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

Classification of the Bachet Elliptic Curves $y^2 = x^3 + a^3$ in $\mathbf{F}_p$, where $p \equiv 1\,(mod\,6)$ is Prime

Nazli Yildiz İkikardes, Gokhan Soydan, Musa Demirci, Ismail Naci Cangul

***Abstract*—**In this work, we first give in what fields $\mathbf{F}_p$, the cubic root of unity lies in $\mathbf{F}_p^*$, in Q_p and in K_p^* where Q_p and K_p^* denote the sets of quadratic and non-zero cubic residues modulo p. Then we use these to obtain some results on the classification of the Bachet elliptic curves $y^2 \equiv x^3 + a^3$ modulo p, for $p \equiv 1\,(mod\,6)$ is prime.

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

I. Introduction

Let $w \neq 1$ be the cubic root of unity. w appears in many calculations regarding elliptic curves, e.g.[2], [3]. The authors used it to find rational points on Bachet elliptic curves $y^2 = x^3 + a^3$ in $\mathbf{F}_p$, where $\mathbf{F}_p$ is a field of characteristic > 3.

In [9], 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 [10], 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 [8], 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 $y^2 = x^3 - N^2x$. 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 [6], Parshin obtaines an inequality to give an effective bound for the height of rational points on a curve. In [7], the problem of boundedness of torsion for elliptic curves over quadratic fields is settled.

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

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 [2], and [3].

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 we start by a solution $(3, 5)$ to $y^2 - x^3 = -2$, by applying duplication formula, we get a series of rational solutions $(3, 5),\ \left(\frac{129}{10^2},\ \frac{-383}{10^3}\right),\ \left(\frac{2340922881}{7660^2}, \frac{113259286337292}{7660^3}\right),\ ....$

Here we give a classification of Bachet elliptic curves for all values of a between 1 and $p - 1$. In doing these, we often need to know when w is a quadratic or cubic residue.

Let Q_p and K_p denote the set of quadratic and cubic residues, respectively.

II. The Cubic Root of Unity Modulo p $\equiv 1$ (mod 6) is Prime

When a prime p is congruent to 1 modulo 6, we have a lot of nice number theoretical results concerning cubic root w of unity. First, we can say when w is an integer modulo p.

Lemma 2.1: The cubic root of unity $w = \frac{-1+\sqrt{-3}}{2}$ lies in $\mathbf{F}_p^*$ if and only if $p \equiv 1\ (mod\ 6)$ is prime.

Proof: Let $w = \frac{-1+\sqrt{-3}}{2} = \frac{-1+\sqrt{3}i}{2}$. We want to show that $w \in \mathbf{F}_p^* = \mathbf{F}_p \backslash \{0\}$.

First, we will show that $\sqrt{-3} \in \mathbf{F}_p^*$. To do this, we will show the existence of a $t \in \mathbf{Z}_p$ so that $-3 \equiv t^2(modp)$. In other words, we need to show that $(\frac{-3}{p}) = +1$, where $(\frac{\cdot}{\cdot})$ denotes the Legendre symbol. Now

$$\begin{aligned}(\frac{-3}{p}) &= (\frac{-1}{p})(\frac{3}{p}) \\ &= (-1)^{\frac{p-1}{2}}(\frac{p}{3})(-1)^{\frac{p-1}{2}\cdot\frac{3-1}{2}} \quad byGaussReciprocitylaw, \\ &= (-1)^{p-1}(\frac{p}{3})\end{aligned}$$

and as $p \equiv 1\ (mod\ 6)$, we have $(\frac{p}{3}) = (\frac{1}{3}) = +1$ and $p-1$ even, implying $(\frac{-3}{p}) = +1$.

Secondly, $(2,p) = 1$ and 2 has a multiplicative inverse u in $\mathbf{F}_p^*$. Then $2.u \equiv 1(modp)$ and $\frac{-1+\sqrt{-3}}{2} = u.(-1+\sqrt{-3})$ and as $\sqrt{-3}$ and hence $-1+\sqrt{-3}$ lies in $\mathbf{F}_p$, $w \in \mathbf{F}_p^*$. Going backwards, we obtain the result. ■

The following result gives us the values of p where $w \in \mathbf{Q}_p$.

Lemma 2.2: $w \in Q_p \Leftrightarrow p \equiv 1\ (mod\ 6)$ is prime.

Proof:

$$\begin{aligned} w \in Q_p &\Leftrightarrow \exists t \in U_p \ \ such \ \ that\ t^2 \equiv w(modp) \\ &\Leftrightarrow \ \exists\ t \in U_p\ such\ that\ t^6 \equiv w^3 \equiv 1(modp).\end{aligned}$$

Also by Fermat's little theorem, we have $t^{p-1} \equiv 1(modp)$ for $t \in U_p$. Then $6|(p-1)$ and $p \equiv 1(mod6)$. ■

For example, $w = 4, 9, 11, 5, ...$ for $p = 7, 13, 19, 31, ...$, respectively.

Now we give the following result to determine for what prime values of p, w is a cubic residue modulo p. If $w \equiv 0(modp)$, then $\frac{-1+\sqrt{-3}}{2} \equiv 0(modp)$ giving $4 \equiv 0(modp)$, a contradiction. So $w \in K_p^*$.

Theorem 2.1: Let w be the cubic root of unity. Then

$$w \in K_p^* \Longleftrightarrow p \equiv 1(mod18).$$

Proof: $w \in K_p^* \Longleftrightarrow \exists b \in U_p$ such that $w = b^3 \neq 1$, where U_p denotes the set of units modulo p.

$$\begin{aligned} &\Longleftrightarrow \ \exists\ b \in U_p\ such\ that\ w^3 = b^9 = 1 \\ &\Longleftrightarrow \ \exists\ b \in U_p\ such\ that ø(b) = 9.\end{aligned}$$

But as $(b,p) = 1$, we know by Fermat's little theorem that $b^{p-1} \equiv 1(modp)$. By the definition of order, $9|(p-1) \Longleftrightarrow p = 1+9k$, $k \in \mathbf{Z}$. As p is prime, k must be even, and by letting $k = 2t$, $t \in \mathbf{Z}$, we get $p = 1+18t \equiv 1(mod18)$. ■

In particular,

Corollary 2.2: Let $p \equiv 1(mod6)$ be prime. Then

a) If $p \equiv 1(mod18)$, then all three or none of a, aw and aw^2 lie in K_p^*.

b) If $p \neq 1(mod18)$, then only one of a, aw and aw^2 lies in K_p^*.

Proof: **a)** Let $p \equiv 1(mod\,18)$ and let $a \in K_p^*$. Then by theorem 3, $w \in K_p$. As K_p^* is a multiplicative group, the result follows.

If $a \notin K_p^*$, the result similarly follows.

b) Let $p \equiv 1(mod\,6)$ and $p \neq 1(mod\,18)$. Then by theorem 3, $w \notin K_p$.

Firstly, assume that $a \in K_p^*$. Then aw and aw^2 do not belong to K_p^*.

Secondly, let $a \notin K_p^*$. Now we first assume that $aw \in K_p$. That is, there exists a $t \in U_p$ such that $aw \equiv t^3(mod\,p)$. Then $aw^2 \equiv t^3.w(mod\,p)$. Again by theorem 3, $aw^2 \notin K_p^*$ as $t^3 \in K_p^*$ and $w \notin K_p^*$. Now we finally assume that $aw^2 \in K_p$. Then similarly $aw = aw^2.w^2 = t^3w^2 \notin K_p^*$ as $t^3 \in K_p$ and $w^2 \notin K_p^*$. ■

Similarly,

Corollary 2.3: Let $p \equiv 1(mod\,6)$ be prime and $p \neq 1(mod\,18)$. Let $a \notin K_p^*$. Then

$$aw^k \in K_p \Longleftrightarrow aw^{3-k} \notin K_p^*$$

for $k = 1, 2$.

III. Bachet Elliptic Curves Modulo Prime $p \equiv 1(mod\,6)$

Now we are ready to use the results obtained in part 2 to give some results regarding Bachet elliptic curves. First

Theorem 3.1: Let $p \equiv 1(mod\,6)$ be prime. There are three values of x, for $y = 0$, on the elliptic curve $y^2 \equiv x^3 + a^3(mod\,p)$, having sum equal to 0 modulo p.

Proof: For $y = 0$, $x^3 \equiv -a^3(mod\,p)$ has solutions $x = -a$, $-aw$ and $-aw^2$. The result then follows. ■

Theorem 3.2: Let $p \equiv 1(mod\,18)$ be prime. If $a \in K_p^*$ then three values of x obtained for $y = 0$ on the elliptic curve $y^2 \equiv x^3 + a^3(mod\,p)$ lie in K_p^*.

If $a \notin K_p^*$, then none of the three values of x obtained for $y = 0$ on the elliptic curve $y^2 \equiv x^3 + a^3(mod\,p)$ lie in K_p^*.

Proof: For $y = 0$, $x^3 \equiv -a^3(mod\,p)$ has solutions $x = -a$, $-aw$ and $-aw^2$. The result then follows. ■

Also we have,

Theorem 3.3: Let $p \equiv 1(mod\,6)$ be prime. For $a \in \mathbf{F}_p^*$, there are $\frac{p-1}{3}$ elliptic curves $y^2 \equiv x^3 + a^3(mod\,p)$.

Proof: For a fixed value of a between 1 and $p-1$, we know that we obtain the same value of y for $x = a$, $x = aw$ and $x = aw^2$. Therefore the $p-1$ values of a can be grouped into $\frac{p-1}{3}$ groups each consisting of three values of a. ■

Theorem 3.4: Let $p \equiv 1(mod\,18)$ be prime. If $a \in K_p^*$, then there are $\frac{p-1}{9}$ elliptic curves $y^2 \equiv x^3 + a^3(mod\,p)$.

Proof: Let $p \equiv 1(mod\,6)$ be prime. We know by theorem 8 that there are $\frac{p-1}{3}$ elliptic curves $y^2 \equiv x^3 + a^3(mod\,p)$ for $a \in \mathbf{F}_p^*$. If also $p \equiv 1(mod\,9)$, (that is $p \equiv 1(mod\,18)$ by the Chinese remainder theorem) then we can group these $\frac{p-1}{3}$ values of a into groups of three, consisting of $\{a, aw, aw^2\}$ for $a \in K_p^*$. Therefore when $p \equiv 1(mod\,18)$, there are $\frac{p-1}{9}$ sets of the values of a, for $a \in K_p^*$.

Example 3.1: Let $p = 37$. Then $K_{37}^* = \{1, 6, 8, 10, 11, 14, 23, 26, 27, 29, 31, 36\}$. Here $w = 26 \in \mathbf{F}_{37}^*$

by lemma 1 and $w \in K_{37}^*$ by theorem 3. Then the $\frac{37-1}{9} = 4$ sets of the values of a can be obtained as follows:

$\{a = 1,\ aw = 26,\ aw^2 = 10\}$
$\{a = 6,\ aw = 8,\ aw^2 = 23\}$
$\{a = 11,\ aw = 27,\ aw^2 = 36\}$
$\{a = 14,\ aw = 31,\ aw^2 = 29\}$

One obtains the same elliptic curve for each of three elements a, aw, aw^2 in one of these sets.

■

We know by theorem 8 that there are $\frac{p-1}{3}$ elliptic curves for $a \in \mathbf{F}_p^*$. Now we have

Theorem 3.5: Let $p \equiv 1\ (mod\ 18)$ be prime. For $y = 0$, there are three points with $x \in K_p^*$, on the $\frac{p-1}{9}$of the $\frac{p-1}{3}$ curves appearing for each triple of elements a, aw, aw^2.

Let $p \equiv 1\ (mod\ 6)$ be prime and $p \neq 1\ (mod\ 18)$. Then each of the $\frac{p-1}{3}$ curves consisting of a triple a, aw, aw^2 contains exactly one element of K_p^*.

Proof: The first part follows from Theorem 9.

For the second part, as $p \neq 1\ (mod\ 18)$, we know that $w \notin K_p^*$ by Theorem 3. By Theorem 8, the values of a between 1 and $p-1$ are divided into $\frac{p-1}{3}$ sets. By Corollary 4b), only one of a, aw, aw^2 belongs to K_p^* . ■

Theorem 3.6: Let $p \equiv 1\ (mod\ 6)$ be prime. Out of these $\frac{p-1}{3}$ curves, exactly $\frac{p-1}{6}$ contains three points $(x, 0)$ where $x \in Q_p$, and $\frac{p-1}{6}$ contains three points $(x, 0)$ where $x \notin Q_p$.

Proof: For $y = 0$, $x^3 \equiv -a^3 (mod\, p)$ and as the number of quadratic and non quadratic residues are equal, we have $\frac{p-1}{6}$ sets consisting of three values of $a \in Q_p$ and $\frac{p-1}{6}$ consisting of three values of $a \notin Q_p$, by Lemma 2. ■

REFERENCES

[1] Namlı, D., *Cubic Residues* , PhD Thesis, Balikesir University, (2001)

[2] 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).

[3] 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).

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

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

[6] 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.

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

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

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

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