CREAT. MATH. INFORM.
Volume **31** (2022), No. 1,
Pages 51 - 56

Online version at https://semnul.com/creative-mathematics/
Print Edition: ISSN 1584 - 286X; Online Edition: ISSN 1843 - 441X
DOI: https://doi.org/10.37193/CMI.2022.01.05

Counting points on elliptic curves modulo a prime power

JASBIR S. CHAHAL and OMAR KHADIR

ABSTRACT. Let $p > 3$ be a prime number and $r > 0$ an integer. In this paper, we give a formula for counting the points of elliptic curves over the modular ring $\mathbb{Z}/p^r\,\mathbb{Z}$.

1. INTRODUCTION

During the last fifteen years of the last century, there were several major breakthroughs in number theory, which rendered the study of elliptic curves indispensable. Most of them were triggered by Frey's paper [6] in which he proposed a strategy to prove Fermat's Last Theorem by converting it into a problem in the arithmetic of elliptic curves. Following Frey's suggestion, Ribet [21] proved that a proof of (a weaker version of) the so-called Taniyama-Shimura conjecture proves Fermat's Last Theorem. It was this weaker version of the Taniyama-Shimura conjecture which Wiles [26] proved to complete the proof. It was truly a monumental achievement. Fermat's Last Theorem had defied all attempts to prove it for over three centuries. Another important, but unrelated to the proof of Fermat's Last Theorem, is Lenstra's paper [15] on factoring integers with elliptic curves. Although his method was inspired by the classical Pollard's (p - 1) method, it is much more powerful. Miller [17] suggested an analogue of the Diffie-Hellman protocol for sharing a common secret key before communicating over a public channel while Koblitz [11] proposed an analogue of Massey-Omura and ElGamal cryptosystems.
In 1991 the KMOV cryptosystem [12], based on a combination of RSA and the elliptic curves was published. It was an important application of elliptic curves to public key cryptography.
The elliptic curves method defined over finite fields $\mathbb{F}_q$ of q elements are well-suited for constructing secure cryptosystems [5, 13, 19]. To this end one needs to compute the number of the points on the curve [10, p. 423], [2].
The first deterministic polynomial time algorithm was constructed in 1985 by Schoof [7, 22, 23]. It was improved successively by Atkin [1] and Elkies [4]. However the method is practical only if q is small. In [14], the authors discuss the equivalence between counting points modulo n and factoring n.
In this work, we give a formula for $\#E_n(a, b)$, the number of solutions of the equation

$$y^2 = x^3 + ax + b \pmod{n} \tag{1.1}$$

when n is a power prime. To the best of our knowledge, this problem has not been studied before.
The paper is organized as follows: In Section 2 we present an overview of elliptic curves. In Section 3, we describe our contribution. Section 4 contains an application of our formula to a special case. We conclude our discussion in Section 5.
Throughout this paper, we shall use standard notation. In particular, $\mathbb{N}$ (resp. $\mathbb{N}^+$) is the

Received: 21.05.2021. In revised form: 08.11.2021. Accepted: 15.11.2021
2010 *Mathematics Subject Classification.* 14H52, 11T71.
Key words and phrases. *elliptic curves, Hensel's lemma.*
Corresponding author: Omar Khadir; khadir@hotmail.com

set of non-negative (resp. positive) integers. The cardinality of a set S is denoted by $\#S$. Let $f(x,y)$ be a polynomial with cœfficients in $\mathbb{Z}$ and n an integer. By

$$f(x,y) \equiv 0 \pmod{n} \tag{1.2}$$

we mean the equation

$$f(x,y) = 0 \tag{1.3}$$

over the ring $A = \mathbb{Z}/n\mathbb{Z}$ obtained from (1.2) by its reduction modulo n. By a solution of (1.2) we mean a solution of (1.2) with (x,y) in A.
We begin with a brief review of elliptic curves. (For details, see [1, 3, 8, 24, 25]).

2. Overview on elliptic curves

1) Elliptic curves over the Field $\mathbb{R}$
Let a, b be two fixed numbers in $\mathbb{R}$ with $4a^3 + 27b^2 \neq 0$. The elliptic curve E, or $E(a,b)$ to show its dependence on a, b, defined over $\mathbb{R}$ or ($E/\mathbb{R}$ for short) is the set of points (x,y) in the projective plane $\mathbb{P}^2$ that verify

$$y^2 = x^3 + ax + b. \tag{2.4}$$

If $P = (x_1, y_1)$ and $Q = (x_2, y_2)$ are two points on the affine part of E then the line (PQ) will necessary meet the curve in a third point $R = (x_3, y_3)$. When $P = Q$ the line (PQ) becomes the tangent. To ovoid singular points, we suppose that $4a^3 + 27b^2 \neq 0$. When $x_1 = x_2$ and $y_1 = -y_2$, i.e when (PQ) is vertical, R is the point at infinity at both end of this line, denoted by O.
We define an addition on $E(a,b)$ by setting $P+Q$ to be the reflection R' of R in the $x-axis$, i.e. $P + Q = (x_3, -y_3)$. See Figure 1.
The following is well-known.

Theorem 2.1. *The set $E(a,b)$ is an Abelian group.*

From the geometrical situation, we can compute purely algebraically the coordinates x_3, y_3. Indeed:

$$\begin{cases} \text{1. If } x_1 \neq x_2 \text{ then } \begin{cases} x_3 = \lambda^2 - (x_1 + x_2) \\ y_3 = \lambda(x_1 - x_3) - y_1 \end{cases} \quad \text{where } \lambda = \dfrac{y_2 - y_1}{x_2 - x_1}. \\ \text{2. If } x_1 = x_2 \text{ and } y_1 = y_2 = 0 \text{ then } P + Q = O. \\ \text{3. If } x_1 = x_2 \text{ and } y_1 = -y_2 \text{ with } y_1 \neq 0, \text{ then } P + Q = O. \\ \text{4. If } x_1 = x_2 \text{ and } y_1 = y_2 \neq 0 \text{ then } \begin{cases} x_3 = \lambda^2 - 2x_1 \\ y_3 = \lambda(x_1 - x_3) - y_1 \end{cases} \\ \quad \text{where } \lambda = \dfrac{3x_1^2 + a}{2y_1}. \end{cases} \tag{2.5}$$

Now let $n > 1$ be an integer and a, b in $\mathbb{Z}$ with $4a^3 + 27b^2 \not\equiv 0 \bmod n$. We denote by $E_n(a,b)$ the set of solutions of the elliptic curve

$$y^2 \equiv x^3 + ax + b \pmod{n} \tag{2.6}$$

in the ring $A = \mathbb{Z}/n\mathbb{Z} = \{0, 1, \ldots, n-1\}$. In this set up, we lose the geometry, but algebraically everything works perfectly. Let us first assume that $n = p$, an odd prime, so that A is the finite field $\mathbb{F}_p$ of p elements.

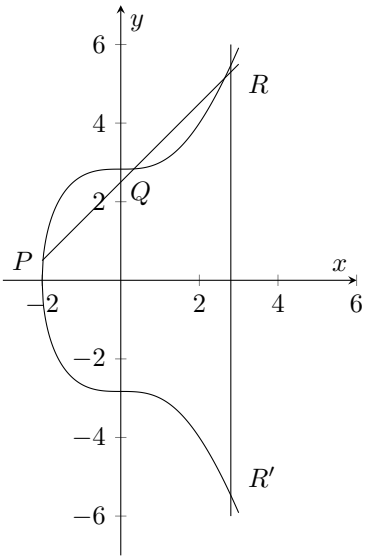

Figure 1. The elliptic curve $y^2 = x^3 + 8$

2) Elliptic curves over the field $\mathbb{F}_p = \mathbb{Z}/p\mathbb{Z} = \{0, 1, \ldots, p-1\}$
We define the elliptic curve $E/\mathbb{F}_p$ as the set $E(\mathbb{F}_p)$ of points with coordinates $\mathbb{F}_p$ $(a, b \in \mathbb{F}_p)$ on the affine curve defined by

$$y^2 \equiv x^3 + ax + b, \tag{2.7}$$

togetter with its point O at infinity.
Because $\mathbb{Z}/p\mathbb{Z}$ is a field, we can define the addition operation by taking the formulas (2.5) in the field $\mathbb{F}_p$. The set $E(\mathbb{F}_p)$ is again a finite Abelian group with O as the identity.
The following estimate on the cardinality of $E(\mathbb{F}_p)$ is a famous theorem of Hasse, he proved in 1934, (Cf. [3, 11]).

Theorem 2.2.

$$|\#E(\mathbb{F}_p) - (p+1)| \leq 2\sqrt{p}. \tag{2.8}$$

Note that (2.8) remains valid if p is replaced by $q = p^r$, $r \geq 1$, (See [3]).

3) Elliptic curves over the ring $\mathbb{Z}/n\mathbb{Z}$
We now assume that n is arbitrary, not necessary a prime. Again we denote the set of solutions of (1.1) in $\mathbb{Z}/n\mathbb{Z}$ by $E_n(a, b)$. We cannot define an addition operation on, say unequal points $P_j = (x_j, y_j)$ in $E_n(a, b)$, $j = 1, 2$, unless $x_1 - x_2$ is a unit in the ring $\mathbb{Z}/n\mathbb{Z}$, which happens if and only if $x_1 - x_2$ is coprime to n, the failure of which is in fact the main idea behind the elliptic curve method to find factors of n.

3. Our contribution

Let $p > 3$ be a prime number, $r > 1$ an integer and $a, b \in \mathbb{Z}$ with $4a^3 + 27b^2 \not\equiv 0 \bmod p$.

Now consider a fixed point (X_0, Y_0) in $E_{p^{r-1}}(a, b)$ such that $0 \leq X_0, Y_0 < p^{r-1}$. We put

$$A_{(X_0,Y_0)} = \{(x, y) \in E_{p^r}(a, b) \mid x \bmod p^{r-1} \text{ is } X_0 \text{ and } y \bmod p^{r-1} \text{ is } Y_0\}. \tag{3.9}$$

Lemma 3.1. *If $-\dfrac{a}{3}$ is not a square modulo p then the cardinality of the set $A_{(X_0,Y_0)}$ is p.*

Proof. For each natural integer $i \in \{0, 1, 2, \ldots, p-1\}$, put $Y_i = Y_0 + ip^{r-1}$. Define the polynomials $f_{Y_i}(X) = X^3 + aX - {Y_i}^2 + b$. We have $f_{Y_i}(X_0) \equiv 0 \bmod p^{r-1}$ and $f'_{Y_i}(X_0) \equiv f'_{Y_0}(X_0) \not\equiv 0 \bmod p$. So by Hensel's lifting lemma [20, p. 87] there exists a unique element x_i, $0 \leq x_i < p^r$, such that $f_{Y_i}(x_i) \equiv 0 \bmod p^r$ and $x_i \bmod p^{r-1} = X_0$. Therefore the point (x_i, Y_i) belongs to the elliptic curve $E_{p^r}(a, b)$. As, modulo p^r, all the constructed values Y_i are different, we conclude that the cardinality of $A_{(X_0,Y_0)}$ is at least equal to p.
Consider $(x, y) \in A_{(X_0,Y_0)}$, $0 \leq y < p^r$. The Euclidean division of y by the prime power p^{r-1} gives : $y = p^{r-1}q + s$ where $0 \leq q < p$ and $0 \leq s < p^{r-1}$. By the definition of the set $A_{(X_0,Y_0)}$ we have $y \bmod p^{r-1} = Y_0$. So $s = Y_0$ and then $y = Y_q$. Moreover, the integer x verifies simultaneously $f_{Y_q}(x) \equiv 0 \bmod p^r$ and X_0 is the reduction of x mod p^{r-1}. By the uniqueness of elements x_i in Hensel's lemma, x must be equal to x_q. So $(x, y) = (x_q, Y_q)$ and then the cardinality of the set $A_{(X_0,Y_0)}$ cannot be greater than p. Therefore $\#A_{(X_0,Y_0)} = p$. □

The hypothesis of the lemma means that integers a and -3 must not be both squares or both non-squares modulo p. And since exactly half of the elements in the multiplicative group $(\mathbb{Z}/p\mathbb{Z})^*$ are squares [9, p. 289], the parameter a has at least $(p-1)/2$ possibilities. We now give examples of elliptic curves $E_{p^r}(a, b)$ for which parameter a satisfies the hypothesis of Lemma 3.1.

Example 3.1. 1) Let g be a primitive root modulo p. Set $a = -3g \bmod p$.
We have $(\frac{-a}{3})^{\frac{p-1}{2}} \equiv g^{\frac{p-1}{2}} \equiv -1 \bmod p$. The equation of the associate elliptic curve is $y^2 \equiv x^3 - 3gx + b \bmod$.
2) Let $p = 2q + 1 > 7$ be a safe prime [16, p. 164] [18, p. 171].
a) As $g = -3$ is always a primitive root modulo p. So the elliptic curve defined by $y^2 \equiv x^3 + a^2x + b \bmod p$, $a \not\equiv 0 \bmod$, satisfies the lemma.
b) If $q \equiv 1 \bmod 4$, $g = 2$ is a primitive root then $a = -3g = -6$. The equation of the elliptic curve is $y^2 \equiv x^3 - 6x + b \bmod p$.
c) If $q \equiv 3 \bmod 4$, $g = -2$ is a primitive root then $a = -3g = 6$. The equation of the elliptic curve is $y^2 \equiv x^3 + 6x + b \bmod p$.

Lemma 3.2. *Let $p > 3$ be a prime integer. If $-\frac{a}{3}$ is not a square modulo p then the sets $A_{(X,Y)}$ with (X, Y) in $E_{p^{r-1}}(a, b)$ are all pairwise disjoint.*

Proof. Let (X, Y) and (X', Y') be two distinct points in $E_{p^{r-1}}(a, b)$.
Suppose that the intersection of the two sets $A_{(X,Y)}$ and $A_{(X',Y')}$ is not empty. Let $(x, y) \in A_{(X,Y)} \cap A_{(X',Y')}$. We have;:
$(x, y) \in A_{(X,Y)} \Longrightarrow (x, y) \in E_{p^r}(a, b)$, $x \bmod p^{r-1}$ is X and $y \bmod p^{r-1}$ is Y.
Also $(x, y) \in A_{(X',Y')} \Longrightarrow x \bmod p^{r-1}$ is X' and $y \bmod p^{r-1}$ is Y'. As $x \bmod p^{r-1}$ and $y \bmod p^{r-1}$ are unique, we get $X = X'$ and $Y = Y'$. This is a contradiction with the fact that $(X, Y) \neq (X', Y')$. □

Theorem 3.3. *Let $p > 3$ be a prime integer and $r \in \mathbb{N}^+$. If $-\frac{a}{3}$ is not a square modulo p then*

$$\#E_{p^r}(a, b) = p^{r-1}\#E_p(a, b) \tag{3.10}$$

Proof. It is easy to check that every element (x, y) of $E_{p^r}(a, b)$ is also an element of the set $A_{(X_0,Y_0)}$ where $X_0 = x \bmod p^{r-1}$ and $Y_0 = y \bmod p^{r-1}$. On an other hand, by Lemma 3.1 and Lemma 3.2, the collection $A_{(X,Y)}$ where (X, Y) are in $E_{p^{r-1}}(a, b)$ constitues a partition

of $E_{p^r}(a,b)$. Therefore $\#E_{p^r}(a,b) = \sum_{(X,Y)\in E_{p^{r-1}}(a,b)} \#A_{(X,Y)} = p\#E_{p^{r-1}}(a,b)$. The proof follows by an induction on the natural number r. □

By Theorem 3.3 and the Schoof algorithm [22, 23] we are able to efficiently compute the cardinality of $E_{p^r}(a,b)$.

Let n be a natural number. By the fundamental theorem of arithmetic, $n = \prod_{i=1}^{r} p_i^{\alpha_i}$, where $r \in \mathbb{N}^+$ and the p_i are prime integers. Putting together, we have the following result:

Corollary 3.1. *If for all $i \in \{1,2,\ldots,r\}$, $p_i > 3$ and $-\frac{a}{3}$ is not a square modulo p_i then*

$$\#E_n(a,b) = \prod_{i=1}^{r} p_i^{\alpha_i - 1} \prod_{i=1}^{r} \#E_{p_i}(a,b) \tag{3.11}$$

Proof. By the Chinese remainder theorem the curve $E_n(a,b)$ is isomorphic to the cartesian product $\prod_{i=1}^{r} E_{p_i^{\alpha_i}}(a,b)$. So:

$$\#E_n(a,b) = \prod_{i=1}^{r} \#E_{p_i}(a,b) = \prod_{i=1}^{r} p_i^{\alpha_i-1}\#E_{p_i}(a,b) = \prod_{i=1}^{r} p_i^{\alpha_i-1} \prod_{i=1}^{r} \#E_{p_i}(a,b).$$ □

4. Applications

The results of Section 3 lead to some new ones.

Proposition 4.1. *Let $p > 3$ be a prime number such that $p \equiv 3 \bmod 4$ and let $r \in \mathbb{N}^+$. Suppose that $a \not\equiv 0 \bmod p$. If $\frac{a}{3}$ is a square modulo p then the cardinality of the elliptic curve $y^2 \equiv x^3 + ax \bmod p^r$ is p^r.*

Proof. Let p be a prime number and $a \not\equiv 0 \bmod p$. If $p \equiv 3 \bmod 4$ then the cardinality of the elliptic curve $E_p(a,0)$ defined by $y^2 \equiv x^3 + ax \bmod p$ is p, see for instance [25, p. 115]. Here we don't count the neutral element O. The rest is an immediate consequence of Theorem 3.3. □

We also have the fact:

Proposition 4.2. *Let $p = \alpha^2 + \beta^2$ be a prime number such that $p \equiv 1 \bmod 4$, $\alpha, \beta \in \mathbb{N}$, β even and $\alpha + \beta \equiv 1 \bmod 4$. We Suppose that $a \not\equiv 0 \bmod p$.*
If $\frac{a}{3}$ is a square modulo p, then for any $r \in \mathbb{N}$, the cardinality of $E_{p^r}(a,0)$ defined by $y^2 \equiv x^3 + ax \bmod p^r$ is:
$p^{r-1}(p-2\alpha)$ if $-a$ is a fourth power modulo p,
$p^{r-1}(p+2\alpha)$ if $-a$ is a square power modulo p but not a fourth power modulo p, and
$p^{r-1}(p \pm 2\beta)$ if $-a$ is not a fourth power modulo p.

Proof. Use Theorem 3.3 and see [25, p. 115] for the cardinality of $y^2 \equiv x^3 + ax \pmod p$ when $p \equiv 1 \pmod 4$. □

5. Conclusion

This paper reduces the problem of counting points on $E_{p^r}(a,b)$ to that of counting points on $E_p(a,b)$

REFERENCES

[1] Atkin, A. O. L. *The Number of points on an elliptic curve modulo a prime.* manuscript, Chicago IL, January 1, (1988).

[2] Borissov, Y.; Markov, M. An Efficient Approach to Point-Counting on Elliptic Curves from a Prominent Family over the Prime Field $\mathbb{F}_p$. *Mathematics* **9** (2021), no. 12, 1431, https://doi.org/10.3390/math9121431

[3] Chahal, J.; Osserman, B. Riemann hypothesis for elliptic curves. *Amer. Math. Monthly* **115**, (2009), 431–442.

[4] Elkies, N. D. *Explicit Isogenies*. manuscript, Boston MA, (1992).

[5] Fangguo, Z.; Zhuoran, Z.; Peidong, G. ECC^2: error correcting code and elliptic curve based cryptosystem. *Inform. Sci.* **526** (2020), 301–320.

[6] Frey, G. Links between stable elliptic curves and certain diophantine equations. *Ann. Univ. Sarav. Ser. Math.* **1** (1986), no. 1, 1–40.

[7] Gaudry, P. *Algorithmes de comptage de points d'une courbe définie sur un corps fini*, Explicit methods in number theory, Panor. Synthśes, **36**, Soc. Math. France, Paris, (2013), 19-49.

[8] Hankerson, D.; Menezes, A.; Vanstone, S. Guide to elliptic curve cryptography. *Springer-Verlag, New York* 2004.

[9] Ireland, D.; Rosen, A. *A classical introduction to modern number theory*. Second edition, Springer, (1990).

[10] Joux, A. *Algorithmic cryptanalysis*. Chapman & Hall, (2009).

[11] Koblitz, N. Elliptic Curve Cryptosystems. *Math. Comp.* **48** (1987), no. 177, 203–209.

[12] Koyama, K.; Maurer, U. M.; Okamoto, T.; Vanstone, S. A. *New publickey schemes based on elliptic curves over the ring* $\mathbb{Z}_n$. LNCS 576, Proceedings of Crypto'91, Springer-Verlag, pp. 252–266, (1992).

[13] Kumar, M.; Gupta, P. An Efficient and Authentication Signcryption Scheme Based on Elliptic Curves. *Matematika* **35** (2019), No. 1, 1–11.

[14] Kunihiro, N.; Koyama, K. Equivalence of counting the number of points on elliptic curve over the ring $\mathbb{Z}_n$ and factoring n. *Lecture Notes in Comput. Sci.* **1043** (1998), 47–58.

[15] Lenstra, H. W., Jr. Factoring integers with elliptic curves. *Ann. of Math.* **126** (1987), 649–673.

[16] Menezes, J. A.; Van Oorschot, P. C.; Vanstone, S. A. *Handbook of applied cryptography*. CRC press, (1996).

[17] Miller, V. S. Use of elliptic curves in cryptography. *Advances in cryptology*—CRYPTO '85 *(Santa Barbara, Calif., 1985)*, 417–426, Lecture Notes in Comput. Sci., 218, *Springer, Berlin*, (1986).

[18] Mollin, R. *An introduction to cryptography*. Second edition, Chapman. & Hall/CRC, (2007).

[19] Naveed, A. A.; Ikram, U.; Hayat, U. A fast and secure public-key image encryption scheme based on Mordell elliptic curves. *O*pt Lasers Eng. **137** (2021).

[20] Niven, I.; Zuckerman, H. S.; Mongomery, H. L. *An introduction to the theory of numbers*. Fifth edition, John Wiley & sons corp, (1991).

[21] Ribet, K. A. *From the Taniyama-Shimura conjecture to Fermat's last theorem*, Annales de la faculté des sciences de Toulouse, 5e série, **11** (1990), no. 1, 116–139.

[22] Schoof, R. *Elliptic curves over finite fields and the computation of square roots mod* p. Math. Comp. **43** (1985), 483–494.

[23] Schoof, R. *Counting points of elliptic curves over finite fields*. J. Th. des Nombres, Bordeau, **7** (1995), 219–254.

[24] Silverman, J. H. *The arithmetic of elliptic curves*. Second edition, Springer, (2009).

[25] Washington, L. C. *Elliptic curves, number theory and cryptography*. Second edition, Taylor & Francis (2008).

[26] Wiles, A. Modular elliptic curves and Fermat's last theorem. *Ann. of Math.* **141** (1995), 443–551.

DEPARTMENT OF MATHEAMTICS
BRIGHAM YOUNG UNIVERSITY
PROVO, UT 84602-6539, USA
Email address: jasbir@math.byu.edu

HASSAN II UNIVERSITY OF CASABLANCA
LABORATORY OF MATHEAMTICS, CRYPTOGRAPHY
MECHANICS AND NUMERICAL ANALYSIS
FSTM, MOHAMMEDIA, MOROCCO
Email address: khadir@hotmail.com