(Deep) Learning About Elliptic Curve Cryptography

Diana Maimuţ[1][a], Cristian Matei[1][b] and George Teşeleanu[2][c]

[1]*Advanced Technologies Institute, 10 Dinu Vintilă, Bucharest, Romania*

[2]*Simion Stoilow Institute of Mathematics of the Romanian Academy, 21 Calea Grivitei, Bucharest, Romania*

Keywords: Elliptic Curve, Elliptic Curve Cryptography, Schoof's Algorithm, Artificial Intelligence.

Abstract: Motivated by the interest in elliptic curves both from a theoretical (algebraic geometry) and applied (cryptography) perspective, we conduct a preliminary study on the underlying mathematical structure of these mathematical structures. Hence, this paper mainly focuses on investigating artificial intelligence techniques to enhance the efficiency of Schoof's algorithm for point counting across various elliptic curve distributions, achieving varying levels of success.

1 INTRODUCTION

Dating back to ancient Greece with the study of Diophantine equations, elliptic curves have become very interesting objects in modern mathematics[1] due to their intriguing underlying mathematical structure and the wide range of applications. Elliptic curves have been around from the foundations of geometry to the proof of Fermat's last theorem[2] and further on, often being defined as the solution set of a polynomial system.

We further present two possible applications of our current work, reflecting our dual focus on real world scenarios and fundamental research related to the mathematical description of elliptic curves.

Elliptic Curve Cryptography. Elliptic curve cryptography (ECC) was originally introduced in (Miller, 1986; Koblitz, 1987) as a new public key cryptography paradigm, while Lenstra's factorization algorithm (Lenstra, 1987) was the first reported use of elliptic curves for cryptanalysis. Throughout the years, ECC has drawn more and more attention due to its high level security and an appealing characteristic related to implementation efficiency: keys are shorter than those used in other cryptographic algorithms.

On the other side, elliptic curves are of interest in the context of quantum safe algorithms, which have attracted researchers' attention during the last years. We refer the reader to (NIS,) for specific details. Recently, vulnerabilities of post-quantum ECC algorithms have been reported in the literature (Castryck and Decru, 2023). Given this, we believe it is of great interest to conduct a detailed analysis of the underlying mathematical structure of elliptic curves to identify future proposals that could be suitable candidates for replacing vulnerable schemes.

BSD Conjecture. We further delve into the theoretical side of our motivation. Let $E(\mathbb{Q})$ and $E(\mathbb{F}_q)$ be an elliptic curve over $\mathbb{Q}$ and $\mathbb{F}_q$, respectively. The Birch and Swinnerton-Dyer (BSD) conjecture (Birch and Swinnerton-Dyer, 1965) establishes a connection between the rank of $E(\mathbb{Q})$, which reflects its algebraic characteristics, and an analytic feature of its L-function. The authors used a computer to study the values of the L-function at $Re(s) = 1$,

$$L(E,1) = \prod_{q \text{ prime}} \frac{q}{|E(\mathbb{F}_q)|}$$

and observed that as the algebraic rank of $E(\mathbb{Q})$ increases, the number of points on $E(\mathbb{F}_q)$ also tends to increase. More generally (He et al., 2022b), the L-function of $E(\mathbb{Q})$ can be expressed as an Euler product for $Re(s) \gg 0$,

$$L(E,s) = \prod_{q \text{ prime}} L_q(E,s)^{-1},$$

where $L_q(E,s) = 1 - a_q(E) \cdot q^{-1} + q^{1-2s}$ and $a_q(E) = q + 1 - |E(\mathbb{F}_q)|$.

[a] https://orcid.org/0000-0002-9541-5705

[b] https://orcid.org/0000-0001-9233-0573

[c] https://orcid.org/0000-0003-3953-2744

[1] especially number theory and algebraic geometry

[2] late 1990's

Maimuţ, D., Matei, C. and Teşeleanu, G.
(Deep) Learning About Elliptic Curve Cryptography.
DOI: 10.5220/0013095100003899

In *Proceedings of the 11th International Conference on Information Systems Security and Privacy (ICISSP 2025) - Volume 2*, pages 437-444
ISBN: 978-989-758-735-1; ISSN: 2184-4356

Motivated by the BSD conjecture, Mestre (Mestre, 1982) and Nagao (Nagao, 1992), followed by subsequent researchers Elkies and Koblitz (Elkies and Klagsbrun, 2020), and Bobba (Bober, 2013), introduced certain sums (see (Kazalicki and Vlah, 2023, Section 2) for a list of Mestre-Nagao sums) that are heuristically expected to detect curves of high analytic rank. One such example is the following

$$S_0(t) = \frac{1}{\log t} \sum_{\substack{q<t \\ \text{good reduction}}} \frac{a_q(E)\cdot \log q}{q}.$$

Given the above, it is of clear scientific interest to study the cardinality of $E(\mathbb{F}_q)$ as the curve's coefficients[3] A and B are fixed and the prime varies.

Motivation. An AI-based method aiming at enhancing Schoof's algorithm for finding the number of points of an elliptic curve is proposed in (Maimuţ and Matei, 2022). The authors focus on elliptic curves of prime order. The obtained results can be of general interest in terms of ECC algorithms and may also be combined with already established algorithmic improvements to obtain better software implementation timings.

Our method is based on the one presented in (Maimuţ and Matei, 2022), while the main difference between the two methods is given by the way we constructed our datasets. In (Maimuţ and Matei, 2022), the dataset is composed of various triplets of the form (p,A,B). In other words, both the prime p and the elliptic curve $E(A,B)$ vary, whereas in the present work we consider two separate situations. Firstly, we fix an elliptic curve and then we study the behaviour of the normalized Frobenius trace $\widetilde{\delta}$ of $E(A,B)$ as the prime p varies. Secondly, we fix the prime p and we analyze the value of $\widetilde{\delta}$ when the pair (A,B) takes various values.

We choose this approach because, from a theoretical point of view, it should produce better results than the more general setting found in (Maimuţ and Matei, 2022). Also, we further divide the curves considered in two classes, namely the CM curves and non-CM curves, as the distribution of the values of $|E(A,B|$ varies greatly for each class. The main objective of this paper is to improve the results found in (Maimuţ and Matei, 2022) by considering particular cases. The use of Machine Learning (ML) models is motivated by the connection between Hasse's bound for $\widetilde{\delta}$ and the range of the activation functions used for ML models.

Further Motivation. For the negative results we present in some of our experiments, we provide the reader with a twofold explanation.

1. Impossibility results, as well as unsuccessful directions are often underestimated or rarely reported in the literature (Howitt and Wilson, 2014; Truran, 2013), leading to the risk of repeated errors. We strongly believe that by sharing our outcomes we can contribute to a collective learning process. Our approach is in accordance with the recommendation in (Tao, b) to document mistakes in order to prevent their recurrence in the future.
2. In the majority of scientific reports and papers, authors often depict their results as if they were achieved in a straightforward manner. This paradigm contributes to a distorted perception of research (Medawar, 1963; Howitt and Wilson, 2014; Tao, a; Weidman, 1965), promoting the misconception that failure and unexpected outcomes might not be considered natural directions of scientific attempts (Howitt and Wilson, 2014; Schwartz, 2008). On the practical side, we aim at providing readers with meaningful insights into the design phase of elliptic curve-based cryptographic primitives or protocols.

Related Work. A machine learning (ML) classifier was used in (He et al., 2023) to predict the rank and torsion order of an elliptic curve or a genus 2 curve. In the case of elliptic curves over $\mathbb{Q}$, rank 0 curves were distinguished from those with rank 1 by logistic regression with accuracy $> 97\%$. Based on their torsion order, $E(\mathbb{Q})$ with order 1 where distinguished from ones with order 2 with precision 99.9%. For other classifications we refer the reader to (He et al., 2023).

In (He et al., 2022a), the authors develop a ML model that distinguishes between complex multiplication (CM) elliptic curves and non-CM elliptic curves with a reported accuracy of 100%. This model takes as input vectors containing the values of the Frobenius trace δ for primes p up to 10000. This task is not considered hard, since for a CM curve the probability that $\delta = 0$ is 50%, whereas for a non-CM curve it is negligible.

The authors of (Alessandretti et al., 2023) consider using ML models for predicting certain quantities that appear in the BSD conjecture (Birch and Swinnerton-Dyer, 1965), represented by the problem of finding the number of points that have coordinates in $\mathbb{Q}$. When considering only the Weierstrass coefficients as input, the authors obtained unsatisfactory results. They also compare this task with the failure of predicting prime numbers using ML. However, when

[3] $E(\mathbb{F}_q): y^2 = x^3 + Ax + B$

also including the BSD quantities as input, the results were more favourable.

In (He et al., 2022b), the authors uncovered an intriguing oscillation pattern within the averages of Frobenius traces among elliptic curves with consistent rank and conductor values within a defined range. This discovery emerged through the application of ML and computational methods, yet it does not provide a mathematical explanation for the phenomenon, dubbed "murmurations" for its resemblance to bird flight patterns. Later, this bias was detected in more general families of arithmetic *L*-fuctions (Sutherland, 2022; Lee et al., 2023). These discoveries lead to the computations of a murmuration density, a notion introduced in (Sarnak, 2023), for holomorphic newforms by Zubrilina (Zubrilina, 2023).

The classification of the rank of an elliptic curve based on the trace of Frobenius endomorphism and its conductor was studied in (Kazalicki and Vlah, 2023). For this purpose the authors trained a deep convolutional neural network (CNN). For comparison they also trained a simple fully connected neural networks Ω using the value of one of the six Mestre-Nagao sums. According to (Kazalicki and Vlah, 2023) the classifiers based on the first three Mestre-Nagao sums have the best performance of all considered Mestre-Nagao sums. Also, CNN-based classifiers were significantly better than Ω. Inspired by this approach, (Bujanović et al., 2024) investigates the detection of elliptic curve ranks, for values 0 and 1 using $S_0(B)$ and their conductor.

Structure of the Paper. In Section 2, we introduce various notations and discuss elliptic curve preliminaries. Our main results and related experiments are discussed in Section 3: we tackle both the cases of prime number variation over a fixed elliptic curve and elliptic curve variation over a fixed prime number with an AI-based setup. We conclude and provide the reader with future work ideas in Section 4.

2 ELLIPTIC CURVES PRELIMINARIES

2.1 Notations

We further consider elliptic curves E in their reduced Weierstrass form, *i.e.*:

$$y^2 = x^3 + Ax + B, \qquad (1)$$

defined over a finite field $\mathbb{F}_p$, where p is prime. We denote by $E(A,B)$ the elliptic curve defined by the pair (A,B). The notation $|E(A,B)|$ refers to the cardinality of the elliptic curve $E(A,B)$. For simplicity, we further use δ instead of the well established $a_q(E)$ in the literature.

A point $(x,y) \in E(A,B)$ with coordinates in the algebraic closure of $\mathbb{F}_p$ is called a torsion point if it has finite order. We further denote by $E_{A,B}[\ell]$ the ℓ-torsion points of $E(A,B)$.

The Jacobi symbol of an integer a modulo an integer N is represented by $J_N(a)$.

The mean is denoted by μ, while the average absolute deviation by *AAD*.

2.2 Group Order

We first recall Hasse's theorem which we use throughout the paper.

Theorem 2.1 (Hasse). The number of points n of an elliptic curve defined over a finite field of size p satisfies the inequality

$$|n - p - 1| \leq 2\sqrt{p}. \qquad (2)$$

In (Schoof, 1985), Schoof published the first deterministic and polynomial-time algorithm that computes the order of an elliptic curve defined over a finite field. The algorithm starts off by using Theorem 2.1, which provides an interval of possible values for the order of the elliptic curve. That specific interval has the width $4\sqrt{p}$.

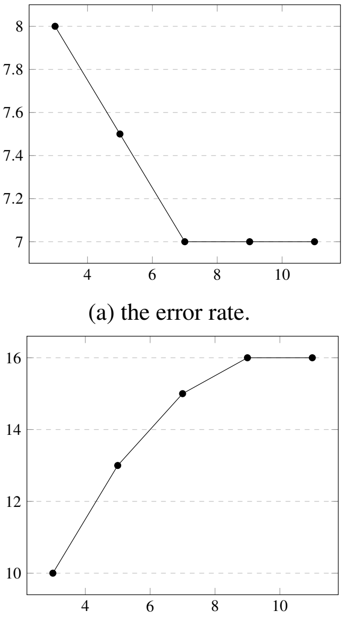
Since the order can be written as $n = p + 1 - \delta$, where δ is the trace of the Frobenius endomorphism (Washington, 2008), the problem of finding the order reduces to that of finding the value of δ. The next step involves computing the value of δ modulo for some primes, such that their product is greater than $4\sqrt{p}$. Finally, the Chinese Remainder Theorem (Washington, 2008) produces the value of δ, which is needed for finding the order.

2.3 Complex Multiplication of Elliptic Curves

Elliptic curves fall into two categories: with or without complex multiplication. This classification has important consequences for determining the cardinality of a given elliptic curve.

Definition 2.1. An elliptic curve defined over $\mathbb{C}$ has complex multiplication (CM) if its endomorphism ring satisfies the condition that $End(E) \supsetneq \mathbb{Z}$.

Example. Consider the elliptic curve E_1 defined over $\mathbb{C}$ given by the equation $y^2 = x^3 + x$. The endomorhism $\phi : E_1 \longrightarrow E_1$ given by $\phi(x,y) = (-x, iy)$ is not a multiply-by-n map (*i.e.* the map that sends $P \in E_1$ to $nP \in E_1$). Hence, E_1 does have CM.



(a) the error rate.

(b) the reduced Hasse interval.

Figure 1: The relationship between the number of neural network layers and the error rate/the reduced Hasse interval.

Definition 2.2. Let E be an elliptic curve given by Equation (1), with $A, B \in K$, where K is a field of characteristic not equal to 2 or 3. The j-invariant of E is defined as

$$j(E) = 1728 \cdot \frac{4A^3}{4A^3 + 27B^2}.$$

The j-invariant of an elliptic curve is a useful tool that can also be used to decide whether a curve has CM or not. In (He et al., 2022a), the authors list all the values of the j-invariant over $\mathbb{C}$ that correspond to elliptic curves that have CM, namely

$$0,\ 2^4\,3^3\,5^3,\ -2^{15}\,3\,5^3,\ 2^6\,3^3,\ 2^3\,3^3\,11^3,\ -3^3\,5^3,$$
$$3^3\,5^3\,17^3,\ 2^6\,5^3, -2^{15}, -2^{15}\,3^3,\ -2^{18}\,3^3\,5^3,$$
$$-2^{15}\,3^3\,5^3\,11^3,\ -2^{18}\,3^3\,5^3\,23^3\,29^3.$$

Thus, one can instantly check this just by performing an easy calculation.

Example. The elliptic curve $E_1(\mathbb{C}) : y^2 = x^3 + x$ has the j-invariant equal to 1728 and this value appears in the previously mentioned list. This implies that E_1 does have CM.

Example. The elliptic curve $E_2(\mathbb{C}) : y^2 = x^3 + x + 2$ has the j-invariant equal to $432/7$ and this value does not appear in the list discussed above. This implies that E_2 does not have CM.

Remark. Consider a fixed elliptic curve E, defined over $\mathbb{F}_p$ for some p, given by Equation (1). As the value of the prime number p varies, different values of $n = |E(A,B)|$ will be obtained. Let $\delta = p + 1 - n$ and $\widetilde{\delta} = \delta/(2\sqrt{p})$. Using Equation (2), the value of $\widetilde{\delta}$ must lie in the interval $(-1,1)$, for any p.

The distribution of the values of $\widetilde{\delta}$ is significantly different in the CM case compared to the non-CM case. The theorem describing the distribution in the CM case is due to Hecke (Hecke, 1918; Hecke, 1920) and Deuring (Deuring, 1953; Deuring, 1955; Deuring, 1956; Deuring, 1957).

Theorem 2.2. We define the set

$$P_1 = \{p \leq x : \widetilde{\delta} \in [\alpha, \beta] \setminus \{0\}\}.$$

If E does have CM, then for asymptotically half of the primes p we have $\widetilde{\delta} = 0$. Also, for any interval $[\alpha, \beta] \subset [-1, 1]$ we have

$$\lim_{x \to \infty} \frac{|P_1|}{\pi(x)} = \frac{1}{2\pi} \int_{\alpha}^{\beta} \frac{du}{\sqrt{1-u^2}}.$$

The result describing the distribution in the non-CM case is known as the Sato-Tate conjecture (Tate, 1965) and was proven by Clozel, Harris, Shepherd-Barron, Taylor (Barnet-Lamb et al., 2011).

Theorem 2.3. We define the set

$$P_2 = \{p \leq x : \widetilde{\delta} \in [\alpha, \beta]\}.$$

If E does not have CM, then for any interval $[\alpha, \beta] \subset [-1, 1]$ we have

$$\lim_{x \to \infty} \frac{|P_2|}{\pi(x)} = \frac{2}{\pi} \int_{\alpha}^{\beta} \sqrt{1-u^2}\, du.$$

2.4 Quadratic Twist

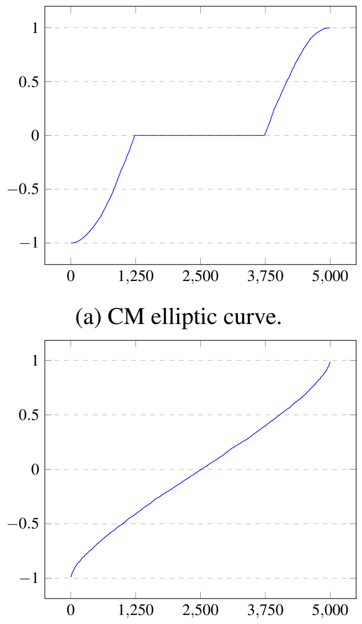
Let $d \in \mathbb{F}_p^*$ be a quadratic non-residue. The quadratic twist of the curve $E(A,B)$, denoted by $E^d(A,B)$, is defined as $E^d(A,B) = E(Ad^2, Bd^3)$. We further state two results that link the cardinalities of $E(A,B)$ and $E^d(A,B)$.

Theorem 2.4. The number of points on $E(A,B)$ over $\mathbb{F}_p$ can be computed using the following formula

$$n = p + 1 + \sum_{x \in \mathbb{F}_p} J_p(x^3 + Ax + B).$$

Corollary 2.4.1. Let E be an elliptic curve over $\mathbb{F}_p$ such that $|E(A,B)| = p + 1 - \delta$ and $d \in \mathbb{F}_p^*$. Then the number of points on the quadratic twist of E is given by

$$|E^d(A,B)| = p + 1 - J_p(d) \cdot \delta.$$



(a) CM elliptic curve.

(b) Non-CM elliptic curve.

Figure 2: The distribution of the $\widetilde{\delta}$ values for 5000 primes.

3 MAIN RESULTS

3.1 Our AI Setup

To achieve our proof of concept goal, in our implementation we initially generated the required elliptic curves by means of Schoof's algorithm. Based on these examples, we trained, validated, and tested the neural network model we chose. This network was composed of 10 dense hidden layers with the number of units decreasing from 512 to 8. Note that decreasing the number of units, as stated before, is a straightforward technique used in AI algorithms. We used 70% of the data for training our model, 15% for validation and 15% for testing. These values are the default ones used in practice when the size of the dataset is relatively small (Burkov, 2019).

The reason we decided to have 10 hidden layers was to obtain the best compromise in terms of error rate and code optimization (especially with respect to time complexity). In Figure 1a we provide the reader with a graphical representation of the relationship between the number of neural network layers and the error rate of the algorithm proposed in (Maimuţ and Matei, 2022). Moreover, in Figure 1b we offer a graphical representation of the relation between the number of layers and the width reduction of Hasse's interval. Note that for 10 hidden layers, in (Maimuţ and Matei, 2022) the authors obtain an interval reduction of 16% compared with the classical Schoof algorithm. Therefore, 16% is our baseline for our experiments.

Remark. We have also considered the use of Recurrent Neural Networks (RNNs), for which we have provided as input the previous 100 values in the sequence of δ-values. The results obtained were very similar to the ones presented, so we decided not to further investigate this option.

3.2 Prime Number Variation over a Fixed Elliptic Curve

Let $(A,B) \in \mathbb{F}_p \times \mathbb{F}_p$ be fixed and consider prime numbers $p \geq 5$ that define an elliptic curve E over $\mathbb{F}_p$. As stated in Section 2.3, we have two categories: CM and non-CM curves.

In order to visualize these two different distributions, we generated the $\widetilde{\delta}$ values of two different curves, one that has CM ($A = 1$ and $B = 0$, see Section 2.3) and another that does not have CM ($A = 1$ and $B = 2$, see Section 2.3), for 5000 primes p in Figure 2. Before plotting the results, we have also sorted the $\widetilde{\delta}$ values in ascending order.

Remark. If E has CM, then we know that $P(\widetilde{\delta} = 0) = P(n = p+1) = 50\%$. Also, if $\widetilde{\delta} = 0$, then E is a supersingular elliptic curve, which means that solving the Discrete Logarithm Problem becomes an easier task.

3.2.1 Implementation

We ran the code for our algorithms on a workstation using Windows 10 OS, with the following specifications: Intel(R) Core(TM) i9-7920X CPU 2.90GHz with 24 cores and 64 Gigabytes of RAM. The programming language we used for implementing our algorithms was Python, and the AI library we chose was TensorFlow.

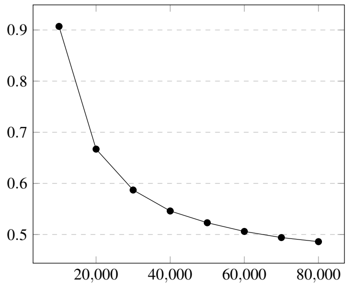


Figure 3: Error rate versus data size.

The most time consuming part of our setup was data generation. Therefore, to lower the time needed to perform our experiments we tested the influence of the data size on the error rate of our proposal for a non-CM curve with $A = 1$ and $B = 2$ using the neural network described in Section 3.1. We provide the reader with a graphical representation of the relationship between the data size and the error rate in Figure 3. It is easy to see that the error rate for the first 70000 primes (15%) is not significantly different from the one for the first 80000 primes (15.2%). Regarding the data generation running time, we have 7 days for 70000 primes and 9 days for 80000 primes. Hence, we selected a data size of 70000 for our further experiments.

The results of our experiments are graphically represented in Figure 6a. The experimental data is provided in the full version of the paper. In the case of non-CM curves we obtain a reduction of Hasse's interval of 14.88%. Unfortunately, in this case the proposal of (Maimuţ and Matei, 2022) (denoted by baseline) has a better reduction (of 1.08% less). Also, we report a running time of around 7-8 days.

For CM curves, the reduction is approximately equal to 17.85%. Therefore, we obtain a better reduction (of 1.86% more) than the baseline. In this case, we report an execution time of 4-5 days.

In these two cases, the probability that the order $|E(A,B)|$ satisfies the AI computed Hasse interval is approximately 90%, which is also the success rate of our probabilistic algorithm. The obtained probability was computed by finding the number of testing examples, which satisfied this reduced interval.

Remark. Our experiments were ran in parallel, which lead to an increased execution time of all the instances. Moreover, our source code is unoptimized. Hence, we expect better running times than the ones reported in the current work.

3.3 Elliptic Curve Variation over a Fixed Prime Number

Since CM curves are rare, we will no longer split the curves based on this criterion. Therefore, we fix a prime number $p \geq 5$ and consider all the pairs $(A,B) \in \mathbb{F}_p \times \mathbb{F}_p$ that define an elliptic curve E over $\mathbb{F}_p$.

In order to determine how many such pairs exist, we consider the case in which $\Delta = 4A^3 + 27B^2 = 0 \pmod{p}$. Put differently, we find the number of pairs (A,B) that need to be excluded. If $A = 0$, then this is equivalent to $B = 0$. If we assume that $A \neq 0$, then $\Delta = 0$ can be rearranged as

$$\frac{9B^2}{4A^2} = \frac{A}{-3}.$$

Hence, we can see that this relation holds whenever the term $-3^{-1}A$ is a quadratic residue modulo p.

The function $f : \mathbb{Z}_p^* \longrightarrow Z_p^*$ given by $f(x) = -3^{-1}x$ is a group isomorphism, which means that there are $(p-1)/2$ values of A which will produce a quadratic residue and there exist exactly two values of B for each such value of A. In conclusion, there are p pairs $(A,B) \in \mathbb{F}_p \times \mathbb{F}_p$ for which $\Delta = 0 \pmod{p}$ and the remaining $p^2 - p$ pairs define an elliptic curve defined over $\mathbb{F}_p$.

Let $S_1[\delta]$ and $S_2[\delta]$ be the following sets

$$S_1[\delta] = \{(A,B) \in \mathbb{F}_p \times \mathbb{F}_p : \Delta \neq 0 \text{ and } n = p + 1 - \delta\}$$

and

$$S_2[\delta] = \{(A,B) \in \mathbb{F}_p \times \mathbb{F}_p : \Delta \neq 0 \text{ and } n = p + 1 + \delta\},$$

where $\delta \in \{1, 2, \ldots, \lfloor 2\sqrt{p} \rfloor\}$.

The following lemma tells us that the distribution of the number of curves of a given cardinality is symmetric. A visual representation of Lemma 3.1 is provided in Figures 4 and 5.

Lemma 3.1. The sets $S_1[\delta]$ and $S_2[\delta]$ have the same cardinality.

Proof. Let $d \in \mathbb{F}_p^*$ such that $J_p(d) = -1$. Using Corollary 2.4.1 we obtain that for any curve $E(A,B) \in S_1[\delta]$, *i.e* $|E(A,B)| = p + 1 - \delta$, its quadratic twist $E^d(A,B)$ has cardinality $p + 1 - J_p(d) \cdot \delta = p + 1 + \delta$, and thus $E^d(A,B) \in S_2$. □

3.3.1 Implementation

The results of our experiments are graphically represented in Figure 6b. The experimental data is provided in the full version of the paper. We can see that we obtain a negative result in this case. Namely, a reduction of 14.55% for 3-digits, 14.85% for 4-digits and 14.99% for 5-digits. This translates into 1.19% less than the baseline. The success rate of our approach remains approximately 90%. Note that in the case of 5 digits primes, we ran the code for 4-5 days.

4 CONCLUSIONS

In this work, we explored AI techniques to enhance the efficiency of Schoof's algorithm across various elliptic curve distributions. We presented experimental results for two cases: prime number variation over a fixed elliptic curve and elliptic curve variation over a fixed prime number. We obtained different success rates and reported them.

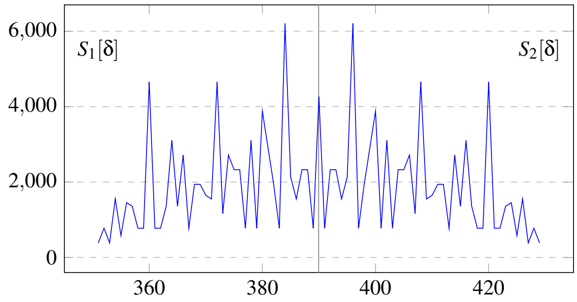


Figure 4: The distribution of $S_1[\delta]$ and $S_2[\delta]$ for $p = 389$.

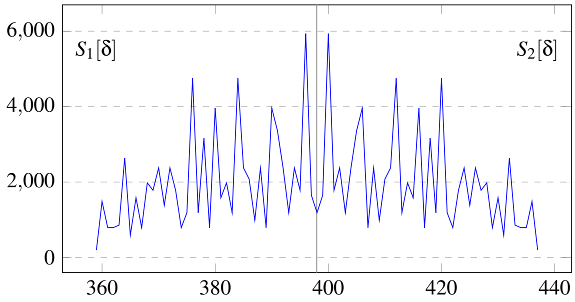
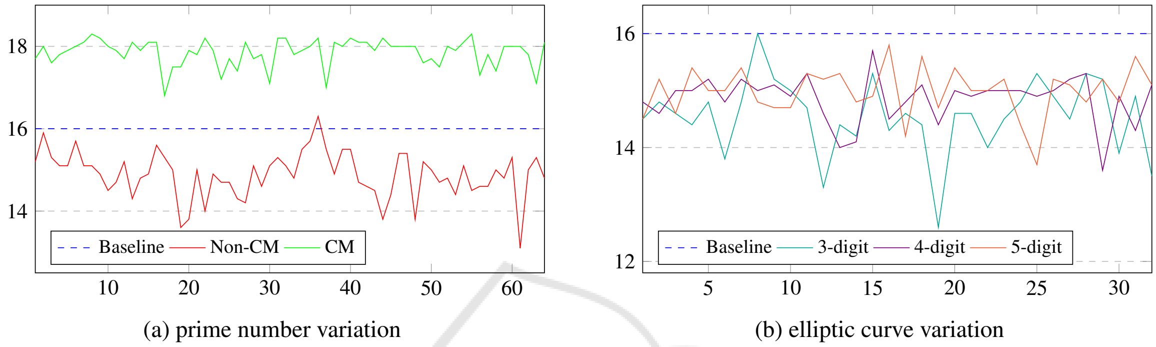


Figure 5: The distribution of $S_1[\delta]$ and $S_2[\delta]$ for $p = 397$.



(a) prime number variation

(b) elliptic curve variation

Figure 6: Hasses's interval reduction.

Future Work. A natural extension of the current work is to try and adapt our methods to hyperelliptic curve point counting algorithms for genus 2 (Gaudry and Schost, 2012) or 3 (Abelard, 2018) curves.

An interesting research direction stated in (Batterman et al., 2023) is the use of machine learning techniques to provide support (or not) for the Bias Conjecture[4].

We consider applying more advanced AI techniques for the mathematical computations inside Schoof's algorithm as another compelling future work idea.

Finally, we believe that conducting timing comparisons between our improved Schoof algorithm and the SEA algorithm[5] (Dewaghe, 1998) is an intriguing direction for future investigation.

REFERENCES

Post-quantum cryptography. https://csrc.nist.gov/Projects/Post-Quantum-Cryptography.

Abelard, S. (2018). *Counting Points on Hyperelliptic Curves in Large Characteristic: Algorithms and Complexity*. PhD thesis, Université de Lorraine.

Alessandretti, L., Baronchelli, A., and He, Y.-H. (2023). Machine Learning Meets Number Theory: the Data Science of Birch–Swinnerton-Dyer. In *Machine Learning: In Pure Mathematics And Theoretical Physics*, pages 1–39. World Scientific.

Barnet-Lamb, T., Geraghty, D., Harris, M., and Taylor, R. (2011). A Family of Calabi–Yau Varieties and Potential Automorphy II. *Publications of the Research Institute for Mathematical Sciences*, 47(1):29–98.

Batterman, Z., Jambhale, A., Miller, S. J., Narayanan, A. L., Sharma, K., Yang, A., and Yao, C. (2023). Applications of Moments of Dirichlet Coefficients in Elliptic Curve Families. *arXiv preprint arXiv:2311.17215*.

Birch, B. J. and Swinnerton-Dyer, H. P. F. (1965). Notes on Elliptic Curves II. *Journal für die reine und angewandte Mathematik*, 218:79–108.

Bober, J. (2013). Conditionally Bounding Analytic Ranks of Elliptic Curves. *The Open Book Series*, 1(1):135–144.

Bujanović, Z., Kazalicki, M., and Novak, L. (2024). Murmurations of Mestre-Nagao sums. *arXiv preprint arXiv:2403.17626*.

Burkov, A. (2019). *The Hundred-Page Machine Learning Book*, volume 1.

Castryck, W. and Decru, T. (2023). "an efficient key recovery attack on sidh". In *EUROCRYPT'23*, volume 14008 of *Lecture Notes in Computer Science*, pages 423–447. Springer Nature Switzerland.

Deuring, M. (1953). Die Zetafunktion einer algebraischen Kurve vom Geschlechte Eins. *Nachr. Akad. Wiss. Göttingen. Math.-Phys. Kl. Math.-Phys.-Chem. Abt.*, pages 85–94.

[4] The conjecture states that the largest term in the second moment expansion which does not average to zero is on average negative.

[5] an extension of Schoof's algorithm by Elkies and Atkin

Deuring, M. (1955). Die Zetafunktion einer algebraischen Kurve vom Geschlechte Eins II. *Nachr. Akad. Wiss. Göttingen. Math.-Phys. Kl. IIa*, pages 13–42.

Deuring, M. (1956). Die Zetafunktion einer algebraischen Kurve vom Geschlechte Eins III. *Nachr. Akad. Wiss. Göttingen. Math.-Phys. Kl. IIa*, pages 37–76.

Deuring, M. (1957). Die Zetafunktion einer algebraischen Kurve vom Geschlechte Eins IV. *Nachr. Akad. Wiss. Göttingen. Math.-Phys. Kl. IIa*, pages 55–80.

Dewaghe, L. (1998). Remarks on the Schoof-Elkies-Atkin Algorithm. *Mathematics of Computation*, 67(223):1247–1252.

Elkies, N. D. and Klagsbrun, Z. (2020). New Rank Records for Elliptic Curves Having Rational Torsion. In *ANTS XIV*, pages 233–250.

Gaudry, P. and Schost, É. (2012). Genus 2 Point Counting over Prime Fields. *Journal of Symbolic Computation*, 47(4):368–400.

He, Y.-H., Lee, K.-H., and Oliver, T. (2022a). Machine-Learning the Sato–Tate Conjecture. *Journal of Symbolic Computation*, 111:61–72.

He, Y.-H., Lee, K.-H., and Oliver, T. (2023). Machine Learning Invariants of Arithmetic Curves. *Journal of Symbolic Computation*, 115:478–491.

He, Y.-H., Lee, K.-H., Oliver, T., and Pozdnyakov, A. (2022b). Murmurations of Elliptic Curves.

Hecke, E. (1918). Eine neue Art von Zetafunktionen und ihre Beziehungen zur Verteilung der Primzahlen. *Mathematische Zeitschrift*, 1(4):357–376.

Hecke, E. (1920). Eine neue Art von Zetafunktionen und ihre Beziehungen zur Verteilung der Primzahlen: Zweite Mitteilung. *Mathematische Zeitschrift*, 6(1):11–51.

Howitt, S. M. and Wilson, A. N. (2014). Revisiting "Is the Scientific Paper a Fraud?". *EMBO Reports*, 15(5):481–484.

Kazalicki, M. and Vlah, D. (2023). Ranks of Elliptic Curves and Deep Neural Networks. *Research in Number Theory*, 9(3):53.

Koblitz, N. (1987). Elliptic Curve Cryptosystems. *Mathematics of Computation*, 48(177):203–209.

Lee, K.-H., Oliver, T., and Pozdnyakov, A. (2023). Murmurations of Dirichlet characters. *arXiv preprint arXiv:2307.00256*.

Lenstra, H. W. (1987). Factoring Integers with Elliptic Curves. *Annals of Mathematics*, 126(3):649–673.

Maimuţ, D. and Matei, A. C. (2022). Speeding-Up Elliptic Curve Cryptography Algorithms. *Mathematics*, 10(19):3676.

Medawar, P. (1963). Is the Scientific Paper a Fraud? *The Listener*, 70(12):377–378.

Mestre, J.-F. (1982). Construction d'une Courbe Elliptique de Rang ≥ 12. *CR Acad. Sci. Paris Sér. I Math.*, 295(12):643–644.

Miller, V. S. (1986). Use of Elliptic Curves in Cryptography. In *Proceedings of the CRYPTO '85*, volume 218 of *Lecture Notes in Computer Science*, pages 417–426. Springer.

Nagao, K.-I. (1992). Examples of Elliptic Curves over $\mathbb{Q}$ with rank ≥ 17. *Proceedings of the Japan Academy, Series A, Mathematical Sciences*, 68(9):287 – 289.

Sarnak, P. (2023). Root Numbers and Murmurations. In *ICERM Workshop*.

Schoof, R. (1985). Elliptic Curves Over Finite Fields and the Computation of Square Roots mod p. *Mathematics of Computation*, pages 483–494.

Schwartz, M. A. (2008). The Importance of Stupidity in Scientific Research. *Journal of Cell Science*, 121(11):1771–1771.

Sutherland, A. V. (2022). Letter to Michael Rubinstein and Peter Sarnak. https://math.mit.edu/~drew/RubinsteinSarnakLetter.pdf.

Tao, T. Ask Yourself Dumb Questions - and Answer Them! https://terrytao.wordpress.com/career-advice/ask-yourself-dumb-questions-and-answer-them/.

Tao, T. Use The Wastebasket. https://terrytao.wordpress.com/career-advice/use-the-wastebasket/.

Tate, J. T. (1965). Algebraic Cycles and Poles of Zeta Functions. In *Arithmetical Algebraic Geometry*, pages 93–110. Harper & Row.

Truran, P. (2013). *Practical Applications of the Philosophy of Science: Thinking About Research*. Springer Science & Business Media.

Washington, L. C. (2008). *Elliptic Curves: Number Theory and Cryptography*. Chapman & Hall/CRC, 2 edition.

Weidman, D. R. (1965). Emotional Perils of Mathematics. *Science*, 149(3688):1048–1048.

Zubrilina, N. (2023). Murmurations. *arXiv preprint arXiv:2310.07681*.