# An $O(\log^2 p)$ Approach to Point-Counting on Elliptic Curves From a Prominent Family Over the Prime Field $\mathbb{F}_p$

Yuri Borissov
*Department of Mathematical Foundations of Informatics*
*Institute of Mathematics and Informatics*
*Bulgarian Academy of Sciences*
Sofia, Bulgaria
youri@math.bas.bg

Miroslav Markov
*Department of Mathematical Foundations of Informatics*
*Institute of Mathematics and Informatics*
*Bulgarian Academy of Sciences*
Sofia, Bulgaria
miro@math.bas.bg

***Abstract*—We elaborate an approach for determining the order of an elliptic curve from the family $\mathcal{E}_p = \{E_a : y^2 = x^3 + a \pmod p), a \neq 0\}$ where $p$ is a prime number $> 3$. The essence of this approach consists in combining the well-known Hasse bound with an explicit formula for that order reduced to modulo $p$. It allows to advance an efficient technique of complexity $O(\log^2 p)$ for computing simultaneously the six orders associated with the family $\mathcal{E}_p$ when $p \equiv 1 \pmod 3$, thus improving the best known algorithmic solution for that problem with an order of magnitude.**

***Index Terms*—elliptic curve over $\mathbb{F}_p$, Hasse bound**

## I. Introduction

The elliptic curves over finite fields play an important role in modern cryptography. We refer to [1] for an introduction concerning their cryptographic significance (see, as well, the pioneering works of V. Miller and N. Koblitz from 1980's [2], [3]). Briefly speaking, the advantage of the so-called elliptic curve cryptography (ECC) over the non-ECC is that it requires smaller keys to provide same level of security.

It is well-known that to avoid successful relevant attacks against an ECC system, the number of points on the involved curve (called order of the curve) must have at least one very large prime factor. In particular, if the order itself is a (large) prime then the entire capabilities of curve are exploited to achieving maximum security.

An efficient algorithm (of complexity at most a constant times $\log^8 q$ bit-operations where $q$ is the order of employed finite field) which computes the order of a given elliptic curve of general type is present in [4]. In this paper, however, we are interested in the whole family of curves $\mathcal{E}_p = \{E_a : y^2 = x^3 + a \pmod p), \ a \neq 0\}$ of cardinality $p - 1$. So, it seems that there is no deterministic way to apply the Schoof algorithm (or its improvement, the SEA algorithm) for finding the orders of all curves in $\mathcal{E}_p$ when $p$ is large, although it is still feasible taking into account the existence of only six equiprobable possibilities (see, Proposition 8) and the so-called coupon collector's problem from probability theory (see, e.g. [5]).

Nevertheless, there are more efficient approaches to the problem of interest, like the algorithmic solution presented in [6] that takes $O(\log^3 p)$ bit operations. Moreover, an even better approach (to which this article is devoted) does exist. There are two main differences between the approach followed in [6] and our own:

- C. Munuera and J. Tena propose to use a general-purpose probabilistic algorithm [7] for finding out square root of arbitrary quadratic residue modulo $p$ in order to find $\sqrt{-3}$ where $p \equiv 1 \pmod 3$. Their algorithm is of complexity $O(\log^3 p)$, whereas our proposal for this task improves to complexity $O(\log^2 p)$ due to an efficient targeted way for computing that specific value;
- The authors of [6] find solutions of the Diophantine equation $F(X,Y) = X^2 + XY + Y^2 = 3p$, while we solve for $X^2 + 3Y^2 = p$. However, both tasks are carried out by appropriate utilizations of the Euclidean algorithm involving $p$ and $\sqrt{-3} \bmod p$, thus both take $O(\log^2 p)$ bit operations (see, e.g. [8] or [9]).

In conclusion, although our proposal is probabilistic as well it outperforms this followed in [6] with an order of magnitude.

For an analytic solution of the problem considered here, we refer to [10] where it is obtained explicit formulae for the order of a curve $E_a \in \mathcal{E}_p$ in terms of a proper representation of the prime $p$ in the form $p = X^2 + Y^2 - XY$ for some integers $X$ and $Y$. Those formulas, however, distinguish between many separate cases, and the computational efficiency is certainly beyond author's goals (see, for details, [10, Theorem 1]). One also may find some particular instances of this problem as exercises in [11, Ch. 8, Ex. 15, 27].

Finally, it is worth pointed out that the results obtained by the approach followed in this article are comprehensive and compact, despite that some long-established facts from the theory of quadratic partitions of primes are used. Also, that approach has been described in [12] but its efficiency demonstrated only in case $p \equiv 7 \pmod{12}$, while in the present paper the idea is further refined and elaborated in full generality.

The paper is organized as follows. In the next section we give some preliminaries. Section III exposes our approach to the problem including the amended computational estimates for large $p$. Section IV provides an example with a specially constructed prime modulo. Some conclusions are drawn in the last section.

## II. Preliminaries

Let $p$ be a prime $> 3$ and $\mathbb{Z}_p$ be the ring of residues modulo $p$ which can be identified as well with the prime field $\mathbb{F}_p$. We consider a family of elliptic curves defined as $\mathcal{E}_p = \{E_a : y^2 = x^3 + a \pmod p,\ a \in \mathbb{Z}_p^*\}$ where $\mathbb{Z}_p^* = \mathbb{Z}_p \setminus \{0\}$ is the multiplicative group of $\mathbb{Z}_p$. Our aim is to find a suitable way (involving closed-form formulae) for computing the order $\#E_a$ of a general member of that family, the curve $E_a$, in terms of the parameters $a$ and $p$.

For basic number-theoretic notions as the absolute least and least non-negative residues, as well as the Legendre symbol $(\frac{z}{p})$ of an integer $z$ modulo prime $p$, we refer to [13, pp. 93, 289] respectively. Notations "$\equiv$" for congruence modulo $p$ and "$=$" in $\mathbb{Z}_p$ will be used in interchangeable manner, depending on the context.

Hereinafter, we recall some necessary supplementary notions and facts (possibly with slight abuses).

An element $z \in \mathbb{Z}_p^*$ is called a quadratic residue modulo $p$ if there exists $x \in \mathbb{Z}_p^*$ such that $z = x^2$. Analogously, for $d > 2$, an element of $z \in \mathbb{Z}_p^*$ is called $d-$th power residue modulo $p$ if there exists $x \in \mathbb{Z}_p^*$ such that $z = x^d$. The set of all $d-$th power residues form a subgroup of $\mathbb{Z}_p^*$. We will denote the subgroups of quadratic and cubic residues ($d = 2, 3$) modulo $p$ by $\mathcal{QR}_p$ and $\mathcal{CR}_p$, respectively.

The next fact appears to be an immediate extension of the celebrated Euler criterion from elementary number theory (see, e.g. [14, Ch. 7.5]).

**Proposition 1.** *If $d$ is a factor of $p - 1$ then the monomial $\mathbf{m}(z) = z^{\frac{p-1}{d}}$ takes exactly $d$ distinct values in $\mathbb{Z}_p^*$ each one of them $\frac{p-1}{d}$ times. These values are the $d-$th roots of unity in $\mathbb{Z}_p^*$, i.e. solutions of the equation: $Z^d = 1$. In particular, $\mathbf{m}(z)$ equals to $1$ if and only if $z$ is a $d-$th power residue.*

It is well-known that $-3 \in \mathcal{QR}_p$ if and only if $p \equiv 1 \pmod 3$ (of course, $\sqrt{-3}$ modulo $p$ takes two values with opposite signs to each other). The following statement, which is crucial for the efficiency of our approach, shows how to find such a square root.

**Proposition 2.** *Let $z$ be a cubic non-residue modulo $p$ where $p \equiv 1$ ($mod$ $3$). Then $2z^{\frac{p-1}{3}} + 1$ is equal to one of the square roots of $-3$ modulo $p$.*

*Proof.* Indeed, according to Proposition 1, the assumption $z \notin \mathcal{CR}_p$ implies $z' = z^{\frac{p-1}{3}}$ is a third root of unity in $\mathbb{Z}_p^*$ different from 1. Thus, $z'$ satisfies the equation $Z^2 + Z + 1 = 0$, i.e. $z' = \frac{-1\pm\sqrt{-3}}{2}$ or equivalently $\pm\sqrt{-3} = 2z' + 1$. □

**Remark 1**: *Proposition 1 (with $d = 3$) easily implies that if $p \equiv 1$ ($mod$ $3$) the cardinality of the set of cubic non-residues modulo $p$ equals to $\frac{2}{3}(p-1)$. This can be interpreted as a reasoning that a randomly selected element of $\mathbb{Z}_p^*$ is a cubic non-residue with probability of $2/3$. So, provided there is a high-quality generator of random integers in the interval $[2, p-1]$, a cubic non-residue can be found after $1.5$ attempts on average. In turn, the square roots of $-3$ modulo $p$ can be efficiently determine by using Proposition 2.*

The next proposition expresses a folklore fact that is decisive for our work.

**Proposition 3.** *For an odd prime $p$ let $S_k(p) = 1^k + 2^k + \ldots + (p-1)^k$ where $k = 0, 1, \ldots$. Then it holds:*

$$S_k(p) \pmod p = \begin{cases} 0, & \textit{if } k \not\equiv 0 \pmod{p-1} \\ -1, & \textit{otherwise.} \end{cases}$$

For completeness, we give an alternative proof of the exposed in [12].

*Proof.* We use the fact that $\mathbb{Z}_p^*$ is a cyclic group. Let $g$ be its generating element, i.e., for any $z \in \mathbb{Z}_p^*$ there exists an $i : 0 \leq i \leq p-2$ such that $z = g^i$. This means that $S_k(p) = \sum_{z=1}^{p-1} z^k \equiv \sum_{i=0}^{p-2} (g^i)^k \pmod p$. Putting $u = g^k$ the last congruence implies $S_k(p) \pmod p = \sum_{i=0}^{p-2} u^i$. Now, there are two cases to be considered:

- if $k \not\equiv 0 \pmod{p-1}$, since the order of $\mathbb{Z}_p^*$ is $p-1$ then $u \neq 1$, which in turn gives that $S_k(p) \pmod p = (u^{p-1} - 1)/(u-1) = 0$.
- otherwise, by the same reasoning $S_k(p) \equiv p-1 \pmod p$, which completes the proof. □

There is no explicit formula for the number of points on a general type elliptic curve over $\mathbb{Z}_p$. The most relevant well-known result in this direction is the following bound (see, e.g. [15, Ch. 4]).

**Theorem 4.** *(**Hasse**) The number of points $N$ on an elliptic curve over $\mathbb{Z}_p$ satisfies $|(N-1) - p| \leq 2\sqrt{p}$.*

At the end of this section, we recall a needed fact from the theory of quadratic partitions of primes. This is a long-standing result due to C.G.J. Jacobi (1827) later elaborated by M.A. Stern (1832) (see, [16, vol. III, p. 55] about historical facts).

**Proposition 5.** *If $p$ is a prime of the form $p = 6k + 1$ for which $p = X^2 + 3Y^2$ then*

$$\pm 2X = \frac{(2k+1)\ldots(3k)}{k!} \; (mod\ p)$$

*where the sign utilized is such that $\pm X \equiv 1$ ($mod$ $3$).*

## III. Our approach

As it is mentioned in Introduction the general framework of our approach was described in [12]. We briefly exhibit here its basic steps.

The following proposition helps to fix unambiguously the number $N$ of points on a given elliptic curve, provided one can compute the absolute least residue of $N-1$ modulo $p$ denoted by $\mathcal{ALR}(N-1,p)$.

**Proposition 6.** *In notations of Theorem 4, for a prime $p \geq 17$, it holds:*

$$N = \mathcal{ALR}(N-1,p) + p + 1$$

*Proof.* Indeed, if $p \geq 17$ then evidently $2\sqrt{p} < \frac{p}{2}$. Thus, the Hasse theorem implies $|(N-1)-p| < \frac{p}{2}$ which means that $\mathcal{ALR}(N-1,p) = (N-1)-p$. □

**Remark 2**: *Note that if one can compute $z \pmod{m}$, or equivalently the least non-negative residue $R$ of an integer $z$ modulo odd $m$, he/she could easily get:*

$$\mathcal{ALR}(z,m) = \begin{cases} R, & \text{if } R < \frac{m}{2} \\ R-m, & \text{otherwise.} \end{cases}$$

### *A. An explicit formula for the order of elliptic curve $E_a \in \mathcal{E}_p$ reduced to modulo $p$*

Initially, we yield the following congruence:

$$\#E_a - 1 \equiv H(a,p) \pmod{p} \tag{1}$$

where

$$H(a,p) = \sum_{i=0}^{\frac{p-3}{2}} \binom{\frac{p-1}{2}}{i} a^i S_{3l}(p), \tag{2}$$

with $l = \frac{p-1}{2} - i$ and sums $S_{3l}(p)$ defined in Proposition 3.

Further, we evaluate $H(a,p) \pmod{p}$ using Proposition 3 and observing that the involved powers are only multiples of 3 in the interval $[3, 3\frac{p-1}{2}]$. Thus, there are two distinct cases to be considered:

- $p \equiv 5 \pmod{6}$
  In this case, Proposition 3 implies that all summands in the right-hand-side of Eq. (2) vanish mod $p$. So, $H(a,p) \equiv 0 \pmod{p}$, and Congr. (1) alongside with Proposition 6 imply that for each $a$ it holds $\#E_a = p+1$. Indeed, this is a well-known fact (see, e.g. [11, Ch. 18, Ex.1]).
- $p \equiv 1 \pmod{6}$
  In this essential case, it can be easily seen that $H(a,p)$ contains exactly one nonzero summand modulo $p$, i.e., that for $i = \frac{p-1}{6}$. Thus, it holds:

$$H(a,p) \equiv \binom{\frac{p-1}{2}}{\frac{p-1}{6}} a^{\frac{p-1}{6}} S_{p-1}(p) \equiv$$

$$-\binom{\frac{p-1}{2}}{\frac{p-1}{6}} a^{\frac{p-1}{6}} \pmod{p}, \tag{3}$$

Finally, together with Proposition 6, this immediately implies the following:

**Theorem 7.** *For a prime $p \geq 19$ such that $p \equiv 1 \ (mod\ 6)$, it holds:*

$$\#E_a = \mathcal{R}(a,p) + p + 1, \tag{4}$$

*where $\mathcal{R}(a,p)$ denotes the absolute least residue of (3).*

The next proposition addresses the issue about spectrum of values $\#E_a$ when $a$ varies over $\mathbb{Z}_p^*$.

**Proposition 8.** *If $p$ is a prime $\equiv 1 \ (mod\ 6)$ then the order of the curves from $\mathcal{E}_p$ takes exactly six distinct values each one $\frac{p-1}{6}$ times in accordance with the sixth roots of unity in $\mathbb{Z}_p^*$: $\pm 1, \pm\zeta, \pm(\zeta + \sqrt{-3})$ where $\zeta = \frac{-1-\sqrt{-3}}{2}$.*

**Sketch of proof.** The cases $p = 7, 13$ are checked directly. For $p \geq 19$, the proof is an immediate consequence of Theorem 7 and Proposition 1 applied for $d = 6$. □

The reader can find a detailed proof of Proposition 8 in [12].

### *B. Computational issues of point-counting in $\mathcal{E}_p$ when $p$ is a large $\equiv 1 \ (mod\ 6)$*

In this subsection, we refine and improve the algorithmic technique described in [12].

A key part of those computations is that of $\binom{\frac{p-1}{2}}{\frac{p-1}{6}} \pmod{p}$. Fortunately, this problem can be addressed by noticing that if $p$ is of the form $p = 6k+1$ then it holds:

$$\binom{\frac{p-1}{2}}{\frac{p-1}{6}} = \frac{(2k+1)\dots(3k)}{k!}.$$

Hence, Proposition 5 allows modular computation of this binomial coefficient to be performed by taking the proper $X$ from a solution of the quadratic Diophantine equation $X^2 + 3Y^2 = p$ with two unknowns $X$ and $Y$. Such a solution can be found by applying similar method as that exhibited in [17], and consisting of two steps:

- *Step 1.* Find a square root of $-3$ in $\mathbb{Z}_p^*$;
- *Step 2.* Find $X$ by applying partly the Euclidean algorithm for $p$ and the already found $\sqrt{-3} \in \mathbb{Z}_p^*$.

As follows by Proposition 2, *Step 1* can be performed if one knows in advance a cubic non-residue mod $p$. If, for a given $p$, such a non-residue is not available, it can be found after 1.5 attempts on average following Remark **1**. Namely, in every such attempt for a randomly selected integer $z \in [2, p-1]$ we compute the element $z' = z^{\frac{p-1}{3}}$ and check whether $z' \neq 1$. If this happens then $2z'+1$ is one of the possible $\sqrt{-3}$ in demand. (Remind, that when $p \equiv 7 \pmod{12}$ there is a simple deterministic way to find square root of any quadratic residue $\zeta$ by computing $\zeta^{\frac{p+1}{4}}$.) Thus, roughly speaking, the amount of work in *Step 1* is proportional to $\log^2 p$ taking into account the complexity of single multiplication [18]. Also, notice that the harder *Step 2* is of bit-complexity upper bounded by $O(\log^2 p)$ (the details can be seen , e.g. in [9, Theorem 3.13]).

Besides that, the six possible distinct values of the second multiplier $a^{\frac{p-1}{6}}$ in expression (3) are linearly expressed in terms of the already found $\sqrt{-3}$.

In conclusion, the total computational complexity for finding simultaneously the orders associated with the family $\mathcal{E}_p$ is dominated by that of modular computation of the binomial coefficient, and hence around $O(\log^2 p)$.

## IV. Example

The example present here illustrates our *probabilistic* approach. We choose as modulo the following prime

$$p = 2^{256} + 2^{56} + 2^{44} + 1$$

which is congruent to $1 \pmod{12}$.

Consecutively, we:

- calculate $\pm\sqrt{-3} \pmod{p}$ applying the randomness based approach:
    - ○ choose a random number $z \in [2, p-1]$ :

      94188671383219429491545384564715608389913166226587832329892090934494399146731

    - ○ calculate $z' = z^{\frac{p-1}{3}}$ :

      121964523850189669698047272281867547026457315478178020020606570771434058573O2

    - ○ $z' \neq 1$, thus $2z' + 1$ is a square root of $-3$ in $\mathbb{F}_p^*$:

      24392904770037933939609454456373509405291463095635604004121314154286811714605;

- solve the Diophantine equation $X^2 + 3Y^2 = p$ and calculate $\binom{\frac{p-1}{2}}{\frac{p-1}{6}} \pmod{p} = 2X$ :

  115792089237316195423570985008687907852841577627951526351327127403406468497407;

- calculate $\zeta_1 = \frac{-1-\sqrt{-3}}{2}$ and $\zeta_2 = \zeta_1 + \sqrt{-3}$:

  103595636852297228453766257780501153150624253117822762037396999005955947754986,
  121964523850189669698047272281867547026457315478178020020606570771434058573O2;

- calculate the values of expression (3) using $1, \zeta_1$ and $\zeta_2$ in the role of multiplier $a^{\frac{p-1}{6}}$, and take their opposites. Finally, we find out the six orders associated with $\mathcal{E}_p$:

  115792089237316195423570985008687907853698391703329601727588184762792238727172,
  115792089237316195423570985008687907852841577627951526351327127403406468497408,
  115792089237316195423570985008687907852597821732376135963590559300783091641217,
  * 115792089237316195423570985008687907853942147598904992115324752865415615583363,
  115792089237316195423570985008687907853513740561215954427194224185722730468481,
  * 115792089237316195423570985008687907853026228770065173651721087980475976756099.

  Examining the above numbers by the APR-CL primality test, we detect the presence of two prime orders (remarked by "*") which correspond to $\#E_{31}$ and $\#E_{11}$.

## V. Conclusion

Less or more convenient formulae to compute the orders of elliptic curves over finite fields do exist in contemporary literature (see, e.g. [10], [15], [19], etc.). In this article, we derive an explicit formula for the order of a curve in the family $\mathcal{E}_p = \{E_a : y^2 = x^3 + a \pmod{p}, a \neq 0\}$ reduced modulo $p$. Alongside with the famous Hasse bound, this formula resolves the problem we deal with comprehensively and concisely. Moreover, our approach permits to determine transparently the spectrum of orders for fixed $p \equiv 1 \pmod 6$, as well as to re-prove the corresponding known fact in the complementary case $p \equiv 5 \pmod 6$. Besides that, based on classical results for quadratic partitions of primes, we describe an efficient algorithmic technique (with complexity $O(\log^2 p)$) to compute simultaneously the six orders associated with $\mathcal{E}_p$ in cases of interest. This technique improves the best previously known algorithmic solution [6] with an order of magnitude, thus enabling under the same cost to achieve values of the parameter $p$ peculiar to higher security ECC systems. It is especially useful when looking (say, by random search) for a prime order elliptic curves belonging to the family of considered type for a changing modulo $p$.

The following abbreviations are used in this manuscript:

| | |
|---|---|
| ECC | Elliptic Curve Cryptography |
| SEA | Schoof-Elkies-Atkin |
| APR-CL | Adleman-Pomerance-Rumely-Cohen-Lenstra |

## References

[1] H. van Tilborg, "Elliptic curve cryptosystems; too good to be true?" *Nieuw Archief Voor Wiskunde*, vol. 5, no. 3, pp. 220–225, 2001.

[2] V. S. Miller, "Use of elliptic curves in cryptography," in *Conference on the theory and application of cryptographic techniques*. Springer, 1985, pp. 417–426.

[3] N. Koblitz, "Elliptic curve cryptosystems," *Mathematics of computation*, vol. 48, no. 177, pp. 203–209, 1987.

[4] R. Schoof, "Counting points on elliptic curves over finite fields," *Journal de théorie des nombres de Bordeaux*, vol. 7, no. 1, pp. 219–254, 1995.

[5] J. S. Croucher, "Collecting coupon–a mathematical approach." *Australian Senior Mathematics Journal*, vol. 20, no. 2, pp. 31–35, 2006.

[6] C. Munuera and J. G. Tena, "An algorithm to compute the number of points on elliptic curves of j-invariant 0 or 1728 over a finite field," *Rendiconti del Circolo Matematico di Palermo*, vol. 42, no. 1, pp. 106–116, 1993.

[7] R. Peralta, "A simple and fast probabilistic algorithm for computing square roots modulo a prime number (corresp.)," *IEEE transactions on information theory*, vol. 32, no. 6, pp. 846–847, 1986.

[8] D. E. Knuth, *The art of computer programming, volume 2: Seminumerical Algorithms*. Addison-Wesley Longman Publishing Co., Inc., 1997.

[9] J. von zur Gathen and J. Gerhard, *Modern Computer Algebra*. Cambridge University Press, 2013.

[10] B. B. Kırlar, "On the elliptic curves $y^2 = x^3 - c$ with embedding degree one," *Journal of Computational and applied Mathematics*, vol. 235, no. 16, pp. 4724–4728, 2011.

[11] K. Ireland and M. Rosen, *A Classical Introduction to Modern Number Theory*. Springer-Verlag, 1990.

[12] Y. Borissov and M. Markov, "An approach for computing the number of points on elliptic curve $y^2 = x^3 + a \pmod{p}$ via explicit formula for that number modulo p," in *2019 Ninth International Workshop on Signal Design and its Applications in Communications (IWSDA)*. IEEE, 2019, pp. 1–5.

[13] H. Rosen Kenneth, *Elementary number theory and its applications*. Addison-Weley Publishing Company, 1984.

[14] G. Hardy, E. Wright, R. Heath-Brown, J. Silverman, and A. Wiles, *An Introduction to the Theory of Numbers*. Oxford University Press, 2008.

[15] L. C. Washington, *Elliptic curves: number theory and cryptography*. CRC press, 2008.

[16] L. E. Dickson, *History of the Theory of Numbers: Quadratic and Higher Forms*. Courier Corporation, 2012, vol. 3.

[17] P. Wilker, "An efficient algorithmic solution of the diophantine equation $u^2 + 5v^2 = m$," *Mathematics of Computation*, vol. 35, no. 152, pp. 1347–1352, 1980.

[18] H. Cohen, *A course in computational algebraic number theory*. Springer Science & Business Media, 2013, vol. 138.

[19] J. H. Silverman, *The arithmetic of elliptic curves*. Springer Science & Business Media, 2009, vol. 106.