THE NUMBER OF POINTS ON ELLIPTIC CURVES

\[ E_0^3 : y^2 = x^3 + a^3 \text{ OVER } \mathbb{F}_p \text{ MOD } 24 \]

SOONHO YOU, HWASIN PARK AND HYUN KIM

Abstract. In this paper, we calculate the number of points on elliptic curves \( E_a^3 : y^2 = x^3 + a^3 \) over \( \mathbb{F}_p \text{ mod } 24 \) and \( E_b^3 : y^2 = x^3 + b \) over \( \mathbb{F}_p \text{ mod } 6 \), where \( b \) is cubic non-residue in \( \mathbb{F}_p^* \). For example, if \( p \equiv 1 \pmod{12} \) is a prime, and \( a \) and \( a(2t - 3) \) are quadratic residues modulo \( p \) with \( 3t^2 \equiv 1 \pmod{p} \), then the number of points in \( E_a^3 : y^2 = x^3 + a^3 \) is congruent to 0 modulo 24.

1. introduction

Let \( \mathbb{F} \) be a number field. We will study plane algebraic curves defined by the equation,

\[ E : y^2 + a_1xy + a_3y = x^3 + a_2x^2 + a_4x + a_6, \]

where the \( a_i \)'s are in \( \mathbb{F} \). This is called a Weierstrass equation over \( \mathbb{F} \). If \( \text{Char}(\mathbb{F}) \neq 2 \), then we can simplify the equation by completing the square. That is, replacing \( y \) by \((\frac{1}{2})(y - a_1x - a_3) \) gives an equation of the form \( E : y^2 = 4x^3 + b_2x^2 + 2b_4x + b_6 \), where \( b_2 = a_2^4 + 4a_2, b_4 = 2a_4 + a_1a_3, b_6 = a_5^2 + 4a_6, \) and \( b_8 = a_7a_6 + 4a_2a_6 + a_1a_3a_4 + a_2a_3^2 - a_4^2 \).

If \( \text{Char}(\mathbb{F}) \neq 2,3 \), then we can also reduce the equation to

\[ E : y^2 = x^3 - 27c_4x - 54c_6, \]

where \( c_4 = b_2^2 - 24b_4 \) and \( c_6 = b_3^2 + 36b_2b_4 - 216b_6 \). We usually write \( E : y^2 = x^3 + Ax + B \), where \( A = -27c_4, B = -54c_6 \).

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 [Si].

Received July 13, 2009. Accepted August 21, 2009.

Key words and phrases: elliptic curves.
It has been always interesting to look for the number of points over a given field $\mathbb{F}_p$. In [S], three algorithms to find the number of points on an elliptic curve over a finite field are given. Also in [DISC], [DSC], [ISDC2] 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.

In 2003, H. Park, D. Kim and H. Lee calculated the number of points on elliptic curves $E_0^A : y^2 = x^3 + Ax$ over $\mathbb{F}_p \mod 8$ ([PKL], [ISDBC]).

The purpose of this paper is to give a straightforward calculation of the number mod 24 of points on elliptic curves over a finite field. In [KKP], the following questions was proposed: let $E : y^2 = x^3 + f(k)x + g(k)$ be an elliptic curve over a finite field $\mathbb{F}_p$ and $\alpha$ be a nonnegative integer.

1. Can one find $f(k)$ and $g(k)$ satisfying $\#E(\mathbb{F}_p) \equiv \alpha \pmod n$ 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 find $f(k)$ and $g(k)$ satisfying $\#E(\mathbb{F}_p) \equiv \alpha \pmod n$ for a fixed $n$ and for all such primes $p$?

In this regard, we note the following two propositions.

**Proposition 1.1.** [KKP] Let $p$ be a prime number greater than 3 and $k$ be an integer such that $p \nmid k(9k + 4)$. Let $E(\mathbb{F}_p)$ be the set of points of an elliptic curve $E$. If $E$ is given by the Weierstrass equation $E : y^2 = x^3 - (6k + 3)x - (3k^2 + 6k + 2)$, then the number of elements in $E(\mathbb{F}_p)$ is congruent to 0 modulo 3.

**Proposition 1.2.** [KKP] Let $p$ be a prime number greater than 5 and $E$ have the Weierstrass equation $E : y^2 = x^3 - 12x - 11$. Then

\[
\#E(\mathbb{F}_p) \equiv \begin{cases} 
6 \pmod{12} & \text{if } p \equiv 3, 7 \pmod{20} \\
0 \pmod{12} & \text{if } p \equiv 1, 9, 11, 13, 17, 19 \pmod{20}
\end{cases}
\]

where $\#E(\mathbb{F}_p)$ is the number of points of $E$.

**Proposition 1.3.** ([K] p.145, [Si] p.323)

1. Let $p \neq 2, 3$. Then $E_A^B$ is supersingular if and only if $\#E_A^B = p + 1$.
2. If $p \equiv 3 \pmod 4$ is a prime and $E_0^A : y^2 = x^3 + Ax$ is an elliptic curve over $\mathbb{F}_p$, then $\#E_0^A = p + 1$.
3. If $p \equiv 2 \pmod 3$ is a prime and $E_0^B : y^2 = x^3 + B$ is an elliptic curve over $\mathbb{F}_p$, then $\#E_0^B = p + 1$.

**Proposition 1.4.** [KKP] Let $E_A^B : y^2 = x^3 + Ax + B$ be an elliptic curve over $\mathbb{F}_p$ and $P = (x, y)$ be a point in $E_A^B(\mathbb{F}_p)$ which is not a point at
The number of points on elliptic curves $E_0^3 : y^2 = x^3 + a^3$ over $\mathbb{F}_p \mod 24$ infinity, where $E_B^A(\mathbb{F}_p)$ is the group of points on $E$. Then the followings are equivalent.

1. $P = (x, y)$ is a point of order 3 in $E_B^A(\mathbb{F}_p)$.
2. $3x^4 + 6Ax^2 + 12Bx - A^2$ is congruent to 0 to modulo $p$.

And we denoted by $N_p(f(x))$ the number of solutions of the congruence equation $f(x) \equiv 0 \pmod{p}$. Let $(\cdot)$ be the Legendre symbol and let $D = a_1^2a_2^2 - 4a_2^3a_3 - 27a_3^2 + 18a_1a_2a_3$ be the discriminant of the cubic polynomial $x^3 + a_1x^2 + a_2x + a_3$.

**Lemma 1.5.** If $p > 3$ is a prime, $a_1, a_2, a_3 \in \mathbb{Z}$ and $p \nmid D$, then

$$N_p(x^3 + a_1x^2 + a_2x + a_3) = \begin{cases} 0 \text{ or } 3, & \text{if } (\frac{D}{p}) = 1 \\ 1, & \text{if } (\frac{D}{p}) = -1. \end{cases}$$

**Proof.** See Cohen [C, pp.198-199], Dickson [D] or Stickelberger [St].

**Proposition 1.6.** [IR] Let $p$ and $q$ be odd primes. Then the followings are satisfied.

1. If $p \equiv 1 \pmod{4}$, then $(\frac{-1}{p}) = 1$.
2. If $p \equiv \pm 1 \pmod{12}$, then $(\frac{3}{p}) = 1$.

In section 2, we calculate the number of points on elliptic curves $E_0^3 : y^2 = x^3 + B$ over $\mathbb{F}_p$ according to whether $B$ is a cubic residue or non-residue.

2. **The number of points on elliptic curves $E_0^3 : y^2 = x^3 + a^3$ over $\mathbb{F}_p \mod 24$**

By Proposition 1.3 (3), if $p \equiv 5, 11 \pmod{12}$, then $#E_0^B = p + 1$. So, we consider when $p \equiv 1, 7 \pmod{12}$. And we give the results concerning the number of points $#E_0^B$ on the elliptic curve $E_0^B : y^2 = x^3 + B$ according to whether $B = a^3$ for some $a \in \mathbb{F}_p^*$ or not. In this section, we show the case $B = a^3$, and in next section we show the case $b$ is cubic non-residue in $\mathbb{F}_p^*$.

**Lemma 2.1.** Let $a \in \mathbb{F}_p^*$. Then $#E_0^a(\mathbb{F}_p) \equiv 0 \pmod{2}$. 
Proof. Let $E_0^3 : y^2 = x^3 + a^3 = (x + a)(x^2 - ax + a^2) \pmod{p}$ be an elliptic curve defined over $\mathbb{F}_p$. Taking $P_1 = (-a, 0)$, then we obtain that $P_1 \in E_0^3$ and $2P_1 = O$. So, $\#E_0^3 \equiv 0 \pmod{2}$.

Lemma 2.2. Let $a \in \mathbb{F}_p^*$ and $P_1 = (0, a^2)$. Then the followings are satisfied.

1. If $\left(\frac{a}{p}\right) = 1$, then $\#E_0^3 \equiv 0 \pmod{3}$ and $3P_1 = O$.
2. If $\left(\frac{a}{p}\right) = -1$ and if $p \equiv 1 \pmod{6}$, then $\#E_0^3 \not\equiv 0 \pmod{3}$ and if $p \equiv 5 \pmod{6}$, then $\#E_0^3 \equiv 0 \pmod{3}$.

Proof. (1) Let $E_A^3 : y^2 = x^3 + Ax + B$ be an elliptic curve over $\mathbb{F}_p$. By Proposition 1.4, if $3x^4 + 6Ax^2 + 12Bx - A^2$ is congruent to 0 modulo $p$, then $P = (x, y)$ is a point of order 3 in $E_A^3(\mathbb{F}_p)$. That is, $\#E_A^3 \equiv 0 \pmod{3}$. We will check whether such a point $P = (x, y)$ exists or not. Put $A = 0$, and $B = a^3$, then $3x^4 + 6Ax^2 + 12Bx - A^2 = 3x^4 + 12a^3x = 3x(x^3 + 4a^3) \equiv 0 \pmod{p}$. We get results concerning the number of points $\#E_0^3$ on the elliptic curve $E_0^3 : y^2 = x^3 + a^3 \pmod{p}$ according to whether $x \equiv 0 \pmod{p}$ or $x^3 + 4a^3 \equiv 0 \pmod{p}$. We will find the case that such a point $P = (x, y)$ exists when $x \equiv 0 \pmod{p}$. If $\left(\frac{a^3}{p}\right) = \left(\frac{a}{p}\right) = 1$, then the point $P_1 = (0, a^2)$ exists in $E_0^3(\mathbb{F}_p)$. Thus $P_1 = (0, a^2)$ is a point of order 3 in $E_0^3(\mathbb{F}_p)$, and so $\#E_0^3 \equiv 0 \pmod{3}$.

In other words, if $\left(\frac{a}{p}\right) = 1$, then $\#E_0^3 \equiv 0 \pmod{3}$.

(2) Let us consider the case $\left(\frac{a}{p}\right) = -1$. By Lemma 1.5, let $a_1 = 0, a_2 = 0, a_3 = 4a^3$, then $D = -27 \cdot (4a^3)^2$ and $\left(\frac{D}{p}\right) = \left(-\frac{27 \cdot 4a^6}{p}\right) = \left(-\frac{27}{p}\right) \left(-\frac{2}{p}\right)$. Therefore, if $p \equiv 5 \pmod{6}$, then $\left(\frac{2}{p}\right) = -1$ and $N_p(x^3 + 4ax^2 + 2ax + 3) = 1$. Thus there exists $x_2 \in \mathbb{F}_p$ of $(x_2, y_2) \in E_0^3(\mathbb{F}_p)$ such that $x_2^3 + 4a^3 \equiv 0 \pmod{p}$. By substituting such $(x_2, y_2)$ into $E_0^3(\mathbb{F}_p)$ and using $y_2^2 = x_2^3 + a^3 = -4a^3 + a^3 = -3a^3$, we see that $\left(-\frac{3a^3}{p}\right) = \left(-\frac{3}{p}\right) \left(-\frac{a}{p}\right)$. If $p \equiv 11 \pmod{12}$, then $\left(-\frac{3}{p}\right) = \left(-\frac{1}{p}\right) \left(-\frac{3}{p}\right) = (1) \cdot (1) = 1$ and $\left(-\frac{3a^3}{p}\right) = \left(-\frac{3}{p}\right) \left(-\frac{a}{p}\right) = (1) \cdot (1) = 1$. And if $p \equiv 5 \pmod{12}$, then $\left(-\frac{3}{p}\right) = \left(-\frac{1}{p}\right) \left(-\frac{3}{p}\right) = (1) \cdot (1) = 1$ and then $\left(-\frac{3a^3}{p}\right) = \left(-\frac{3}{p}\right) \left(-\frac{a}{p}\right) = (1) \cdot (1) = 1$. So, if $p \equiv 5 \pmod{6}$, then there exists $y_2$ of a point $(x_2, y_2) \in E_0^3(\mathbb{F}_p)$ such that $x_2^3 + 4a^3 \equiv 0 \pmod{p}$ and $y_2^2 = x_2^3 + a^3$. Therefore, $\#E_0^3 \equiv 0 \pmod{3}$. 


The number of points on elliptic curves \( E_0^3 : y^2 = x^3 + a^3 \) over \( \mathbb{F}_p \) mod 24 441

Next, we assume that \( p \) is congruent to 1 modulo 6. Indeed, if we assume that \((x_2, y_2)\) is a point of \( E_0^3(\mathbb{F}_p) \) such that \( x_2^3 + 4a^3 \equiv 0 \pmod{p} \), then \( y_2^2 = x_2^3 + a^3 = -4a^3 + a^3 = -3a^3 \) and \( (-3a^3) = (-3a^3) = (-3a^3) \).

On the other hand, if \( p \equiv 1 \pmod{12} \), then \( (-3a^3) = (-3a^3) = 1 \cdot 1 = 1 \) and \( (-3a^3) = (-3a^3) = 1 \cdot (-1) = -1 \). And if \( p \equiv 7 \pmod{12} \), then \( (-3a^3) = (-3a^3) = (-1) \cdot (-1) = 1 \) and \( (-3a^3) = (-3a^3) = 1 \cdot (-1) = -1 \). So, if \( p \equiv 1 \pmod{6} \) and \( (\frac{a}{p}) = -1 \), then there does not exist \( y_2 \) of \((x_2, y_2) \in E_0^3(\mathbb{F}_p) \) such that \( x_2^3 + 4a^3 \equiv 0 \pmod{p} \) and \( y_2^2 = x_2^3 + a^3 \pmod{p} \). Therefore, for a prime \( p \) congruent to 1 modulo 6 we get \#\( E_0^3 \) \( \neq 0 \pmod{3} \).

**Lemma 2.3.** For elliptic curves \( E_0^3 : y^2 = x^3 + a^3 \) over \( \mathbb{F}_p \) where \( a \in \mathbb{F}_p \), let \( E_0^3(\mathbb{F}_p)[2] = \{ P \in \mathbb{F}_p : 2P = O \} \) be a subgroup of \( E_0^3(\mathbb{F}_p) \).

1. If \( p \equiv 1 \pmod{6} \), then \( E_0^3(\mathbb{F}_p)[2] \cong \mathbb{Z}_2 \times \mathbb{Z}_2 \).
2. If \( p \equiv 5 \pmod{6} \), then \( E_0^3(\mathbb{F}_p)[2] \cong \mathbb{Z}_2 \).

**Proof.** It follows that \( E_0^3 : y^2 = x^3 + a^3 \equiv (x + a)(x^2 - ax + a^2) \). It is well known that \( ax^2 + bx + c \equiv 0 \pmod{p} \) is solvable if and only if \((\frac{b}{p}) = 1 \), where \( D = b^2 - 4ac \). Consider \( x^2 - ax + a^2 \equiv 0 \pmod{p} \) and \( D = a^2 - 4a^2 = -3a^2 \).

1. If \( p \equiv 1 \pmod{6} \), that is, \((\frac{-3a^2}{p}) = (-\frac{3}{p}) = (-\frac{1}{p})(\frac{3}{p}) = 1 \), then \( E_0^3 : y^2 = x^3 + a^3 \equiv (x + a)(x^2 - ax + a^2) = (x + a)(x - \alpha)(x - \beta) \), thus \( E_0^3(\mathbb{F}_p)[2] \cong \mathbb{Z}_2 \times \mathbb{Z}_2 \). Here three values of \( x \) are \(-a\), \(-aw \) and \(-aw^2 \) where \( w = (\frac{-1 + \sqrt{-3}}{2}) \).

2. If \( p \equiv 5 \pmod{6} \), i.e., \((\frac{-3a^2}{p}) = (\frac{-3}{p}) = (\frac{-1}{p})(\frac{3}{p}) = -1 \), then \( E_0^3(\mathbb{F}_p)[2] \cong \mathbb{Z}_2 \).

**Lemma 2.4.** For elliptic curves \( E_0^3 : y^2 = x^3 + a^3 \equiv (x + a)(x - \alpha)(x - \beta) \) over \( \mathbb{F}_p \) where \( a, \alpha, \beta \in \mathbb{F}_p \), let \( P_1 = (-a, 0) \). If \( p \equiv 5, 7 \pmod{12} \), then there is no point \( P_2 \in E_0^3(\mathbb{F}_p) \) such that \( 2P_2 = P_1 \) or \( 2P_2 = (\alpha, 0) \) or \( 2P_2 = (\beta, 0) \).

**Proof.** Let \( P_2 = (x_2, y_2) \) in \( E_0^3(\mathbb{F}_p) \). Since \( y^2 = \frac{3ax^2}{2y} \), the tangent line \( L \) through \( P_2 \) has an equation of the form \( L : y = \frac{3ax^2}{2y_2}(x - x_2) + y_2 \). It is easily seen that \( x^3 - (\frac{3ax^2}{2y_2}(x - x_2) + y_2)^2 + a^3 \equiv 0 \pmod{p} \) have roots \( x_2 \) and \(-a \) where \( P_1 = (-a, 0) \), and \( P_2 = (x_2, y_2) \) are points of \( L \cap E_0^3 \).
To find $P_2 = (x_2, y_2)$ such that $2P_2 = P_1$, we calculate the sum of three roots of $x^3 - (\frac{3a^2}{4p^2})(x - x_2) + y_2)^2 + a^3 \equiv 0 \pmod{p}$. Thus we derive that $x_2 + x_2 + (-a) = \frac{9x_2^3}{4y_2} = \frac{9x_2^3}{4(x_2^3 + a^3)}$ and

\begin{equation}
    x_2^3 + 4ax_2^3 - 8a^3x_2 + 4a^4 \equiv 0 \pmod{p}.
\end{equation}

Next, setting $x_2 = x - a$ in (2.0.1), we have $x^4 - 6a^2x^2 + 9a^4 = (x^2 - 3a^2)^2 \equiv 0 \pmod{p}$. If $\left(\frac{3a^2}{p}\right) = \left(\frac{2}{p}\right)$, then we have a possibility for finding an element $x_2 \in \mathbb{F}_p$ such that $2P_2 = P_1$.

But, since $p \equiv 5, 7 \pmod{12}$, then $\left(\frac{3a^2}{p}\right) = \left(\frac{2}{p}\right) = -1$. Therefore there is no point $P_2 = (x_2, y_2)$ such that $2P_2 = P_1$.

Let us consider the cases of $(\alpha, 0)$ or $(\beta, 0)$. Assume that $x^3 + a^3 = (x + a)(x - \alpha)(x - \beta)$, where $\alpha, \beta \in \mathbb{F}_p^*$, that is, $\alpha^3 + a^3 = \beta^3 + a^3 = 0$. Put $P_3 = (\alpha, 0)$. In a similar way, when working with $(-a, 0)$ and then $x_2 = x - a$, we derive that $x_2^3 - 4ax_2^3 - 8x_2a^3 - 4a^3 \equiv 0 \pmod{p}$ and $x^4 - 6a^2x^2 - (a^3 + a^3)8x - 3a^4 + 12a^3\alpha = (x^2 - 3a^2)^2 \equiv 0 \pmod{p}$.

If $p \equiv 5, 7 \pmod{12}$, then $\left(\frac{2}{p}\right) = -1$. So there is no point $P_2 \in E_0^3(\mathbb{F}_p)$ such that $2P_2 = P_3$. Like the above two cases, there is no point $P_2 \in E_0^3(\mathbb{F}_p)$ such that $2P_2 = (\beta, 0)$. Therefore, the Lemma follows.

\begin{corollary}
    If $p \equiv 7 \pmod{12}$, then $\#E_0^3(\mathbb{F}_p) \equiv 4 \pmod{8}$.
\end{corollary}

\textbf{Proof.} By Lemma 2.3, if $p \equiv 7 \pmod{12}$, then $E_0^3(\mathbb{F}_p)[2] \cong \mathbb{Z}_2 \times \mathbb{Z}_2$. So, $4 \mid \#E_0^3(\mathbb{F}_p)$. But, $8 \nmid \#E_0^3(\mathbb{F}_p)$ by Lemma 2.4.

\begin{lemma}
    Let $E_0^3 : y^2 = x^3 + a^3 = (x + a)(x - \alpha)(x - \beta)$ be an elliptic curve over $\mathbb{F}_p$ and let $P_1 = (-a, 0)$.
    \begin{enumerate}
        \item If $p \equiv 1 \pmod{12}$ and $\left(\frac{2\sqrt[3]{a^3 - 3a}}{p}\right) = 1$, then there exists a point $P_2 = (x_2, y_2) \in E_0^3(\mathbb{F}_p)$ such that $2P_2 = P_1$.
        \item If $p \equiv 1 \pmod{12}$ and $\left(\frac{2\sqrt[3]{a^3 - 3a}}{p}\right) = -1$, then there is no point $P_2 = (x_2, y_2) \in E_0^3(\mathbb{F}_p)$ such that $2P_2 = P_1$ or $2P_2 = (\alpha, 0)$ or $2P_2 = (\beta, 0)$.
        \item If $p \equiv 11 \pmod{12}$, then there exists a point $P_2(x_2, y_2) \in E_0^3(\mathbb{F}_p)$ such that $2P_2 = P_1$.
    \end{enumerate}
\end{lemma}

\textbf{Proof.} By the proof of Lemma 2.4, if $\left(\frac{3a^2}{p}\right) = \left(\frac{3}{p}\right) = 1$, then there exists an element $x_2 = x - a \in \mathbb{F}_p$ such that $x^2 = 3a^2$. So, we consider the cases of $p \equiv 1, 11 \pmod{12}$.
The number of points on elliptic curves $E_0^3 : y^2 = x^3 + a^3$ over $\mathbb{F}_p$ mod 24 443.

First, since $y^2 = x^3 + a^3 = (x - a)^3 + a^3 = x^3 - 3ax^2 + 3a^2x - a^3 + a^3 = x^3 - 3ax^2 + 3a^2x = x^3 - 3ax^2 + x^3 = x^3(2x - 3a)$, if $(\frac{\sqrt[3]{(2\sqrt[3]{3} - 3a)}}{p}) = 1$ or $(\frac{\sqrt[3]{(-2\sqrt[3]{3} - 3a)}}{p}) = 1$, then there exists $y_2 \in \mathbb{F}_p$ such that $2P_2 = P_1$.

Here, if $p \equiv 11$ (mod 12), then $(\frac{\sqrt[3]{(2\sqrt[3]{3} - 3a)}}{p}, \frac{\sqrt[3]{(-2\sqrt[3]{3} - 3a)}}{p}) = (-\frac{3a^2}{p}) = (-\frac{3}{p}) = -1$. So there exists $P_2 = (x_2, y_2) \in E_0^3(\mathbb{F}_p)$ such that $2P_2 = P_1$.

Second, we will show that if $p \equiv 1$ (mod 12) and $(\frac{\sqrt[3]{(2\sqrt[3]{3} - 3a)}}{p}, \frac{\sqrt[3]{(-2\sqrt[3]{3} - 3a)}}{p}) = 1$, then there exists a point $P_2 = (x_2, y_2) \in E_0^3(\mathbb{F}_p)$ such that $2P_2 = P_1$. And if $p \equiv 1$ (mod 12) and $(\frac{\sqrt[3]{(2\sqrt[3]{3} - 3a)}}{p}, \frac{\sqrt[3]{(-2\sqrt[3]{3} - 3a)}}{p}) = -1$, then there is no point $P_2 = (x_2, y_2) \in E_0^3(\mathbb{F}_p)$ such that $2P_2 = P_1$.

We know that $ax^2 + bx + c \equiv 0$ (mod $p$) is solvable if and only if $(\frac{b}{p}) = 1$ with $D = b^2 - 4ac$.

Since $(\frac{b}{p}) = (-\frac{3a^2}{p}) = (-\frac{3}{p}) = 1$, $(\frac{3a^2}{p} - ax + a^2) \equiv 0$ (mod $p$) is solvable. This implies that there exist $\alpha, \beta$ satisfying $x^3 + a^3 = (x + a)(x^2 - ax + a^2) = (x + a)(x - \alpha)(x - \beta)$. By the proof of Lemma 2.4, since $(\frac{3a^2}{p}) = (\frac{2}{p}) = 1$, there exists a possible element $\alpha \in \mathbb{F}_p$ such that $2P_2 = (\alpha, 0)$. Since $(x^2 - 3a^2)^2 \equiv 0$ (mod $p$), one can readily check that

$$x_2^3 + a^3 = (x + \alpha)^3 + a^3 = x^3 + 3\alpha x^2 + 3\alpha^2 x + \alpha^3 + a^3 = x^3 + 3\alpha x^2 + x^3 = 2x^3 + 3a x^2 = x^2(2x + 3\alpha) = 3\alpha^2(\pm 2\sqrt[3]{3} + 3\alpha) = 3\alpha^3(\pm 2\sqrt[3]{3} + 3) = -3a^3(\pm 2\sqrt[3]{3} + 3).$$

Since $(\frac{-3a^3(\pm 2\sqrt[3]{3} + 3)}{p}) = (\frac{a(\pm 2\sqrt[3]{3} + 3)}{p})$ and $(\frac{a(2\sqrt[3]{3} - 3)}{p}) = -1$, we can check that $(\frac{a(2\sqrt[3]{3} + 3)}{p}) = (\frac{2\sqrt[3]{3} + 3)}{p}) = (\frac{2}{p}) = 1$ and $(\frac{a(-2\sqrt[3]{3} - 3)}{p}) = (\frac{-3a^2}{p}) = (-\frac{3}{p}) = 1$. It follows that $(\frac{a(\pm 2\sqrt[3]{3} + 3)}{p}) = -1$ and $(\frac{a(-2\sqrt[3]{3} + 3)}{p}) = -1$.

Thus, there is no point $P_2 = (x_2, y_2)$ such that $2P_2 = (\alpha, 0)$ by Proposition 1.4. Similarly, there is no point $P_2$ such that $2P_2 = (\beta, 0)$.

This completes the proof. \qed
**Theorem 2.7.** Let \( a \in \mathbb{F}_p^* \). Then the following table is satisfied.

\[
\begin{array}{ccc}
P & \left( \frac{a}{p} \right) & \left( \frac{a(2\sqrt{3}-3)}{p} \right) & \#E_0^a(\mathbb{F}_p) \\
1 \pmod{12} & 1 & 1 & 0 \pmod{24} \\
& 1 & -1 & 12 \pmod{24} \\
& -1 & 1 & 8 \text{ or } 16 \pmod{24} \\
& -1 & -1 & 4 \text{ or } 20 \pmod{24} \\
5 \pmod{12} & 1 \text{ or } -1 & 6 \pmod{12} \\
7 \pmod{12} & 1 & 12 \pmod{24} \\
11 \pmod{12} & 1 \text{ or } -1 & 12 \pmod{24} \\
\end{array}
\]

**Proof.** By Lemma 2.1, Lemma 2.2, Lemma 2.3, Lemma 2.4, Corollary 2.5 and Lemma 2.6, it is clear. \( \square \)

**Example 2.8.** The number of solutions of \( E_0^a : y^2 = x^3 + a^3 \) is as follows:

\[
\begin{array}{c|c|c|c}
E_0^a(\mathbb{F}_p) & p & \left( \frac{a}{p} \right) & \#E_0^a(\mathbb{F}_p) \\
\hline
E_0^7(\mathbb{F}_p) & 7 & 1 & 12 \\
E_0^{13}(\mathbb{F}_p) & 13 & 1 & 12 \\
E_0^{19}(\mathbb{F}_p) & 19 & 1 & 12 \\
E_0^{31}(\mathbb{F}_p) & 31 & 1 & 36 \\
E_0^{37}(\mathbb{F}_p) & 37 & 1 & 48 \\
E_0^{97}(\mathbb{F}_p) & 97 & 1 & 84 \\
E_0^{-1}(\mathbb{F}_p) & 19 & -1 & 28 \\
E_0^7(\mathbb{F}_p) & 7 & 1 & 12 \\
E_0^3(\mathbb{F}_p) & 37 & -1 & 28 \\
\end{array}
\]

3. **The number of points on elliptic curves** \( E_0^b : y^2 = x^3 + b \) **over** \( \mathbb{F}_p \) **mod 6**

In this section, we calculate the number of points on elliptic curves \( E_0^b : y^2 = x^3 + b \) over \( \mathbb{F}_p \) mod 6, where \( b \) is a cubic non-residue in \( \mathbb{F}_p^* \).

**Lemma 3.1.** Let \( a \in \mathbb{F}_p^* \). Then, \( \#E_0^a(\mathbb{F}_p) \equiv 0 \pmod{3} \).

**Proof.** Let \( P = (0, a) \in E_0^a(\mathbb{F}_p) \), then \( 3x^4 + 12a^2x = 3x(x^3 + 3a^2) = 0 \) and \( 3P = O \), by Proposition 1.4. So, \( \#E_0^a(\mathbb{F}_p) \equiv 0 \pmod{3} \). \( \square \)

**Example 3.2.** For elliptic curves \( E_0^4 : y^2 = x^3 + 4 \) **over** \( \mathbb{F}_p \), we compute the number of the points of \( E_0^4(\mathbb{F}_p) \) as follows.
The number of points on elliptic curves $E_0^3 : y^2 = x^3 + a^3$ over $\mathbb{F}_p$ mod 24 445

<table>
<thead>
<tr>
<th>$p$</th>
<th>$#E_0^3(\mathbb{F}_p)$</th>
</tr>
</thead>
<tbody>
<tr>
<td>7</td>
<td>3</td>
</tr>
<tr>
<td>13</td>
<td>21</td>
</tr>
<tr>
<td>19</td>
<td>21</td>
</tr>
<tr>
<td>31</td>
<td>36</td>
</tr>
<tr>
<td>37</td>
<td>39</td>
</tr>
<tr>
<td>97</td>
<td>93</td>
</tr>
</tbody>
</table>

**Lemma 3.3.** For elliptic curves $E_0^{-a^2} : y^2 = x^3 - a^2$ over $\mathbb{F}_p$, where $a \in \mathbb{F}_p^*$:

1. If $p \equiv 1, 5, 11 \pmod{12}$, then $\#E_0^{-a^2}(\mathbb{F}_p) \equiv 0 \pmod{3}$.
2. If $p \equiv 7 \pmod{12}$, then $\#E_0^{-a^2}(\mathbb{F}_p) \not\equiv 0 \pmod{3}$.

**Proof.** First, if $x = 0$, then $3x^3 - 12a^2x = 3x(x^3 - 4a^2) \equiv 0 \pmod{p}$ and $y^2 = -a^2$. Thus if $(-a^2) = (-1) = 1$, then there exists a point $P = (0, y^2) \in E_0^{-a^2}(\mathbb{F}_p)$ such that $3P = O$, by Proposition 1.4. That is, if $p \equiv 1 \pmod{4}$, then $\#E_0^{-a^2}(\mathbb{F}_p) \equiv 0 \pmod{3}$.

Second, we consider the case $p \equiv 3 \pmod{4}$ and $x^3 - 4a^2 \equiv 0 \pmod{p}$.

By Lemma 1.5, $(\frac{D}{p}) = (\frac{-27.16a^4}{p}) = (\frac{-3}{p}) = -(\frac{3}{p})$ and so, if $p \equiv 11 \pmod{12}$, then $(\frac{D}{p}) = -1$. Thus, $N_p(x^3 - 4a^2) = 1$. It follows that there exists an element $y_2 \in \mathbb{F}_p$ satisfying $x^3 - 4a^2 \equiv 0 \pmod{p}$ and $x^3 - a^2 = 4a^2 - a^2 \equiv y_2^2 \pmod{p}$. By Proposition 1.4, we have $\#E_0^{-a^2}(\mathbb{F}_p) \equiv 0 \pmod{3}$. Now, we will show that if $p \equiv 7 \pmod{12}$ then $\#E_0^{-a^2}(\mathbb{F}_p) \not\equiv 0 \pmod{3}$. By Lemma 1.5, $(\frac{D}{p}) = (\frac{-27.16a^4}{p}) = (\frac{-3}{p}) = -(\frac{3}{p}) = 1$. So, $N_p(x^3 - 4a^2) = 0$ or 3. Suppose that $N_p(x^3 - 4a^2) = 3$, i.e., $x^3 - 4a^2 = (x - \alpha)(x - \beta)(x - \gamma)$ where $\alpha, \beta, \gamma \in \mathbb{F}_p^*$. Since $\alpha^3 = 4a^2$ for $(\alpha, y_2) \in E_0^{-a^2}(\mathbb{F}_p)$, $y_2^2 = 4a^2 - a^2$. But $(-\frac{a^2}{p}) = (\frac{3}{p}) = -1$. Thus there does not exist $y_2 \in \mathbb{F}_p$, satisfying $(\alpha, y_2) \in E_0^{-a^2}(\mathbb{F}_p)$. Therefore, in this case, $\#E_0^{-a^2}(\mathbb{F}_p) \not\equiv 0 \pmod{3}$. 

**Example 3.4.** For elliptic curves $E_0^{-4} : y^2 = x^3 - 4$ over $\mathbb{F}_p$, we compute the number of the points of $E_0^3(\mathbb{F}_p)$ as follows.

<table>
<thead>
<tr>
<th>$p$</th>
<th>$#E_0^{-4}(\mathbb{F}_p)$</th>
</tr>
</thead>
<tbody>
<tr>
<td>7</td>
<td>13</td>
</tr>
<tr>
<td>13</td>
<td>21</td>
</tr>
<tr>
<td>19</td>
<td>19</td>
</tr>
<tr>
<td>31</td>
<td>28</td>
</tr>
</tbody>
</table>
Lemma 3.5. For elliptic curves $E_0^a : y^2 = x^3 + a$ over $\mathbb{F}_p$, where $a \in \mathbb{F}_p^*$,

1. If $(\frac{a}{p})_3 = 1$, then $\#E_0^a(\mathbb{F}_p) \equiv 0 \pmod{2}$.
2. If $(\frac{a}{p})_3 \neq 1$, then $\#E_0^a(\mathbb{F}_p) \not\equiv 0 \pmod{2}$.

Proof. Let $g$ be a primitive root modulo $p$. And put $a = g^k$ where $k = 0, 1, 2 \pmod{3}$. If $a = g^3t$ for some $t \in \mathbb{Z}$, then $E_0^a : y^2 = x^3 + a = x^3 + g^{3t} = (x + g^t)(x^2 - xg^t + g^{2t})$. Put $P = (-g^t, 0)$. Then $2P = O$ and so $\#E_0^a(\mathbb{F}_p) \equiv 0 \pmod{2}$. And if $a = g^{3t+1}$ or $a = g^{3t+2}$ for some $t \in \mathbb{Z}$, there does not exist $x \in \mathbb{F}_p^*$ such that $x^3 + a \equiv 0 \pmod{p}$. So, in this case, $\#E_0^a(\mathbb{F}_p) \neq 0 \pmod{2}$.

Example 3.6. For elliptic curves $E_0^a : y^2 = x^3 + a$ over $\mathbb{F}_p$, we compute the number of the points on $E_0^a$ for each $a \in \mathbb{F}_p^*$ and for $p = 13$ and $p = 19$.

| $a$ | $(\frac{a}{13})_3$ | $\#E_0^a(\mathbb{F}_{13})$ | $a$ | $(\frac{a}{19})_3$ | $\#E_0^a(\mathbb{F}_{19})$
<table>
<thead>
<tr>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
</tr>
</thead>
<tbody>
<tr>
<td>1, 12</td>
<td>1</td>
<td>12</td>
<td>1, 7, 11</td>
<td>1</td>
<td>12</td>
</tr>
<tr>
<td>5, 8</td>
<td>1</td>
<td>16</td>
<td>8, 12, 18</td>
<td>1</td>
<td>28</td>
</tr>
<tr>
<td>2, 11</td>
<td>$\neq$ 1</td>
<td>19</td>
<td>2, 3, 14</td>
<td>$\neq$ 1</td>
<td>13</td>
</tr>
<tr>
<td>3, 10</td>
<td>$\neq$ 1</td>
<td>9</td>
<td>4, 6, 9</td>
<td>$\neq$ 1</td>
<td>21</td>
</tr>
<tr>
<td>4, 9</td>
<td>$\neq$ 1</td>
<td>21</td>
<td>5, 16, 17</td>
<td>$\neq$ 1</td>
<td>27</td>
</tr>
<tr>
<td>6, 7</td>
<td>$\neq$ 1</td>
<td>7</td>
<td>10, 13, 15</td>
<td>$\neq$ 1</td>
<td>19</td>
</tr>
</tbody>
</table>

Lemma 3.7. Let $g$ be a primitive root modulo $p$. If $p \equiv 1 \pmod{6}$, then $\#E_0^g(\mathbb{F}_p) \not\equiv 0 \pmod{3}$.

Proof. By Proposition 1.4, if $3x^4 + 6Ax^2 + 12Bx - A^2$ is congruent to 0 modulo $p$, then $P = (x, y)$ is a point of order 3 in $E_0^g(\mathbb{F}_p)$. That is, $\#E_0^g \equiv 0 \pmod{3}$. We will show that there is no point $P = (x, y) \in E_0^g(\mathbb{F}_p)$ satisfying $3P = O$.

Now, we assume that $3x^4 + 6Ax^2 + 12Bx - A^2 = 3x^4 + 12g^4x + 3x(x^3 + 4g) \equiv 0 \pmod{p}$. Hence, we can check two cases, that is, $x \equiv 0 \pmod{p}$ and $x^3 + 4g \equiv 0 \pmod{p}$.

First, we consider the case that such a point $P = (x, y)$ exists when $x \equiv 0 \pmod{p}$. Let $P = (0, y_2)$. Since $(\frac{y_2}{p}) = -1$, there is no point $P = (0, y_2)$ in $E_0^g(\mathbb{F}_p)$ such that $y_2^2 = g$. Thus $\#E_0^g \not\equiv 0 \pmod{3}$.

Second, let $a_1 = 0, a_2 = 0, a_3 = 4g$ by Lemma 1.5, then $D = -(27 \cdot (4g)^3) = \frac{(-27 \cdot 4g^2}{p} = \frac{(-3)}{p} = \frac{(-1)}{p}$. Therefore, if $p \equiv 1 \pmod{6}$, then $\left(\frac{D}{p}\right) = 1$ and $N_p(x^3 + 4g) = 0$ or 3. Assume that $N_p(x^3 + 4g) = 3$, that is, there exists a point $Q = (x_2, y_2) \in E_0^g(\mathbb{F}_p)$
The number of points on elliptic curves $E_{a0}^3 : y^2 = x^3 + a^3$ over $\mathbb{F}_p$ mod 24 447 satisfying $x_2^3 + 4g \equiv 0 \pmod{p}$. Then $x_2^3 + g = -4g + g = -3g$ and $\left(-\frac{3g}{p}\right) = -1$.

So, if $p \equiv 1 \pmod{6}$, then there does not exist a point $(x_2, y_2) \in E_{a0}^3(\mathbb{F}_p)$. Therefore, for a prime $p$ congruent to 1 modulo 6, we get $\#E_{a0}^3 \not\equiv 0 \pmod{3}$.

**Proposition 3.8** ([PPK1], [PPK2]). Let $B = \{E_{a0}^b : y^2 = x^3 + b, 1 \leq b \leq p - 1\}$. If $p \equiv 1 \pmod{6}$, then there are six isomorphism classes of elliptic curves in $B$, i.e.,

- $E_{a0}^1 : y^2 = x^3 + 1$,
- $E_{a0}^3 : y^2 = x^3 + g$,
- $E_{a0}^4 : y^2 = x^3 + g^4$,
- $E_{a0}^5 : y^2 = x^3 + g^5$.

**Lemma 3.9.** If $a$ is not a quadratic non-residue modulo $p$ with $p \equiv 1 \pmod{6}$, then $\#E_{a0}^3(\mathbb{F}_p) \not\equiv 0 \pmod{3}$.

**Proof.** By Proposition 3.8, we only consider three cases, that is, $a = g$, $g^3$, $g^5$, where $g$ is a primitive root modulo $p$. And by Lemma 3.7, if $a = g$, then it is clear. Similarly, it is clear when $a = g^3$ and $g^5$. \qed

**Proposition 3.10** ([SDIC]). Let $p$ be a prime. If $(p - 1, 3) = 1$, then the congruence $x^3 \equiv a \pmod{p}$ has a solution for each $a \in \mathbb{F}_p$, that is, $a$ is a cubic residue in $\mathbb{F}_p$.

**Theorem 3.11.** For elliptic curves $E_{b0}^b : y^2 = x^3 + b$ over $\mathbb{F}_p$ where $b$ is cubic non-residue in $\mathbb{F}_p^*$, If $p \equiv 1 \pmod{6}$, then the following table is satisfied.

<table>
<thead>
<tr>
<th>$(\frac{b}{p})$</th>
<th>$#E_{b0}^b(\mathbb{F}_p)$</th>
</tr>
</thead>
<tbody>
<tr>
<td>$1$</td>
<td>$\equiv 3 \pmod{6}$</td>
</tr>
<tr>
<td>$-1$</td>
<td>$\equiv 1, 5 \pmod{6}$</td>
</tr>
</tbody>
</table>

**Proof.** By Proposition 3.10, if $b$ is a cubic non-residue for some $b \in \mathbb{F}_p$, then $p = 3k + 1$ for some $k \in \mathbb{Z}$, that is, $p \equiv 1 \pmod{6}$. By Lemma 3.1, Lemma 3.5 and Lemma 3.9, the table is satisfied. \qed

**Example 3.12.** For elliptic curves $E_{b0}^b : y^2 = x^3 + b$ over $\mathbb{F}_p$ where $b$ is cubic non-residue in $\mathbb{F}_p^*$, we compute the number of points on $E_{b0}^b$ for each $b \in \mathbb{F}_p$ and for $p = 13$ and $p = 19$ as follows.
Soonho You, Hwasin Park And Hyun Kim

\[
\begin{array}{|c|c|c|c|}
\hline
b & \left( \frac{b}{13} \right) & \left( \frac{b}{19} \right) & \#E_0^{\text{tr}}(\mathbb{F}_{13}) \\
\hline
3, 10 & -1 & 1 & 9 \\
4, 9 & -1 & 1 & 21 \\
2, 11 & -1 & -1 & 19 \\
6, 7 & -1 & -1 & 7 \\
1, 12 & 1 & 1 & 12 \\
5, 8 & 1 & -1 & 16 \\
\hline
b & \left( \frac{b}{19} \right) & \#E_0^{\text{tr}}(\mathbb{F}_{19}) \\
\hline
4, 6, 9 & -1 & 1 & 21 \\
5, 16, 17 & -1 & 1 & 27 \\
2, 3, 14 & -1 & -1 & 13 \\
10, 13, 15 & -1 & -1 & 19 \\
1, 7, 11 & 1 & 1 & 12 \\
8, 12, 18 & 1 & -1 & 28 \\
\hline
\end{array}
\]

References


[DISC] Demirci, M., Ikikardes, Y. N., Soydan, G., Cangul, I. N., Frey Elliptic Curves \( E : y^2 = x^3 - n^2x \) on finite field \( \mathbb{F}_p \) where \( p \equiv 1 \) (mod 4) is prime, to be printed.

[DSC] Demirci, M., Soydan, G., Cangul, I. N., Rational points on Elliptic Curves \( E : y^2 = x^3 + a^3 \) in \( \mathbb{F}_p \) where \( p \equiv 1 \) (mod 4) is prime, Rocky Mountain Journal of Mathematics, 37, no 5, 2007.


The number of points on elliptic curves $E_0^a : y^2 = x^3 + a^3$ over $\mathbb{F}_p \mod 2449$


