International Journal of Engineering, Mathematical and Physical Sciences
ISSN: 2517-9934
Vol:1, No:1, 2007

The Number of Rational Points on Elliptic Curves $y^2 = x^3 + a^3$ on Finite Fields

Musa Demirci, Nazlı Yıldız İkikardeş, Gökhan Soydan, İsmail Naci Cangül

***Abstract*—In this work, we consider the rational points on elliptic curves over finite fields $\mathbf{F}_p$. We give results concerning the number of points $N_{p,a}$ on the elliptic curve $y^2 \equiv x^3 + a^3 (mod\, p)$ according to whether a and x are quadratic residues or non-residues. We use two lemmas to prove the main results first of which gives the list of primes for which -1 is a quadratic residue, and the second is a result from [1]. We get the results in the case where p is a prime congruent to 5 modulo 6, while when p is a prime congruent to 1 modulo 6, there seems to be no regularity for $N_{p,a}$.

***Keywords*—Elliptic curves over finite fields, rational points, quadratic residue.

I. Introduction

Let $\mathbf{F}$ be a field of characteristic greater than 3. The study of rational points on elliptic curves

$$y^2 = x^3 + Ax + B \quad (1)$$

over $\mathbf{F}_p$ is very interesting and many mathematicians starting with Gauss have studied them, see ([9],p.68,[12],p.2). In this paper, a special class of these curves, called Bachet elliptic curves, is studied. These are given with the equation

$$y^2 = x^3 + a^3, \quad (2)$$

where a is an element in the field. We fix the number a and let x vary on Q_p or $Q_p^{'}$, where these denote the sets of quadratic residues and non-residues, respectively.

In [6], starting with a conjecture from 1952 of Dénes which is a variant of Fermat-Wiles theorem, Merel illustrates the way in which Frey elliptic curves have been used by Taylor, Ribet, Wiles and the others in the proof of Fermat-Wiles theorem. Serre, in [7], gave a lower bound for the Galois representations on elliptic curves over the field Q of rational points. In the case of a Frey curve, the conductor N of the curve is given by the help of the constants in the abc conjecture. In [5], Ono recalls a result of Euler, known as Euler's concordant forms problem, about the classification of those pairs of distinct non-zero integers M and N for which there are integer solutions (x, y, t, z) with $xy \neq 0$ to $x^2 + My^2 = t^2$ and $x^2 + Ny^2 = z^2$. When $M = -N$, this becomes the congruent number problem, and when $M = 2N$, by replacing x by $x - N$ in $E(2N, N)$, a special form of the Frey elliptic curves is obtained as $y^2 = x^3 - N^2 x$. Using Tunnell's conditional solution to the congruent number problem using elliptic curves and modular forms, Ono studied the elliptic curve $y^2 = x^3 + (M + N)x^2 + MNx$ denoted by $E_Q(M, N)$ over Q. He classified all the cases and hence reduced Euler's problem to a question of ranks. In [3], Parshin obtaines an inequality to give an effective bound for the height of rational points on a curve. In [4], the problem of boundedness of torsion for elliptic curves over quadratic fields is settled.

If F is a field, then an elliptic curve over F has, after a change of variables, a form

$$y^2 = x^3 + Ax + B$$

where A and $B \in F$ with $4A^3 + 27B^2 \neq 0$ in F. Here $D = -16\left(4A^3 + 27B^2\right)$ is called the discriminant of the curve. Elliptic curves are studied over finite and infinite fields. Here we take F to be a finite prime field F_p with characteristic $p > 3$. Then $A, B \in F_p$ and 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 on F_p and is denoted by $E\left(F_p\right)$. N_p denotes the number of rational points on this curve. It must be finite.

In fact one expects to have at most $2p + 1$ points (together with *o)*(for every x, there exist a maximum of 2 $y^{'}$s). But not all elements of F_p have square roots. In fact only half of the elements of F_p have a square root. Therefore the expected number is about $p + 1$.

Here we shall deal with Bachet elliptic curves $y^2 = x^3 + a^3$ modulo p. Some results on these curves have been given in [8], and [11].

A historical problem leading to Bachet elliptic curves is that how one can write an integer as a difference of a square and a cube. In another words, for a given fixed integer c, search for the solutions of the Diophantine equation $y^2 - x^3 = c$. This equation is widely called as Bachet or Mordell equation. This is because L. J. Mordell, in twentieth century, made a lot of advances regarding this and some other similar equations. The existance of duplication formula makes this curve interesting. This formula was found in 1621 by Bachet. When (x, y) is a solution to this equation where $x,\ y \in Q$, it is easy to show that $\left(\frac{x^4 - 8cx}{4y^2},\ \frac{-x^6 - 20cx^3 + 8c^2}{8y^3}\right)$ is also a solution for the same equation. Furthermore, if (x, y) is a solution such that $xy \neq 0$ and $c \neq 1,\ -432$, then this leads to infinitely many solutions, which could not proven by Bachet. Hence if an integer can be stated as the difference of a cube and a square, this could be done in infinitely many ways. For example if

Musa Demirci, Gokhan Soydan and Ismail Naci Cangul are with the Uludag University, Department of Mathematics, Faculty of Science, Bursa-TURKEY, emails: mdemirci@uludag.edu.tr, gsoydan@uludag.edu.tr, cangul@uludag.edu.tr. Nazli Yildiz İkikardes is with the Balikesir University, Department of Mathematics, Faculty of Science, Balkesir-TURKEY. email: nyildiz@balikesir.edu.tr. This work was supported by the research fund of Uludag University project no: F-2004/40 and F-2003/63.

we start by a solution $(3,5)$ to $y^2 - x^3 = -2$, by applying duplication formula, we get a series of rational solutions $(3,5)$, $\left(\frac{129}{10^2}, \frac{-383}{10^3}\right)$, $\left(\frac{2340922881}{7660^2}, \frac{113259286337292}{7660^3}\right)$, ...Let $N_{p,a}$ denote the number of rational points on (2) modulo p. When $p \equiv 1\ (mod\ 6)$, there is no rule for $N_{p,a}$. In this paper, we calculate $N_{p,a}$ when $p \equiv 5\ (mod\ 6)$. First we have

Lemma 1.1: If $p \equiv 5\ (mod\ 12)$, then $-1 \in Q_p$, and if $p \equiv 11\ (mod\ 12)$, then $-1 \in Q_p^{'}$.

II. Calculating $N_{p,a}$ when $p \equiv 5 (mod\, 6)$ is prime.

Theorem 2.1: Let $p \equiv 5\ (mod\ 6)$ be prime and $a \in Q_p$ be fixed. Then for $x \in Q_p$

$$N_{p,a} = \frac{p-3}{2}.$$

Proof: When $x \in Q_p$, it is well-known that

$$N_{p,a} = \sum\nolimits_{x\in Q_p} (1 + \chi(x^3 + a^3))$$

$$= \sum\nolimits_{x\in Q_p} 1 + \sum\nolimits_{x\in Q_p} \chi(x^3 + a^3)$$

$$= \frac{p-1}{2} + \sum\nolimits_{x\in Q_p} \chi(x^3 + a^3)$$

$$= \frac{p-1}{2} + \sum\nolimits_{x\in Q_p} \chi(a^3x^3 + a^3),$$

as the set of a^3x^3's is the same as the set of x^3's when $p \equiv 2\ (mod\ 3)$. Hence using the multiplicativity of χ, we have

$$\begin{aligned} N_{p,a} &= \frac{p-1}{2} + \chi(a^3).\sum\nolimits_{x\in Q_p} \chi(x^3 + 1) \\ &= \frac{p-1}{2} + \sum\nolimits_{x\in Q_p} \chi(x^3 + 1) \end{aligned}$$

as $\chi(a^3) = \chi(a) = 1$ for $a \in Q_p$. Then we only need to show that

$$\sum\nolimits_{x\in Q_p} \chi(x^3 + 1) = -1. \tag{3}$$

Note that, as $x \in Q_p$, x takes $\frac{p-1}{2}$ values between 1 and $p-1$. Therefore we can write (3) as

$$\sum\nolimits_{x\in Q_p}^{p-1} \chi(x^3 + 1) = -1.$$

For $x = p - 1$, $\chi((p-1)^3 + 1) = 0$. Then (3) becomes

$$\sum\nolimits_{x\in Q_p}^{p-2} \chi(x^3 + 1) = -1.$$

First, let $p \equiv 5\ (mod\ 12)$. Then as we can think of p as $p \equiv 2\ (mod\ 3)$, all elemets of $\mathbf{F}_p$ are cubic residues. Therefore the set consisting of the values of x^3 is the same with the set of values of x. Therefore the last eqnarray becomes ∎

$$\sum\nolimits_{x\in Q_p}^{p-2} \chi(x + 1) = -1. \tag{4}$$

Recall that the number of consecutive pairs of quadratic residues in $\mathbf{F}_p$ is given by the formula

$$n_p = \frac{1}{4}(p - 4 - (-1)^{\frac{p-1}{2}}),$$

see ([1], p.128).

There are two cases to consider.

A) Let $p \equiv 1\ (mod\ 4)$. Then by the Chinese reminder theorem we know that $p \equiv 5\ (mod\ 12)$. Here, $-1 \in Q_p$ by lemma 1. Hence

$$n_p = \frac{p-5}{4}. \tag{5}$$

By lemma 1, there are $\frac{p-1}{2} - 1 = \frac{p-3}{2}$ values of x between 1 and $p-2$ lying in Q_p. By (5), $\frac{p-5}{4}$ of the values of $x+1$ are also in Q_p. Finally, in (4), there are $\frac{p-5}{4}$ times $+1$ and $\frac{p-3}{2} - \frac{p-5}{4} = \frac{p-1}{4}$ times -1, implying the result.

B) Let $p \equiv 3\ (mod\ 4)$. Then $-1 \in Q_p^{'}$ and by the Chinese reminder theorem we have $p \equiv 11\ (mod\ 12)$. Similarly to A), we deduce

$$n_p = \frac{p-3}{4}.$$

By lemma 1, there are $\frac{p-1}{2} - 0 = \frac{p-1}{2}$ values of x between 1 and $p-2$ lying in Q_p, as $p - 1 \in Q_p^{'}$. For such values of x, there are $\frac{p-3}{4}$ values of $x+1$ also in Q_p. Therefore in (4), there are $\frac{p-3}{4}$ times $+1$ and $\frac{p-1}{2} - \frac{p-3}{4} = \frac{p+1}{4}$ times -1, implying the result.

We already have shown that the number $N_{p,a}$ is $\frac{p-3}{2}$ when a and x belong to Q_p. Authors, in [11], showed that, excluding the point at infinity, the total number of rational points on (2) is p. Therefore we can easily deduce the following:

Theorem 2.2: Let $p \equiv 5\ (mod\ 6)$ be prime and $a \in Q_p$ be fixed. Then for $x \in Q_p^{'}$

$$N_{p,a} = \frac{p+3}{2}.$$

Proof: Immediately follows from Theorem 2 and the remark above. ∎

This concludes the calculation of $N_{p,a}$ when $a \in Q_p$. Now we consider the other possibility.

Theorem 2.3: Let $p \equiv 5\ (mod\ 6)$ be prime and $a \in Q_p^{'}$ be fixed. Then for $x \in Q_p$

$$N_{p,a} = \frac{p-1}{2}.$$

Recall that

$$N_{p,a} = \frac{p-1}{2} + \sum\nolimits_{x\in Q_p} \chi(x^3 + a^3).$$

We first need

Lemma 2.1: a) Let $p \equiv 5\ (mod\ 12)$ be prime. Then $a \in Q_p \Longleftrightarrow p - a \in Q_p$.

b) Let $p \equiv 11\ (mod\ 12)$ be prime. Then $a \in Q_p \Longleftrightarrow p - a \in Q_p^{'}$.

Proof: a) Let $p \equiv 5\ (mod\ 12)$ be prime. Then

$$(\frac{p-a}{p}) = (\frac{-a}{p}) = (\frac{-1}{p})(\frac{a}{p}),$$

where $(\frac{\cdot}{p})$ denotes the Legendre symbol modulo p. By lemma 1, we have $-1 \in Q_p$ and hence $(\frac{-1}{p}) = +1$. Therefore if $a \in Q_p$, we have $(\frac{p-a}{p}) = +1$; i.e. $p - a \in Q_p$.

b) Similarly follows. ∎

Lemma 2.2: For $x = p - a$, $\chi(x^3 + a^3) = (\frac{x^3+a^3}{p}) = 0$.

Now we have two cases to consider because of the lemma 6.

(i) Let $p \equiv 5 \ (mod\ 12)$ be prime. Then $|\varphi_p| = \frac{p-1}{2}$ is even. Then for exactly half of the values of $x \in Q_p$, $\chi(x^3 + a^3)$ is $+1$ and for the other half, $\chi(x^3 + a^3) = -1$. Then

$$\sum\nolimits_{x \in Q_p} \chi(x^3 + a^3) = 0.$$

(ii) Let $p \equiv 11 \ (mod\ 12)$. Then $\frac{p-1}{2}$ is odd. By lemma 6 only for $x = p - a$, $\chi(x^3 + a^3) = 0$, and the rest is divided into two as in (i) that is there are $\frac{p-3}{4}$ quadratic and $\frac{p-3}{4}$ non-quadratic residues together with 0, implying

$$\sum\nolimits_{x \in Q_p} \chi(x^3 + a^3) = 0.$$

Connecting (i) and (ii), we get

Let $p \equiv 5 \ (mod\ 6)$ be prime. Then

$$\sum\nolimits_{x \in Q_p} \chi(x^3 + a^3) = 0.$$

This theorem completes the proof of Theorem 4.

References

[1] Andrews, G. E., *Number Theory,* Dover Publications, (1971), ISBN 0-486-68252-8.

[2] Washington, L. C., *Elliptic Curves, Number Theory and Cryptography,* Chapman&Hall/CRC, 2003.

[3] Parshin, A. N., *The Bogomolov-Miyaoka-Yau inequality for the arithmetical surfaces and its applications,* Seminaire de Theorie des Nombres, Paris, 1986-87, 299-312, Progr. Math., 75, Birkhauser Boston, MA, 1998.

[4] Kamienny, S., *Some remarks on torsion in elliptic curves,* Comm. Alg. 23 (1995), no. 6, 2167-2169.

[5] Ono, K., *Euler's concordant forms,* Acta Arith. 78 (1996), no. 2, 101-123.

[6] Merel, L., *Arithmetic of elliptic curves and Diophantine eqnarrays,* Les XXemes Journees Arithmetiques (Limoges, 1997), J. Theor. Nombres Bordeaux 11 (1999), no. 1, 173-200.

[7] Serre, J.-P., *Propriétés galoisiennes des points d'ordre fini des courbes elliptiques,* Invent. Math. 15 (1972), 259-331.

[8] Demirci, M. & Soydan, G. & Cangül, I. N., *Rational points on the elliptic curves* $y^2 = x^3 + a^3 \ (mod\, p)$ *in* F_p *where p*$\equiv$ $1(mod 6)$ *is prime,* Rocky J.of Maths, (to be printed).

[9] Schmitt, S. Zimmer, H. G., *Elliptic Curves A Computational Approach*, Walter De Gruyter, (2003), ISBN 3-11-016808-1

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

[11] Soydan, G. & Demirci, M. & Ikikardeş, N. Y. & Cangül, I. N., *Rational points on the elliptic curves* $y^2 = x^3 + a^3 \ (mod\, p)$ *in* F_p *where p*$\equiv 5$ $(mod 6)$ *is prime,* (submitted).

[12] Silverman, J. H., *The Arithmetic of Elliptic Curves,* Springer-Verlag, (1986), ISBN 0-387-96203-4.

[13] Silverman, J. H.,Tate, J., *Rational Points on Elliptic Curves,* Springer-Verlag, (1992), ISBN 0-387-97825-9.