Honam Mathematical J. **34** (2012), No. 1, pp. 093–101
http://dx.doi.org/10.5831/HMJ.2012.34.1.93

THE NUMBER OF POINTS ON ELLIPTIC CURVES $E_A^0 : y^2 = x^3 + Ax$ OVER $\mathbb{F}_p$ MOD 24

Hwasin Park, Soonho You, Daeyeoul Kim and Minhee Kim

Abstract. Let E_A^B denote the elliptic curve $E_A^B : y^2 = x^3+Ax+B$. In this paper, we calculate the number of points on elliptic curves $E_A^0 : y^2 = x^3 + Ax$ over $\mathbb{F}_p$ mod 24. For example, if $p \equiv 1 \pmod{24}$ is a prime, $3t^2 \equiv 1 \pmod{p}$ and $A(-1 + 2t)$ is a quartic residue modulo p, then the number of points in $E_A^0 : y^2 = x^3 + Ax$ is congruent to 0 modulo 24.

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 [Si]. 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 $E_A^0 : y^2 = x^3 + Ax$ 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 this article, we derive a type of generalization of their results ([PKL], [ISDBC]) by means of elliptic curves mod 24.

Received December 29, 2011. Accepted February 7, 2012.
2000 Mathematics Subject Classification. 11A15, 11G07.
Key words and phrases. elliptic curves.

2. The number of points on elliptic curves E_A^0 : $y^2 = x^3 + Ax$ over $\mathbb{F}_p$ mod 24

Let p be a prime, and let t be an element of $\mathbb{F}_p^* = \mathbb{F}_p - \{0\}$ such that $3t^2 \equiv 1 \pmod{p}$. Then such an element t exists when $p \equiv 1, 11 \pmod{12}$. Now, for simplicity we set

q_4: quartic residue in $\mathbb{F}_p$,

q_2: quadratic residue but quartic non-residue in $\mathbb{F}_p$,

q_1: quadratic non-residue in $\mathbb{F}_p$ and

$\left(\frac{a}{p}\right)_3 = 1$ if $x^3 \equiv a \pmod{p}$ is solvable.

Theorem 2.1. 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	$-1 \pm 2t$	$A(-1 \pm 2t)$	$\#E_A^0(\mathbb{F}_p)$
$1 \pmod{24}$	q_4	q_4	q_4	$0 \pmod{24}$
	q_4	q_2	q_2	8 *or* $16 \pmod{24}$
	q_4	q_1	q_1	8 *or* $16 \pmod{24}$
	q_2	q_2	q_4	$12 \pmod{24}$
	q_2	q_4	q_2	4 *or* $20 \pmod{24}$
	q_2	q_1	q_1	4 *or* $20 \pmod{24}$
	q_1	q_1	q_4	$18 \pmod{24}$
	q_1	q_1	q_2	2 *or* $10 \pmod{24}$
	q_1	q_4	q_1	2 *or* $10 \pmod{24}$
	q_1	q_2	q_1	2 *or* $10 \pmod{24}$
$11 \pmod{24}$			*all*	$12 \pmod{24}$
$13 \pmod{24}$	q_4	q_4	q_4	$12 \pmod{24}$
	q_4	q_2	q_2	4 *or* $20 \pmod{24}$
	q_4	q_1	q_1	4 *or* $20 \pmod{24}$
	q_2	q_2	q_4	$0 \pmod{24}$
	q_2	q_4	q_2	8 *or* $16 \pmod{24}$
	q_2	q_1	q_1	8 *or* $16 \pmod{24}$
	q_1	q_1	q_4	$18 \pmod{24}$
	q_1	q_1	q_2	2 *or* $10 \pmod{24}$
	q_1	q_4	q_1	2 *or* $10 \pmod{24}$
	q_1	q_2	q_1	2 *or* $10 \pmod{24}$
$23 \pmod{24}$			*all*	$0 \pmod{24}$

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

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

To prove this theorem, we need the following propositions and lemmas.

Proposition 2.2 ([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 $E_A^0 : y^2 = x^3 + Ax$ is an elliptic curve over $\mathbb{F}_p$, then $\#E_A^0 = p + 1$.
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 $\#E_0^B = p + 1$.

By Proposition 2.2 (2), if $p \equiv 7, 11 \pmod{12}$ is a prime and $E_A^0 : y^2 = x^3 + Ax$ is an elliptic curve over $\mathbb{F}_p$ then $\#E_A^0 = p + 1$. So, we consider the elliptic curve $E_A^0 : y^2 = x^3 + Ax$ when $p \equiv 1, 5 \pmod{12}$.

Proposition 2.3 ([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 infinity, where $E_A^B(\mathbb{F}_p)$ is the group of points on E. Then the followings are equivalent*

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

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

Lemma 2.4. *If $p > 3$ is a prime, a_1, a_2, $a_3 \in \mathbb{Z}$ and $p \nmid D$, then*

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

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

Proposition 2.5 ([IR]). *Let p and q be odd primes. Then the followings are satisfied.*

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

Proposition 2.6 ([ISDBC],[PKL]). *If p is a prime, then when $p \equiv 1 \pmod 8$,*

$$\#E_A^0 = \begin{cases} 0 \pmod 8 & \text{if } A \text{ is a quartic residue in } \mathbb{F}_p \\ 4 \pmod 8 & \text{if } A \text{ is quadratic residue but quartic non-residue in } \mathbb{F}_p \\ 2 \pmod 8 & \text{if } A \text{ is quadratic non-residue in } \mathbb{F}_p \end{cases}$$

and when $p \equiv 5 \pmod 8$,

$$\#E_A^0 = \begin{cases} 4 \pmod 8 & \text{if } A \text{ is a quartic residue in } \mathbb{F}_p \\ 0 \pmod 8 & \text{if } A \text{ is quadratic residue but quartic non-residue in } \mathbb{F}_p \\ 2 \pmod 8 & \text{if } A \text{ is quadratic non-residue in } \mathbb{F}_p. \end{cases}$$

Example 2.7. *Let $p = 5$. Then we get the following.*

A	q_i	$\#E_A^0(\mathbb{F}_5)$
1	q_4	4
2	q_1	2
3	q_1	10
4	q_2	8

Now, we will give the results concerning $\#E_A^0$ over $\mathbb{F}_p$ modulo 3.

Lemma 2.8. *Let $E_A^0 : y^2 = x^3 + Ax$ be an elliptic curve over $\mathbb{F}_p$. If $\left(\frac{3}{p}\right) = -1$, then $\#E_A^0 \not\equiv 0 \pmod 3$.*

Proof. Assume that $\#E_A^0 \equiv 0 \pmod 3$. Then there exists a point $P = (x, y) \in E_A^0(\mathbb{F}_p)$ satisfying $3P = O$. By Proposition 2.3, we deduce that $f(x) = 3x^4 + 6Ax^2 - A^2 \equiv 0 \pmod p$, and hence $3(x^2 + A)^2 \equiv 4A^2 \pmod p$. We easily check that $\left(\frac{(x^2+A)^2}{p}\right) = \left(\frac{4}{p}\right) = \left(\frac{A^2}{p}\right) = 1$, and $\left(\frac{3}{p}\right) = -1$ by assumption. It is a contradiction. So, $\#E_A^0 \not\equiv 0 \pmod 3$. □

Corollary 2.9. *Let $E_A^0 : y^2 = x^3 + Ax$ be an elliptic curve over $\mathbb{F}_p$. If $p \equiv 5, 7 \pmod{12}$ are primes, then $\#E_A^0 \not\equiv 0 \pmod 3$.*

Proof. Since $\left(\frac{3}{5}\right) = \left(\frac{3}{7}\right) = -1$, we derive that $\#E_A^0 \not\equiv 0 \pmod 3$, by Lemma 2.8.

□

Example 2.10. *Let* $p = 7$.
If $A = 1$, *then* $\#E_1^0 : y^2 = x^3 + x = 16 \not\equiv 0 \pmod 3$.
If $A = 2$, *then* $\#E_2^0 : y^2 = x^3 + 2x = 20 \not\equiv 0 \pmod 3$.

If $p \equiv 5, 7 \pmod{12}$, then $\left(\frac{3}{p}\right) = -1$ and $3t^2 \not\equiv 1 \pmod p$. Now, we will consider the cases when $p \equiv 1, 11 \pmod{12}$.

Lemma 2.11. *Let* $3t^2 \equiv 1 \pmod p$ *with* $t \in \mathbb{F}_p$. *Then*

$$\left(\frac{-1+2t}{p}\right) = \begin{cases} \left(\frac{-1-2t}{p}\right) & if\ \ p \equiv 1 \pmod{12} \\ -\left(\frac{-1-2t}{p}\right) & if\ \ p \equiv 11 \pmod{12}. \end{cases}$$

Proof. Since $\left(\frac{-1+2t}{p}\right)\left(\frac{-1-2t}{p}\right) = \left(\frac{1-4t^2}{p}\right) = \left(\frac{1-3t^2-t^2}{p}\right) = \left(\frac{-t^2}{p}\right) = \left(\frac{-1}{p}\right)\left(\frac{t^2}{p}\right) = \left(\frac{-1}{p}\right)$, we get the result by Proposition 2.5 (1). □

Lemma 2.12. *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* $\mathbb{F}_p$.

Proof. Assume that $-A \pm 2tA$ are quartic residues in $\mathbb{F}_p$.

Let $x^2 \equiv -A \pm 2tA \pmod p$, where x is a quadratic residue in $\mathbb{F}_p$. Also, we have $x^2 + A \equiv \pm 2tA \pmod p$ and $(x^2+A)^2 \equiv t^2(2A)^2 \pmod p$. It follows from $3t^2 \equiv 1 \pmod p$ and $3(x^2 + A)^2 \equiv 4A^2 \pmod p$ that

$$3x^4 + 6Ax^2 - A^2 \equiv 0 \pmod p. \tag{2.0.1}$$

Here, we put $f(x) = 3x^4 + 6Ax^2 - A^2$. Since $3t^2 \equiv 1 \pmod p$, $\left(\frac{2t}{p}\right)\left(\frac{2t-1}{p}\right) = \left(\frac{4t^2-2t}{p}\right) = \left(\frac{t^2-2t+3t^2}{p}\right) = \left(\frac{t^2-2t+1}{p}\right) = \left(\frac{(t-1)^2}{p}\right) = 1$. That is, $\left(\frac{2t}{p}\right) = \left(\frac{2t-1}{p}\right)$. Similarly, $\left(\frac{-2t}{p}\right) = \left(\frac{-2t-1}{p}\right)$. Since $x^2 \equiv -A \pm 2tA \pmod p$, $\left(\frac{-1\pm 2t}{p}\right) = \left(\frac{A}{p}\right)$. By Lemma 2.11 we know that $\left(\frac{-1+2t}{p}\right) = \left(\frac{-2t-1}{p}\right) = \left(\frac{2t}{p}\right) = \left(\frac{-2t}{p}\right) = \left(\frac{A}{p}\right)$. So we deduce that

$$\left(\frac{\pm 2tA}{p}\right) = 1. \tag{2.0.2}$$

Therefore, there exists a point $P(x,y)$ in $E_A^0 : y^2 = x^3 + Ax = x(x^2 + A) = x(\pm 2tA)$ such that $f(x) \equiv 0 \pmod p$, because x and $\pm 2tA$ are quadratic residues in $\mathbb{F}_p$. That is, $\#E_A^0 : y^2 = x^3 + Ax \equiv 0 \pmod 3$ by Proposition 2.3.

Conversely, we assume that $\#E_A^0 : y^2 = x^3 + Ax \equiv 0 \pmod 3$. We first consider the case where $-A \pm 2tA$ are quartic non-residues in $\mathbb{F}_p$. Since $\#E_A^0 : y^2 = x^3 + Ax \equiv 0 \pmod 3$, $3x^4 + 6Ax^2 - A^2 \equiv 0 \pmod p$, by Proposition 2.3. Then, $x^2 \equiv -A \pm 2tA \pmod p$ by (2.0.1).

Now, if $-A \pm 2tA$ are quadratic non-residues in $\mathbb{F}_p$, then there does not exist a point $P(x,y)$ of $E_A^0 : y^2 = x^3 + Ax$ such that $f(x) \equiv 0 \pmod p$. Finally, if $-A \pm 2tA$ are quadratic residues but quartic non-residues in $\mathbb{F}_p$, then x is a quadratic non-residue. And since $\pm 2tA$ are quadratic residues in $\mathbb{F}_p$ by (2.0.2), $x(\pm 2tA)$ are quadratic non-residues in $\mathbb{F}_p$. Consequently, there does not exist a point $P(x,y)$ of $E_A^0 : y^2 = x^3 + Ax$ such that $f(x) \equiv 0 \pmod p$. Therefore, if $-A \pm 2tA$ are quartic non-residues in $\mathbb{F}_p$, then $\#E_A^0 : y^2 = x^3 + Ax \not\equiv 0 \pmod 3$. □

Example 2.13. *Let $p = 13$. Then roots of $3t^2 \equiv 1 \pmod{13}$ are $t = \pm 3$ and $-1 \pm 2t = 5,\ 6$. Then we get the following table.*

A	$-A \pm 2tA$	$\#E_A^0(\mathbb{F}_{13})$
$7, 8, 11$	q_4	*18*
$2, 5, 6$	q_2	*10*
$1, 3, 9$	q_1	*20*
$4, 10, 12$	q_1	*8*

And let $p = 37$. Then roots of $3t^2 \equiv 1 \pmod{37}$ are $t = \pm 5$ and $-1 \pm 2t = 9,\ 26$. Then we get the following table.

A	$-A \pm 2tA$	$\#E_A^0(\mathbb{F}_{37})$
$1, 7, 9, 10, 12, 16, 26, 33, 34$	q_4	*36*
$3, 4, 11, 21, 25, 27, 28, 30, 36$	q_2	*40*
$5, 6, 8, 13, 17, 19, 22, 23, 35$	q_1	*26*
$2, 14, 15, 18, 20, 24, 29, 31, 32$	q_1	*50*

Corollary 2.14. *Let $p \equiv 1 \pmod{12}$ be a prime and let $3t^2 \equiv 1 \pmod p$ with $t \in \mathbb{F}_p^*$. And let g be a primitive root modulo p.*

1. *If $-1 \pm 2t$ is a quartic residue in $\mathbb{F}_p$, then*
   $\#E_1^0 : y^2 = x^3 + x \equiv 0 \pmod 3$ *and* $\#E_{g^2}^0 : y^2 = x^3 + g^2 x \not\equiv 0 \pmod 3$.
2. *If $-1 \pm 2t$ is a quadratic residue but quartic non-residue in $\mathbb{F}_p$, then*

$\#E_1^0 : y^2 = x^3 + x \not\equiv 0 \pmod 3$ and $\#E_{g^2}^0 : y^2 = x^3 + g^2x \equiv 0 \pmod 3$.

Proof. First, let $-1 \pm 2t$ be a quartic residue in $\mathbb{F}_p$. Since $A = 1$ is a quartic residue in $\mathbb{F}_p$, $1 \cdot (-1 \pm 2t) = -1 \pm 2t$ is a quartic residue. By Lemma 2.12, $\#E_1^0 : y^2 = x^3 + x \equiv 0 \pmod 3$. And $g^2 \cdot (-1 \pm 2t)$ is a quadratic residue but quartic non-residue in $\mathbb{F}_p$. So $\#E_{g^2}^0 : y^2 = x^3 + g^2x \not\equiv 0 \pmod 3$.

Secondly, let $-1 \pm 2t$ be a quadratic residue but quartic non-residue in $\mathbb{F}_p$. Since $1 \cdot (-1 \pm 2t) = -1 \pm 2t$ is a quadratic residue but quartic non-residue in $\mathbb{F}_p$, $\#E_1^0 : y^2 = x^3 + x \not\equiv 0 \pmod 3$. And $g^2 \cdot (-1 \pm 2t)$ is a quartic residue in $\mathbb{F}_p$. So $\#E_{g^2}^0 : y^2 = x^3 + g^2x \equiv 0 \pmod 3$. □

Proof of Theorem 2.1

By Proposition 2.2, Proposition 2.6, Corollary 2.9 and Lemma 2.12, the proof of Theorem 2.1 is complete.

Example 2.15. *Let $p = 7$, then $\#E_A^0(\mathbb{F}_7) = 8$ for all $A \in \mathbb{F}_7$ is as the following table.*

A	$E_A^0(F_7)$
1	$O, (0,0), (1,3), (1,4), (3,3), (3,4), (5,2), (5,5)$
2	$O, (0,0), (4,3), (4,4), (5,3), (5,4), (6,2), (6,5)$
3	$O, (0,0), (1,2), (1,5), (2,0), (3,1), (3,6), (5,0)$
4	$O, (0,0), (2,3), (2,4), (3,2), (3,5), (6,3), (6,4)$
5	$O, (0,0), (2,2), (2,5), (3,0), (4,0), (6,1), (6,6)$
6	$O, (0,0), (1,0), (4,2), (4,5), (5,1), (5,6), (6,0)$

References

[C] H. Cohen, *A Course in Computational Algebraic Number Theory,* Grad. Texts in Math., 138, Springer-verlag, Berlin, 1993, 198-199.

[D] L. E. Dickson, *Criteria for the irreducibility of functions in a finite field,* Bull. Amer. Math. Soc. 13(1906), 1-8.

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

[DSC] 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 $p \equiv 1 \pmod 4$ is prime,* Rocky Mountain Journal of Mathematics, 37, no 5, 2007.

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

[ISDBC] 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.

[ISDC] N. Y. Ikikardes, G. Soydan, M. Demirci and I. N. Cangul, *Classification of the Bachet Elliptic Curves* $y^2 = x^3 + a^3$ *in* $\mathbb{F}_p$*, where* $p \equiv 1 \pmod 6$ *is Prime,* Int. J. Math. Sci. (WASET) 1 (2007), no. 4, 239-241.

[ISDC2] N. Y. Ikikardes, G. Soydan, M. Demirci 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.

[K] A. W. Knapp, *Elliptic curves*, Princeton Uinversity Press, New Jersey 1992.

[KKP] D. Kim, J. K. Koo and Y. K. Park, *On the elliptic curve modulo p,* Journal of Number Theory 128(2008), 945-953.

[PKL] H. Park, D. Kim and E. Lee, *The numbers of points elliptic curves* $E : y^2 = x^3 + cx$ *over* $\mathbb{F}_p$ *mod 8,* Commun. Korean Math. Soc. 18 (2003), 31-37.

[S] R. Schoof, *Counting points on elliptic curves over finite fields,* Journal de Theorie des Nomvres de Bordeaux, 7(1995), 219-254.

[Si] J. H. Silverman, *The arithmetic of elliptic curves,* Graduate Texts in Mathematics, 106. Springer-Verlag, New York, 1992.

[St] L. Stickelberger, *Uber eine neue Eigenschaft der Diskriminanten algebraischer Zahlkorper,* in:Verh. I. Internat. Math. Kongress, Zurich, 1987, 182-193.

H. S. Park
Department of Mathematics, Chonbuk National University,
Chonju 561-756, Korea.
E-mail: park@jbnu.ac.kr

S. H. You
Department of Mathematics, Chonbuk National University,
Chonju 561-756, Korea.
E-mail: m2zzang@hanmail.net

D. Y. Kim
Division of Fusion and Convergence of Mathematical Sciences, National Institute for Mathematical Sciences,
Dajeon 305-390, Korea.
E-mail: daeyeoul@nims.re.kr

M. H. Kim
Department of Mathematics, Chonbuk National University,

Chonju 561-756, Korea.
E-mail: minabout@hanmail.net