mathematics

MDPI

Article

An Efficient Approach to Point-Counting on Elliptic Curves from a Prominent Family over the Prime Field $\mathbb{F}_p$

Yuri Borissov * and Miroslav Markov

Department of Mathematical Foundations of Informatics, Institute of Mathematics and Informatics, Bulgarian Academy of Sciences, 1113 Sofia, Bulgaria; miro@math.bas.bg
* Correspondence: youri@math.bas.bg

Abstract: Here, we elaborate an approach for determining the number of points on elliptic curves 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 the quantities of interest-reduced modulo p. It allows to advance an efficient technique to compute the six cardinalities associated with the family $\mathcal{E}_p$, for $p \equiv 1 \pmod 3$, whose complexity is $\tilde{O}(\log^2 p)$, thus improving the best-known algorithmic solution with almost an order of magnitude.

Keywords: elliptic curve over $\mathbb{F}_p$; Hasse bound; high-order residue modulo prime

Citation: 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* **2021**, *9*, 1431. https://doi.org/10.3390/math9121431

Academic Editor: Angel Martin-del-Rey

Received: 10 May 2021
Accepted: 18 June 2021
Published: 19 June 2021

1. 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 the 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 the curve are exploited to achieve maximum security.

An efficient deterministic algorithm (of a complexity of, at most, constant times $\log^8 q$ bit-operations where q is the order of an employed finite field) which computes the order of a given elliptic curve of a 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 $p - 1$. Thus, it seems that there is no deterministic way to apply the Schoof 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 Corollary 1) and the so-called coupon collector's problem from the probability theory (see, e.g., [5]). Of course, a similar claim is valid in respect to the probabilistic improvement of the Schoof algorithm, that is, the SEA algorithm [4] with expected running time, heuristically, $\tilde{O}(\log^4 p)$.

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:

- Munuera and Tena proposed to use a general-purpose probabilistic algorithm [7] for finding out the 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 $\tilde{O}(log^2 p)$ due to an efficient targeted method 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]).

Hence, our proposal outperforms that in [6] with almost an order of magnitude, although it is of probabilistic type, too.

For an analytic solution of the problem considered here, we refer to [10], where explicit formulae are obtained 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 the 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 pointing out that the results obtained by the approach followed in this article are comprehensive and compact, despite the fact that some long-established facts from the theory of quadratic partitions of primes are used. Additionally, that approach has been described in [12], but its efficiency is demonstrated only in the 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 3 exposes our approach to the problem including the amended computational estimates for large p. Section 4 provides an example with a specially constructed prime modulo, and also discusses the results of an program experiment to compare the performance of our proposed algorithmic technique with that of the SEA algorithm in the considered scenario. Some conclusions are drawn in the last section.

2. Preliminaries

Let p be a prime > 3 and $\mathbb{Z}_p$ be the ring of residues modulo p, which can also be identified 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 method (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 least non-negative and absolute least residues of an integer z modulo another (odd) integer m, we refer to ([13], p. 93). Notations "$\equiv$" for congruence modulo p and "$=$" in $\mathbb{Z}_p$ will be used in an 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 the $d-$th order residue modulo p if there exists $x \in \mathbb{Z}_p^*$ such that $z = x^d$. The set of all $d-$th order 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 the 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 $\mathbb{Z}_p^*$, that is, 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 $p \equiv 1 \pmod 3$. 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 $Z^2 + Z + 1 = 0$, that is, $z' = \frac{-1 \pm \sqrt{-3}}{2}$ or equivalently $\pm\sqrt{-3} = 2z' + 1$. □

Remark 1. *Proposition 1 (with $d = 3$) easily implies that if $p \equiv 1 \pmod 3$, 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 $2/3$. Thus, 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 determined 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:*

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

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

Proof. We use the fact that $\mathbb{Z}_p^*$ is a cyclic group. Let g be its generating element, that is, for any $z \in \mathbb{Z}_p^*$, there exists an $i : 0 \le i \le p-2$ 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 $u = g^k$ as the last congruence implies that $S_k(p) \pmod p = \sum_{i=0}^{p-2} u^i$. 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, the same reasoning implies $S_k(p) \equiv p - 1 \pmod p = -1$. □

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

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 Jacobi (1827) later elaborated by Stern (1832) (see, [16] vol. III, p. 55 about historical details).

Proposition 4. *If p is a prime of the form $p = 6k + 1$ for which $p = X^2 + 3Y^2$, then*

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

where the sign utilized is such that $\pm X \equiv 1 \pmod 3$.

3. Our Approach

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

The following proposition helps to unambiguously fix 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 5. *In notations of Theorem 1, 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:*

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

3.1. An Explicit Formula for the Order of Elliptic Curve $E_a \in \mathcal{E}_p$ Reduced 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.
(For the reader's convenience, in the Appendix A we present a derivation of the expression for $H(a,p)$, which has already been obtained in [12].)

Further, we evaluate $H(a,p) \pmod p$ using Proposition 3 and observe 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 for all summands on the right-hand-side of Equation (2) vanish mod p. So, $H(a,p) \equiv 0 \pmod p$, and in turn for each a, it holds that $\#E_a = p+1$. 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, that is, 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 5, this immediately implies the following:

Theorem 2. *For a prime $p \geq 19$ such that $p \equiv 1 \pmod 6$, it holds:*

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

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

An immediate consequence (except the trivial cases $p = 7, 13$) of Proposition 1 with $d = 6$, and Theorem 2 is next.

Corollary 1. *If p is a prime $\equiv 1 \pmod 6$, 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 $\zeta = \frac{-1-\sqrt{-3}}{2}$.*

Remark 3. *Although the claim of Corollary 1 is known in one or another form (see, e.g., [17]), it seems that the uniform distribution of the curves' order has not been widely discussed in the literature.*

3.2. Computational Aspects of Point-Counting in $\mathcal{E}_p$ When p Is a Large Prime

In this subsection, we refine and re-estimate the algorithmic technique described roughly 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:

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

Hence, Proposition 4 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 a similar method as that exhibited in [18], 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. Thus, taking into account the complexity of single multiplication (squaring) (see, e.g., [19,20]), the expected amount of work in *Step 1* is, heuristically, $\tilde{O}(\log^2 p)$. Additionally, notice that *Step 2* is of complexity $O(\log^2 p)$ (see, e.g., [9] Theorem 3.13 about details).

Remark 4. *If $p \equiv 7 \pmod{12}$, there is an efficient deterministic way to find a square root of any quadratic residue ζ, that is, by computing $\zeta^{\frac{p+1}{4}}$. In particular, this can be applied for $\zeta = -3$ (see [12]).*

Besides that, as can be seen by Corollary 1, 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 summary, the above considerations show the validity of the next theorem:

Theorem 3. *The total computational complexity for simultaneously finding out the six orders linked with family $\mathcal{E}_p$ by the proposed algorithmic technique is $\tilde{O}(\log^2 p)$.*

4. Example and Efficiency Comparison with the SEA Algorithm

4.1. An Example

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

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

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

The numerical data presented below are in the hexadecimal number system. Consecutively, we:

- Calculate $\pm\sqrt{-3} \pmod{p}$:
  - choose a random number $z \in [2, p-1]$:
    `D03CE6183277A6719AD52F362919187D79CA6A50D000975EC4903782F08DAAEB`
  - calculate $z' = z^{\frac{p-1}{3}}$:
    `1AF6F28A07E19B1F1FCCB53D1A166E14092BC3AF668514D3D2ABE80CBD6C0A16`
  - $z' \neq 1$, thus $2z'+1$ is a square root of -3 in $\mathbb{F}_p^*$:
    `35EDE5140FC3363E3F996A7A342CDC281257875ECD0A29A7A557D0197AD8142D;`
- Find X by applying the Euclidean algorithm for p and the found $\sqrt{-3} \in \mathbb{Z}_p^*$, and calculate $(\frac{p-1}{2}^{\frac{p-1}{6}}) \pmod{p} = 2X$:
  `FFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFEBDB3CE472111CA9F0DC134D795D6BFFF;`
- Calculate $\zeta_1 = \frac{-1-\sqrt{-3}}{2}$ and $\zeta_2 = \zeta_1 + \sqrt{-3}$:
  `E5090D75F81E64E0E0334AC2E5E991EBF6D43C50997AEB2C2E5427F34293F5EA,`
  `1AF6F28A07E19B1F1FCCB53D1A166E14092BC3AF668514D3D2ABE80CBD6C0A16;`
- Calculate the values of expression (3) using $1, \zeta_1$ and ζ_2 in the role of multiplier $a^{\frac{p-1}{6}}$, and take their opposites. Finally, we find out the six orders associated with $\mathcal{E}_p$:
  `1000000000000000000000000000000001424C31B8DEEE3560F43EEB286A294004,`
  `FFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFEBDB3CE472111CA9F0DC134D795D6C000,`
  `FFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFE065220C024EA85B297C0746F361E6B81,`
  * `1000000000000000000000000000000001F9ADDF3FDB157A4D6A3FAB90C9E19483,`
  `1000000000000000000000000000000000B761AD86FC2744EC7700D0685FB85481,`
  * `FFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFF489E527903D8BB138AFF4F97A047AB83.`

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

4.2. Efficiency Comparison with the SEA Algorithm

In the program experiments for comparing efficiency of the SEA algorithm with the proposed one, both working at instances of considered task, we used a common laptop with an Intel Core i7-6820HQ at 2.7 GHz (four cores). The algorithm implementation is written in Python, whereas SEA's one is a highly optimized code written in C from the PARI/GP computer algebra system designed specifically for fast computations in the number theory.

In Table A1 of the Appendix B, we give a list of 257−bit primes used as experimental data input. As shown in Table A2, our method is between 20 to 67 times faster, although the implementation is not optimized. We also carried out an experiment with a sporadic 857−bit prime input, whereby the SEA computes the orders for 22.5 s, while our own performs the work for 33.1 milliseconds, that is, almost 680 times faster. The latter fact indicates that the method is much more efficient than the SEA algorithm for large primes, say, above 800 bits.

5. Conclusions

Less or more convenient formulae to compute the orders of elliptic curves over finite fields do exist in contemporary literature (see, e.g., [10,15,21], etc.). In this article, we derive an explicit formula for the order of a curve in the family $\mathcal{E}_p = \{E_a : y^2 = x^3 + a$

$(\mathrm{mod}\ p), a \neq 0\}$ reduced modulo p. Alongside the famous Hasse bound, this formula comprehensively and concisely resolves the problem we deal with. Moreover, our approach permits the transparent determination of 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 $\tilde{O}(\log^2 p)$) to simultaneously compute the six orders associated with $\mathcal{E}_p$ in cases of interest. The experimental results confirm theoretical estimations for efficiency within expected slight abuse due to still unoptimized implementation. This technique improves the best previously known algorithmic solution [6] with almost 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 prime order elliptic curves belonging to families of considered type if the modulo p is varied.

Author Contributions: Conceptualization, Y.B. and M.M.; methodology, Y.B.; software, M.M.; validation, Y.B.; formal analysis, Y.B. and M.M.; investigation, Y.B. and M.M.; resources, Y.B. and M.M.; data curation, Y.B. and M.M.; writing—original draft preparation, Y.B. and M.M.; writing—review and editing, Y.B. and M.M.; visualization, Y.B. and M.M.; supervision, Y.B.; project administration, Y.B.; funding acquisition, Y.B. and M.M. All authors have read and agreed to the published version of the manuscript.

Funding: This research was partially supported by the Bulgarian National Science Fund under Contract KP-06-N32/2-2019.

Institutional Review Board Statement: Not applicable.

Informed Consent Statement: Not applicable.

Data Availability Statement: All data are contained within the article.

Conflicts of Interest: The authors declare no conflict of interest.

Abbreviations

The following abbreviations are used in this manuscript:

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

Appendix A. Derivation of the Expression for $H(a, p)$

Excluding the point at infinity and taking into consideration the meaning of Legendre symbol, for the cardinality $\#E_a - 1 = N'$ of the set of "real" points lying on the curve $E_a \in \mathcal{E}_p$, it could be obtained the following expression:

$$N' = \sum_{x=0}^{p-1}[1 + (\frac{x^3 + a}{p})] = p + \sum_{x=0}^{p-1}(\frac{x^3 + a}{p}) \tag{A1}$$

Next, reducing Equation (A1) modulo p and making use of the Euler criterion, we obtain:

$$N' \equiv \sum_{x=0}^{p-1}(\frac{x^3 + a}{p}) \equiv [(\frac{a}{p}) + h(a, p)] \pmod p \tag{A2}$$

where $h(a, p)$ denotes the sum $\sum_{x=1}^{p-1}(x^3 + a)^{\frac{p-1}{2}}$.

Further, performing the binomial expansion and changing the order of summation, we have:

$$h(a,p) = \sum_{x=1}^{p-1} \sum_{i=0}^{\frac{p-1}{2}} \binom{\frac{p-1}{2}}{i} x^{3(\frac{p-1}{2}-i)} a^i =$$

$$\sum_{x=1}^{p-1} x^{3\frac{p-1}{2}} + \binom{\frac{p-1}{2}}{1} a \sum_{x=1}^{p-1} x^{3\frac{p-3}{2}} + \ldots + \binom{\frac{p-1}{2}}{\frac{p-3}{2}} a^{\frac{p-3}{2}} \sum_{x=1}^{p-1} x^3 + a^{\frac{p-1}{2}} \sum_{1}^{p-1} 1. \quad \text{(A3)}$$

Since the last summand above equals to $a^{\frac{p-1}{2}}(p-1) \equiv -(\frac{a}{p}) \pmod{p}$ then Equation (A2) is simplified to

$$N' \equiv H(a,p) \pmod{p}, \quad \text{(A4)}$$

where the expression for $H(a,p)$ is obtained from (A3) by removing the last summand.

Appendix B. Tables for Comparing the Efficiency

Table A1. Prime Numbers $p_i, i = 1, ..., 10$.

p_i	Prime Number (HEX)
p_1	1744AA82FB357A0A99A571EABF8E72B860517859044F993E2606ECAF7BC6CB169
p_2	1032FAF22DC31F3E339E3F0CAC8BF44F21B383D3A687A41326A4CC77EAC31D881
p_3	19C7E604E23D3DEF8A371353FD8EFA4C9F7503083CD2FCE2EA7FEF1120EC3B3E9
p_4	1750F9C8F1490EEDC1B05F0CA012ED4B42925C588AA5FFCC285F84E802EA71C65
p_5	161D8802C08AC9AB133B20100B50C4CF1710A7BEDBA3292B56567D996DE3CEF4D
p_6	1BF6DA0DA929F9784E07C6835AD78389B06CBD5FB776F9F2371AC79B7C7FC1B6D
p_7	1946A87890B83A015439E75B2BA2C20C9D742E7A85B592815A5D6C11DDACD4695
p_8	1819AA8747CF5595260B5A3D7FF8E800DD365E21E26DEBC306F7E48B12C2E2A29
p_9	18864DC62E42429367F6826C5F2AAF1401875EA94E1DA3D70DB1BB7D049F90525
p_{10}	1304670800156954405D850ABD3086D0E8AC7B898E4CC9F18000CF2B9087DBD15

Table A2. Efficiency Comparison.

Test №	Prime p_i	SEA Execution Time (ms)	Our Method Execution Time (ms)
1	p_1	829.7	12.4
2	p_2	251.8	12.3
3	p_3	636.4	12.2
4	p_4	430.9	11.5
5	p_5	436.8	11.1
6	p_6	284.7	12.3
7	p_7	355.4	10.9
8	p_8	558.0	12.2
9	p_9	398.1	11.1
10	p_{10}	393.2	11.1

References

1. Van Tilborg, H. Elliptic curve cryptosystems; too good to be true? *Nieuw Arch. Voor Wiskd.* **2001**, *5*, 220–225.
2. Miller, V.S. Use of elliptic curves in cryptography. In *Conference on the Theory and Application of Cryptographic Techniques*; Springer: Berlin, Germany, 1985; pp. 417–426.
3. Koblitz, N. Elliptic curve cryptosystems. *Math. Comput.* **1987**, *48*, 203–209. [CrossRef]
4. Schoof, R. Counting points on elliptic curves over finite fields. *J. ThéOrie Des Nombres Bordx.* **1995**, *7*, 219–254. [CrossRef]
5. Croucher, J.S. Collecting Coupon—A Mathematical Approach. *Aust. Sr. Math. J.* **2006**, *20*, 31–35.
6. Munuera, C.; Tena, J.G. An algorithm to compute the number of points on elliptic curves of j-invariant 0 or 1728 over a finite field. *Rend. Del Circ. Mat. Palermo* **1993**, *42*, 106–116. [CrossRef]
7. Peralta, R. A simple and fast probabilistic algorithm for computing square roots modulo a prime number (Corresp). *IEEE Trans. Inf. Theory* **1986**, *32*, 846–847. [CrossRef]
8. Knuth, D.E. *The Art of Computer Programming, Volume 2: Seminumerical Algorithms*, 3rd ed.; Addison-Wesley Longman Publishing Co., Inc.: Boston, MA, USA, 1997.
9. Von zur Gathen, J.; Gerhard, J. *Modern Computer Algebra*; Cambridge University Press: Cambridge, UK, 2013.
10. Kırlar, B.B. On the elliptic curves $y^2 = x^3 - c$ with embedding degree one. *J. Comput. Appl. Math.* **2011**, *235*, 4724–4728. [CrossRef]
11. Ireland, K.; Rosen, M. *A Classical Introduction to Modern Number Theory*, 2nd ed.; Springer: New York, NY, USA, 1990.
12. Borissov, Y.; Markov, M. 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 Proceedings of the 2019 Ninth International Workshop on Signal Design and Its Applications in Communications (IWSDA), Dongguan, China, 20–24 October 2019; pp. 1–5.
13. Rosen Kenneth, H. *Elementary Number Theory and Its Applications*, 6th ed.; Addison-Weley Publishing Company: Boston, MA, USA, 2011.
14. Hardy, G.; Wright, E.; Heath-Brown, R.; Silverman, J.; Wiles, A. *An Introduction to the Theory of Numbers*; Oxford University Press: Oxford, UK, 2008.
15. Washington, L.C. *Elliptic Curves: Number Theory and Cryptography*; CRC Press: Boca Raton, FL, USA, 2008.
16. Dickson, L.E. *History of the Theory of Numbers: Quadratic and Higher Forms*; Courier Corporation: North Chelmsford, MA, USA, 2012; Volume 3.
17. Bos, J.W.; Halderman, J.A.; Heninger, N.; Moore, J.; Naehrig, M.; Wustrow, E. Elliptic curve cryptography in practice. In *International Conference on Financial Cryptography and Data Security*; Springer: Berlin, Germany, 2014; pp. 157–175.
18. Wilker, P. An efficient algorithmic solution of the Diophantine equation $u^2 + 5v^2 = m$. *Math. Comput.* **1980**, *35*, 1347–1352.
19. Harvey, D.; Hoeven, J. Integer Multiplication in Time O(nlogn). 2020. Available online: https://hal.archives-ouvertes.fr/hal-02070778v2 (accessed on 7 June 2021).
20. Cohen, H. *A Course in Computational Algebraic Number Theory*; Springer Science & Business Media: New York, NY, USA, 2013; Volume 138.
21. Silverman, J.H. *The Arithmetic of Elliptic Curves*; Springer Science & Business Media: New York, NY, USA, 2009; Volume 106.