Journal of New Theory

ISSN: 2149-1402

47 (2024) 20-27

Journal of New Theory

https://dergipark.org.tr/en/pub/jnt

Open Access

Mestré's Finite Field Method for Searching Elliptic Curves with High Ranks

Şeyda Dalkılıç[1], **Ercan Altınışık**[2]

Article Info

Received: 10 Apr 2024

Accepted: 23 May 2024

Published: 30 Jun 2024

doi:10.53570/jnt.1467401

Research Article

Abstract — The theory of elliptic curves is one of the popular topics of recent times with its unsolved problems and interesting conjectures. In 1922, Mordell proved that the group of $\mathbb{Q}$-rational points on an elliptic curve is finitely generated. However, the rank of this group, signifying the number of independent generators, can be arbitrarily high for certain curves, a fact yet to be definitively proven. This study leverages the computer algebra system Magma to investigate curves with potentially high ranks using a technique developed by Mestré.

Keywords *Mestré method, elliptic curve, rank, height matrix, magma*

Mathematics Subject Classification (2020) 14H52, 20K15

1. Introduction

Elliptic curves possess a fascinating and yet unsolved property: their rank. The set of rational points on an elliptic curve forms a finitely generated abelian group. Mordell's Theorem guarantees this group is isomorphic to a finite direct sum of cyclic groups. The rank of the elliptic curve signifies the number of these cyclic groups with infinite order, which directly corresponds to the number of independent points of infinite order within the group. Determining the rank of an elliptic curve presents a significant challenge. There currently exists no known algorithm for calculating it efficiently. Additionally, a fundamental open question in number theory revolves around the existence of an upper bound for the rank of elliptic curves. While it is widely believed that elliptic curves can possess a rank of any non-negative integer, a definitive proof remains elusive. This lack of a proven upper bound fuels the ongoing search for elliptic curves with the highest possible rank.

Several key advancements have been made in determining the maximum possible rank of elliptic curves. Penney and Pomerance [1,2] established lower bounds, proving that the rank can be greater than 6 and 7, respectively. Subsequently, Grunewald and Zimmert [3] pushed this bound further by demonstrating the existence of curves with a rank exceeding 8. Brumer and Kramer [4] achieved a rank greater than 9. Mestré [5–8] introduced a breakthrough with two novel methods for estimating elliptic curve rank. He significantly raised the known lower bounds by applying these methods and showcasing specific examples. His works [5–9] demonstrably showed that the rank of certain elliptic curves can be greater than 11, 12, 14 and 15. Building upon Mestré's groundwork, Nagao and Fermigier [10–13] achieved

[1]seyda468@gmail.com; [2]ealtinisik@gazi.edu.tr (Corresponding Author)

[1,2]Department of Mathematics, Faculty of Science, Gazi University, Ankara, Türkiye

further progress. They specialized in a family of curves introduced by Mestré over the field of rational functions in one variable, $\mathbb{Q}(t)$. This specialization allowed them to prove that the rank over the rational field $\mathbb{Q}$ is greater than 17 and $19-22$. Notably, the current record for the highest discovered rank, at 28, was achieved by Noam Elkies. It's worth mentioning that Martin and McMillen [14] also played a crucial role by independently discovering specific elliptic curves with ranks of 23 and 24, respectively.

Recent research in rank studies has tackled three key areas: calculating ranks for specific families of curves [15–19], exploring how rank behaves for curves constructed from special number sequences [20–28] and analyzing rank distributions within families and across field extensions [29–31]. Dujella [32] provided an enumeration of the strategies for generating high-rank Diaphontine elliptic curves. The contributions of Elkies and Klagsburn [33] are also noteworthy in that they established new rank records for specific torsion groups. Another noteworthy work is Kazlicki's attempt to develop a rank classification system using deep neural networks [34]. Although various studies continue to be conducted in different ways, there is not yet a complete method that yields high-rank curves. The majority of existing studies employ the Mestré method and Mestré's sum [7]. Therefore, the finite field method of Mestré was selected as the subject of this study.

This paper is divided into three distinct sections. The initial section establishes the fundamental groundwork by presenting the essential definitions and theorems relevant to elliptic curve ranks. Following the foundational elements, we introduce the method developed by Mestré for finding elliptic curves with high ranks. Finally, the third section analyzes the data obtained through the custom codes we developed using the MAGMA software program.

2. Preliminaries

We begin our discussion with the definition of elliptic curves.

Definition 2.1. [35] Let $\mathbb{K}$ be a field. An elliptic curve over $\mathbb{K}$ can be defined as

i. A genus one curve with one $\mathbb{K}$-rational point,

ii. A plane cubic with a $\mathbb{K}$-rational point or

iii. A Weierstrass cubic, $y^2 = x^3 + px + q$.

Example 2.2. The curve

$$YZ^2 = X^3 - XZ^2$$

over $\mathbb{Q}$ is an elliptic curve with the point at infinity denoted $\mathcal{O} = [0, 1, 0]$ in homogeneous coordinates. If we write $x = X/Z$ and $y = Y/Z$ in the equation, then we obtain the Weierstrass form of the equation as

$$y^2 = x^3 - x$$

The set of $\mathbb{K}$ rational points on the curve is given by

$$E(\mathbb{K}) = \{\mathcal{O}\} \cup \{(x, y) \in \mathbb{K}\}$$

Theorem 2.3. [36] The group $E(\mathbb{K})$ is finitely generated.

Mordell proved this theorem for the field $\mathbb{Q}$ in 1922 and Weil generalized it to any field $\mathbb{K}$ in 1928. It can be stated by the Mordell Theorem along with the general structure theory of finitely generated abelian groups that

$$E(\mathbb{K}) \cong E(\mathbb{K})_{tors} \times \mathbb{Z}^r$$

The group $E(\mathbb{K})$ is called the Mordell-Weil group. The subgroup $E(\mathbb{K})_{tors}$ consists of points with finite order and is referred to as the torsion subgroup. Formally, this subgroup is defined as follows:

$$E(\mathbb{K})_{tors} = \{P \in E(\mathbb{K}) : \exists n \in \mathbb{N} \text{ that } nP = \mathcal{O}\}$$

The free part of the Mordell-Weil group is generated by r points of $E(\mathbb{K})$ with infinite order. Here r is called the rank of $E(\mathbb{K})$.

Theorem 2.4 (Mazur Theorem, Conjecture of Ogg)**.** [37,38] Let $E(\mathbb{Q})_{tors}$ be the torsion subgroup of the Mordell-Weil group of an elliptic curve over $\mathbb{Q}$. Then, $E(\mathbb{Q})_{tors}$ is isomorphic to one of the following fifteen groups:

i. $\mathbb{Z}/m\mathbb{Z}$, $1 \leq m \leq 10$ or $m = 12$

ii. $\mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/2v\mathbb{Z}$, $1 \leq v \leq 4$

The Conjecture of Ogg was proven by Barry Mazur [37] in 1977. However, many unsolved questions still exist with on ranks of elliptic curves. Determining the rank of an elliptic curve remains a significant challenge. No known algorithm efficiently calculates the rank for any curve. Additionally, it is unproven whether an upper bound exists on the rank. While the possibility of arbitrarily high ranks is widely accepted, complete proof remains elusive [33]. This study utilizes one of Mestré's influential methods, which were the first to construct elliptic curves with demonstrably high ranks. Notably, in 1982, Mestré [6] introduced a groundbreaking method to construct elliptic curves over the rational numbers ($\mathbb{Q}$) with demonstrably high ranks. This method allowed him to find curves with 8 and $10-12$ ranks in [5,6]. These achievements marked a significant step forward in the field. Mestré presented two methods for searching elliptic curves. The method, which is the subject of this article, is known as the "Finite Field Method" as proposed by Campbell [39].

3. Mestré's Finite Field Method

We introduce a key conjecture underpinning Mestré's method. Intriguing and far-reaching, the Birch and Swinnerton-Dyer conjecture (BSD) is a central pillar in studying elliptic curves, offering a profound connection between their arithmetic and analytic properties. Indeed, the BSD conjecture plays a fundamental role in understanding the underlying principles of our approach.

Definition 3.1. [40] Let E be an elliptic curve defined over the field of rational numbers, $\mathbb{Q}$. Denote its conductor by N. We define its associated $L-$function by $L(E, s)$, where s is a complex number:

$$\begin{aligned} L(E,s) &= \sum_n a_n n^{-s} \\ &= \prod_{p|N} \left(1 - a_p p^{-s}\right)^{-1} \prod_{p\nmid N} \left(1 - a_p p^{-s} + p^{1-2s}\right)^{-1} \end{aligned}$$

Conjecture 3.2 (Birch-Swinnerton-Dyer Conjecture)**.** [41] The function L of an elliptic curve is extendable into a holomorphic function in the neighborhood of 1 and its order in 1 is equal to the rank of the Mordell-Weil group of E over $\mathbb{Q}$.

The Birch and Swinnerton-Dyer Conjecture (BSD Conjecture) is relevant to the context of elliptic curves and their $L-$functions, but it doesn't directly provide a bound for the rank of an elliptic curve. However, it establishes a connection between the rank and the behavior of the $L-$function at a specific point, which can be used to infer information about the rank under certain conditions.

Mestré's algorithm is the following [5,6]:

Let

$$E : y^2 + y = x^3 + a_4 x + a_6$$

be an elliptic curve over $\mathbb{Q}$, p be a good reduction prime for E and N_p be several points of E modulo p. An analysis of Weil's exponential formulas [6] applied to the $L-$function of the elliptic curve E reveals a potential discrepancy between the rank, r, implied by the large size of N_p for numerous prime numbers p, and a potentially higher rank suggested by the analytic behavior of the $L-$ function under this analysis. As a result, to obtain elliptic curves with high ranks, one builds curves such that N_p is maximal for all p inferior or equal to P_0, which is an integer depending on the computing capabilities available. Then,

$$\Delta = -(4a_4)^3 - 27(1+4a_6)^2$$

We provide four integers P_0, P_1, k_0, and k_0' to our search.

i. Let M be an integer and

$$M_0 = \prod_{p \leq M} p$$

The congruences modulo p that coefficients a_4 and a_6 of an elliptic curve attain when N_p is maximized for each $p \leq P_0$ are calculated.

ii. The congruences (a_4, a_6) modulo M_0, which ensures the maximal value of N_P for all integers $p \leq P_0$, are derived by a simple application of the Chinese remainder theorem.

iii. For each pair of congruences (a_4, a_6), the negative value a_4 of minimum absolute value congruent to a_4 and for each of the values $a_4' = a_4 - kM_0$, $0 \leq k \leq k_0$, are searched, a_6' congruent to a_6 and minimizing $|\Delta|$ are calculated. Then, each curve with coefficients a_4' and $a_6'' = a_6' + kM_0$, $\mid k \mid \leq k_0'$, are considered.

iv. For each of these curve N_P are calculated for $P_0 \leq p \leq P_1$, then

$$S = \sum_{P_0 \leq p \leq P_1} \left(\frac{p-1}{N_p} - 1 \right) \log p$$

Curves such that S is greater than a constant S_0 dependent only on P_0 and P_1 are rejected.

v. If E is such that $S \leq S_0$, integer points of this curve are searched for example in the interval

$$[e_1, e_1 + 5000]$$

where e_1 being the abscissa of an order 2 point of E.

vi. If we do not find an integer point, the curve is rejected; otherwise, the matrix of the heights of the points obtained and the rank of the height matrix are calculated.

Mestré [5] obtained many curves with rank 6, 7, 8, and 9 for $P_0 = 17$, $P_1 = 50$, $k_0 = 20$, and $k_0' = 50$. He also obtained a curve with rank 12 for $P_0 = 37$, $P_1 = 101$, $k_0 = 1$, and $k_0' = 8$.

4. Results on our Search for Finding Curves with High Ranks

We implemented Mestré's finite field method [5] in Magma software to estimate the rank of elliptic curves. Running our code with parameters $P_0 = 17$, $P_1 = 50$, $k_0 = 20$, and $k_0' = 50$, we successfully reproduced Mestré's results of sieves with ranks $7-9$. Our code identified numerous elliptic curves with rank 7. Due to space limitations, we omit specific examples of these curves here, but they are available upon request. The results of our investigation are presented in Table 1.

Table 1. Searching results

Rank	TorsionSubgruop	Curve
7	trivial	$y^2 + y = x^3 - 1201837x - 28298094$
7	trivial	$y^2 + y = x^3 - 3243877x - 44634414$
7	trivial	$y^2 + y = x^3 - 1832467x - 37997784$
7	trivial	$y^2 + y = x^3 - 4385017x - 37997784$
7	trivial	$y^2 + y = x^3 - 4234867x - 26491674$
7	trivial	$y^2 + y = x^3 - 2733367x - 46401564$
7	trivial	$y^2 + y = x^3 - 1321957x - 37212384$
7	trivial	$y^2 + y = x^3 - 3363997x - 33638814$
7	trivial	$y^2 + y = x^3 - 1199107x - 42174684$
7	trivial	$y^2 + y = x^3 - 8256157x - 33496014$
7	trivial	$y^2 + y = x^3 - 9907807x - 32985504$
7	trivial	$y^2 + y = x^3 - 1078987x - 47515404$
7	trivial	$y^2 + y = x^3 - 5163067x - 35773674$
7	trivial	$y^2 + y = x^3 - 598507x - 34242144$
7	trivial	$y^2 + y = x^3 - 6214117x - 45473364$
7	trivial	$y^2 + y = x^3 - 7235137x - 29137044$
7	trivial	$y^2 + y = x^3 - 1739647x - 38326224$
8	trivial	$y^2 + y = x^3 - 2667847x - 25888344$
8	trivial	$y^2 + y = x^3 - 2842567x - 50714124$
8	trivial	$y^2 + y = x^3 - 3688867x - 49646694$
8	trivial	$y^2 + y = x^3 - 3224767x - 37444434$
9	trivial	$y^2 + y = x^3 - 3151057x - 34517034$

The curve

$$E : y^2 + y = x^3 - 3151057x - 34517034$$

has 9 independent points on $\mathbb{Q}$. The Torsion Subgroup is trivial. Points of E are

$$P_1 = (90641/4, 27205059/8)$$

$$P_2 = (20221, -2864331)$$

$$P_3 = (8945/4, 512371/8)$$

$$P_4 = (1325657/484, -1160700207/10648)$$

$$P_5 = (741102/361, -317934960/6859)$$

$$P_6 = (1636928/289, -1988611043/4913)$$

$$P_7 = (3097593/361, -5333671306/6859)$$

$$P_8 = (5325049/64, -12285322125/512)$$

and

$$P_9 = (3872137/676, -7243647215/17576)$$

Applying our implementation of Mestré's method to primes $p = 19$ and $p = 23$, we were not able to identify any elliptic curves with a rank greater than 6. These findings are consistent with the observations reported in Mestré's work [5]. The curve discovered during the scan does not correspond to any entries on Dujella's website [14, 42], which serves as a repository for elliptic curve ranks. Our Magma implementation encountered errors and did not complete the computations for primes 29, 31 and 37. This suggests that analyzing these cases might require more extensive computational resources than those available on personal computers.

5. Conclusion

In this study, we implemented Mestrés method for searching elliptic curves with high ranks using a Magma code. This approach yielded a comprehensive list of elliptic curves with ranks $7-9$. Notably, these curves were not previously documented in the referenced literature [5,6] or on Dujella's website, a leading resource for rank records. While we have not identified curves exceeding rank 9, our exploration has exposed potential limitations in our current Magma code regarding time and memory efficiency. Future efforts can be focused on optimizing the code to handle computations for even higher ranks.

Author Contributions

All the authors equally contributed to this work. This paper is derived from the first author's doctoral dissertation supervised by the second author. They all read and approved the final version of the paper.

Conflicts of Interest

All the authors declare no conflict of interest.

References

[1] D. Penney, C. Pomerance, *A search for elliptic curves with large rank*, Mathematics of Computation 28 (127) (1974) 851–853.

[2] D. Penney, C. Pomerance, *Three elliptic curves with rank at least seven*, Mathematics of Computation 29 (131) (1975) 965–967.

[3] F. Grunewald, R. Zimmert, *Uber einige rationale elliptische Kurven mit treiem Rang* ≥ 8, Journal für die Reine und Angewandte Mathematik 1977 (296) (1977) 100–107.

[4] A. Brumer, K. Kramer, *The rank of elliptic curves*, Duke Mathematical Journal 44 (1977) 715–743.

[5] J.-F. Mestre, *Construction d'une courbe elliptique de rang* ≥ 12, Comptes Rendus de l'Académie des Sciences Paris 295 (1982) 643–644.

[6] J.-F. Mestre, *Courbes elliptiques et formules explicites*, Séminaire de Théorie des Nombres de Grenoble 10 (1982) 1–10.

[7] J.-F. Mestre, *Courbe elliptiques de rang* ≥ 11 *sur* $\mathbb{Q}(t)$, Comptes Rendus de l'Académie des Sciences 313 (1991) 139–142.

[8] J.-F. Mestre, *Courbe elliptiques de rang* ≥ 12 *sur* $\mathbb{Q}(t)$, Comptes Rendus de l'Académie des Sciences 313 (1991) 171–174.

[9] J.-F. Mestre, *Un exemple de courbe elliptique sur* $\mathbb{Q}$ *de rang* ≥ 15, Comptes Rendus de l'Académie des Sciences Paris Serie I Mathematics 314 (1992) 453–455.

[10] K. Nagao, *Examples of elliptic curves over* $\mathbb{Q}$ *with rank* ≥ 17, Proceedings of the Japan Academy Serie A Mathematical Sciences 68 (1992) 287–289.

[11] K. Nagao, *An example of elliptic curve over* $\mathbb{Q}$ *with rank* ≥ 20, Proceedings of the Japan Academy Serie A Mathematical Sciences 69 (1993) 291–293.

[12] K. Nagao, T. Kouya, *An example of elliptic curve over* $\mathbb{Q}$ *with rank* ≥ 21, Proceedings of the Japan Academy Serie A Mathematical Sciences 70 (1994) 104–105.

[13] S. Fermigier, *Une courbe elliptique definie sur* $\mathbb{Q}$ *de rang* ≥ 22, Acta Arithmetica 82 (4) (1997) 359–363.

[14] A. Dujella, *History of elliptic curves rank records* (nd), https://web.math.pmf.unizg.hr/ duje/tors/rankhist.html, Accessed 8 April 2024.

[15] S.-W. Kim, *Searching the ranks of elliptic curves* $y^2 = x^3 - px$, International Journal of Algebra 12 (8) (2018) 311–318.

[16] S.-W. Kim, *Ranks in elliptic curves of the forms* $y^2 = x3 + Ax^2 + Bx$, International Journal of Algebra 12 (8) (2018) 311–318.

[17] S.-W. Kim, *Ranks in elliptic curves of the forms* $y^2 = x^3 \mp Ax$, International Journal of Contemporary Mathematical Sciences 18 (1) (2023) 19–31.

[18] S.-W. Kim, *Ranks in elliptic curves* $y^2 = x^3 - 37px$ *and* $y^2 = x^3 - 61px$ *and* $y^2 = x^3 - 67px$ *and* $y^2 = x^3 - 947px$, International Journal of Algebra 17 (3) (2023) 121–142.

[19] R. Mina, J. Bacani, *Elliptic curves of type* $y^2 = x^3 - 3pqx$ *having ranks zero and one*, Malaysian Journal of Mathematical Sciences 17 (1) (2023) 67–76.

[20] F. Khoshnam, D. Moody, *High rank elliptic curves with torsion Z/4Z induced by Kihara's elliptic curves*, Integers: The Electronic Journal of Combinatorial Number Theory 16 (8) (2016) A70 12 pages.

[21] G. Celik, G. Soydan, *Elliptic curves containing sequences of consecutive cubes*, Rocky Mountain Journal of Mathematics 47 (7) (2018) 2163–2174.

[22] G. Celik, M. Sadek, G. Soydan, *Rational sequences on different models of elliptic curves*, Glasnik Matematicki 54 (74) (2019) 53–64.

[23] A. Dujella, M. Kazalicki, J. C. Peral, *Elliptic curves with torsion groups* $\mathbb{Z}/8\mathbb{Z}$*and* $\mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/6\mathbb{Z}$, Revista de la Real Academia de Ciencias Exactas, Físicas y Naturales Serie A Matemáticas 115 (4) (2021) 169 24 pages.

[24] A. Dujella, M. Mıkıc, *Rank zero elliptic curves induces by rational diophantine triples*, Rad Hrvatske Akademije Znanosti i Umjetnosti Matematicke Znanosti 24 (2020) 29–37.

[25] A. Dujella, G. Soydan, *On elliptic curves induced by rational Diophantine quadruples*, Proceedings of the Japan Academy Mathematical Sciences, Series A; Ueno Park 98 (1) (2022) 1–6.

[26] L. Halbeisen, N. Hungerbühler, *Heron triangles and their elliptic curves*, Journal of Number Theory 213 (2020) 232–253.

[27] L. Halbeisen, N. Hungerbühler, A. Zargar, *A family of congruent number elliptic curves of rank three*, Quaestiones Mathematicae 46 (6) (2023) 1131–1137.

[28] N. Garcia-Fritz, H. Pasten, *Elliptic curves with long arithmetic progressions have large rank*, International Mathematics Research Notices 2021 (10) (2021) 7394–7432.

[29] A. Dujella, J. Peral, *An elliptic curve over $\mathbb{Q}(u)$ with torsion $\mathbb{Z}/4\mathbb{Z}$ and rank* 6, Rad Hrvatske Akademije Znanosti i Umjetnosti Matematicke Znanosti 28 (2024) 185–192.

[30] L. Beneish, K. Debanjana, R. Anwesh, *Rank jumps and growth of Shafarevich-Tate Groups for elliptic curves in $\mathbb{Z}/p\mathbb{Z}$ extensions*, Journal of the Australian Mathematical Society 116 (2024) 1–38.

[31] P. J. Cho, K. Jeong, *On the distribution of analytic ranks of elliptic curves*, Mathematische Zeitschrift 305 (3) (2023) 42 20 pages.

[32] A. Dujella, J. Peral, *Construction of high rank elliptic curves*, The Journal of Geometric Analysis 31 (7) (2021) 6698–6724.

[33] N. Elkies, Z. Klagsbrun, *New rank records for elliptic curves having rational torsion*, in: S. Galbraith (Ed.), Ants XIV: Proceedings of the Fourteenth Algorithmic Number Theory Symposium, Berkeley, 2020, pp. 233–250.

[34] M. Kazalicki, D. Vlah, *Ranks of elliptic curves and deep neural networks*, Research in Number Theory 9 (3) (2023) 53 20 pages.

[35] M. Schütt, T. Shioda, Mordell–Weil Lattices, Springer, Singapore, 2019.

[36] J. H. Silverman, J. T. Tate, Rational Points on Elliptic Curves, 2nd Edition, Springer International Publishing, Switzerland, 2009.

[37] B. Mazur, *Modular curves and the Eisenstein ideal*, Publications Mathématiques de l'IHÉS 47 (1977) 133–186.

[38] B. Mazur, D. Goldfeld, *Rational isogenies of prime degree*, Inventiones Mathematicae 44 (2) (1978) 129–162.

[39] G. Campell, *Finding elliptic curves and families of elliptic curves over Q of large rank*, Doctoral Dissertation The State University of New Jersey (1999) New Brunswick.

[40] Á. Lozano-Robledo, Elliptic curves, modular forms, and their L-functions, 1st Edition, American Mathematical Society, United States of America, 2011.

[41] B. Bırch, H. Swinnerton-Dyer, *Notes on elliptic curves. I.*, Journal für die reine und angewandte Mathematik 212 (1963) 7–25.

[42] K. Rubin, A. Silverberg, *Ranks of elliptic curves*, Bulletin of the American Mathematical Society 39 (2002) 455–474.