



On the Arithmetic of Elliptic Curves over Finite Fields and Their Applications

First A. Author¹, Second B. Author^{2*}

¹Department of Mathematics, University of Algiers, Algeria

²National Higher School of Mathematics, Algiers, Algeria

first.author@univ-alger.edu.dz, second.author@nhsm.edu.dz

Abstract

This abstract provides a template for submissions to the National Conference on Number Theory and its Interactions (NCNTI 2025). The abstract should summarize the motivation, key methods, and main results of your work. We investigate the properties of certain families of elliptic curves, providing new estimates for the distribution of their ranks. These results are then applied to cryptographic protocols. All submissions should strictly follow this L^AT_EX template to ensure a uniform presentation in the conference proceedings.

Keywords: *Elliptic curves, Number theory, Galois representations, Cryptography, Diophantine equations.*

1. Introduction

The study of rational points on elliptic curves is a central problem in number theory.

Definition 1.1 (Elliptic Curve). *An elliptic curve E over a field K is a smooth, projective algebraic curve of genus one, on which there is a specified point O .*

2. Main Results

Our primary result establishes a new bound on the Tate-Shafarevich group for a specific class of curves.

Theorem 2.1 (Mordell-Weil). *Let E be an elliptic curve defined over \mathbb{Q} . Then its group of rational points $E(\mathbb{Q})$ is a finitely generated abelian group.*

Conjecture 2.2. *The rank of an elliptic curve over \mathbb{Q} can be arbitrarily large.*

The proof of the main theorem relies on the following lemma.

Lemma 2.3. *A key lemma would be stated here.*

Remark: Authors are invited to submit a two-page abstract in English by the submission deadline. Please use this NCNTI 2025 Latex template. The abstract should include the title, author(s) information, and keywords. All submissions must be in PDF format.



References

- [1] J. H. Silverman. *The Arithmetic of Elliptic Curves*. Springer, 2nd edition, 2009.
- [2] A. Wiles. Modular elliptic curves and Fermat's Last Theorem. *Annals of Mathematics*, **141**(3): 443–551, 1995.
- [3] F. Author. Title of the Thesis. *PhD thesis, University, City*, 2024.