 1 \pmod 2 \\ 12 \pmod{24} & \text{if } A(-1+2t) = q_2 \text{ and } r \equiv 2 \pmod 4 \\ 0 \pmod{24} & \text{if } A(-1+2t) = q_2 \text{ and } r \equiv 0 \pmod 4 \\ 18 \pmod{24} & \text{if } A(-1+2t) = q_4 \text{ and } r \equiv 1 \pmod 2 \\ 12 \pmod{24} & \text{if } A(-1+2t) = q_4 \text{ and } r \equiv 2 \pmod 4 \\ 0 \pmod{24} & \text{if } A(-1+2t) = q_4 \text{ and } r \equiv 0 \pmod 4. \end{cases}$$

(5) *If* $p \equiv 5 \pmod{24}$ *is a prime, then*

$$\#E_A^0(F_{p^r}) \equiv \begin{cases} 4 \pmod{24} & \text{if } A = q_4 \text{ and } r \equiv 1,3 \pmod 8 \\ 8 \pmod{24} & \text{if } A = q_4 \text{ and } r \equiv 2,6 \pmod 8 \\ 16 \pmod{24} & \text{if } A = q_4 \text{ and } r \equiv 4 \pmod 8 \\ 20 \pmod{24} & \text{if } A = q_4 \text{ and } r \equiv 5,7 \pmod 8 \\ 0 \pmod{24} & \text{if } A = q_4 \text{ and } r \equiv 0 \pmod 8 \\ 8 \pmod{24} & \text{if } A = q_2 \text{ and } r \equiv 1,2,3,6 \pmod 8 \\ 16 \pmod{24} & \text{if } A = q_2 \text{ and } r \equiv 4,5,7 \pmod 8 \\ 0 \pmod{24} & \text{if } A = q_2 \text{ and } r \equiv 0 \pmod 8 \\ 2 \pmod{24} & \text{if } A = q_1 \text{ and } r \equiv 1,3 \pmod 8 \\ 20 \pmod{24} & \text{if } A = q_1 \text{ and } r \equiv 2,6 \pmod 8 \\ 16 \pmod{24} & \text{if } A = q_1 \text{ and } r \equiv 4 \pmod 8 \\ 10 \pmod{24} & \text{if } A = q_1 \text{ and } r \equiv 5,7 \pmod 8 \\ 0 \pmod{24} & \text{if } A = q_1 \text{ and } r \equiv 0 \pmod 8 \\ 10 \pmod{24} & \text{if } A = q_1' \text{ and } r \equiv 1,3 \pmod 8 \\ 20 \pmod{24} & \text{if } A = q_1' \text{ and } r \equiv 2,6 \pmod 8 \\ 16 \pmod{24} & \text{if } A = q_1' \text{ and } r \equiv 4 \pmod 8 \\ 2 \pmod{24} & \text{if } A = q_1' \text{ and } r \equiv 5,7 \pmod 8 \\ 0 \pmod{24} & \text{if } A = q_1' \text{ and } r \equiv 0 \pmod 8 \end{cases}$$

or

$$\#E_A^0(F_{p^r}) \equiv \begin{cases} 20 \pmod{24} & \text{if } A = q_4 \text{ and } r \equiv 1,3 \pmod 8 \\ 8 \pmod{24} & \text{if } A = q_4 \text{ and } r \equiv 2,6 \pmod 8 \\ 16 \pmod{24} & \text{if } A = q_4 \text{ and } r \equiv 4 \pmod 8 \\ 4 \pmod{24} & \text{if } A = q_4 \text{ and } r \equiv 5,7 \pmod 8 \\ 0 \pmod{24} & \text{if } A = q_4 \text{ and } r \equiv 0 \pmod 8 \\ 16 \pmod{24} & \text{if } A = q_2 \text{ and } r \equiv 1,3,4 \pmod 8 \\ 8 \pmod{24} & \text{if } A = q_2 \text{ and } r \equiv 2,5,6,7 \pmod 8 \\ 0 \pmod{24} & \text{if } A = q_2 \text{ and } r \equiv 0 \pmod 8 \\ 2 \pmod{24} & \text{if } A = q_1 \text{ and } r \equiv 1,3 \pmod 8 \\ 20 \pmod{24} & \text{if } A = q_1 \text{ and } r \equiv 2,6 \pmod 8 \\ 16 \pmod{24} & \text{if } A = q_1 \text{ and } r \equiv 4 \pmod 8 \\ 10 \pmod{24} & \text{if } A = q_1 \text{ and } r \equiv 5,7 \pmod 8 \\ 0 \pmod{24} & \text{if } A = q_1 \text{ and } r \equiv 0 \pmod 8 \\ 10 \pmod{24} & \text{if } A = q_1' \text{ and } r \equiv 1,3 \pmod 8 \\ 20 \pmod{24} & \text{if } A = q_1' \text{ and } r \equiv 2,6 \pmod 8 \\ 16 \pmod{24} & \text{if } A = q_1' \text{ and } r \equiv 4 \pmod 8 \\ 2 \pmod{24} & \text{if } A = q_1' \text{ and } r \equiv 5,7 \pmod 8 \\ 0 \pmod{24} & \text{if } A = q_1' \text{ and } r \equiv 0 \pmod 8. \end{cases}$$

(6) *If* $p \equiv 17 \pmod{24}$ *is a prime, then*

$$\#E_A^0(F_{p^r}) \equiv \begin{cases} 8 \pmod{24} & \text{if } A = q_4 \text{ and } r \equiv 1,2,3,6 \pmod 8 \\ 16 \pmod{24} & \text{if } A = q_4 \text{ and } r \equiv 4,5,7 \pmod 8 \\ 0 \pmod{24} & \text{if } A = q_4 \text{ and } r \equiv 0 \pmod 8 \\ 4 \pmod{24} & \text{if } A = q_2 \text{ and } r \equiv 1,3 \pmod 8 \\ 8 \pmod{24} & \text{if } A = q_2 \text{ and } r \equiv 2,6 \pmod 8 \\ 16 \pmod{24} & \text{if } A = q_2 \text{ and } r \equiv 4 \pmod 8 \\ 20 \pmod{24} & \text{if } A = q_2 \text{ and } r \equiv 5,7 \pmod 8 \\ 0 \pmod{24} & \text{if } A = q_2 \text{ and } r \equiv 0 \pmod 8 \\ 2 \pmod{24} & \text{if } A = q_1 \text{ and } r \equiv 1,3 \pmod 8 \\ 20 \pmod{24} & \text{if } A = q_1 \text{ and } r \equiv 2,6 \pmod 8 \\ 16 \pmod{24} & \text{if } A = q_1 \text{ and } r \equiv 4 \pmod 8 \\ 10 \pmod{24} & \text{if } A = q_1 \text{ and } r \equiv 5,7 \pmod 8 \\ 0 \pmod{24} & \text{if } A = q_1 \text{ and } r \equiv 0 \pmod 8 \\ 10 \pmod{24} & \text{if } A = q_1' \text{ and } r \equiv 1,3 \pmod 8 \\ 20 \pmod{24} & \text{if } A = q_1' \text{ and } r \equiv 2,6 \pmod 8 \\ 16 \pmod{24} & \text{if } A = q_1' \text{ and } r \equiv 4 \pmod 8 \\ 2 \pmod{24} & \text{if } A = q_1' \text{ and } r \equiv 5,7 \pmod 8 \\ 0 \pmod{24} & \text{if } A = q_1' \text{ and } r \equiv 0 \pmod 8 \end{cases}$$

or

$$\#E_A^0(F_{p^r}) \equiv \begin{cases} 16 \pmod{24} & \text{if } A = q_4 \text{ and } r \equiv 1,3,4 \pmod 8 \\ 8 \pmod{24} & \text{if } A = q_4 \text{ and } r \equiv 2,5,6,7 \pmod 8 \\ 0 \pmod{24} & \text{if } A = q_4 \text{ and } r \equiv 0 \pmod 8 \\ 20 \pmod{24} & \text{if } A = q_2 \text{ and } r \equiv 1,3 \pmod 8 \\ 8 \pmod{24} & \text{if } A = q_2 \text{ and } r \equiv 2,6 \pmod 8 \\ 16 \pmod{24} & \text{if } A = q_2 \text{ and } r \equiv 4 \pmod 8 \\ 4 \pmod{24} & \text{if } A = q_2 \text{ and } r \equiv 5,7 \pmod 8 \\ 0 \pmod{24} & \text{if } A = q_2 \text{ and } r \equiv 0 \pmod 8 \\ 2 \pmod{24} & \text{if } A = q_1 \text{ and } r \equiv 1,3 \pmod 8 \\ 20 \pmod{24} & \text{if } A = q_1 \text{ and } r \equiv 2,6 \pmod 8 \\ 16 \pmod{24} & \text{if } A = q_1 \text{ and } r \equiv 4 \pmod 8 \\ 10 \pmod{24} & \text{if } A = q_1 \text{ and } r \equiv 5,7 \pmod 8 \\ 0 \pmod{24} & \text{if } A = q_1 \text{ and } r \equiv 0 \pmod 8 \\ 10 \pmod{24} & \text{if } A = q_1' \text{ and } r \equiv 1,3 \pmod 8 \\ 20 \pmod{24} & \text{if } A = q_1' \text{ and } r \equiv 2,6 \pmod 8 \\ 16 \pmod{24} & \text{if } A = q_1' \text{ and } r \equiv 4 \pmod 8 \\ 2 \pmod{24} & \text{if } A = q_1' \text{ and } r \equiv 5,7 \pmod 8 \\ 0 \pmod{24} & \text{if } A = q_1' \text{ and } r \equiv 0 \pmod 8. \end{cases}$$

Proof. Among the above results, the proof will be given only for the first case. In the case when $p \equiv 1 \pmod{24}$, $6 \mid b$ (for $p = a^2 + b^2$), $-1 + 2t = q_4$ and $\#E_A^0(F_p) \equiv 0 \pmod{24}$, we find $v \equiv 2 \pmod{24}$ if $\#E_A^0(F_p) = p + 1 - v$. For the evaluation of $N_r = p^r + 1 - (\alpha^r + \beta^r)$, let $M_r = \alpha^r + \beta^r$. Then, we find the recurrence formula of $M_r = vM_{r-1} - pM_{r-2}$ (for $r \geq 3$) from the relations of $\alpha + \beta = v$ and $\alpha\beta = p$. Using $M_1 = v \equiv 2 \pmod{24}$, $M_2 = v^2 - 2p \equiv 2$

(mod 24) and $M_r = vM_{r-1} - pM_{r-2} = 2M_{r-1} - M_{r-2}$, it is obvious that $M_r \equiv 2 \pmod{24}$ for all $r \geq 1$. Therefore,

$$N_r = p^r + 1 - (\alpha^r + \beta^r) = 1^r + 1 - M_r \equiv 1 + 1 - 2 \equiv 0 \pmod{24}.$$

Other cases are similarly proven. □

Theorem 3.3. *Let $E_0^{B^3} : y^2 = x^3 + B^3$ be an elliptic curve modulo p with $p \equiv 1 \pmod 6$, and $t \in \mathbb{Z}$ such that $3t^2 \equiv 1 \pmod p$.*

(1) *Let $p = a^2 + b^2 \equiv 1 \pmod{12}$ be a prime with $6 \mid b$. Then*

$$\#E_0^{B^3}(F_{p^r}) \equiv \begin{cases} 0 \pmod{24} & \text{if } \left(\frac{B}{p}\right) = 1 \\ 4 \pmod{24} & \text{if } \left(\frac{B}{p}\right) = -1 \text{ and } r \equiv 1 \pmod 2 \\ 0 \pmod{24} & \text{if } \left(\frac{B}{p}\right) = -1 \text{ and } r \equiv 0 \pmod 2. \end{cases}$$

(2) *If $p = a^2 + b^2 \equiv 1 \pmod{12}$ is a prime with $2 \mid b$ and $3 \nmid b$, then*

$$\#E_0^{B^3}(F_{p^r}) \equiv \begin{cases} 12 \pmod{24} & \text{if } \left(\frac{B}{p}\right) = 1 \text{ and } r \equiv 1 \pmod 2 \\ 0 \pmod{24} & \text{if } \left(\frac{B}{p}\right) = 1 \text{ and } r \equiv 0 \pmod 2 \\ 16 \pmod{24} & \text{if } \left(\frac{B}{p}\right) = -1 \text{ and } r \equiv 1 \pmod 2 \\ 0 \pmod{24} & \text{if } \left(\frac{B}{p}\right) = -1 \text{ and } r \equiv 0 \pmod 2. \end{cases}$$

(3) *If $p \equiv 7 \pmod{12}$ is a prime, then*

$$\#E_0^{B^3}(F_{p^r}) \equiv \begin{cases} 12 \pmod{24} & \text{if } \left(\frac{B}{p}\right) = 1 \text{ and } r \equiv 1 \pmod 2 \\ 0 \pmod{24} & \text{if } \left(\frac{B}{p}\right) = 1 \text{ and } r \equiv 0 \pmod 2 \\ 4 \pmod{24} & \text{if } \left(\frac{B}{p}\right) = -1 \text{ and } r \equiv 1 \pmod 2 \\ 0 \pmod{24} & \text{if } \left(\frac{B}{p}\right) = -1 \text{ and } r \equiv 0 \pmod 2. \end{cases}$$

Proof. Among the above results, we will prove only for the first case. In the case when $p \equiv 1 \pmod{12}$, $6 \mid b$ (for $p = a^2 + b^2$), and $\#E_0^{B^3}(F_p) \equiv 0 \pmod{24}$, we find $v \equiv 2 \pmod{24}$ if $\#E_0^{B^3}(F_p) = p + 1 - v$. For the evaluation of $N_r = p^r + 1 - (\alpha^r + \beta^r)$, let $M_r = \alpha^r + \beta^r$. Then, we find the recurrence formula of $M_r = vM_{r-1} - pM_{r-2}$ (for $r \geq 3$) from the relations of $\alpha + \beta = v$ and $\alpha\beta = p$. Using $M_1 = v \equiv 2 \pmod{24}$, $M_2 = v^2 - 2p \equiv 2 \pmod{24}$ and $M_r = vM_{r-1} - pM_{r-2} = 2M_{r-1} - M_{r-2}$, it is obvious that $M_r \equiv 2 \pmod{24}$ for all $r \geq 1$. Therefore, $N_r = p^r + 1 - (\alpha^r + \beta^r) = 1^r + 1 - M_r \equiv 1 + 1 - 2 \equiv 0 \pmod{24}$. Other cases are similarly proven. □

The following proposition, which is conjectured by E. Artin in his thesis and proved by Hasse in the 1930's, shows that this heuristic reasoning is correct.

Proposition 3.4 (Hasse, 1922 [12, p. 131])**.** *Let K be a finite field with p elements and let E/K be an elliptic curve. Then*

$$|\#E(K) - p - 1| \leq 2\sqrt{p}.$$

Equivalently, the number of solutions is bounded above by the number $(\sqrt{p}+1)^2$.

Example 3.5. Let $p = 13$. We know that $13 + 1 - 2\sqrt{13} < 7 \leq \#E_A^0(F_{13}) < 21 \leq 13 + 1 + 2\sqrt{13}$ by Hasse's theorem. On the other hand, we know by Theorem 1.1 that

$$\begin{aligned}
&\#E_1^0(F_{13}) \equiv 20 \pmod{24},\\
&\#E_4^0(F_{13}) \equiv 8 \pmod{24},\\
&\#E_2^0(F_{13}) \equiv 10 \pmod{24} \ \ (2 \cdot 5 = 10 = q_2), \text{ and}\\
&\#E_8^0(F_{13}) \equiv 18 \pmod{24} \ \ (8 \cdot 5 = 40 = q_4),
\end{aligned}$$

where 2 is a primitive root modulo 13. Thus, we have $\#E_1^0(F_{13}) = 20$, $\#E_4^0(F_{13}) = 8$, $\#E_2^0(F_{13}) = 10$, and $\#E_8^0(F_{13}) = 18$.

References

[1] I. F. Blake, G. Seroussi, and N. P. Smart, *Elliptic Curves in Cryptography*, Reprint of the 1999 original. London Mathematical Society Lecture Note Series, 265. Cambridge University Press, Cambridge, 2000.

[2] B. M. Brewer, *On certain character sums*, Trans. Amer. Math. Soc. **99** (1961), 241–245.

[3] M. Demirci, G. Soydan, and I. N. Cangul, *Rational points on elliptic curves $E : y^2 = x^3 + a^3$ in $\mathbb{F}_p$ where $p \equiv 1 \pmod 6$ is prime*, Rocky Mountain J. Math. **37** (2007), no. 5, 1483–1491.

[4] I. Inam, O. Bizim, and I. N. Cangul, *Rational points on Frey elliptic curves $E : y^2 = x^3 - n^2x$*, Adv. Stud. Contemp. Math. (Kyungshang) **14** (2007), no. 1, 69–76.

[5] I. Inam, G. Soydan, M. Demirci, O. Bizim, and I. N. Cangul, *Corrigendum on "The number of points on elliptic curves $E : y^2 = x^3 + cx$ over $\mathbb{F}_p$ mod 8"*, Commun. Korean Math. Soc. **22** (2007), no. 2, 207–208.

[6] K. Ireland and M. Rosen *A Classical Introduction to Mordern Number Theory*, Springer-Verlag, 1981.

[7] A. W. Knapp, *Elliptic Curves*, Princeton Uinversity Press, New Jersey 1992.

[8] H. Park, D. Kim, and E. Lee *The number of points on elliptic curves $E : y^2 = x^3 + cx$ over $\mathbb{F}_p$ mod* 8, Commun. Korean Math. Soc. **18** (2003), no. 1, 31–37.

[9] H. Park, S. You, H. Park, D. Kim, and H. Kim *The number of points on elliptic curves $E_A^0 : y^2 = x^3 + Ax$ over $\mathbb{F}_p$ mod* 24, Honam Math. J. **34** (2012), no.1, 93–101.

[10] A. R. Rajwade, *A note on the number of solutions N_p of the congruence $y^2 \equiv x^3 - Dx \pmod p$*, Proc. Cambfidge Philos. Soc. **67** (1970), 603–605.

[11] R. Schoof, *Counting points on elliptic curves over finite fields*, J. Théor. Nombres Bordeaux **7** (1995), no. 1, 219–254.

[12] J. H. Silverman, *The Arithmetic of Elliptic Curves*, Springer-Verlag, New York, 1986.

[13] Z. H. Sun, *Supplements to the theory of quartic residues*, Acta Arith. **97** (2001), no. 4, 361–377.

[14] B. A. Venkov, *Elementary Number Theory*, translated form the Russian and edited by H. Alderson, Wolters-Noordhoff, Groningen, 1970.

[15] A. Weil, *Sur les courbes algébriques et les variétés qui s'en déduisent*, Hermann, Paris, 1948.
[16] S. You, H. Park, and H. Kim *The Number of points on elliptic curves* $E_0^{a^3} : y^2 = x^3 + a^3 b$ *over* $\mathbb{F}_p$ *mod* 24, Honam Math. J. **31** (2009), no. 3, 437–449.

Wonju Jeon
National Institute for Mathematical Sciences
Daejeon 305-811, Korea
E-mail address: wjeon@nims.re.kr

Daeyeoul Kim
National Institute for Mathematical Sciences
Daejeon 305-811, Korea
E-mail address: daeyeoul@nims.ac.kr