Miskolc Mathematical Notes
Vol. 10 (2009), No 2, pp. 129-136

HU e-ISSN 1787-2413
DOI: 10.18514/MMN.209.182

The group structure of Bachet elliptic curves over finite fields F_p

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

Miskolc Mathematical Notes
Vol. 10 (2009), No. 2, pp. 129–136

HU e-ISSN 1787-2413

THE GROUP STRUCTURE OF BACHET ELLIPTIC CURVES OVER FINITE FIELDS F_p

NAZLI YILDIZ IKIKARDES, MUSA DEMIRCI, GÖKHAN SOYDAN, AND ISMAIL NACI CANGÜL

Received 3 December, 2007

Abstract. Bachet elliptic curves are the curves $y^2 = x^3 + a^3$ and, in this work, the group structure $E(\mathbb{F}_p)$ of these curves over finite fields $\mathbb{F}_p$ is considered. It is shown that there are two possible structures $E(\mathbb{F}_p) \cong C_{p+1}$ or $E(\mathbb{F}_p) \cong C_n \times C_{nm}$, for $m,n \in \mathbb{N}$, according to $p \equiv 5 \pmod 6$ and $p \equiv 1 \pmod 6$, respectively. A result of Washington is restated in a more specific way saying that if $E(\mathbb{F}_p) \cong Z_n \times Z_n$, then $p \equiv 7 \pmod{12}$ and $p = n^2 \mp n + 1$.

2000 *Mathematics Subject Classification:* 11G20, 14H25, 14K15, 14G99

Keywords: elliptic curves over finite fields, rational points

1. INTRODUCTION

Let p be a prime. We shall consider the elliptic curves

$$E:\ y^2 \equiv x^3 + a^3 \pmod p, \tag{1.1}$$

where a is an element of $\mathbb{F}_p^* = \mathbb{F}_p \setminus \{0\}$. Let us denote the group of the points on E by $E\left(\mathbb{F}_p\right)$.

If $\mathbb{F}$ is a field, then an elliptic curve over $\mathbb{F}$ has, after a change of variables, the following form:

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

where $A, B \in \mathbb{F}$ with $4A^3 + 27B^2 \neq 0$ in $\mathbb{F}$. 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 $\mathbb{F}$ to be a finite prime field $\mathbb{F}_p$ with characteristic $p > 3$. Then $A, B \in \mathbb{F}_p$. The set of points $(x, y) \in \mathbb{F}_p \times \mathbb{F}_p$ on E, together with a *point σ at infinity*, is called the set of $\mathbb{F}_p$-*rational points* of E on $\mathbb{F}_p$ and is denoted by $E\left(\mathbb{F}_p\right)$. 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 (including σ) (for every x, there exist at most two values of y). But not all elements of $\mathbb{F}_p$ have square roots. In fact

This work was supported by the research fund of Uludag University project No. F-2003/63 and F-2004/40.

only half of the elements of $\mathbb{F}_p$ have a square root. Therefore, the expected number is about $p+1$.

It is known that

$$N_p = p + 1 + \sum_{x=0}^{p-1} \chi\left(x^3 + Ax + B\right).$$

Here we use the fact that the number of solutions of $y^2 \equiv u \pmod{p}$ is $1+\chi(u)$. The following theorem of Hasse quantifies this result.

Theorem 1.1 (Hasse, 1922)**.** *The inequality* $N_p < \left(\sqrt{p}+1\right)^2$ *holds.*

Now we look at the algebraic structure of $E\left(\mathbb{F}_p\right)$. Let $P\left(x_1, y_1\right)$ and $Q\left(x_2, y_2\right)$ be two points on $E : y^2 = x^3 + Ax + B$. Let also

$$m = \begin{cases} \frac{y_2 - y_1}{x_2 - x_1} & \text{if } P \neq Q, \\ \frac{3x_1^2 + A}{2y_1} & \text{if } P \neq Q, \end{cases}$$

where $y_1 \neq 0$, while when $y_1 = 0$, the point is of order 2. If we put

$$x_3 = m^2 - x_1 - x_2 \quad \text{and} \quad y_3 = m(x_1 - x_3) - y_1\,,$$

then

$$P + Q = \begin{cases} \sigma & \text{if } x_1 = x_2 \text{ and } y_1 + y_2 = 0, \\ Q & \text{if } P = Q, \\ (x_3, y_3) & \text{in the other cases.} \end{cases}$$

By definition $-P = (x, -y)$.

Because of the definition of addition in an arbitrary field, it takes very long to make any addition and the results are very complicated.

Here we shall deal with Bachet elliptic curves $y^2 = x^3 + a^3$ modulo p. Let $N_{p,a}$ denote the number of rational points on this curve. Some results on these curves have been given in [1] and [4].

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. The existence 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 $x, y \in \mathbb{Q}$, 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.

If $p \equiv 5 \pmod 6$, it is well known that $E\left(\mathbb{F}_p\right) \cong C_{p+1}$, the cyclic group of order $p+1$, see [2]. But when $p \equiv 1 \pmod 6$, there is no result giving the group structure of $E\left(\mathbb{F}_p\right)$. In this work, we discuss this situation. We show that this group is isomorphic to a direct product of two cyclic groups C_n and C_{nm}, i. e.,

$$E\left(F_p\right) \cong C_n \times C_{nm}$$

for $m, n \in \mathbb{N}$. If we denote the order of $E\left(\mathbb{F}_p\right)$ by $N_{p,a}$, then

$$N_{p,a} = n^2 m = p + 1 - b,$$

where $b > 0$ when $a \in Q_p$, and $b < 0$ otherwise. Here b is the trace of the Frobenius endomorphism.

2. Bachet elliptic curves having a group of the form $C_n \times C_{nm}$

Let E be the curve in (1.1). Then its twist is defined as the curve $y^2 \equiv x^3 + g^3 a^3$, where g is an element of Q'_p, the set of quadratic non-residues modulo p. As usual, Q_p denotes the set of quadratic residues modulo p. Here note that if $a \in Q_p$, then $ga \in Q'_p$ and when $a \in Q'_p$, then $ga \in Q_p$. It is easy to show that b of (1.1) and of its twist have different signs. Therefore

Theorem 2.1. *Let $p \equiv 1 \pmod 6$ be a prime. If (1.1) has the group isomorphic to $C_n \times C_{nm}$ with order $n^2 m = p + 1 - b$, then its twist is isomorphic to $C_r \times C_{rs}$ with order $r^2 s = p + 1 + b$.*

Let us set $t = |b|$, that is,

$$t = \left|p + 1 - N_{p,a}\right|.$$

We first have

Theorem 2.2. *The following assertions hold:*

(a) *Let $p \equiv 1 \pmod{12}$ be a prime. Then*

$$b \equiv 2 \pmod{12} \quad \textit{iff} \quad N_{p,a} \equiv 0 \pmod{12}$$

and

$$b \equiv 10 \pmod{12} \quad \textit{iff} \quad N_{p,a} \equiv 4 \pmod{12}.$$

(b) *Let $p \equiv 7 \pmod{12}$ be a prime. Then*

$$b \equiv 4 \pmod{12} \quad \textit{iff} \quad N_{p,a} \equiv 4 \pmod{12}$$

and

$$b \equiv 8 \pmod{12} \quad \textit{iff} \quad N_{p,a} \equiv 0 \pmod{12}.$$

Proof. (a) Let $p \equiv 1 \pmod{12}$ be a prime. Then we can write this as $p = 1+12n$, $n \in \mathbb{Z}$. Also $b \equiv 2 \pmod{12}$ can be stated as $b = 2+12m$, $m \in \mathbb{Z}$. By substituting these, we get

$$b \equiv 2 \pmod{12} \iff N_{p,a} = p+1-b$$

and hence $N_{p,a} = 1+12n+1-(2+12m) = 12(n-m)$ and this is only valid when $N_{p,a} \equiv 0 \pmod{12}$. Similarly,

$$b \equiv 10 \pmod{12} \iff N_{p,a} = p+1-b = 1+12n+1-(10+12m)$$

and therefore $N_{p,a} = -8+12(n-m)$ and this means that $N_{p,a} \equiv 4 \pmod{12}$. Part (b) is proved in a similar fashion. □

Theorem 2.3. *Let $p \equiv 1 \pmod{6}$ be a prime. Then b is not divisible by 6.*

Proof. Let us consider the curve $y^2 = x^3+1$. It has a point of order 6. Therefore its reduction modulo p has also a point of order 6. Therefore

$$b \equiv p+1-N_{p,a} \equiv 2-0 \equiv 2 \pmod{6}.$$

The other possibility for the curve is $y^2 = x^3+a^3$ with a is a quadratic non-residue. It is the quadratic twist of the other curve, so has $b \equiv -2 \pmod{6}$. Therefore in both cases b is non-zero modulo 6. □

Corollary 2.1. *Let $p \equiv 1 \pmod{6}$ be a prime. Then $N_{p,a} \equiv 0 \pmod{4}$ or $N_{p,a} \equiv 4 \pmod{6}$.*

Also one obtains the following result:

Corollary 2.2. *If $p \equiv 1 \pmod{12}$ is a prime, then $b \equiv \mp 2 \pmod{12}$ and if $p \equiv 7 \pmod{12}$ is a prime, then $b \equiv \mp 4 \pmod{12}$.*

We now have the following result about the number of points on curves (1.1).

Theorem 2.4. *Let $p \equiv 1 \pmod{6}$ be a prime. Then:*

(a) *If $t \equiv 2 \pmod{6}$, then (1.1) has $b = t$ and $N_{p,a} \equiv 0 \pmod{6}$, and its twist has $b = -t$ and $N_{p,a} \equiv 4 \pmod{6}$.*
(b) *If $t \equiv 4 \pmod{6}$, then (1.1) has $b = t$ and $N_{p,a} \equiv 4 \pmod{6}$, and its twist has $b = -t$ and $N_{p,a} \equiv 0 \pmod{6}$.*

Proof. Let $p \equiv 1 \pmod{6}$ be a prime. Let us put $p = 1+6n$, $n \in \mathbb{Z}$. Let $t \equiv 2 \pmod{6}$. If $b = t$, then $b \equiv 2 \pmod{6}$ and we put $b = 2+6m$, $m \in \mathbb{Z}$. Therefore

$$\begin{aligned} N_{p,a} &= p+1-b = 6n+1+1-2-6m \\ &= 6(n-m) \end{aligned}$$

implying that $N_{p,a} \equiv 0 \pmod{6}$.
The other parts can be proven similarly. □

We then immediately have the following result concerning the elements of order 3:

Corollary 2.3. *The following assertions hold:*

(a) *Let* $p \equiv 1 \pmod{12}$ *be a prime. If* $t \equiv 2 \pmod{12}$, *then* (1.1) *has* $b = t$ *and* $N_{p,a} \equiv 0 \pmod{12}$ *and* $E\left(\mathbb{F}_p\right)$ *has elements of order* 3. *Its twist has* $b = -t$ *and* $N_{p,a} \equiv 4 \pmod{12}$ *implying that there are no elements of order* 3.

If $t \equiv 10 \pmod{12}$, *then* (1.1) *has* $b = t$ *and* $N_{p,a} \equiv 4 \pmod{12}$ *and* $E\left(\mathbb{F}_p\right)$ *has no elements of order* 3, *while its twist has* $b = -t$ *and* $N_{p,a} \equiv 0 \pmod{12}$ *implying that the group has elements of order* 3.

(b) *Let* $p \equiv 7 \pmod{12}$ *be a prime. If* $t \equiv 4 \pmod{12}$, *then* (1.1) *has* $b = t$ *and* $N_{p,a} \equiv 4 \pmod{12}$ *and therefore has no points of order* 3, *while its twist has* $b = -t$ *and* $N_{p,a} \equiv 0 \pmod{12}$ *having elements of order* 3.

If $t \equiv 8 \pmod{12}$, *then* (1.1) *has* $b = t$ *and* $N_{p,a} \equiv 0 \pmod{12}$ *implying that it has elements of order* 3 *while its twist has* $b = -t$ *and* $N_{p,a} \equiv 4 \pmod{12}$ *having no such elements.*

The elements of order 3 are important in the classification of these elliptic curves modulo p. We now show that their number is either 2 or 8.

Theorem 2.5. *Let* $p \equiv 1 \pmod{6}$ *be a prime. If* $N_{p,a} \equiv 0 \pmod{6}$, *then there are* 2 *or* 8 *points of order* 3.

Proof. By [3], there are at most 9 points together with the point at infinity $\emptyset$, forming a subgroup which is either trivial, cyclic of order 3 or the direct product of two cyclic groups of order 3. As we want to determine the number of elements of order 3, this group cannot be trivial. Then it is C_3 or $C_3 \times C_3$ and it is well-known that it contains 2 or 8 elements of order 3, respectively. □

In fact, if we let $E\left(\mathbb{F}_p\right) \cong C_n \times C_{nm}$, then when 3 divides n, $E\left(\mathbb{F}_p\right)$ has 8 points of order 3, and if not, it has 2 points of order 3.

We are now going to give one of the main results in Theorem 2.8. We first need the following results:

Corollary 2.4. *Let* p *be a prime. Then for only* $x = 0$ *among all values of* x *in* $\mathbb{F}_p$, $x^3 + 1$ *takes the value* 1.

Proof. It is clear that $x = 0$ satisfies the condition. The fact that no other value of x satisfies $x^3 + 1 = 1$ is clear from the fact that p is a prime. □

Theorem 2.6. *Let* $p \equiv 1 \pmod{6}$ *be a prime. There are* 3 *values of* x *between* 1 *and* p *so that* $x^3 + 1 \equiv 0 \pmod{p}$.

Proof. It is obvious that $x^3 \equiv a \pmod{p}$ has three solutions in $\mathbb{F}_p$ for every $a \neq 0$. For $a = -1$, the proof follows. □

Theorem 2.7. *Let* $p \equiv 1 \pmod{6}$ *be a prime. Then*

$$\sum_{x \in \mathbb{F}_p} \chi\left(x^3 + 1\right) \equiv 4 \pmod{6}.$$

Proof. For each $x \in \mathbb{F}_p$, calculate the p values of x^3+1. By Corollary 2.4, one of these values is 1. By Theorem 2.6, three of them are 0. The rest $p-4$ values of x^3+1 are grouped into $\frac{p-4}{3}$ triples. As $p \equiv 1 \pmod 6$, $\frac{p-4}{3}$ is odd. Indeed, let us write $p = 1+6k$, $k \in \mathbb{Z}$. Then $\frac{p-4}{3} = 2k-1$. Let us suppose that out of these triples, s triples are in Q_p and $2k-1-s$ are in Q'_p. If a triple is in Q_p, then it adds $+3$ to the sum $\sum_{x\in\mathbb{F}_p} \chi\left(x^3+1\right)$, and if it is in Q'_p, -3 is added. Therefore

$$\begin{aligned}\sum_{x\in\mathbb{F}_p} \chi\left(x^3+1\right) &= 1+3\cdot 0+s\cdot(+3)+(2k-1-s)\cdot(-3)\\ &= 6(s-k)+4\end{aligned}$$

implying the result. □

Theorem 2.8. *Let $p \equiv 1 \pmod 6$ be a prime. Then $a \in Q_p$ iff $N_{p,a} \equiv 0 \pmod 6$.*

Proof. It is well-known that

$$N_{p,a} = p+1+\sum_{x\in\mathbb{F}_p} \chi\left(x^3+a^3\right).$$

By putting $p = 1+6n$ for $n \in \mathbb{Z}$, we get $N_{p,a} = 6n+2+\sum_{x\in\mathbb{F}_p} \chi\left(x^3+a^3\right)$. Now as $\chi(a) = 1$, and as the set of the values of x^3 is the same as the set of the values of a^3x^3, we can write

$$\begin{aligned}\sum_{x\in\mathbb{F}_p} \chi\left(x^3+a^3\right) &= \sum_{x\in\mathbb{F}_p} \chi\left(a^3x^3+a^3\right)\\ &= \sum_{x\in\mathbb{F}_p} \chi\left(a^3\right)\chi\left(x^3+1\right)\\ &= \sum_{x\in\mathbb{F}_p} \chi\left(x^3+1\right),\end{aligned}$$

and by Theorem 2.7, this sum is congruent to 4 modulo 6. Hence, by putting

$$\sum_{x\in\mathbb{F}_p} \chi\left(x^3+a^3\right) = 4+6r, \quad r \in \mathbb{Z},$$

we get $N_{p,a} = 6n+2+4+6r$ implying that $N_{p,a} \equiv 0 \pmod 6$. □

Corollary 2.5. *Let $p \equiv 1 \pmod 6$ be a prime. If $N_{p,a} \equiv \pmod 6$, then $b \equiv 2 \pmod 6$.*

Proof. As $N_{p,a} = p+1-b = p+1+\sum_{x\in\mathbb{F}_p} \chi\left(x^3+a^3\right)$, we know that $b = -\sum_{x\in\mathbb{F}_p} \chi\left(x^3+a^3\right)$. By Theorem 2.7, the result follows. □

Similarly, we have

Theorem 2.9. *Let $p \equiv 1 \pmod 6$ be a prime. Then $a \in Q'_p$ iff $N \equiv 4 \pmod 6$.*

Corollary 2.6. *Let $p \equiv 1 \pmod 6$ be a prime. Let E be the curve given by (1.1). Then:*

(a) *$a \in Q_p$ iff $E\left(\mathbb{F}_p\right)$ has 2 or 8 elements of order 3.*
(b) *$a \in Q'_p$ iff $E\left(\mathbb{F}_p\right)$ has no elements of order 3.*

Proof. This is clear from Corollary 2.3 and Theorem 2.8. □

3. Bachet elliptic curves having a group of the form $C_n \times C_n$

Now we shall consider the case where the Bachet elliptic curves have a group isomorphic to $C_n \times C_n$ for same n. This is only possible when $p \equiv 1 \pmod 6$, as otherwise when $p \equiv 5 \pmod 6$, $E\left(\mathbb{F}_p\right)$ is isomorphic to the cyclic group C_{p+1}. We shall consider a result of Washington and refine it.

Theorem 3.1 ([5])**.** *Let E be an elliptic curve over $\mathbb{F}_q$ where q is a prime power and suppose $E\left(\mathbb{F}_q\right) \cong \mathbb{Z}_n \times \mathbb{Z}_n$ for some integer n. Then either $q = n^2 + 1$, $q = n^2 \mp n + 1$, or $q = (n \mp 1)^2$.*

Now we give a more specific result for Bachet elliptic curves given by (1.1) over $\mathbb{F}_q$.

Theorem 3.2. *Let E be the elliptic curve in (1.1). Suppose that*

$$E\left(\mathbb{F}_p\right) \cong \mathbb{Z}_n \times \mathbb{Z}_n .$$

Then $p \equiv 7 \pmod{12}$ and $p = n^2 \mp n + 1$.

Proof. By Theorem 3.1, there are three possibilities $p = n^2 + 1$, $p = n^2 \mp n + 1$, and $p = n^2 \mp 2n + 1$. The latter one is immediately rules out as p cannot be a square. We need only to show that p cannot be equal to $n^2 + 1$.

If $p = n^2 + 1$, then $n^2 = p - 1$ and hence $p - 1$ is in Q_p. But it is known that $p - 1$ could be in Q_p only when $p \equiv 1, 5 \pmod{12}$ is a prime. Therefore the result follows. □

References

[1] M. Demirci, G. Soydan, and I. N. Cangul, "Rational points on elliptic curves $y^2 = x^3 + a^3$ in $\mathbf{F}_p$ where $p \equiv 1 \pmod 6$ is prime," *Rocky Mountain J. Math.*, vol. 37, no. 5, pp. 1483–1491, 2007. [Online]. Available: http://dx.doi.org/10.1216/rmjm/1194275930

[2] S. Schmitt and H. G. Zimmer, *Elliptic curves. A computational approach*, ser. de Gruyter Studies in Mathematics. Berlin: Walter de Gruyter & Co., 2003, vol. 31, with an appendix by Attila Pethő.

[3] R. Schoof, "Nonsingular plane cubic curves over finite fields," *J. Combin. Theory Ser. A*, vol. 46, no. 2, pp. 183–211, 1987. [Online]. Available: http://dx.doi.org/10.1016/0097-3165(87)90003-3

[4] G. Soydan, M. Demirci, N. Y. Ikikardes, and I. N. Cangul, "Rational points on elliptic curves $y^2 = x^3 + a^3$ in $\mathbf{F}_p$, where $p \equiv 5 \pmod 6$ is prime," *Int. J. Math. Sci. (WASET)*, vol. 1, no. 4, pp. 247–250 (electronic), 2007.

[5] L. C. Washington, *Elliptic curves. Number theory and cryptography*, ser. Discrete Mathematics and its Applications (Boca Raton). Chapman & Hall/CRC, Boca Raton, FL, 2003.

Authors' addresses

Nazli Yildiz Ikikardes
Department of Mathematics, Balikesir University, Balikesir, Turkey
E-mail address: nyildiz@balikesir.edu.tr

Musa Demirci
Department of Mathematics, Uludağ University, 16059 Bursa, Turkey

Gökhan Soydan
Department of Mathematics, Uludag University, 16059 Bursa, Turkey

Ismail Naci Cangül
Department of Mathematics, Uludağ University, 16059 Bursa, Turkey
E-mail address: cangul@uludag.edu.tr