17th International Workshop on Algebraic and Combinatorial Coding Theory,
October 11-17, 2020, online, Bulgaria, pp. 106-109

2020 Algebraic and Combinatorial Coding Theory (ACCT) | 978-1-6654-0287-3/20/$31.00 ©2020 IEEE | DOI: 10.1109/ACCT51235.2020.9383390

Point-Counting on Elliptic Curves Belonging to One Prominent Family: Revisited

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

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

***Abstract*—An approach to computing orders of elliptic curves from the family $\{D_a : y^2 = x^3 + ax \pmod p,\ a \neq 0\}$ with p being a prime number, is presented. The method combines an explicit formula for the orders of curves reduced modulo p with the well-known Hasse bound. Besides its efficiency (the algorithm takes at most $O(\log^2 p)$ bit operations), this approach allows to determine in a transparent way the spectrum of curve orders when p is fixed.**

***Index Terms*—Elliptic curve over $\mathbb{Z}_p$, Hasse bound, Gauss congruence**

I. Introduction

The elliptic curves over finite fields are essential part of the contemporary cryptography. For an introduction about their cryptographic significance, we direct the readers to [1]. Briefly speaking, cryptographic primitives and protocols based on elliptic curves are at an advantage over those based on different mathematical machinery since they provide security of reasonable level by relatively short cryptographic keys. For instance, the very popular digital cryptocurrency Bitcoin involves Elliptic Curve Cryptography (ECC) employing cryptographic keys of length only 256 bits. Bitcoin is also based on the modern blockchain technology which has enormous number of applications in doing business nowadays (for some recent see, e.g., [2] and [3]).

A crucial issue in constructing an ECC system is to ensure that the number of points on the involved elliptic curve (called its order) has no only small prime factors since, otherwise, small subgroups attacks can be efficiently carried out. Arguments of that kind indicate how exceptionally important is to have a knowledge about the order of an intended for use curve.

There exists an efficient algorithm computing the order of a given elliptic curve of general type (see, e.g. [4]). In this paper, however, we consider the family of elliptic curves $\mathcal{D}_p = \{D_a : y^2 = x^3 + ax \pmod p,\ a \neq 0\}$ of cardinality $p-1$, where a direct application of this algorithm is not feasible for large p. Therefore, explicit closed-form formulae in terms of parameters a and p that address the problem of interest, are needed.

For an analytic solution regarding this problem, we refer to [5, Section 4.4]. However, Theorem 4.23 that summarizes the results leaves incompleteness about the sign of the involved Frobenius trace for some values of the parameter. Probably the refinement is left as an exercise for readers of the textbook [5] since author's comment is "this is a much more delicate problem and we omit it".

An algorithmic solution that we have been recently aware is given in [6], namely, for the case of elliptic curves with $j-$invariant 1728. But, as the authors of [6] have pointed out their algorithm requires $O(\log^3 p)$ bit operations whereas our approach improves to complexity $O(\log^2 p)$.

It should be pointed out as well that the approach followed in the present article is an extension of our previous work on the same problem regarding the family $\mathcal{E}_p = \{E_a : y^2 = x^3 + a \pmod p\ a \neq 0\}$ [9], and it works equally well in both cases as the results obtained are comprehensive and compact, although some long-established facts from the theory of quadratic partitions of primes are used.

The organization of this paper is as follows. In the next section, we state the problem and give some preliminaries. In Section III, our approach is exposed, including its computational efficiency for large p. Section IV discusses an example with specific modulo. Finally, we draw some conclusions.

II. Preliminaries

Let $\mathbb{Z}_n$ be the ring of residues modulo an integer $n \geq 2$. We mostly consider the ring $\mathbb{Z}_p$ for an odd prime p, and let $\mathbb{Z}_p^* =$

$\mathbb{Z}_p \setminus \{0\}$ denote the multiplicative group of $\mathbb{Z}_p$. We assume the readers are familiar with basic number-theoretic notions as the Legendre symbol $(\frac{z}{p})$ of an integer z modulo p; the absolute least residue and the least non-negative residue, abbreviated for shorter $\mathcal{ALR}$ and $\mathcal{LNR}$, respectively. The notations "$\equiv$" for congruence modulo p and "$=$" in $\mathbb{Z}_p$ will be interchangeably utilized through this paper.

Our goal is to describe a satisfactory way (including closed-form formulae) for determining the order of a general curve D_a from the family $\mathcal{D}_p$ in terms of a and p.

We recall one basic property of the Legendre symbol stated here as lemma.

Lemma 1. *For any integer z it holds:* $(\frac{z}{p}) \equiv z^{\frac{p-1}{2}} \pmod p$.

Lemma 1 is generally known as the Euler criterion for determining whether the integer z is quadratic residue modulo p. The next fact appears to be an immediate extension of that criterion (see, e.g. [8, Ch. 7.5]).

Proposition 2. *If d is a factor of $p-1$ then the monomial $z^{\frac{p-1}{d}}$ accepts exactly d distinct values in $\mathbb{Z}_p^*$ each one $\frac{p-1}{d}$ times. These values are the solutions of the equation: $Z^d = 1$, i.e., $d-$th roots of unity in $\mathbb{Z}_p^*$.*

For completeness, we present a proof of this proposition.

Proof. Recall that $\mathbb{Z}_p^*$ is a cyclic group isomorphic to the additive group of $\mathbb{Z}_{p-1}$, and let g be its generating element, i.e., $\mathbb{Z}_p^* = \{g^0 = 1, g, \ldots, g^{p-2}\}$. For fixed $r : 0 \le r < d$, let $I_r = \{i \in \mathbb{Z}_{p-1} : i \equiv r \ (mod\ d)\}$ and $C_r = \{g^i : i \in I_r\}$. Obviously, the sets $C_r, 0 \le r < d$ form a partition of $\mathbb{Z}_p^*$, and each one of them is of size $\frac{p-1}{d}$. Further, it is easy to show that $z^{\frac{p-1}{d}}$ is invariant over C_r for fixed r. Indeed, taking into account that the order of $\mathbb{Z}_p^*$ is $p-1$, for any $\zeta \in C_r$ it holds: $\zeta^{\frac{p-1}{d}} = c^r$ where the constant c equals to $g^{\frac{p-1}{d}}$. Now, let r_1, r_2 be two distinct residues modulo d, say $r_1 < r_2$. Suppose it holds $c^{r_1} = c^{r_2}$, i.e., $c^{r_2-r_1} = (g^{\frac{p-1}{d}})^{(r_2-r_1)} = 1$. Then we reach a contradiction to assumption that g is a generating element of $\mathbb{Z}_p^*$ since $\frac{p-1}{d}(r_2 - r_1) < \frac{p-1}{d} \times d < p-1$. Thus, $c^{r_1} \ne c^{r_2}$ for any $r_1 \ne r_2$ which means that monomial $z^{\frac{p-1}{d}}$ takes distinct values over the subsets $C_r, 0 \le r < d$. Finally, to prove that these are the $d-$th roots of unity in $\mathbb{Z}_p^*$ just observe the following: $(c^r)^d = ((g^{\frac{p-1}{d}})^r)^d = ((g^{\frac{p-1}{d}})^d)^r = (g^{p-1})^r = 1$. □

The next proposition expresses a crucial fact for this work.

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

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

The proof of this proposition is exhibited in [9].

Yet another fact, we need, is the famous Hasse bound (see, e.g. in [5, Ch. 4]).

Theorem 4. *(**Hasse bound**) The number of points N on an elliptic curve over $\mathbb{Z}_p$ satisfies:*

$$|(N-1) - p| \le 2\sqrt{p}.$$

At the end of this section, we recall an old but useful fact due to C.F. Gauss (see, [11, vol. II, p. 234] for historical details).

Proposition 5. *(**Gauss' observation**) If a prime $p = 4k+1$ is expressed in the form $X^2 + Y^2$, for X odd and Y even, then $\pm X$ equals the minimum residue (i.e., the $\mathcal{ALR}$) modulo p of*

$$\frac{1}{2}\frac{(k+1)\ldots(2k)}{k!},$$

and this residue is positive or negative according as the positive value of X is of the form $4m+1$ or $4m+3$.

A recent discussion on Gauss' observation (congruence) one can find in [12, p. 192, 202] (see, as well [7, Ch. 8, Ex. 26]).

III. Our approach

The next proposition allows to fix unambiguously the order of an elliptic curve over $\mathbb{Z}_p$ if its residual modulo p could be computed.

Proposition 6. *(see, **[9]**) For a prime $p \ge 17$, in notations of Theorem 4, let $r = \mathcal{LNR}(N-1, p)$. Then it holds:*

$$N = \begin{cases} r + 1 + p, & \text{if } r < \frac{p}{2} \\ r + 1, & \text{otherwise.} \end{cases}$$

For readers convenience, we sketch out the proof.

Sketch of proof. Obviously, if $p \ge 17$ the Hasse theorem implies $|(N-1) - p| < 2\sqrt{p} < \frac{p}{2}$ which means that $\mathcal{ALR}(N-1, p) = (N-1) - p$. Now, the proof easily follows by the evident relation between $\mathcal{ALR}$ and $\mathcal{LNR}$. □

A. Explicit formulae for the orders elliptic curves in $\mathcal{D}_p$ reduced to modulo p

Let, for convenience, $N' = \#D_a - 1$ for a fixed curve $D_a \in \mathcal{D}_p$. Proceeding similarly as in [9], we easily obtain:

$$N' \equiv h(a, p) \pmod p \tag{1}$$

where

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

in notations for the power sums introduced by Proposition 3 where $k(i) = 3\frac{p-1}{2} - 2i$.

Further, we estimate $h(a, p) \pmod p$ using Proposition 3 and observing that involved powers are only the odd (or even) integers from interval $[\frac{p-1}{2}, 3\frac{p-1}{2}]$. Thus, there are two distinct cases to be considered:

- $p \equiv 3 \pmod 4$
  In this case, there is no index i such that $k(i) = p-1$. Hence, Proposition 3 implies that all summands in the RHS of (2) reduced modulo p vanish. Thus, $h(a, p) \equiv 0$

$(\mathrm{mod}\ p)$, and Congr. (1) together with the Hasse bound easily imply $N' = p$. So, for each a it holds $\#D_a = p + 1$, which is an well-known fact (see, e.g. [7, Ch. 18.4, Theorem 5]);

- $p \equiv 1 \pmod 4$
  In this essential case it is easy to see that expression (2) contains exactly one nonzero summand, i.e., when $i = \frac{p-1}{4}$. Therefore, by Proposition 3, it holds:

$$h(a,p) \equiv \binom{\frac{p-1}{2}}{\frac{p-1}{4}} a^{\frac{p-1}{4}} S_{p-1}(p) \equiv$$

$$-\binom{\frac{p-1}{2}}{\frac{p-1}{4}} a^{\frac{p-1}{4}} \pmod p,$$

  or equivalently by Congr. (1):

$$N' \equiv -\binom{\frac{p-1}{2}}{\frac{p-1}{4}} a^{\frac{p-1}{4}} \pmod p. \tag{3}$$

Finally, from Congr. (3) and Proposition 6, we immediately derive the main result of this work.

Theorem 7. *For a prime $p \geq 17$ such that $p \equiv 1 \pmod 4$, it holds:*

$$\#D_a = \begin{cases} p + 1 + \mathcal{R}(a,p), & \text{if } \mathcal{R}(a,p) < \frac{p}{2} \\ 1 + \mathcal{R}(a,p), & \text{otherwise,} \end{cases} \tag{4}$$

where $\mathcal{R}(a,p)$ stands for the $\mathcal{LNR}$ of the right-hand-side of Congr. (3).

B. The spectrum of $\#D_a$ when a varies over $\mathbb{Z}_p^*$

The next proposition highlights the essential case $p \equiv 1 \pmod 4$.

Proposition 8. *Let p be a prime ≥ 17. Then if $p \equiv 1 \pmod 4$, the order of curves from $\mathcal{D}_p$ takes exactly four distinct values each one $\frac{p-1}{4}$ times in accordance with the fourth roots of unity in $\mathbb{Z}_p^*$: $\pm 1, \pm\sqrt{-1}$.*

Sketch of proof. Congr. (3) indicates that for fixed p the order of a curve $D_a \in \mathcal{D}_p$ is determined from the second multiplier $a^{\frac{p-1}{4}}$, the last accepting as values the fourth distinct roots of unity if a varies over $\mathbb{Z}_p^*$ according to Proposition 2. □

Remark 1. As an immediate corollary of Theorem 4.23 from [5] one may derive that the order of elliptic curve from the family $\mathcal{D}_p$ is always even number, which cannot be directly seen from Theorem 7.

C. Computational aspects for large p

Hereinafter, we describe an efficient approach for computing the orders of curves in $\mathcal{D}_p$ when p is a large prime.

A key part in this computation is that of $\binom{\frac{p-1}{2}}{\frac{p-1}{4}} \pmod p$. Luckily, that problem can be addressed by Proposition 5 observing that if p is of the form $p = 4k + 1$ then it holds:

$$\binom{\frac{p-1}{2}}{\frac{p-1}{4}} = \frac{(k+1)\ldots(2k)}{k!}.$$

Hence, that proposition allows modular computation of the binomial coefficient of interest to be carried out by solving the quadratic Diophantine equation $X^2 + Y^2 = p$. The solution could be found by a method presented in [13] being a considerable simplification of an early method discovered by Hermite and Serret [14] - [15]. In brief, it consists of two steps:

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

Step 1 can be accomplished efficiently knowing in advance a quadratic non-residue mod p (for details and how to pick up or find such a non-residue see, e.g., [13, *Remark*, p.1012]). However, the following proposition is valid.

Proposition 9. *For arbitrary finite set of positive integers $\{n_1, n_2, \ldots, n_s\}$ there exist a prime number $P \equiv 1 \pmod 4$ such that all $n_i, 1 \leq i \leq s$ are quadratic residues modulo P.*

The proof makes use of some deep number-theoretic facts of flavor distinct from those employed so far (e.g., Dirichlet's theorem on arithmetic progressions), and is omitted here.

Nevertheless, based on Proposition 2, a square root of -1 modulo p can be found after two attempts on average provided there is a high-quality generator of random integers in the interval $I_p = [2, p-1]$. Each one of these attempts consists of computing for a randomly selected $\mathcal{R} \in I_p$, the element $\mathcal{R}' = \mathcal{R}^{\frac{p-1}{4}}$, and checking whether the latter $\neq \pm 1$. If this happens then $\mathcal{R}'$ is the $\sqrt{-1}$ in demand. (The reader is directed to [16, Ch. 10] or to an early work [17] for further rationale of the approach based on randomness.) Roughly speaking, the amount of work in *Step 1* is proportional to $\log^2 p$. Similarly, *Step 2* has a bit-complexity upper bounded by $O(\log^2 p)$ (see, e.g., [18, Theorem 3.13]).

Having in mind Proposition 8, to find simultaneously the four orders linked with the family $\mathcal{D}_p$ one could proceed as follows. After computing $2X$, multiply that value by the already found $\sqrt{-1}$ and then take the opposite values modulo p. In conclusion, the total complexity of the task for determining the orders of interest is upper bounded by $O(\log^2 p)$.

IV. Example

We illustrate our approach by an example with the prime $p = 2^{224} - 2^{96} + 1$. Note that this modulo is employed in secp224r1 elliptic curve domain parameters (NIST 224-bit specification).

The numerical data presented herein are in decimal number system. We proceed as follows:

- calculate $\sqrt{-1} \pmod p$ applying the randomness based approach described in the previous section:
  - choose a random number $\mathcal{R}$:
    30141282139465925369411011477990165749121892982311618920155 73
  - calculate $\mathcal{R}' = \mathcal{R}^{\frac{p-1}{4}}$:
    33383626035532199968744214068876337120407194562837320960170307916 56
    so, $\mathcal{R}' \neq \pm 1 \pmod p$ and it is a $\sqrt{-1} \pmod p$.

- solve the Diophantine equation $X^2 + Y^2 = p$, get the odd positive X and calculate $\binom{\frac{p-1}{2}}{\frac{p-1}{4}} \pmod p = 2X$:

  57890107301813950983563826207292 82

- multiply the above value with the already found $\sqrt{-1}$ and then take the opposites of latter two values mod p. Afterwards, we find out the four orders linked with $\mathcal{D}_p$:

  26959946667150639794667015087019624884547186078631209787127445569600,

  26959946667150639794667015087019636462568646441421406499892687028164,

  26959946667150639794667015087019622052238908448795226442971178695282,

  26959946667150639794667015087019639294876924071257389844048953902482

Finally, it is worth pointing out that the last curve order is an even semi-prime number, i.e. equals twice a prime.

V. Conclusion

Revisiting the problem of computing the order of an elliptic curve from the family $\mathcal{D}_p$, we reveal a remarkably simple explicit formula when that order is reduced modulo p. This formula in combination with the famous Hasse bound resolves the problem comprehensively and concisely. Besides that, based on a classical result about quadratic partitions of primes, we describe an efficient technique to compute simultaneously the orders of interest having complexity upper bounded by $O(\log^2 p)$. Hence, the proposed algorithmic technique improves upon the best previously known solution of that kind in an order of magnitude.

Acknowledgments

The authors would like to thank Peter Boyvalenkov and Lyubomir Borissov for the helpful discussions and comments which substantially improved the manuscript. This work is supported in part by the Bulgarian National Science Fund under Contract KP-06-N32/2-2019.

References

[1] H. C.A. van Tilborg, "Elliptic curve cryptosystems; too good to be true?", *NAW 5/2*, nr 3, pp. 220–225, 2001.

[2] B. Tsvetkov, H. Kostadinov, "DLT smart contract platforms for software lifecycle management", *AIP Conference Proceedings*, 2164(1), 120015, 2019.

[3] B. Tsvetkov, H. Kostadinov, "Using DLT in software lifecycle management", *Studies in Computational Intelligence*, to appear 2021.

[4] R. Schoof, "Counting points on elliptic curves over finite fields", *Journal de théorie des nombres de Bordeaux*, vol. 7(1), pp. 219–254, 1995.

[5] L.C. Washington, *Elliptic Curves: Number Theory and Cryptography*, Chapman-Hall, New York, 2003.

[6] C. Munuera and J. Tena, "An algorithm to compute the number of points on elliptic curves of j-invariant 0 or 1728 over finite field", *Rendinconti del Circolo Matematico di Palermo*, Serie 2, Tomo XLII, pp. 106–116, 1993.

[7] K. Ireland and M. Rosen, *A Classical Introduction to Modern Number Theory*, 2nd ed., Springer-Verlag, New York, 1990.

[8] G. H. Hardy, and E.M. Wright, *An introduction to the theory of numbers*, 6th ed. Oxford, England: Clarendon Press, 2008.

[9] 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", *Proceedings of the Ninth IWSDA 2019*, Dongguan, China, October 20 - 24, pp. 1–5, 2019.

[10] J. H. Silverman, *The Arithmetic of Elliptic Curves*, Springer-Verlag, Berlin, etc., 1986.

[11] L. E. Dickson, *History of the Theory of Numbers*, 1919, Chelsea Publ. Company, Reprinted, New York, 1952, 1966.

[12] F. Lemmermeyer, *Reciprocity Laws: From Euler to Eisenstein*, Springer Monographs in Mathematics, Springer-Verlag, Berlin, 2000.

[13] J. Brillhart, "Note on representing a prime as a sum of two squares", *Mathematics of Computation*, vol. 26, pp. 1011-1013, 1972.

[14] C. Hermite, "Note au sujet de l'article précédent", *J. Math. Pures Appl.*, v. 1848, p. 15; also "Note sur théorème rélatif aux nombres entières", *Oevres*, Vol. 1, p. 264, 1848.

[15] J. A. Serret, "Sur un théorème rélatif aux nombres entières", *J. Math. Pures Appl.*, v. 1848, pp. 12–14, 1848.

[16] S. Wright, "Quadratic residues and non-residues: selected topics", *arXiv:1408.0235v7 [math.NT]* 21 Oct 2016.

[17] N. S. Aladov, "On the distribution of quadratic residues and nonresidues modulo a prime number in the sequence 1,2,...,p-1", *Mat. Sb.* 18, pp. 61–75, 1896 (in Russian).

[18] J. von zur Gathen and J. Gerhard, *Modern computer algebra*, 3rd ed., Cambridge University Press, 2013.