Commun. Korean Math. Soc. **18** (2003), No. 1, pp. 31–37

# THE NUMBER OF POINTS ON ELLIPTIC CURVES $E : y^2 = x^3 + cx$ OVER $\mathbb{F}_p$ MOD 8

HWASIN PARK, DAEYEOUL KIM AND EUNHEE LEE

ABSTRACT. In this paper, we calculate the number of points on elliptic curves $y^2 = x^3 + cx$ over $\mathbb{F}_p$ mod 8.

## 1. Introduction

The purpose of this paper is to give a straightforward proof of the number of points on elliptic curves over finite field mod 8. For a rational prime $p$, let $\mathbb{F}_p$ be the finite field of $p$ elements. Let $E : y^2 = x^3 + cx$ be an elliptic curve over $\mathbb{F}_p$ and let $\#E$ be the number of points on this elliptic curve over $\mathbb{F}_p$. We let $p \equiv 1 \pmod 4$ and $\pi = m + ni$ be a prime in $\mathbb{Z}[i]$ satisfying $p = \pi\overline{\pi}$, $\pi \equiv 1 \pmod{2+2i}$. One find the number of points on $E : y^2 = x^3 + cx$ over $\mathbb{F}_p$ ([1], [3], [4], [5], [6], [7], [10]). In this paper, without employing the condition $p = \pi\overline{\pi}$, we compute the number of points on the same elliptic curves mod 8.

We prove the following:

THEOREM 1. *If $p \equiv 1, 5 \pmod 8$ is a rational prime then*

$$\#E \equiv \begin{cases} 0 \pmod 8 & \text{if } c \text{ is a quartic residue in } \mathbb{F}_p \\ 4 \pmod 8 & \text{if } c \text{ is a quadratic residue but quartic non-residue} \\ & \quad \text{in } \mathbb{F}_p \\ 2 \pmod 8 & \text{if } c \text{ is a quadratic non-residue in } \mathbb{F}_p. \end{cases}$$

Only using elementary number theory, for example, the definition of Legendre symbol and Wilson's theorem, etc., we prove Theorem 1. In [8], by supersingular curve theory, we easily show that

$$\text{if} \quad p \equiv 3, 7 \pmod 8 \quad \text{then} \quad \#E = p + 1.$$

Received February 10, 2000.
2000 Mathematics Subject Classification: 11A07, 14H52.
Key words and phrases: congruences, the number of points of elliptic curves over finite fields.

To prove Main theorem, we need the following proposition and corollary.

## 2. Preliminary

PROPOSITION 2.1. ([4]) *Let $p$ be an odd rational prime. Then*

$$\sum_{y=0}^{p-1}\left(\frac{y^2+c}{p}\right)=\begin{cases}-1 & \text{if } c\not\equiv 0 \pmod p,\\ p-1 & \text{if } c\equiv 0 \pmod p.\end{cases}$$

From this proposition, we get the following.

COROLLARY 2.2. *Let $c$ be a quadratic non-residue in $\mathbb{F}_p$. Then*

$$\prod_{i=1}^{\frac{p-1}{2}}\left(\frac{i^2+c}{p}\right)=\begin{cases}+1 & \text{if } p\equiv 1 \pmod 8,\\ -1 & \text{if } p\equiv 5 \pmod 8.\end{cases}$$

PROOF. By Proposition 2.1,

$$\sum_{i=0}^{p-1}\left(\frac{i^2+c}{p}\right)=\left(\frac{c}{p}\right)+2\sum_{i=1}^{\frac{p-1}{2}}\left(\frac{i^2+c}{p}\right)=-1.$$

Since $\left(\frac{c}{p}\right)=-1$, $\sum_{i=1}^{\frac{p-1}{2}}\left(\frac{i^2+c}{p}\right)=0$.

Thus by $\sum_{i=1}^{\frac{p-1}{2}}\left(\frac{i^2+c}{p}\right)=0$, we conclude that $\#\{1\le i\le\frac{p-1}{2}|\left(\frac{i^2+c}{p}\right)=1\}=\#\{1\le i\le\frac{p-1}{2}|\left(\frac{i^2+c}{p}\right)=-1\}$. This completes the proof of corollary. □

## 3. Proof of Theorem 1

PROOF OF THEOREM 1. Let $c$ be a quadratic non-residue in $\mathbb{F}_p$. If $x^3+cx\not\equiv 0 \pmod p$ is a quadratic residue, then $-x^3-cx$ is also a quadratic residue because $\left(\frac{-1}{p}\right)=1$. And we obtain that $E[2]=\{O,(0,0)\}$, where $E[m]=\{P\in E(\mathbb{F}_p): mP=O\}$ with $O$ the infinity point. Thus if $\prod_{i=1}^{\frac{p-1}{2}}\left(\frac{i}{p}\right)\left(\frac{i^2+c}{p}\right)=1$(respectively, $-1$) then the

number of $i$'s satisfying $\left(\frac{i}{p}\right)\left(\frac{i^2+c}{p}\right) = 1$ with $1 \leq i \leq \frac{p-1}{2}$ is an even(resp., odd) integer. From this, we derive that $\#E \equiv 2 \pmod 8$ (respectively, $\#E \equiv 6 \pmod 8$) becasuse $\#E[2] = 2$.

Let $p \equiv 1 \pmod 8$. By Wilson's theorem, we have $(p-1)! \equiv (-1)^{\frac{p-1}{2}} \left(\frac{p-1}{2}!\right)^2 \equiv -1 \equiv g^{\frac{p-1}{2}} \pmod p$ where $g$ is a primitive root modulo $p$. Then

$$\prod_{i=1}^{\frac{p-1}{2}} \left(\frac{i}{p}\right) = \left(\frac{\frac{p-1}{2}!}{p}\right) = 1, \tag{3.1}$$

since $\frac{p-1}{2}! \equiv \pm g^{\frac{p-1}{4}} \equiv \pm g^{2k}$. By Corollary 2.2 and (3.1) we see that

$$\prod_{i=1}^{\frac{p-1}{2}} \left(\frac{i}{p}\right)\left(\frac{i^2+c}{p}\right) = \prod_{i=1}^{\frac{p-1}{2}} \left(\frac{i}{p}\right) \prod_{i=1}^{\frac{p-1}{2}} \left(\frac{i^2+c}{p}\right) = \prod_{i=1}^{\frac{p-1}{2}} \left(\frac{i^2+c}{p}\right) = 1. \tag{3.2}$$

Let $p \equiv 5 \pmod 8$ and $c$ a quadratic nonresidue in $\mathbb{F}_p$. Similarly, we get

$$\prod_{i=1}^{\frac{p-1}{2}} \left(\frac{i}{p}\right) = \left(\frac{\frac{p-1}{2}!}{p}\right) = -1, \tag{3.3}$$

since $(\frac{p-1}{2})! \equiv \pm g^{\frac{p-1}{4}} \equiv \pm g^{2k+1}$.

From Corollary 2.2 and (3.3), we deduce

$$\prod_{i=1}^{\frac{p-1}{2}} \left(\frac{i}{p}\right)\left(\frac{i^2+c}{p}\right) = 1. \tag{3.4}$$

By (3.2) and (3.4), we derive that $\#E \equiv 2 \pmod 8$. If $c$ is a quadratic nonresidue then we get the conclusion.

Now let $p \equiv 1 \pmod 8$ and $c$ be a quadratic residue in $\mathbb{F}_p$. Then there exists $1 \leq \alpha \leq \frac{p-1}{2}$ such that $c \equiv -\alpha^2 \pmod p$. We can compute

$$\prod_{\substack{i=1 \\ i \neq \alpha}}^{\frac{p-1}{2}} \left(\frac{i}{p}\right)\left(\frac{i^2+c}{p}\right) = \prod_{\substack{i=1 \\ i \neq \alpha}}^{\frac{p-1}{2}} \left(\frac{i}{p}\right) \prod_{\substack{i=1 \\ i \neq \alpha}}^{\frac{p-1}{2}} \left(\frac{i^2+c}{p}\right).$$

Let $\alpha^*$ be an arithmetic inverse of $\alpha \pmod p$. By (3.1) then we get

$$\prod_{\substack{i=1\\ i\neq\alpha}}^{\frac{p-1}{2}} \left(\frac{i}{p}\right) = \left(\frac{\alpha^*}{p}\right) \prod_{i=1}^{\frac{p-1}{2}} \left(\frac{i}{p}\right) = \left(\frac{\alpha^*}{p}\right) = \left(\frac{\alpha}{p}\right). \tag{3.5}$$

Also, we derive

$$\begin{aligned}
&\prod_{\substack{i=1\\ i\neq\alpha}}^{\frac{p-1}{2}} \left(\frac{i^2+c}{p}\right) \\
&= \prod_{\substack{i=1\\ i\neq\alpha}}^{\frac{p-1}{2}} \left(\frac{i^2-\alpha^2}{p}\right) = \prod_{\substack{i=1\\ i\neq\alpha}}^{\frac{p-1}{2}} \left(\frac{\alpha^2-i^2}{p}\right)\left(\frac{-1}{p}\right) \\
&= \prod_{\substack{i=1\\ i\neq\alpha}}^{\frac{p-1}{2}} \left(\frac{\alpha^2-i^2}{p}\right) = \prod_{\substack{i=1\\ i\neq\alpha}}^{\frac{p-1}{2}} \left(\frac{\alpha+i}{p}\right) \prod_{\substack{i=1\\ i\neq\alpha}}^{\frac{p-1}{2}} \left(\frac{\alpha-i}{p}\right) \\
&= \left(\frac{\alpha^*}{p}\right)\left(\frac{(2\alpha)^*}{p}\right)\left(\left(\frac{2\alpha}{p}\right) \prod_{\substack{i=1\\ i\neq\alpha}}^{\frac{p-1}{2}} \left(\frac{\alpha+i}{p}\right)\right) \\
&\quad \times \left(\left(\frac{\alpha}{p}\right) \prod_{\substack{i=1\\ i\neq\alpha}}^{\frac{p-1}{2}} \left(\frac{\alpha-i}{p}\right)\right) \\
&= \left(\frac{2^*}{p}\right) \prod_{i=1}^{p-1} \left(\frac{i}{p}\right) \\
&= \left(\frac{2}{p}\right).
\end{aligned} \tag{3.6}$$

By $p \equiv 1 \pmod 8$ and (3.6), we see that

$$\prod_{\substack{i=1\\ i\neq\alpha}}^{\frac{p-1}{2}} \left(\frac{i^2+c}{p}\right) = 1. \tag{3.7}$$

It follows from (3.5) and (3.7) that

$$\prod_{\substack{i=1\\ i\neq\alpha}}^{\frac{p-1}{2}} \left(\frac{i}{p}\right)\left(\frac{i^2+c}{p}\right) = \left(\frac{\alpha}{p}\right).$$

If $\left(\frac{\alpha}{p}\right) = 1$( respectively, $-1$), i.e., $c$ is a quartic residue(resp., a quadratic residue but not quartic) in $\mathbb{F}_p$, then the number of $i$'s satisfying $\left(\frac{i^3+ci}{p}\right) = 1$ is an odd(resp., even). So $\#E \equiv 0$ (resp., $\equiv 4 \pmod 8$), since $\#E[2] = 4$. Also, let $p \equiv 5 \pmod 8$ and $c$ a quadratic residue in $\mathbb{F}_p$. Then by (3.3), we come up with

$$\prod_{\substack{i=1\\ i\neq\alpha}}^{\frac{p-1}{2}} \left(\frac{i}{p}\right) = \left(\frac{\alpha^*}{p}\right)\prod_{i=1}^{\frac{p-1}{2}} \left(\frac{i}{p}\right) = -\left(\frac{\alpha}{p}\right). \tag{3.8}$$

Thus we obtain, by (3.7) and (3.8), that

$$\begin{aligned}\prod_{\substack{i=1\\ i\neq\alpha}}^{\frac{p-1}{2}} \left(\frac{i}{p}\right)\left(\frac{i^2+c}{p}\right) &= \prod_{\substack{i=1\\ i\neq\alpha}}^{\frac{p-1}{2}} \left(\frac{i}{p}\right)\prod_{\substack{i=1\\ i\neq\alpha}}^{\frac{p-1}{2}} \left(\frac{i^2+c}{p}\right)\\ &= -\left(\frac{\alpha}{p}\right)\left(\frac{2}{p}\right) = \left(\frac{\alpha}{p}\right),\end{aligned}$$

since $p \equiv 5 \pmod 8$.

Consequently, if $\left(\frac{\alpha}{p}\right) = 1$( resp., $-1$) then the number of $i$'s satisfying $i^3 + ci$ quadratic residue is an odd( resp., even). So $\#E \equiv 0$(resp., $\#E \equiv 4 \pmod 8$). Therefore we prove the theorem. □

## 4. Remarks

Let $h(-d)$ be the class number of the algebraic number field $\mathbb{Q}(\sqrt{-d})$ and let $g$ be a primitive root modulo $p$. Let $T = \{E : y^2 = x^3 + cx, c \in \mathbb{F}_p\}$. If $p \equiv 1 \pmod 4$ is a prime, then the number of isomorphism classes in $T$ is 4 such as $E_1 : y^2 = x^3 + x$, $E_g : y^2 = x^3 + gx$, $E_{g^2}$ :

$y^2 = x^3 + g^2x$ and $E_{g^3} : y^2 = x^3 + g^3x$. This is a special case of a result due to [9]. We also give a direct proof of this. Note that elliptic curves $E_a : y^2 = x^3 + ax$ and $E_{a'} : y^2 = x^3 + a'x$ are isomorphic over $K$ if and only if there exists $u \in K^* = K - \{0\}$ such that $u^4a' = a$ ([8]).

Using $u$, we get $E_a$ is isomorphic to $E_{ag^{4i}}$ for $1 \leq i \leq \frac{p-1}{4}$. This implies that $E_1$, $E_g$, $E_{g^2}$ and $E_{g^3}$ are distinct isomorphism classes in $T$.

Using $p \equiv \pi\overline{\pi}$, $\pi \equiv 1 \pmod{2+2i}$ and main theorem, we get the following remarks:

(a) If $p \equiv 1, 9 \pmod{16}$ be a rational prime. Then

$$\begin{cases} \#E_1 \equiv 0 \pmod{16}, \\ \\ \#E_{g^2} \equiv 4 \pmod{16}, \\ \\ \#E_g \equiv \#E_{g^3} \equiv \begin{cases} 2 \pmod{16} \text{ if and only if } h(-p) \equiv 0 \pmod{8}, \\ \\ 10 \pmod{16} \text{ if and only if } h(-p) \equiv 4 \pmod{8}, \end{cases} \end{cases}$$

for some primitive root $g$ mod $p$. For the last congruence, we see the same result in [2].

(b) If $p \equiv 5, 13 \pmod{16}$ be a rational prime. Then $\#E_1 \equiv 8 \pmod{16}$, $\#E_g \equiv 2 \pmod{16}$, $E_{g^2} \equiv 4 \pmod{16}$ and $\#E_{g^3} \equiv 10 \pmod{16}$ for some primitive root $g$ mod $p$.

## References


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

[2] E. Brown, *The class number of* $\mathbb{Q}(\sqrt{-p})$ *for* $p \equiv 1 (mod\ 8)$, *a prime*, Proc. Amer. Math. Soc. **31** (1972), 381–383.

[3] H. Davenport and H. Hasse, *Die Nullstellen der Kongruenzzetafunktionen in gewissen zyklischen Fallen*, J. Reine Angew. Math. **172** (1934), 151–182.

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

[5] E. Jacobstahl, *Über die Darstellung der Primzahlen der Form* $4n+1$ *als Summe zweier Quadrate*, J. Reine Angew. Math. **132** (1907), 238–245.

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

[7] ———, *Certain classical congruences via elliptic curves*, J. London Math. Soc. **8** (1974), no. 2, 60–62.

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

[9] E. Waterhouse, *Abelian varieties over finite fields*, Ann. Sci. Ecole Norm. Sup. **2** (1969), 521–560.
[10] A. L. Whiteman, *A theorem of Brewer on character sums*, Duke Math. J. **30** (1963), 545–552.

Department of Mathematics
Chonbuk National University
Chonju 561-756, Korea