On the Family of Elliptic Curves $y^2 = x^3 + b/\mathbb{F}_p$

Han Wu* and Guangwu Xu†‡

Abstract

This paper is devoted to a more precise classification of the family of curves $E_b : y^2 = x^3 + b/\mathbb{F}_p$. For prime $p \equiv 1 \pmod 3$, explicit formula of the number of $\mathbb{F}_p$-rational points on E_b is given based on the the coefficients of a (primary) decomposition of $p = (c + d\omega)\overline{(c + d\omega)}$ in the ring $\mathbb{Z}[\omega]$ of Eisenstein integers. More specifically,

$$\#E_b(\mathbb{F}_p) \in p + 1 - \big\{ \pm (d - 2c), \pm(c + d), \pm(c - 2d) \big\}.$$

The correspondence between these 6 number of points and the 6 isomorphism classes of the groups $E_b(\mathbb{F}_p)$ can be efficiently determined.

For prime $p \equiv 2 \pmod 3$, it is shown that $E_b(\mathbb{F}_p) \cong \mathbb{Z}_{p+1}$. Two efficiently computable isomorphisms are described within the single isomorphism class of groups for representatives $E_1(\mathbb{F}_p)$ and $E_{-3}(\mathbb{F}_p)$

The explicit formulas $\#E_b(\mathbb{F}_p)$ for $p \equiv 1 \pmod p$ are used in searching prime (or almost prime) order Koblitz curves over prime fields. An efficient procedure is described and analyzed. The procedure is proved to be deterministic polynomial time, assuming the Generalized Riemann Hypothesis.

Several tools that are useful in computing cubic residues are also developed in this paper.

Keywords: Elliptic Curves, point counting, Eisenstein integers.

1 Introduction

Let $p > 3$ be a prime. For any $b \in \mathbb{F}_p^*$, $y^2 = x^3 + b$ defines an elliptic curve over $\mathbb{F}_p$. This is a family of simple and interesting curves. For prime $p \equiv 2 \pmod 3$, it is well known that they belong to the family of supersingular curves. Such curves are useful in Pairing based cryptography because of their low embedding degree, on the other hand, one should avoid

*School of Cyber Science and Technology, Shandong University, Qingdao, Shandong, 266237, China

†School of Cyber Science and Technology, Shandong University, Qingdao, Shandong, 266237, China; e-mail: gxu4sdq@sdu.edu.cn.

‡Corresponding author.

supersingular curves in normal elliptic curve cryptography (ECC) due to MOV attack [18] and Frey-Rück attack [11].

However, for suitable prime numbers p, there are curves of the form $y^2 = x^3 + b/\mathbb{F}_p$ that are of great interest in ECC. For example, the Standards for Efficient Cryptography Group (SECG) describes three such curves [1]:

$$\begin{aligned} \text{secp192k1:} &\quad y^2 = x^3 + 3/\mathbb{F}_{p_1} \\ \text{secp224k1:} &\quad y^2 = x^3 + 5/\mathbb{F}_{p_2} \\ \text{secp256k1:} &\quad y^2 = x^3 + 7/\mathbb{F}_{p_3} \end{aligned}$$

where p_1, p_2 and p_3 are primes numbers of length 192, 224, and 256 respectively, which are of certain sparse forms. These curves are called Koblitz curve as they admit efficiently computable endomorphisms. A faster scalar multiplication for this kind of Koblitz curves over a special prime field can be achieved by using the GLV method [12]. It is pointed out that Koblitz curve was introduced as binary anomalous curves $y^2 + xy = x^3 + ax^2 + b/\mathbb{F}_{2^m}$ with $a, b \in \{0, 1\}$ [15]. In the binary case, the Frobenius map τ, which is an efficiently computable endomorphisms, is used in window-τNAF to perform scalar multiplication with a remarkable speed [21, 6, 22].

On the aspect of point counting for $E_b : y^2 = x^3 + b/\mathbb{F}_p$ with prime $p \equiv 1 \pmod 3$, there are many results in literature, some of them can be found in [10, 13, 14, 19, 24]. The approaches are mainly based on cubic character sum as the family of curves is a special case of CM curves and the number of points is governed by a Hecke character. Some recent study provided more concrete information towards to the values of $\#E_b(\mathbb{F}_p)$. For examples, $\sum_{b\in\mathbb{F}_p^*} \#E_{b^3}(\mathbb{F}_p) = p^2 - 1$ was proved in [10]; in [14], $\sum_{b\in\mathbb{F}_p^*} \#E_b(\mathbb{F}_p) = p^2 - 1$ was established and values $\#E_b(\mathbb{F}_p) \pmod{24}$ were examined. It is interesting to note that it was shown in [14] that there exactly 6 isomorphism classes for the groups $E_b(\mathbb{F}_p)$. These 6 classes are represented by $E_1(\mathbb{F}_p), E_g(\mathbb{F}_p), E_{g^2}(\mathbb{F}_p), E_{g^3}(\mathbb{F}_p), E_{g^4}(\mathbb{F}_p)$ and $E_{g^5}(\mathbb{F}_p)$, where g is a primitive root modulo p. However, to get precise values of $\#E_b(\mathbb{F}_p)$, some computational tools are needed, especially for dealing with cubic residues.

The purpose of this paper is to present a systematic study of the family of curves $E_b : y^2 = x^3 + b/\mathbb{F}_p$. These curves have the same j-invariant, but that is not sufficient for determining the precise stricture for the groups of $\mathbb{F}_p$-rational points $E_b(\mathbb{F}_p)$.

For the case that $p \equiv 1 \pmod 3$, we are able to give an explicit formula for the number of points in $E_b(\mathbb{F}_p)$. In this case there is an efficient way to find a pair of integers c, d such that $c \equiv 2 \pmod 3$ and $d \equiv 0 \pmod 3$ and

$$p = c^2 - cd + d^2.$$

In this paper, we give the exact 6 possible values of $\#E_b(\mathbb{F}_p)$, one for each isomorphism class of the groups $E_b(\mathbb{F}_p)$. More precisely

$$\#E_b(\mathbb{F}_p) \in p + 1 - \big\{(d - 2c), -(c + d), (c - 2d), -(d - 2c), (c + d), -(c - 2d)\big\}. \qquad (1)$$

In practice, for each number in $p+1-\{(d-2c), -(c+d), (c-2d), -(d-2c), (c+d), -(c-2d)\}$, it is easy to determine an element $b \in \mathbb{F}_p^*$ such that the number is exactly $\#E_b(\mathbb{F}_p)$. Especially when a primitive root g is available, this task is trivial. Note that because E_{g^r} and $E_{g^{r+3}}$ are twist, so $\#E_{g^r}(\mathbb{F}_p) + \#E_{g^{r+3}}(\mathbb{F}_p) = 2(p+1)$. Thus we only need to get formulas for $\#E_{g^r}(\mathbb{F}_p), \#E_{g^{(r+1) \pmod 6}}(\mathbb{F}_p)$ and $\#E_{g^{(r+2) \pmod 6}}(\mathbb{F}_p)$ for some $0 \leq r < 5$. Let $s = c \pmod 2, t = d \pmod 2$. We choose $r = 4(s+1)t \pmod 6$ and denote $\overline{r+j} = (r+j) \pmod 6$, then one of our results states

$$\#E_{g^r}(\mathbb{F}_p) = p+1-(d-2c), \#E_{g^{\overline{r+1}}}(\mathbb{F}_p) = p+1+(c+d), \#E_{g^{\overline{r+2}}}(\mathbb{F}_p) = p+1-(c-2d).$$

These results can be used to create an efficient procedure to find a Koblitz curve E_b over prime field with the order of group $E_b(\mathbb{F}_p)$ being prime (or almost prime). Knowing which value in (1) is a prime (or almost prime), one would just need to find a right coefficient b. We prove that, assuming Generalized Riemann Hypotheses, such procedure runs in deterministic polynomial time.

For the case that $p \equiv 2 \pmod p$, the curves E_b are known to be supersinger so $\#E_b(\mathbb{F}_p) = p+1$. We show that in this case, there is exactly one isomorphism class, namely the class of cyclic groups of order $p+1$. We also describe two explicit efficiently computable isomorphisms in the class. If b is a quadratic residue, then $E_b(\mathbb{F}_p) \cong E_1(\mathbb{F}_p)$ with a simple isomorphic map. Similarly, if b is a quadratic non-residue, then $E_b(\mathbb{F}_p) \cong E_{-3}(\mathbb{F}_p)$.

The rest of our paper is arranged into four sections. In chapter 2 we provide or prove some useful facts about the ring of Eisenstein integers and elliptic curves. Our main results are discussed in section 3. The application of searching Koblitz curves over prime fields is the content of Section 4. We conclude the paper in Section 5.

2 Preliminaries

We will need a set of basic facts about finite fields, Eisenstein integers and elliptic curves.

Lemma 2.1. *Let p be a prime > 5 and g a primtive root modulo p. Consider the homomorphism*

$$\begin{aligned} \tau : \quad & \mathbb{F}_p^* \to \mathbb{F}_p^* \\ & x \mapsto x^3 \end{aligned}$$

then

1. *If $p \equiv 2 \pmod 3$, τ is an isomorphism;*
2. *If $p \equiv 1 \pmod 3$, $\ker(\tau) = \{1, u, u^2\}$ where $u = g^{\frac{p-1}{3}} \pmod p$.*

Proof. Assume that $p \equiv 2 \pmod 3$, then $x^3 - 1 = 0$ has only one root (namely $x = 1$) in $\mathbb{F}_p$, therefore τ is one-to-one.

Now suppose that $p \equiv 1 \pmod 3$. Thus 1, $g^{\frac{p-1}{3}}$, and $g^{\frac{2(p-1)}{3}}$ are three distinct roots of $x^3 - 1 = 0$, i.e., $\ker(\tau) = \{1, u, u^2\}$. □

Remark. *It is easy to see that -3 is a quadratic residue modulo p if and only if $p \equiv 1 \pmod 3$. In this case if we write U to be such that $U^2 = -3$ and let W be a primitive 3rd root of unit in $\mathbb{F}_p^*$, then*

$$W = g^{\frac{p-1}{3}} = \frac{-1+U}{2}$$

holds in the field $\mathbb{F}_p$ with $\mathbb{F}_p^* = \langle g \rangle$.

When working with prime $p \equiv 1 \pmod 3$, one often needs the ring $\mathbb{Z}[\omega] = \mathbb{Z} + \mathbb{Z}\omega$ of Eisenstein integers, where $\omega = \frac{-1+\sqrt{-3}}{2} \in \mathbb{C}$. As we will see later, there are integers c, d such that $p = c^2 - cd + d^2$, and such pair of (c, d) can be obtained by some efficient method. This efficient construction is important in our later discussion.

Write $\pi = c + d\omega$, then $N(\pi) := \pi\bar{\pi} = c^2 - cd + d^2 = p$. This π is a prime in $\mathbb{Z}[\omega]$. We will need π to be *primary* in the sense that $c \equiv 2 \pmod 3$ and $d \equiv 0 \pmod 3$. For $p \equiv 1 \pmod 3$, we can always find a primary $\pi = c + d\omega$ such that $p = \pi\bar{\pi}$. In fact, we can replace π by one of the element in $A = \{\pm\pi, \pm\omega\pi, \pm\omega^2\pi\}$, as it is actually proved in [13] (Prop. 9.3.5) that there is exactly one primary element in A.

The cubic residue character $\left(\frac{\cdot}{\pi}\right)_3$ is defined as

$$\left(\frac{\alpha}{\pi}\right)_3 = \alpha^{\frac{N(\pi)-1}{3}} \pmod \pi.$$

The values of $\left(\frac{\alpha}{\pi}\right)_3$ can be $1, \omega$ or ω^2. It is an extension of Legendre symbol $\left(\frac{\cdot}{p}\right)$ for quadratic case, and $\left(\frac{\alpha}{\pi}\right)_3 = 1$ iff $x^3 = \alpha \pmod \pi$ is solvable.

Lemma 2.2. *If $p \equiv 1 \pmod 3$, then one can find $c, d \in \mathbb{Z}$ in polynomial time such that*

$$p = c^2 - cd + d^2.$$

Proof. In this case, we know that -3 is a quadratic residue. Let $0 < U < p$ be such that $U^2 \equiv -3 \pmod p$. We assume that U is odd (otherwise replace U by $p - U$), then we get

$$U^2 = -3 \pmod{4p}.$$

Letting $U^2 - 4pt = -3$ for some integer t. This means that the binary quadratic form

$$f(x, y) = px^2 + Uxy + ty^2,$$

which takes the value p at $(1, 0)$, has discriminant $d = -3$. Note that $f(x, y)$ is equivalent to the form

$$g(x, y) = x^2 + xy + y^2,$$

as it also has discriminant $d = -3$. g is in reduced form and Gauss reduction procedure (the 2-dimensional case of LLL algorithm [16]) transforms f to g. Gauss reduction uses number of steps comparable to that of the Euclidean algorithm [9], so one can find $c, d \in \mathbb{Z}$ in polynomial time such that

$$p = c^2 - cd + d^2.$$

□

For any $b \in \mathbb{F}_p^*$, the curve $E_b/\mathbb{F}_p : y^2 = x^3 + b$ is not singular and hence defines an elliptic curve.

Next we derive some simple arguments about the number of points in $E_b/\mathbb{F}_p$.

Lemma 2.3. *If $p \equiv 1 \pmod 3$, then*

$$\#E_b(\mathbb{F}_p) \pmod 3 = \begin{cases} 0, & \text{if } b \text{ is a quadratic residue modulo } p, \\ 1, & \text{if } b \text{ is a quadratic nonresidue modulo } p. \end{cases}$$

Proof. Since $p \equiv 1 \pmod 3$. In this case, as we noted earlier that for $\omega = g^{\frac{p-1}{3}}$, $1, \omega, \omega^2$ are three distinct roots of $x^3 - 1 = 0$. If $(x, y) \in E_b(\mathbb{F}_p) \setminus \{\mathcal{O}\}$ and $x \neq 0$, then $E_b(\mathbb{F}_p)$ must contain two more points of the form $(\omega x, y)$ and $(\omega^2 x, y)$. This implies that

$$|\{(x, y) \in E_b(\mathbb{F}_p) \setminus \{\mathcal{O}\} : x \neq 0\}|$$

is a multiple of 3.

If b is a quadratic residue modulo p, then $E_b(\mathbb{F}_p) \setminus \{\mathcal{O}\}$ contains two more points $(0, \sqrt{b}), (0, -\sqrt{b})$, so $\#E_b(\mathbb{F}_p) \pmod 3 = 0$ by counting the point at infinity.

If b is a quadratic nonresidue modulo p, $|E_b(\mathbb{F}_p) \setminus \{\mathcal{O}\}| = |\{(x, y) \in E_b(\mathbb{F}_p) \setminus \{\mathcal{O}\} : x \neq 0\}|$ so $\#E_b(\mathbb{F}_p) \pmod 3 = 1$. □

Recall that a curve E/F_p is supersingular if $\#E(\mathbb{F}_p) = p + 1$. For the special case E_b, we see that

Lemma 2.4. *For $b \in \mathbb{F}_p^*$*

$$E_b/\mathbb{F}_p : y^2 = x^3 + b$$

is supersingular iff $p \equiv 2 \pmod 3$.

Proof. If $p \equiv 2 \pmod 3$, then it is a standard argument that E_b is supersingular, see, for example, [23] (Proposition 4.33).

Conversely, if $p \not\equiv 2 \pmod 3$, then $p \equiv 1 \pmod 3$, hence by lemma 2.3, $\#E(\mathbb{F}_p) \pmod 3 = 0$ or 1. This contradicts to $\#E_b(\mathbb{F}_p) = p + 1$. □

Remark. *It has been proved that $y^2 = x^3 + 1/\mathbb{F}_p$ is supersingular iff $p \equiv 2 \pmod 3$ in [23] (Proposition 4.37). But our proof uses a completely different method.*

3 Classification

In this section, we classify the groups $E_b(\mathbb{F}_p)$ by their precise number for the case of $p \equiv 1 \pmod 3$ and by their precise group structure for the case of $p \equiv 2 \pmod 3$.

3.1 The case $p \equiv 1 \pmod 3$

Study of equations $y^2 = x^3 + b$ modulo p with $p \equiv 1 \pmod 3$ has been an interesting mathematical topic. In [19], Rajwade derived a formula for points on $E_b/\mathbb{F}_p$ based on cubic character sum. We state the result using notation from [24], where a very clean and short treatment of Rajwade's result was described by Williams.

Theorem (Rajwade)**.** *Let $p \equiv 1 \pmod 3$ be a prime number that has a factorization $p = \pi\overline{\pi}$ in $\mathbb{Z}[\omega]$, with π being primary. Then*

$$\#E_b(\mathbb{F}_p) = p + 1 + \left(\frac{b}{p}\right)\left\{\left(\frac{4b}{\pi}\right)_3 \pi + \left(\frac{4b}{\bar{\pi}}\right)_3 \bar{\pi}\right\}.$$

Note that $\left(\frac{4b}{\bar{\pi}}\right)_3 \bar{\pi} = \overline{\left(\frac{4b}{\pi}\right)_3 \pi}$, we see that

$$\#E_b(\mathbb{F}_p) = p + 1 + 2\left(\frac{b}{p}\right) \Re\left(\left(\frac{4b}{\pi}\right)_3 \pi\right). \tag{2}$$

It can be deduced that from the formula there are 6 possible different cardinalities for the groups $E_b(\mathbb{F}_p)$ with p fixed. In fact, Jeon and Kim [14] proved that for prime $p \equiv 1 \pmod 3$, there are exactly 6 classes of isomorphic groups for all $E_b(\mathbb{F}_p)$ with $b \neq 0$. More precisely, let $\mathbb{F}_p^* = \langle g \rangle$, then any $E_b(\mathbb{F}_p)$ is isomorphic to one of the following groups

$$E_1(\mathbb{F}_p),\ E_g(\mathbb{F}_p),\ E_{g^2}(\mathbb{F}_p),\ E_{g^3}(\mathbb{F}_p),\ E_{g^4}(\mathbb{F}_p),\ E_{g^5}(\mathbb{F}_p).$$

What we would like to emphasize is that the isomorphism is concrete and efficiently computable. Suppose $b = g^k$ and let $r = k \pmod 6$ and $q = \frac{k-r}{6}$. Then the following is obviously an isomorphism:

$$\begin{aligned} \Phi:\ & E_b(\mathbb{F}_p) \to E_{g^r}(\mathbb{F}_p) \\ & (x, y) \mapsto \left(\tfrac{x}{g^{2q}}, \tfrac{y}{g^{3q}}\right),\ \mathcal{O} \mapsto \mathcal{O}. \end{aligned}$$

We are able to describe an explicit and efficiently computable formula for the number of points in $E_b(\mathbb{F}_p)$, based on the result from [19]. Such formula can be useful in several applications. We start by developing some tools for dealing with cubic residues.

Again, we fix a generator g for $\mathbb{F}_p^*$, so that we can only focus on the case of $b \in \{1, g, g^2, g^3, g^4, g^5\}$. Let $\pi = c + d\omega$ be a primary prime in $\mathbb{Z}[\omega]$, we need to compute $\left(\frac{g}{\pi}\right)_3$. This value is either ω or ω^2, since there are two cubic non-residues. Our next result provides

a criterion to determine cubic residues for a rational integer in terms of rational integer operations. It can be used to determine whether $\left(\frac{g}{\pi}\right)_3$ is ω.

Lemma 3.1. *Let $p \equiv 1 \pmod 3$ and $p = c^2 - cd + d^2$ such that $\pi = c + d\omega$ is primary. Let $0 < b < p$ be an integer and denote $V = b^{\frac{p-1}{3}} \pmod p$. Then*

$$\left(\frac{b}{\pi}\right)_3 = \begin{cases} 1, & \text{if } V = 1 \\ \omega, & \text{if } p|(c + dV) \\ \omega^2, & \text{if } p|(c - d - dV). \end{cases}$$

In particular, $\left(\frac{b}{\pi}\right)_3 = \omega$ if and only if $c + dV \equiv 0 \pmod p$.

Proof. The condition for $\left(\frac{b}{\pi}\right)_3 = 1$ is trivial as $\left(\frac{b}{\pi}\right)_3 = b^{\frac{p-1}{3}} \pmod \pi$.

Now we assume that b is a cubic non-residue. Note that $\overline{\pi} = c - d - d\omega$, we only need to check for the condition for $\left(\frac{b}{\pi}\right)_3 = \omega$.

We will prove the following claim.

Claim. $\left(\frac{b}{\pi}\right)_3 = \omega$ if and only if $c + dV \equiv 0 \pmod p$.

Suppose that $\left(\frac{b}{\pi}\right)_3 = \omega$. This is equivalent to

$$b^{\frac{p-1}{3}} \equiv \omega \pmod \pi.$$

Therefore, there are integers x, y such that $V - \omega = (c + d\omega)(x + y\omega) = (cx - dy) + (dx + (c - d)y)\omega$. From

$$\begin{cases} cx - dy = V \\ dx + (c - d)y = -1. \end{cases}$$

This gives $(-c^2 + cd - d^2)y = c + dV$. i.e., So $-py = (c + dV)$, hence $c + dV \equiv 0 \pmod p$.

Conversely, if $c + dV \equiv 0 \pmod p$ but $\left(\frac{b}{\pi}\right)_3 \neq \omega$. Since b is a cubic non-residue modulo π, so $\left(\frac{b}{\pi}\right)_3 = \omega^2 = -1 - \omega$. Using a similar argument as above, we have integer x', y' such that

$$\begin{cases} cx' - dy' = V + 1 \\ dx' + (c - d)y' = 1. \end{cases}$$

But this gives us $py' = (c - d) - dV$. This would force $p|(2c - d)$. This is impossible as $p = \pi\overline{\pi}$ and $(2c - d) = \pi + \overline{\pi}$. □

Remark. *If $\left(\frac{g}{\pi}\right)_3 = \omega^2$, then $\left(\frac{g}{\overline{\pi}}\right)_3 = \omega$. Note that if π is primary, so is $\overline{\pi}$. Therefore, without loss of generality, we can always assume $\left(\frac{g}{\pi}\right)_3 = \omega$.*

We also need to compute the precise value of $\left(\frac{2}{\pi}\right)_3$. It is a well-know result that $\left(\frac{2}{\pi}\right)_3 = 1$ iff $c = 1 \pmod 2$ and $d = 0 \pmod 2$ [13] (Prop.9.6.1). It would be beneficial to have the whole spectrum of $\left(\frac{2}{\pi}\right)_3$, in order to perform certain computational tasks. Here we derive such a computational tool.

Lemma 3.2. *Let $p \equiv 1 \pmod 3$ and $p = c^2 - cd + d^2$ such that $\pi = c + d\omega$ is primary. Let $s = c \pmod 2, t = d \pmod 2$ (with $s, t \in \{0, 1\}$), then*

$$\left(\frac{2}{\pi}\right)_3 = \omega^{(s+1)t}. \tag{3}$$

Proof. Note that in $\mathbb{Z}[\omega]$, $N(2) = 2^2 = 4$. Since $N(\pi) \neq 3$ and $N(\pi) \neq N(2)$, the law of cubic reciprocity applies. So

$$\left(\frac{2}{\pi}\right)_3 = \left(\frac{\pi}{2}\right)_3.$$

By definition, $\left(\frac{\pi}{2}\right)_3 \equiv \pi^{\frac{N(2)-1}{3}} \pmod 2$, namely, $\left(\frac{\pi}{2}\right)_3 \equiv \pi \pmod 2$. This means that

$$\left(\frac{\pi}{2}\right)_3 \equiv s + t\omega \pmod 2.$$

This is equivalent to saying that

$$\left(\frac{\pi}{2}\right)_3 = \begin{cases} 1 & \text{if } c \text{ is odd, } d \text{ is even} \\ \omega & \text{if } c \text{ is even, } d \text{ is odd} \\ \omega^2 & \text{if } c \text{ is odd, } d \text{ is odd.} \end{cases}$$

Turn this to a single expression, we have proved our lemma. □

With all the preparation and computational tools, we are ready to our main result of this subsection.

Theorem 3.1. *Let $p \equiv 1 \pmod 3$ and $p = c^2 - cd + d^2$ such that $\pi = c + d\omega$ is primary, and $\left(\frac{g}{\pi}\right)_3 = \omega$. Let $s = c \pmod 2, t = d \pmod 2$, then for integer $0 \leq r < 6$,*

$$\#E_{g^r}(\mathbb{F}_p) = p + 1 + 2(-1)^r \Re\left(\omega^{2(s+1)t+r}(c + d\omega)\right). \tag{4}$$

More precisely, letting $m = 4(s+1)t \pmod 6$ and denote $\overline{m+j} = (m+j) \pmod 6$, we have

$$\#E_{g^m}(\mathbb{F}_p) = p + 1 - (d - 2c), \#E_{g^{\overline{m+1}}}(\mathbb{F}_p) = p + 1 + (c + d), \#E_{g^{\overline{m+2}}}(\mathbb{F}_p) = p + 1 - (c - 2d).$$

and all $\#E_{g^r}(\mathbb{F}_p)$ with $r = 0, 1, \cdots 5$ can be easily derived from these three cases.

Proof. We shall prove the theorem by using formula (2).

$$\#E_{g^r}(\mathbb{F}_p) = p + 1 + 2\left(\frac{g^r}{p}\right)\Re\left(\left(\frac{4g^r}{\pi}\right)_3 \pi\right).$$

Note that g^r is quadratic residue iff $2|r$, so $\left(\frac{g^r}{p}\right) = (-1)^r$. As we choose π to be such

that $\left(\frac{g}{\pi}\right)_3 = \omega$, so

$$\left(\frac{4g^r}{\pi}\right)_3 = \left(\frac{2}{\pi}\right)_3^2 \left(\frac{g^r}{\pi}\right)_3 = \omega^{2(s+1)t+r}.$$

Thus we have derived the formula for $\#E_{g^r}(\mathbb{F}_p)$:

$$\#E_{g^r}(\mathbb{F}_p) = p + 1 + 2(-1)^r \Re\left(\omega^{2(s+1)t+r}(c + d\omega)\right).$$

When $r = m = 4(s+1)t \pmod 6$, then r is an even number, $\omega^{2(s+1)t+r} = \omega^{6(s+1)t} = 1$, so

$$\#E_{g^r}(\mathbb{F}_p) = p + 1 + 2\Re\left((c + d\omega)\right) = p + 1 - (d - 2c).$$

Similarly, we get

$$\#E_{g^{\overline{m+1}}}(\mathbb{F}_p) = p + 1 + (c + d), \#E_{g^{\overline{m+2}}}(\mathbb{F}_p) = p + 1 - (c - 2d).$$

Note that E_{g^r} is a twist of $E_{g^{r+3}}$ by g [23], so $\#E_{g^r}(\mathbb{F}_p) + \#E_{g^r}(\mathbb{F}_p) = 2(p+1)$ holds. Since $m, \overline{m+1}, \overline{m+2}$ are three consecutive (in the sense of modulo 6) integer in $\{0,1,2,3,4,5\}$, the number of points for $E_{g^k}(\mathbb{F}_p)$ with $k \in \{0,1,2,3,4,5\} \setminus \{m, \overline{m+1}, \overline{m+2}\}$ is easy to get through its twist. □

Remark. *We can explicitly list all cases for the numbers $\#E_{g^r}(\mathbb{F}_p)$:*

$\#E_1(\mathbb{F}_p) = p+1-(d-2c)$,	$\#E_g(\mathbb{F}_p) = p+1-(-c-d)$,	$\#E_{g^2}(\mathbb{F}_p) = p+1-(c-2d)$,	*if c is odd, d is even,*
$\#E_1(\mathbb{F}_p) = p+1-(c-2d)$,	$\#E_g(\mathbb{F}_p) = p+1-(2c-d)$,	$\#E_{g^2}(\mathbb{F}_p) = p+1-(c+d)$,	*if c is even, d is odd,*
$\#E_1(\mathbb{F}_p) = p+1-(c+d)$,	$\#E_g(\mathbb{F}_p) = p+1-(2d-c)$,	$\#E_{g^2}(\mathbb{F}_p) = p+1-(d-2c)$,	*if c is odd, d is odd.*

Corollary 3.1. *We have the following invariants:*

1. *$\#E_1(\mathbb{F}_p)$ is an even number.*
2. $$\#E_1(\mathbb{F}_p) + \#E_g(\mathbb{F}_p) + \#E_{g^2}(\mathbb{F}_p) = 3(p+1) + \Re\left((c\omega + d\omega^2)\left(\frac{2}{\pi}\right)_3\right).$$
3. *For any $0 \le j \le \frac{p-7}{6}$,*

$$\#E_{g^{6j}}(\mathbb{F}_p) + \#E_{g^{6j+1}}(\mathbb{F}_p) + \#E_{g^{6j+2}}(\mathbb{F}_p) + \#E_{g^{6j+3}}(\mathbb{F}_p) + \#E_{g^{6j+4}}(\mathbb{F}_p) + \#E_{g^{6j+5}}(\mathbb{F}_p) = 6(p+1).$$

Proof. (1) and (2) follow directly by examining the formulas of $\#E_{g^r}(\mathbb{F}_p)$.

For (3), we know that

$$\begin{aligned} \#E_{g^{6j}}(\mathbb{F}_p) &+ \#E_{g^{6j+1}}(\mathbb{F}_p) + \#E_{g^{6j+2}}(\mathbb{F}_p) + \#E_{g^{6j+3}}(\mathbb{F}_p) + \#E_{g^{6j+4}}(\mathbb{F}_p) + \#E_{g^{6j+5}}(\mathbb{F}_p) \\ &= (\#E_1(\mathbb{F}_p) + \#E_{g^3}(\mathbb{F}_p)) + (\#E_g(\mathbb{F}_p) + \#E_{g^4}(\mathbb{F}_p)) + (\#E_{g^2}(\mathbb{F}_p) + \#E_{g^5}(\mathbb{F}_p)) \\ &= 6(p+1). \end{aligned}$$

□

Remark. *Certain sums of $\#E_{g^r}(\mathbb{F}_p)$ have been studied in literature. For example, the following were reported in [10, 14]:*

$$\sum_{r=0}^{p-2} \#E_{g^r}(\mathbb{F}_p) = \sum_{r=0}^{p-2} \#E_{g^{3r}}(\mathbb{F}_p) = p^2 - 1.$$

Our results can be used to produce even finer formulas

3.2 The case $p \equiv 2 \pmod 3$

For the case of $p \equiv 2 \pmod 3$, it is well-known that the curves $E_b : y^2 = x^3 + b$ are supersingular and $\#E_{g^r}(\mathbb{F}_p) = p + 1$. However, some interesting algebraic and computational properties are observed. Compared to the case $p \equiv 1 \pmod 3$ where there exist 6 isomorphism classes of groups of $\mathbb{F}_p$-rational points, this case has only one such class, namely, the class of cyclic group of size $p + 1$.

Here is our main result of this subsection.

Theorem 3.2. *Let $p \equiv 2 \pmod 3$ then*

1. *$E_b(\mathbb{F}_p)$ is a cyclic group.*
2. *There are efficiently computable group isomorphisms*

$$\phi : E_b(\mathbb{F}_p) \longrightarrow \begin{cases} E_1(\mathbb{F}_p) & \text{if } \left(\frac{b}{p}\right) = 1, \\ E_{-3}(\mathbb{F}_p) & \text{if } \left(\frac{b}{p}\right) = -1. \end{cases}$$

Proof. 1. By the structure theorem [20, 23], we know that there are positive integers n, m such that $n^2 m = p + 1$ and

$$E_b(\mathbb{F}_p) \cong \mathbb{Z}_n \oplus \mathbb{Z}_{nm}.$$

This implies that there are n^2 points in $E_b(\mathbb{F}_p)$ whose order divides n. Namely $E[n] \subset E_b(\mathbb{F}_p)$ where $E[n]$ is the n-torsion subgroup of $E_b(\overline{\mathbb{F}_p})$. By the Weil pairing over $E[n]$, we see that $\mu_n = \{x \in \overline{\mathbb{F}_p} : x^n = 1\} \subset \mathbb{F}_p^*$. This forces that $n|(p-1)$. However, n also divides $p + 1$, so n must be 1 or 2.

If $n = 2$, then $E_b(\mathbb{F}_p)$ contains 3 points of order 2. Assume these points are $(e_1, 0), (e_2, 0)$ and $(e_3, 0)$, then e_1, e_2, e_3 must be roots of $x^3 = -b$. This cannot be true as by lemma 2.1, $x^3 = -b$ has only one root.

So $n = 1$ and $E_b(\mathbb{F}_p) \cong \mathbb{Z}_{p+1}$.

2. If $\left(\frac{b}{p}\right) = 1$, then $b = \alpha^2$ for some $\alpha \in \mathbb{F}_p^*$. By lemma 2.1, $\alpha = \beta^3$ for some $\beta \in \mathbb{F}_p^*$.

This gives that $b = \beta^6$, and we can explicitly construct an isomorphism

$$\begin{array}{rl} \phi: & E_b(\mathbb{F}_p) \to E_1(\mathbb{F}_p) \\ & (x, y) \mapsto \left(\frac{x}{\beta^2}, \frac{y}{\beta^3}\right),\ \mathcal{O} \mapsto \mathcal{O}. \end{array}$$

If $\left(\frac{b}{p}\right) = -1$, then since $\left(\frac{-3}{p}\right) = -1$, as discussed above, we can get a $\beta \in \mathbb{F}_p^*$ such that $b = -3\beta^6$. This suggests us to use the isomorphism similar to the above.

$$\begin{array}{rl} \phi: & E_b(\mathbb{F}_p) \to E_{-3}(\mathbb{F}_p) \\ & (x, y) \mapsto \left(\frac{x}{\beta^2}, \frac{y}{\beta^3}\right),\ \mathcal{O} \mapsto \mathcal{O}. \end{array}$$

□

4 Searching for Koblitz Curves over Prime Fields

Recall that the binary Koblitz curves are the following elliptic curves defined over $E_a : y^2 + xy = x^3 + ax^2 + 1$ where $a \in \{0, 1\}$. To determine a practical useful Koblitz curves, one needs to find a prime number m such that $\#E_a(F_{2^m}) = n\#E_a(F_2)$ for a prime number n. This can be done easily by using zeta function as a formula for $\#E_a(F_{2^m})$ is available to be used.

We now consider a similar problem for the curve $E_b : y^2 = x^3 + b/\mathbb{F}_p$. With the explicit formula of $E_b(\mathbb{F}_p)$ derived in last section, checking whether $\#E_b(\mathbb{F}_p)$ is a prime or an almost prime (a small multiple of a prime number) becomes easy. Thus determining a practical useful Koblitz curve over prime fields is easy. We will describe such a procedure in this section.

In this section, we will work with primes of the form $3k + 1$. As mentioned earlier, such a prime can be factorized in $\mathbb{Z}[\omega]$:

$$p = c^2 - cd + d^2 = \pi\bar{\pi},$$

with $\pi = c + d\omega$ being primary, i.e., $c \equiv 2 \pmod 3$ and $d \equiv 0 \pmod 3$.

We have obtained explicitly computation of $\#E_b(\mathbb{F}_p)$ in the previous section. As $E_b(\mathbb{F}_p) \cong E_{g^r}(\mathbb{F}_p)$ for some $0 \leq r < 6$, the following table (Table 1) is the point counting summary. To simplify some notation, we use $\mathrm{Tr}(E_b)$ to denote the trace of E_b, namely, $\mathrm{Tr}(E_b) = p + 1 - \#E_b(\mathbb{F}_p)$

If a primitive root g modulo p is available, then we have the set of representatives of the 6 isomorphism classes of the curves: $E_1, E_g, E_{g^2}, E_{g^3}, E_{g^4}$ and E_{g^2}. Practically, this is often the case.

If no primitive root is given, we can still get a set of representatives of the 6 isomorphism classes of the curves, in deterministic polynomial time, assuming the Generalized Riemann Hypothesis (GRH). This is proved by the next proposition. We write

Table 1: Number of points summary for $E_b : y^2 = x^3 + b$

$(c,d) \pmod 2$	$\mathrm{Tr}(E_1$	$\mathrm{Tr}(E_g)$	$\mathrm{Tr}(E_{g^2})$	$\mathrm{Tr}(E_{g^3})$	$\mathrm{Tr}(E_{g^4})$	$\mathrm{Tr}(E_{g^5})$
$(1,0)$	$(d-2c)$	$-(c+d)$	$(c-2d)$	$-(d-2c)$	$(c+d)$	$(2d-c)$
$(0,1)$	$(c-2d)$	$(2c-d)$	$(c+d)$	$-(c-2d)$	$-(2c-d)$	$-(c+d)$
$(1,1)$	$(c+d)$	$(2d-c)$	$(d-2c)$	$-(c+d)$	$-(2d-c)$	$(2c-d)$

$H = \{t | t$ is the sixth power of an lement in $\mathbb{F}_p^*\}$, then H is a subgroup of $\mathbb{F}_p^*$.

Proposition 4.1. *Let $p \equiv 1 \pmod 3$ be a prime. Assuming GRH, there is a deterministic polynomial time algorithm outputs an element $z \in \mathbb{F}_p^*$ such that $1, z, z^2, z^3, z^4, z^5$ are in different cosets of H.*

Proof. An algorithm of Adleman, Manders, and Miller [2] states that for all m, under GRH, there is a deterministic polynomial time algorithm which on input $\alpha \in \mathbb{N}$, outputs the least $x \in \mathbb{N}$ such that $x^m = \alpha$, or "NO" if no such x exists.

Let $H_2 = \{s | s$ is a square in $\mathbb{F}_p^*\}$ and $H_3 = \{c | c$ is a cube in $\mathbb{F}_p^*\}$, then H_2 is a proper subgroup of $\mathbb{F}_p^*$, and since $p \equiv 1 \pmod 3$, H_3 is a proper subgroup of $\mathbb{F}_p^*$, by lemma 2.1.

Let n_q, n_c be the least primes that are not in H_2, H_3 respectively. It has been proved that, under GRH, $n_q, n_c < \log^2 p$, [3, 4, 17].

By the algorithm of Adleman, Manders, and Miller, checking whether $n_c \in H_2, n_q \in H_3$ is achievable in polynomial time. Therefore our result is prove by taking

$$z = \begin{cases} n_q & \text{if } n_q \notin H_3, \\ n_c & \text{if } n_c \notin H_2, \\ n_q n_c & \text{otherwise.} \end{cases}$$

□

We are now ready for a procedure of generating Koblitz curves over prime field for primes to be 1 modulo 3. The output is a number b so that $\#E_b(\mathbb{F}_p)$ is prime.

Procedure 4.1. *Searching Koblitz Curves $E_b : y^2 = x^3 + b/\mathbb{F}_p$ for $p \equiv 1 \pmod 3$.*

Input: prime number p such that $p \equiv 1 \pmod 3$; *Output: $b \in \mathbb{F}_p^*$ such that $\#E_b(\mathbb{F}_p)$ is prime, or "no such b exists".*
1. Write p as $c^2 - cd + d^2$ such that $\pi = c + d\omega$ is primary; *2. For each number in* *3. $p + 1 - \{(d - 2c), -(c + d), (c - 2d), -(d - 2c), (c + d), -(c - 2d)\}$* *4. check its primality;* *5. If a prime number, say n, is found* *6. Compute z as in proposition 4.1;* *7. Compute $\#E_{z^j}(\mathbb{F}_p)$ $(0 \le j < 6)$ by Schoof Algorithm;* *(*or by Schoof-Elkies-Atkin algorithm*)* *8. If for some j, $n = \#E_{z^j}(\mathbb{F}_p)$* *9. Return $b = z^j \pmod p$;* *10. Return "No prime order curve exists for this p";*

Remark. *1. Driving $p = c^2 - cd + d^2$ in step 1 and testing primality in step 4 can be achived in polynomial time. So under GRH, the procedure is deterministic polynomial time if we use Schoof point counting Algorithm in step 7.*

2. This procedure can be more practical if Schoof-Elkies-Atkin algorithm is used in step 7, and if we choose several random $z \in \mathbb{F}_p^*$ to check in step 6. Of course, it will be much better if a primitive root is used in this step.

3. For finding curves whose order is an almost prime number, we just need a slight modification to the above procedure.

Let us see an example.

Example. Let $p = 2^{256} - 2^{224} - 2^{32} + 19919$. This is a prime with $p \equiv 1 \pmod 3$. A primary factor for p is $\pi = c + d\omega$ where

$$\begin{aligned} c &= -68524741867453423335625304140397280874 \\ d &= 300805322263268044042343519469882788769. \end{aligned}$$

In this case, $g = 5$ is a primitive root, so the determination of useful curves is much easier. It is checked that $N = p + 1 + (c + d)$ is a prime. According to table 1, this is the number of point of $E_{g^5}(\mathbb{F}_p)$. In the same isomorphism class, we also find

$$E_{10}(\mathbb{F}_p), E_{11}(\mathbb{F}_p), E_{12}(\mathbb{F}_p), E_{17}(\mathbb{F}_p), E_{21}(\mathbb{F}_p), E_{23}(\mathbb{F}_p), \cdots .$$

The number $p + 1 - (2c - d)$ is an almost prime, in fact, $\frac{p+1-(2c-d)}{7}$ is a prime. This number corresponds to the group $E_g(\mathbb{F}_p)$. So, $E_5(\mathbb{F}_p)$ also has some cryptographic meaning.

5 Conclusion

In this paper, precise formulas for the number of $\mathbb{F}_p$-rational points of $E_b : y^2 = x^3 + b/\mathbb{F}_p$ are derived. When $p \equiv 1 \pmod 3$, the numbers are determined by the coefficients of a primary factor of p in the ring of Eisenstein integers. When $p \equiv 2 \pmod 3$, it is a well-known fact that the number of points of E_b is the constant $p + 1$, we consider the group structure and show that $E_b \cong \mathbb{Z}_{p+1}$.

Our results for the case of $p \equiv 1 \pmod p$ is used in searching prime (or almost prime) order Koblitz curves over prime fields. An efficient procedure is described.

Several useful tools are also developed in this paper.

References

[1] SEC 2: Recommended Elliptic Curve Domain Parameters, *https://www.secg.org/sec2-v2.pdf*, 2010.

[2] L. M. Adleman, K. L. Manders, and G. L. Miller, On taking roots in finite fields, *FOCS 1977*, pp. 175-178.

[3] N. C. Ankeny, The least quadratic non residue, *Ann. of Math.* (2)55(1952), 65-72.

[4] E. Bach, Explicit bounds for primality testing and related problems, *Math. Comp.* 55(1990), no. 191, 355-380.

[5] I. F. Blake, V. K. Murty and G. Xu, Efficient algorithms for Koblitz curves over fields of characteristic three, *Journal of Discrete Algorithms*, 3(2005)113-124.

[6] I. Blake, K. Murty and G. Xu, A note on window τ-NAF algorithm, *Information Processing Letters*, 95(2005), no. 5, 496-502.

[7] I. F. Blake, G. Seroussi and N. Smart, Elliptic Curves in Cryptography, Cambridge University Press, 1999.

[8] I. F. Blake, G. Seroussi and N. Smart, Advances in Elliptic Curve Cryptography, Cambridge University Press, 2005.

[9] H. Cohen, A Course in Computational Algebraic Number Theory, Springer, 2000.

[10] 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 $p \equiv 1 \pmod 6$) is prime, *Rocky Mountain J. Math.* 37 (2007), no. 5, 1483-1491.

[11] G. Frey and H. Ruck, A remark concerning m-divisibility and the discrete logarithm in the divisor class group of curves, *Mathematics of Computations*, **62** (1994) 865-874.

[12] R. Gallant, R. Lambert, and S. Vanstone, Fast point multiplication on elliptic curves with efficient endomorphisms, *Crypto 2001*, LNCS **2139**, 190-200.

[13] K. Ireland and M. Rosen, A classical introduction to modem number theory, Springer, 1990.

[14] W. Jeon, and D. Kim, The number of points on elliptic curves $y^2 = x^3 + Ax$ and $y^2 = x^3 + B^3$ MOD 24, *Communications of the Korean Mathematical Society*, 28(2013)433-447.

[15] N. Koblitz, CM-curves with good cryptographic properties, *Advances in Cryptology-CRYPTO '91*, LNCS **576**, 1992, 279-287.

[16] A. Lenstra, H. Lenstra, and L. Lovász, Factoring polynomials with rational coefficients, *Mathematische Annalen* 261 (1982) 515-534.

[17] Y. Lamzouri, X. Li, and K. Soundararajan, Conditional bounds forthe least quadratic non-residue and related problems, *Math. Comp.* 84(2015), no. 295,2391-2412.

[18] A. Menezes, T. Okamoto and S. Vanstone, Reducing elliptic curve logarithms to logarithms in a finite field, *IEEE Transactions on Information Theory*, **39** (1993), 1639-1646.

[19] A. R. Rajwade, On rational primes p congruent to 1 (mod 3 or 5), *Proc. Cambridge Philos. Sot.* 66 (1969), 61-70.

[20] J. H. Silverman The Arithmetic of Elliptic Curves, 2nd ed., Springer, 2009.

[21] J. Solinas, Efficient arithmetic on Koblitz curves, *Designs, Codes and Cryptography*, **19** (2000), 195-249.

[22] W. Trost and G. Xu, On the Optimal Pre-Computation of Window τNAF for Koblitz Curves, *IEEE Transactions on Computers*, 65(2016), 2918–2924.

[23] L. C. Washington, Elliptic Curves: Number Theory and Cryptography, Second Edition, *CRC Press*, 2008.

[24] K. S. Williams, Note on a cubic character sum, *Aeq. Math.* 12(1975), 229C231. (https://doi.org/10.1007/BF01836550)