An Approach for Computing the Number of Points on Elliptic Curve $y^2 = x^3 + a \ (mod\ p)$ via Explicit Formula for That Number Modulo p

Yuri Borissov[1] and Miroslav Markov[2]

***Abstract*—We present an efficient approach for determining the cardinality of the set of points on each elliptic curve of the family $\mathcal{E}_p = \{E_a : y^2 = x^3 + a \ (mod\ p), a \in \mathbb{Z}_p^*\}$ by applying the famous Hasse's bound together with an explicit formula for that cardinality reduced to modulo p which is derived by us. As a by-product it is shown that for fixed $p \equiv 1 \ (mod\ 6)$ those cardinalities take exactly six distinct values. The latter permits us to provide a reasoning why the curve E_7 employed by Bitcoin system has an optimal resistance among the curves from $\mathcal{E}_p$ against the EC variant of Pohlig-Hellman algorithm when p is the actual modulo used in that system. This approach allows also to give another proof of the known result that in case $p \equiv 2 \ (mod\ 3)$ the cardinalities of all curves from $\mathcal{E}_p$ are equal to $p + 1$.**

I. Introduction

The elliptic curves over finite fields play an important role in modern cryptography. The reader is referred to [1] for an introduction concerning their cryptographic significance. In brief, the advantage of the so-called elliptic curve cryptography (ECC) over the non-ECC is that it requires smaller keys to provide security of the same level.

A crucial issue for usefulness of an elliptic curve is whether the number of its points possesses a sufficiently large prime factor. For instance, the presence of such a factor allows to design ECC system which outstands on the best known general-purpose attack for solving the relevant elliptic curve discrete logarithm problem (ECDLP), namely, a combination of the Pohlig-Hellman and the Pollard's rho algorithms. This is due to the fact that time complexity of this combination of algorithms is $O(\sqrt{p})$ with p being the largest primal divisor of the order of the properly chosen base point. For that reason counting the number of points on a given curve, as a first step for determining the subgroup structure of their group, is important from a cryptographic standpoint.

A very efficient algorithm which computes the cardinality of set of points over an elliptic curve of general type (given its full description) is due to Schoof [2]. In this paper, however, inspired by Certicom's secp256k1 elliptic curve employed in Bitcoin cryptocurrency, we are interested in the whole family of Bitcoin-like curves $\mathcal{E}_p = \{E_a : y^2 = x^3 + a, \ a \neq 0\}$ over $\mathbb{Z}_p$, and address the problem of determining the cardinality $\#E_a$ in terms of the parameter a and modulo p. For a solution of the same problem posed regarding the family of curves $\{D_b : y^2 = x^3 - bx, \ b \neq 0\}$, the reader is referred to [3, Ch. 4.4]. One may find some special cases of the specific problem considered here as exercises in [4, Ch. 8, Ex. 15,27]. A contribution to the problem of interest in general case is presented by the article [5], too. Namely, the author of [5] has obtained explicit formulae for $\#E_a$ in terms of a proper representation of the prime p in the form $p = u^2 + v^2 - uv$ for some integers u and v. His formulas distinguish between many separate cases according to remainder of p modulo 4, the cubic character $\chi_3(2)$ and the values of quadratic, cubic and sextic characters of a (see [5, Theorem 1]). It is deserved mentioning that our approach is more concise treating the problem uniformly in respect of p and splitting the solution into just two cases according to the values of certain expression for $\#E_a \ mod\ p$ versus the threshold $\frac{p}{2}$.

The paper is organized as follows. In the next section, we state the problem and recall some background needed to present the results. In Section III, our approach to the problem is described, including the issues for possible values of cardinalities of interest and the computational aspects of obtained formulae for large p. Section IV gives an example with p being the prime employed in Bitcoin system. Some conclusions are drawn in the last section.

II. Statement of the problem and some background

Let p be an odd prime number 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 $\mathcal{E}_p = \{E_a : y^2 = x^3 + a \ (mod\ p), \ a \in \mathbb{Z}_p^*\}$ 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 determining the cardinality of common member of that family, the curve E_a, in terms of parameters a and p.

For basic number-theoretic notions as the Legendre symbol $(\frac{z}{p})$ of an integer z modulo prime p; the absolutely least residue ($\mathcal{ALR}$) and the least non-negative residue ($\mathcal{LNR}$), we refer to [6, p. 81; p. 46], respectively. We use notations "$\equiv$" for congruence modulo p and "$=$" in $\mathbb{Z}_p$ in an interchangeable manner depending on the context.

We will need the following property of Legendre symbol stated hereinafter as lemma.

[1]Yuri Borissov is with the Department of Mathematical Foundations of Informatics, Institute of Mathematics and Informatics, BAS, G. Bontchev Str. 8, 1113 Sofia, Bulgaria, e-mail: youri@math.bas.bg

[2]Miroslav Markov is with the Department of Mathematical Foundations of Informatics, Institute of Mathematics and Informatics, BAS, G. Bontchev Str. 8, 1113 Sofia, Bulgaria, e-mail: markov.miro@gmail.com

978-1-7281-1669-3/19/$31.00 ©2019 European Union

Lemma 1. For any $z \in \mathbb{Z}$ it holds: $(\frac{z}{p}) \equiv z^{\frac{p-1}{2}} \ (mod\ p)$.

Another necessary lemma is the following well-known fact (see, e.g. [7, Ch. 3]).

Lemma 2. Let n be a positive integer and define $S_k(n) = 1^k + 2^k + \ldots + n^k, k = 0, 1, \ldots$. Then it holds:

$$(k+1)S_k(n) + \binom{k+1}{2} S_{k-1}(n) + \ldots + S_0(n) = (n+1)^{k+1} - 1. \quad (1)$$

More specifically:

$$S_0(n) = n;$$
$$2S_1(n) + S_0(n) = (n+1)^2 - 1;$$
$$etc..$$

There is no exact formula for the number of points on a general type elliptic curve over $\mathbb{Z}_p$. The well-known result in this direction is the following bound given by Hasse in 1934.

Theorem 3. (**Hasse**) The number of points N (excluding the infinite one) on an elliptic curve over $\mathbb{Z}_p$ satisfies:

$$|N - p| \leq 2\sqrt{p}.$$

At the end of this section, we recall a needed fact from the theory of quadratic partitions of primes. This a bit obsolete (but useful) result due to C.G.J. Jacobi (1827) which was later on elaborated by M.A. Stern (1832) (see, [8, vol. III, p. 55] about historical facts).

Proposition 4. If p is a prime of the form $p = 6k + 1$ for which $p = t^2 + 3u^2$ then

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

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

III. Our approach

We start with a simple lemma.

Lemma 5. Let ρ and r denote $\mathcal{ALR}(z, m)$ and $\mathcal{LNR}(z, m)$ of z modulo odd m, respectively. Then it holds:

$$\rho = \begin{cases} r, & \text{if } r < \frac{m}{2} \\ r - m, & \text{otherwise.} \end{cases}$$

The following proposition helps to fix uniquely N, the number of points on a given elliptic curve, provided one can compute $N \ mod\ p$.

Proposition 6. In notations of Theorem 3, let $r = \mathcal{LNR}(N, p)$ for prime $p \geq 17$. Then it holds:

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

Proof. Indeed, if $p \geq 17$ then evidently $2\sqrt{p} < \frac{p}{2}$. Thus, the Hasse theorem implies $|N - p| < \frac{p}{2}$ which means that $\mathcal{ALR}(N, p) = N - p$. Finally, Lemma 5 completes the proof. □

A. An explicit formula for the cardinality of elliptic curve E_a reduced to modulo p

Taking into consideration the meaning of Legendre symbol, for the number N of points lying on fixed curve $E_a \in \mathcal{E}_p$ (excluding the infinite point) it would be obtained the next well-known expression:

$$N = \sum_{x=0}^{p-1} [1 + (\frac{x^3 + a}{p})] = p + \sum_{x=0}^{p-1} (\frac{x^3 + a}{p}) \quad (2)$$

Next, reducing Eq.(2) modulo p and making use of Lemma 1, we obtain:

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

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

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

$$h(a,p) = \sum_{x=1}^{p-1} \sum_{i=0}^{\frac{p-1}{2}} \binom{\frac{p-1}{2}}{i} x^{3(\frac{p-1}{2} - i)} a^i = \sum_{x=1}^{p-1} x^{3\frac{p-1}{2}} + \binom{\frac{p-1}{2}}{1} a \sum_{x=1}^{p-1} x^{3\frac{p-3}{2}} + \ldots + \sum_{1}^{p-1} a^{\frac{p-1}{2}}. \quad (4)$$

As it is easy to see, the last summand equals to $a^{\frac{p-1}{2}}(p-1) \equiv -(\frac{a}{p}) \ (mod\ p)$. So, Eq. (3) is simplified to

$$N \equiv H(a, p) \ (mod\ p), \quad (5)$$

where $H(a, p)$ is obtained from $h(a, p)$ removing that last summand.

In order to simplify further Eq. (5), we prove the following proposition.

Proposition 7. In notations of Lemma 2, for odd prime p it holds:

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

Proof. Taking into account the little Fermat theorem it is sufficient to prove for $0 \leq k < p-1$. We shall make use of Lemma 2 with $n = p-1$. Obviously, $S_0(p-1) = p-1 \equiv -1 \ (mod\ p)$. Suppose the statement holds true for all k: $0 < k < l$ where l is some fixed integer in $[1, p-2]$. To prove for $k = l$, we apply Eq. (1) reducing both sides modulo p. Thus, by the inductive hypothesis, we have: $(l+1)S_l(p-1) - 1 \equiv -1 \ (mod\ p)$, or $(l+1)S_l(p-1) \equiv 0 \ (mod\ p)$. Finally, since $1 \leq l \leq p-2$, the last congruence implies that p divides $S_l(p-1)$ which has to be proved. □

We shall evaluate $H(a, p) \ (mod\ p)$ making use of the above proposition and observing that the involved powers of x are

those integers in the interval $[3, 3\frac{p-1}{2}]$ which are multiples of 3. To this end, (excluding the trivial case $p = 3$) we consider the two essentially distinct cases according to values of $p \ (mod\ 6)$:

- $p \ (mod\ 6) = 5$
  In this case $p - 1 \equiv 1 \ (mod\ 3)$ which by Proposition 7 implies that all summands modulo p in the defining expression of $H(a, p)$ vanish. So, $H(a, p) \equiv 0 \ (mod\ p)$, i.e. by Eq. (5) it follows $N = kp$ for some integer $k \geq 0$. Thus $|N - p| = |(k - 1)p| = |(k - 1)|p$ and by Hasse's bound this is possible only if $k = 1$. To conclude, in the considered case $\#E_a = p + 1$ whatever a would be. This is a well-known fact (see, e.g. [4, Ch. 18, Ex.1]) and means also that all curves from the considered family are supersingular [3, Proposition 4.31].
- $p \ (mod\ 6) = 1$
  Proceeding similarly as in the previous case, we now see that the expression of interest contains only one nonzero summand, i.e. that for $i = \frac{p-1}{6}$. Thus, it holds:

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

$$-\binom{\frac{p-1}{2}}{\frac{p-1}{6}} a^{\frac{p-1}{6}} (mod\ p).$$

Now, alongside with Eq. (5) this implies the next proposition.

Proposition 8. If the prime $p \ (mod\ 6) = 1$ then

$$N \equiv -\binom{\frac{p-1}{2}}{\frac{p-1}{6}} a^{\frac{p-1}{6}} (mod\ p). \tag{6}$$

In turn, the last proposition together with Proposition 6 immediately imply the main result of this work.

Theorem 9. If $p \geq 19,\ p \ (mod\ 6) = 1$ then it holds

$$\#E_a = \begin{cases} p + 1 + \mathcal{R}(a, p), & \text{if } \mathcal{R}(a, p) < \frac{p}{2} \\ 1 + \mathcal{R}(a, p), & \text{otherwise,} \end{cases} \tag{7}$$

where $\mathcal{R}(a, p)$ denotes the least non-negative residue of RHS of congruence (6).

Remark: Notice that the additional "1" in the above expressions stands for the infinite point.

B. The possible values of cardinalities $\#E_a$ when a varies over $\mathbb{Z}_p^*$

Before addressing this issue, we recall some supplementary notions, notations and facts (possibly with slight abuses).
An element z of $\mathbb{Z}_p^*$ is called a quadratic residue modulo p if there exists $x \in \mathbb{Z}_p^*$ such that $z = x^2$. The set of all quadratic residues, denoted by $\mathcal{QR}_p$, is a subgroup of $\mathbb{Z}_p^*$ of order $\frac{p-1}{2}$. The famous Euler criterion stated in that terminology claims that z is a quadratic residue if and only if $z^{\frac{p-1}{2}} = 1$. Analogously, a cubic residue modulo p is an element of $\mathbb{Z}_p^*$ being a cube of another element and the set of all cubic residues, denoted by $\mathcal{CR}_p$, forms a subgroup of $\mathbb{Z}_p^*$. If $p \ (mod\ 3) = 1$ then $|\mathcal{CR}_p| = \frac{p-1}{3}$, and an analog of the Euler criterion about cubic residues in this case states that $z \in \mathcal{CR}_p$ if and only if $z^{\frac{p-1}{3}} = 1$.

Lemma 10. If $p \equiv 1 \ (mod\ 6)$ the monomial $\mathbf{m}(z) = z^{\frac{p-1}{6}}$ takes exactly six distinct values in $\mathbb{Z}_p^*$ each one of them $\frac{p-1}{6}$ times. These values are the sixth roots of unity in $\mathbb{Z}_p^*$: $\pm 1, \pm\zeta, \pm(\zeta + \sqrt{-3})$ where $\zeta = \frac{-1-\sqrt{-3}}{2}$.

Proof. Let $g \in G = \mathcal{QR}_p \cap \mathcal{CR}_p$. By the Euler criterion, we have: $\mathbf{m}^3(g) = g^{\frac{p-1}{2}} = 1$ and $\mathbf{m}^2(g) = g^{\frac{p-1}{3}} = 1$, respectively, which immediately implies $\mathbf{m}(g) = 1$. Now, we shall show that $\mathbf{m}(z_1) = \mathbf{m}(z_2)$ if and only if z_1 and z_2 belong to the same coset of the subgroup G in $\mathbb{Z}_p^*$. Indeed, if $z_2 = z_1 g$ with $g \in G$ then evidently $\mathbf{m}(z_2) = \mathbf{m}(z_1)\mathbf{m}(g) = \mathbf{m}(z_1)$. Backwards, if $\mathbf{m}(z_1) = \mathbf{m}(z_2)$ then $\mathbf{m}(z_1/z_2) = 1$ and the Euler criterion gives $z_1/z_2 \in G$, i.e. they are in the same co-set. The above considerations show the monomial remains constant over the six co-sets of the subgroup G in Z_p^* and takes different value in each one of them. This also implies that every value in the image of $\mathbf{m}(z)$ is accepted $\frac{p-1}{6}$ times. Further, the obvious $\mathbf{m}^6(z) = z^{p-1} = 1$ means that the values of interest satisfy equation: $V^6 = 1$, i.e. they are the sixth roots of unity in $\mathbb{Z}_p^*$. To find them, notice that $V^6 - 1 = (V^3 - 1)(V^3 + 1) = (V - 1)(V^2 + V + 1)(V^3 + 1)$ which imply that the roots are $\pm 1, \pm\zeta, \pm(\zeta + \sqrt{-3})$ where $\zeta = \frac{-1-\sqrt{-3}}{2}$. □

Remark: As it can be easily seen if $p \equiv 1 \ (mod\ 6)$ then it holds $-3 \in \mathcal{QR}_p$ (of course, $\sqrt{-3}$ accepts two values) or equivalently all sixth roots of unity $\in \mathbb{Z}_p^*$. Also, note the above proof shows that values of monomial $\mathbf{m}(z)$ are determined by quadratic and cubic reciprocity of z.

Corollary 11. If $p \equiv 1 \ (mod\ 6)$ then when a varies over $\mathbb{Z}_p^*$ the cardinalities $\#E_a$ take exactly six values in accordance with quadratic and cubic reciprocity of a.

Proof. The cases $p = 7, 13$ are proved by direct check. For $p \geq 19$, the proof is an immediate consequence of Lemma 10 and Theorem 9. □

C. Some computational aspects

In this subsection, we shall point out an efficient way for computing of the six cardinalities $\#E_a, E_a \in \mathcal{E}_p$ when p is a large prime $\equiv 1 \ (mod\ 6)$.

A pivotal part in the computations is that of $\binom{\frac{p-1}{2}}{\frac{p-1}{6}} \ (mod\ p)$. Fortunately, that 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 solving the quadratic diophantine equation $t^2 + 3u^2 = p$ with two unknowns t and u. This solution can be found, for instance, by a method

recommended in [9, p. 366] and consisting of two steps: finding a square root of -3 in $\mathbb{Z}_p^*$, followed by the application of a version of the Euclidean algorithm for p and thus found $\sqrt{-3}$. The probabilistic first step often requires to know in advance a quadratic non-residue mod p which can be yielded after two attempts, on average, each one consisting of random selection of an element in $\mathbb{Z}_p^*$ and check with the help of Euler criterion. (For further details about finding square roots modulo p in general case, e.g., comparison of Tonelli-Shanks's and Cipolla's algorithms, the reader can consult [10].) It is worth mentioning that if $p \ (mod\ 4) = -1$ (as in the case of Bitcoin) there is a simple deterministic way to find square root of a quadratic residue a, i.e., it can be easily seen that $\sqrt{a} = a^{\frac{p+1}{4}}$. Roughly speaking, the amount of work in the first step is proportional to $log\ p$. However, the second step is harder with a bit-complexity bounded by $O(log^2 p)$ (see, e.g. [11, Theorem 3.13]). Moreover, by Lemma 10, the six distinct values of the multiplier $\mathbf{m}(a) = a^{\frac{p-1}{6}}$ (see Eq. 6) are linearly expressible in terms of the already got $\sqrt{-3}$. Therefore, the total computational complexity of our approach to find simultaneously the six cardinalities, is dominated by that of modular computation of the binomial coefficient of interest (luckily enough, carried out only once for the whole family $\mathcal{E}_p$) and hence upper bounded by $O(log^2 p)$.

IV. **Example**

To illustrate our approach, we present an example obtained by taking p to be the modulo of Bitcoin cryptocurrency system. As it is well-known:

$$p = 2^{256} - 2^{32} - 2^9 - 2^8 - 2^7 - 2^6 - 2^4 - 1.$$

Hereinafter, the numerical data are presented in decimal number system.

Consecutively, we:

- calculate $\sqrt{-3}\ (mod\ p) = (-3)^{\frac{p+1}{4}}\ (mod\ p)$:

  46029379406564096854001790410822423644980802362641155959005600444236215071 54,

  11118915129665978573817080596760566548877190442937644844355702396348521316 4509;

- solve the diophantine equation $t^2+3u^2 = p$ and calculate $\binom{\frac{p-1}{2}}{\frac{p-1}{6}}\ (mod\ p) = 2t$:

  67133185248369964381908659669674522742 0;

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

  60197513588986302554485582024885075108884032450952339817679072026166228089408,

  55594575648329892869085402983802832744385952214688224221778511981742606582254;

- calculate the RHS of Congr. (6) using $\pm 1, \pm\zeta_1$ and $\pm\zeta_2$ in the role of multiplier $a^{\frac{p-1}{6}}$. Afterwards, by Theorem 9 we find out the six cardinalities for $\mathcal{E}_p$:

  11579208923731619542357098500868790785259865281315686439563849741121208944424 4,

  11579208923731619542357098500868790785370240505220622369631000487429950784899 1,

  11579208923731619542357098500868790785350889613155860402642424973821490672175 7,

  11579208923731619542357098500868790785394131651812426368327667060460557989908 4,

  11579208923731619542357098500868790785283756427907490438260516314151816149433 7,

  11579208923731619542357098500868790785303107319972252405249091827760276262157 1.

- factorize those cardinalities using the GMP - ECM method implemented in SageMath. Their highest prime factors are:

  56693877878334528364219052443276726520 59,

  10131766773001318469008702396060356387381009972480920692566974370 31,

  21185332237923386731589004422385870303148525396177568452 3,

  19927510177695253241189007035359757442641709999 67,

  41245443549316649091297836755593555342121,

  11579208923731619542357098500868790785283756427907490438260516314151816149433 7.

Finally, it is worth noting that the known value for Bitcoin: $\#E_7$ is confirmed (the last above), and it turns out that is the only prime number among the cardinalities calculated.

V. **Conclusion**

Despite that there is no exact expression for the number of points on a general type elliptic curve over $\mathbb{Z}_p$, in the case of a family $\mathcal{E}_p = \{E_a : y^2 = x^3 + a\ (mod\ p), a \neq 0\}$, as it is shown in Section III, such a formula (modulo p) could be found. This result together with the famous Hasse's theorem allows to determine uniquely the cardinality of every such curve in terms of parameters a and p provided $p \geq 17$. Moreover, we show that cardinalities of interest take exactly six values for fixed $p \equiv 1\ (mod\ 6)$ and can be classified according to the type of quadratic and cubic reciprocity of the parameter a modulo p; while in case $p \equiv 5\ (mod\ 6)$ we reproved the known fact that those cardinalities accept a unique value, i.e., $p + 1$ whatever a would be.

To exemplify the approach developed, we have calculated the six cardinalities of the curves from the family $\mathcal{E}_p$ where p is the prime employed in Bitcoin system. The subsequent factorization of those cardinalities shows the presence of only one prime number among them (coinciding with the known value for $\#E_7$, of course), which is of order 10^{11} greater than the largest amongst the highest prime factors of the others. This reasoning justifies in part the designers' preference for the curve E_7, being the worst-case input for the analog of Pohlig-Hellman algorithm for ECDLP.

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] R. Schoof, "Elliptic curves over finite fields and the computation of square roots mod p", *Math. Comp.*, vol. 44(170), pp. 483–494, 1985.

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

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

[5] B. B. Kirlar, "On the elliptic curves $y^2 = x^3 - c$ with embedding degree one", *Journal of Computational and Applied Mathematics*, vol. 235, pp. 4724–4728, 2011.

[6] I. M. Vinogradov, *Elements of Number Theory*, translated from the fifth revised edition by Saul Kravetz, Mineola, N.Y., Dover Publications Inc. 1954.

[7] G. Polya, *Mathematical Discovery*, John Wiley & Sons, Inc. New York. London, 1962.

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

[9] H. C. Williams, "An m^3 public-key encryption scheme", in *Lectures Notes in Computer Science – Crypto 85* vol. 218, Springer-Verlag, New York, pp. 358–368, 1986.

[10] G. Tornaria, "Square roots modulo p", *LATIN 2002*, pp. 430–434, 2002.

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