A Note on Koblitz Curves over Prime Fields

Han Wu* and Guangwu Xu†

February 20, 2023

Abstract

Besides the well-known class of Koblitz curves over binary fields, the class of Koblitz curves $E_b : y^2 = x^3 + b/\mathbb{F}_p$ over prime fields with $p \equiv 1 \pmod 3$ is also of some practical interest. By refining a classical result of Rajwade for the cardinality of $E_b(\mathbb{F}_p)$, we obtain a simple formula of $\#E_b(\mathbb{F}_p)$ in terms of the norm on the ring $\mathbb{Z}[\omega]$ of Eisenstein integers, that is, for some $\pi \in \mathbb{Z}[\omega]$ with $N(\pi) = p$ and some unit $u \in \mathbb{Z}[\omega]$,

$$\#E_b(\mathbb{F}_p) = N(\pi + u)$$

holds. This establishes an interesting relation between the number of points on this class of curves and the number of elements of their underlying fields, they are given by the norm of two integers of $\mathbb{Z}[\omega]$ whose difference is just a unit. It is also interesting to note that such relationship has already been derived for the case of Koblitz curves over binary fields. Some tools that are useful in the computation of cubic residues are also developed.

Key words: Koblitz curves , Eisenstein integers
MSC(2020) 11A07, 11G20, 11T71

1 Introduction

A widely known class of Koblitz curves are curves defined over $\mathbb{F}_q$ for q relatively small, and a subgroup of the set of rational points over $\mathbb{F}_{q^n}$ is of interest. This

*School of Cyber Science and Technology, Shandong Universtiy, Qingdao 266237, China; e-mail: hanwu97@mail.sdu.edu.cn.

†School of Cyber Science and Technology, Shandong Universtiy, Qingdao 266237, China; e-mail: gxu4sdq@sdu.edu.cn. (Corresponding author)

approach allows efficient scalar point multiplication as well as point counting via the zeta function (e.g. [8, 9, 13, 2, 15]). Such curves can play an important role in certain elliptic curve cryptographic systems. The curves over prime fields $\mathbb{F}_p$ with large p and with a restricted set of coefficients are also of practical interest. This paper will focus on the latter. More specifically, we discuss the class of curves over a prime field $\mathbb{F}_p$ that take the form of

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

where the prime $p \equiv 1 \pmod 3$ and $b \in \mathbb{F}_p^{*1}$. This family of curves is referred to as Koblitz curves because it is a special case of CM curves with simple expression. One of such Koblitz curves described in the Standards for Efficient Cryptography Group (SECG)[1] is

$$\text{secp256k1:} \quad y^2 = x^3 + 7/\mathbb{F}_p$$

where $p = 2^{256} - 2^{32} - 977$ is a prime of 256 bits. This curve has been chosen by some applications (e.g., digital signatures for blockchain platforms Bitcoin and Ethereum).

For a rational prime $p \equiv 1 \pmod 3$, the efficient Lagrange-Gauss algorithm produces a pair of integers c, d such that $p = c^2 - cd + d^2$. In other words, $p = N(\pi = c + d\omega)$, the norm of prime $\pi = c + d\omega$ in the ring $\mathbb{Z}[\omega]$ of Eisenstein integers (we may further require π to be primary in the sense that $c \equiv 2 \pmod 3$ and $d \equiv 0 \pmod 3$).

In 1969, Rajwade [11] (see also [6]) developed a point counting formula for the curves $E_b/\mathbb{F}_p$ ($p \equiv 1 \pmod 3$) in terms of a primary factor π of p. We state the result using notation from [14], where a very clean and short treatment of Rajwade's result was described by Williams:

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

where $\left(\frac{\cdot}{p}\right)$ and $\left(\frac{\cdot}{\pi}\right)_3$ are the Legendre symbol and the cubic residue character respectively. We note that some later work reported point counting formulas similar to that of Rajwade's, e.g., [10, 12]. Some partial results for the number of points of $E_b/\mathbb{F}_p$ can also be found in [5, 7].

The main purpose of this note is to provide a refinement of Rajwade's formula by developing some tools for the computation of cubic residuosity. For prime $p \equiv 1$

[1]We note that when $p \equiv 2 \pmod 3$, $E_b/\mathbb{F}_p$ is known to be a supersingular curve and the group $E_b(\mathbb{F}_p)$ is a cyclic group of order $p + 1$.

(mod 3) with a primary factor π, we are able to derive a very elementary point counting formula for $E_b/\mathbb{F}_p$ in terms π: the number of points of $E_b(\mathbb{F}_p)$ is in fact the norm of the sum of π and a unit

$$\#E_b(\mathbb{F}_p) = N(\pi + u), \tag{2}$$

where u is a unit in $\mathbb{Z}[\omega]$. This result is interesting in several aspects, for examples, it has some applications to Koblitz curves over prime fields, including some new look of their cardinalities and efficient scalar multiplication. Another interesting note is that it establishes a close relationship between $\#E_b(\mathbb{F}_p)$ and $\#\mathbb{F}_p$, they are given by the the norms of two integers of $\mathbb{Z}[\omega]$ whose difference is just a unit in $\mathbb{Z}[\omega]$. It is remarked that such a relationship has already be derived for the class of Koblitz curves over binary fields by using the zeta function, where the ring of integers involved is $\mathbb{Z}(\frac{1-\sqrt{-7}}{2})$ (more detail is given later).

The rest of our paper is arranged into three sections. Section 2 provides some preliminaries and develops some tools. The main results and some discussions are given in the section 3.

2 Preliminaries

This section develops some tools that are useful in the computation of cubic residues and its applications.

Let $\omega = \frac{-1+\sqrt{-3}}{2}$. It is a basic fact that a prime $p \equiv 1 \pmod 3$ is the norm of $\pi = c + d\omega$ in the ring $\mathbb{Z}[\omega]$ of Eisenstein integers [6]. One can use lattice method to prove this fact constructively. We describe such a process below.

Lemma 2.1. *Given prime $p \equiv 1 \pmod 3$ and an integer $0 < U < p$ such that $U^2 + U + 1 \equiv 0 \pmod p$[2], one can find $c, d \in \mathbb{Z}$ in polynomial time such that*

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

Proof. Consider the lattice

$$\Lambda := \{(x, y) \in \mathbb{Z} \times \mathbb{Z} \mid Ux + y \equiv 0 \pmod p\}.$$

[2]Such U, which is a cubic root of unity in $\mathbb{F}_p$, can be easily found for most cases. In general, one can solve it in polynomial time under GRH.

Note that $\mathrm{vol}(\mathbb{R}^2/\Lambda) = p$, the classical Minkowski's convex body theorem says that one can find a nonzero shortest lattice vector $\mathbf{v}$ in the disc $B\big(0, 2\sqrt{\frac{p+0.1}{\pi}}\big)$ of radius $2\sqrt{\frac{p+0.1}{\pi}}$ centered at 0, as $\mathrm{vol}\big(B(0, 2\sqrt{\frac{p+0.1}{\pi}})\big) > 2^2 p$. This implies that $\|\mathbf{v}\|^2 \leq \frac{4(p+0.1)}{\pi}$.

Write $\mathbf{v} = (c, d)$, then there is an integer t such that $cU + d = tp$. We have

$$\begin{aligned} c^2 + d^2 - cd &= c^2 + (-Uc + tp)^2 - c(-Uc + tp) \\ &= c^2(U^2 + U + 1) + (tp - 2Uc - c)tp \equiv 0 \pmod{p}. \end{aligned}$$

On the other hand,

$$c^2 + d^2 - cd \leq \frac{3}{2}(c^2 + d^2) \leq \frac{6(p + 0.1)}{\pi} < 2p.$$

Since $c^2 + d^2 - cd$ is a nonzero multiple of p, we conclude that

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

Using the Lagrange-Gauss algorithm for two dimensional lattice [3], a shortest vector $\mathbf{v} = (c, d)$ of Λ can be found in polynomial time (in $\log p$). □

2.1 Cubic residues

Fix a prime $p \equiv 1 \pmod 3$. Let $\pi = c + d\omega$ be a prime in $\mathbb{Z}[\omega]$ such that $p = N(\pi)$ (i.e., $p = c^2 - cd + d^2$). We require π be *primary* in the sense that $c \equiv 2 \pmod 3$ and $d \equiv 0 \pmod 3$. These extra requirements can always be achieved. In fact, one can replace π by one of the elements in $A = \{\pm\pi, \pm\omega\pi, \pm\omega^2\pi\}$, as it is actually proved in [6] (Prop. 9.3.5) that there is exactly one primary element in A.

Recall that 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 value of $\left(\frac{\alpha}{\pi}\right)_3$ can be $1, \omega$ or ω^2, and $\left(\frac{\alpha}{\pi}\right)_3 = 1$ iff $x^3 = \alpha \pmod \pi$ is solvable.

Our next result provides a criterion to determine cubic residue for a rational integer in terms of rational integer operations.

Lemma 2.2. *Let $\pi = c + d\omega$ be a primary prime with respect to p. Let $0 < b < p$ be*

an integer and denote $V = b^{\frac{p-1}{3}} \pmod p$. *Then*

$$\left(\frac{b}{\pi}\right)_3 = \begin{cases} 1, & \text{if } V = 1, \\ \omega, & \text{if } c + dV \equiv 0 \pmod p, \\ \omega^2, & \text{if } c - d - dV \equiv 0 \pmod p. \end{cases}$$

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 $V - \omega = (c + d\omega)(x + y\omega) = (cx - dy) + (dx + (c - d)y)\omega$. This gives

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

From this, we see that

$$c + dV = (-c^2 + cd - d^2)y = -py \equiv 0 \pmod p.$$

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 can find integers x', y' such that

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

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

Corollary 2.1. *Let g be a primitive root g modulo p. If $\left(\frac{g}{\pi}\right)_3 = \omega^2$, then $\left(\frac{g}{\overline{\pi}}\right)_3 = \omega$.*

Proof. This is simply because $\overline{\pi} = (c - d) - d\omega$, so lemma 2.2 gives the result. □

In some applications (as we shall see in the next section), one chooses a fixed and small primitive root g modulo p and wishes that $\left(\frac{g}{\pi}\right)_3 = \omega$ to make discussion and

calculation cleaner, where π is a primary prime such that $\pi\bar{\pi} = p$. If $\left(\frac{g}{\pi}\right)_3 = \omega^2$, then $\left(\frac{g}{\bar{\pi}}\right)_3 = \omega$. Note that if π is primary, so is $\bar{\pi}$. Therefore, by switching π to $\bar{\pi}$ if necessary, 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-known result that $\left(\frac{2}{\pi}\right)_3 = 1$ iff $c = 1 \pmod 2$ and $d = 0 \pmod 2$ [6] (Prop.9.6.1). However, it is different from the quadratic case as one is not able to get the exact information for the case that 2 is not a cubic residue modulo π. 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 2.3. *Let $\pi = c + d\omega$ be a primary prime with respect to p. 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. □

3 The Main Results

For the curve $E_b : y^2 = x^3 + b/\mathbb{F}_p$ with prime $p \equiv 1 \pmod 3$, there are many results on its point counting in the literature, some of them can be found in [5, 6, 7, 11, 12, 14]. The approaches are mainly based on cubic character sum as it is a CM curve and the number of points is governed by a Hecke character. The first result of this section shows that $\#E_b(\mathbb{F}_p)$ also has a clean formula in terms of the norm function.

An early study on the equation $y^2 = x^3 + b \bmod p$ with $p \equiv 1 \pmod 3$ can be found in [11]. In that paper, Rajwade derived a formula for points on $E_b/\mathbb{F}_p$ based on cubic character sum. The following statement of Rajwade's theorem is taken from [14].

Theorem (Rajwade)**.** *Let $p \equiv 1 \pmod 3$ be a prime number and π be primary such that $p = N(\pi)$. Then*

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

Remarks. *From the theorem, we see that $\#E_b(\mathbb{F}_p) = p+1+2\left(\frac{b}{p}\right)\Re\left(\left(\frac{4b}{\pi}\right)_3\pi\right)$. This indicates that there are 6 possible different cardinalities for the groups $E_b(\mathbb{F}_p)$ with p fixed. In fact, it was proved in [7] that for a 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 $(x, y) \mapsto \left(\frac{x}{g^{2q}}, \frac{y}{g^{3q}}\right)$ extends to an isomorphism $E_b(\mathbb{F}_p) \cong E_{g^r}(\mathbb{F}_p)$.

With those tools developed in Section 2 and Rajwade's theorem, we are able to describe an explicit formula for the number of points in $E_b(\mathbb{F}_p)$ in a very simple form.

Theorem 3.1. *Let $p \equiv 1 \pmod 3$ be a prime number and $\pi = c + d\omega$ be primary such that $p = N(\pi)$. Denote $s = c \pmod 2, t = d \pmod 2$. Then for a primitive root g modulo p with $\left(\frac{g}{\pi}\right)_3 = \omega$, we have for each $j = 0, 1, \cdots, 5$,*

$$\#E_{g^j}(\mathbb{F}_p) = N\big(\pi + u\big),$$

where $u = (-1)^j \omega^{(s+1)t-j}$ *is a unit in* $\mathbb{Z}[\omega]$.

Proof. We shall prove the theorem by using the formula:

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

Note that g^j is a quadratic residue iff $2|j$, so $\left(\frac{g^j}{p}\right) = (-1)^j$. Lemma 2.3 is crucial in our proof, it tells us that $\left(\frac{2}{\pi}\right)_3 = \omega^{(s+1)t}$. Together with the fact that $\left(\frac{g}{\pi}\right)_3 = \omega$, we have

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

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

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

On the other hand

$$\begin{aligned} N\left(\pi + (-1)^j \omega^{(s+1)t-j}\right) &= (\pi + (-1)^j \omega^{(s+1)t-j})(\overline{\pi} + (-1)^j \overline{\omega^{(s+1)t-j}}) \\ &= p + (-1)^j (\pi \overline{\omega^{(s+1)t-j}} + \overline{\pi}\omega^{(s+1)t-j}) + 1 \\ &= p + 1 + 2(-1)^j \Re\left(\omega^{2(s+1)t+j}\pi\right). \end{aligned}$$

Thus the theorem is proved. □

Remarks. *1. This result is for Koblitz curves* E_b *over prime field* $\mathbb{F}_p$*, for* $\pi \in \mathbb{Z}[\omega]$ *with* $p = N(\pi)$*, there is a unit* u *of* $\mathbb{Z}[\omega]$ *such that*

$$\#E_b(\mathbb{F}_p) = N(\pi + u).$$

Recall that a different family of Koblitz curves over binary field $\mathbb{F}_q$ *with* $q = 2^m$*, one of the earliest families of CM curves used in cryptography, is defined as*

$$E_a : y^2 + xy = x^3 + ax^2 + 1/\mathbb{F}_q, \ a \in \mathbb{F}_2.$$

Let $\tau = \frac{(-1)^{1-a}+\sqrt{-7}}{2}$ *(it corresponds to the Frobenius map on* $E_a(\mathbb{F}_q)$*), then* $q = N(\tau^m)$ *in the ring* $\mathbb{Z}[\tau]$*. It is interesting to note that the above result for* $E_b/\mathbb{F}_p$ *is comparable to that of* $E_a/\mathbb{F}_q$ *for binary case. In fact, by using zeta*

function, it is proved that for the unit $u = -1$ in $\mathbb{Z}[\tau]$

$$\#E_a(\mathbb{F}_q) = N(\tau^m + u)$$

holds [9].

2. *Certain sums of $\#E_{g^r}(\mathbb{F}_p)$ have been studied in literature. For example, the following were reported in [5, 7]:*

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

We would like to remark that this can be actually derived in a straightforward manner by using our explicit formula, e.g.,

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

In fact, more finer formulas can be produced.

3. *Finally, we remark that with a minor modification, the primitive root g in theorem 3.1 can be replaced by z defined below. Let n_q and n_c be the least primes that are quadratic non-residue and cubic non-residue modulo p respectively, let* $z = \begin{cases} n_q & \text{if } n_q \text{ is not a cube} \\ n_c & \text{if } n_c \text{ is not a square} \\ n_q n_c & \text{otherwise.} \end{cases}$ *Under GRH, z can be found in polynomial time.*

Acknowledgement

This work is partially supported by the National Natural Science Foundation of China (No. 12271306) and National Key R&D Program of China (grant No. 2022YFB2701700).

References

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

[2] I. F. Blake, V. K. Murty and G. Xu, Nonadjacent radix-τ expansions of integers in Euclidean imaginary quadratic number fields, *Canadian Journal of Mathematics*, 60(2008), 1267-1282.

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

[4] I. B. Damgård and G. S. Frandsen. Efficient algorithms for the gcd and cubic residuosity in the ring of Eisenstein integers, Journal of Symbolic Computation 39 (2005) 643-652.

[5] 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.

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

[7] 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.

[8] N. Koblitz, Algebraic Aspects of Cryptography, Springer, 1999.

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

[10] H. Kuwakado and K. Koyama, Efficient cryptosystems over elliptic curves based on a product of form-free primes, *IEICE Trans. Fundamentals*, Vol. E77-A, No. 8 (1994) pp. 1309-1318.

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

[12] K. Rubin and A. Silverberg, Choosing the correct elliptic curve in the CM method, *Mathematics of Computation*, 79(269), 545-561.

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

[14] K. S. Williams, Note on a cubic character sum, *Aeq. Math.* 12(1975), 229-231. (https://doi.org/10.1007/BF01836550)

[15] W. Yu and G. Xu, Pre-computation scheme of window τNAF for Koblitz curves revisited. *EUROCRYPT 2021*, pp. 187-218, Springer, Heidelberg, 2021.