The Multifaceted Applications of Elliptic Curves and their Relevance in Cryptography

Cleveland State University Dept. of Mathematics and Statistics

Darren Gerrity, M. Grant Johnson, Jay Kropf, Joshua Rockamore

Advisor: Dr. Federico Galetto

Choose Ohio First

ABSTRACT

Elliptic curves are cubic curves similar to the quadratic conic sections that students learn about in a high school Algebra II class. What makes elliptic curves interesting is the multitude of applications that they have to fields such as number theory and cryptography. Our project aims to explore many of the algebraic and geometric concepts behind elliptic curves, in order to provide an accurate and well-motivated description of the elliptic curve cryptography system that is used today. This includes a brief introduction to projective geometry, modular arithmetic, and the group law which gives elliptic curves an algebraic structure. This algebraic structure is the core of most of the applications that elliptic curves are useful for. The cryptography system is used by companies such as Intel and Bitcoin to secure data from outside sources. We will give a brief overview of cryptography in general, as well as demonstration of an elliptic curve cryptography setup. The theory and applications of elliptic curves extend far beyond what we are able to fit into a single project, but what we provide is a cohesive introduction to the rich subject. In summary, this research aims to help people better understand the use and important applications of elliptic curves.

WHAT ARE ELLIPTIC CURVES?

- *Elliptic curves* are algebraic curves defined by a cubic equation where y has degree 2 and x has degree 3.
- They can be reduced to the *Weierstrass form* $\mathbf{y^2 = x^3 + Ax + B}$.

PROJECTIVE GEOMETRY

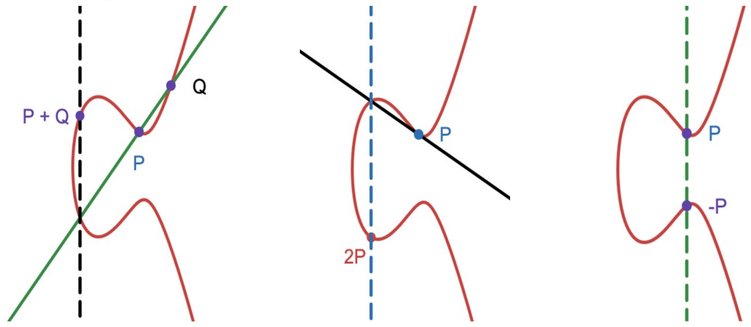
- In Euclidean geometry, parallel lines do not intersect
- In projective geometry, we include extra points called *points at infinity* such that each set of parallel lines intersects at one point at infinity.
- We include the point at infinity where all vertical lines intersect on an elliptic curve. This point is denoted (0:1:0) where a standard "finite" point is denoted (x:y:1).

MODULAR ARITHMETIC

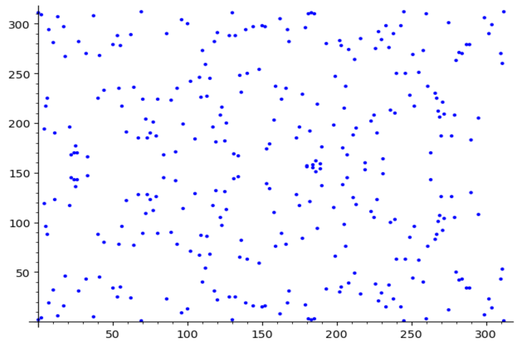
- When working with computers, it is more efficient to use a finite number system.
- We pick a base number m and group together all integers sharing the same remainder when divided by m. This partitions the integer into a finite set of *congruence classes.*
- Addition, multiplication, and subtraction work well in general, but division only works when we have a prime base.

THE GROUP LAW

We can define an addition operation on the points of an elliptic curve using algebraic equations, but the operation has a nice geometric interpretation exhibited below.



- This operation is commutative, associative, has an identity element, and has inverses, just like ordinary addition.
- We can define an elliptic curve and its operation over a number system when all four operations are defined.
- If given a point P and a multiple nP on a finite elliptic curve, it is very difficult, even for computers, to find n if it is not already known. This is useful for cryptography.



This is the curve $y^2=x^3+2x+4$ over the finite field of the integers modulo 313.

ELLIPTIC CURVE DIFFIE-HELLMAN EXCHANGE

Public Parameter Creation

A trusted party chooses and publishes a (large) prime **313** and a point **(53:25:1)** in an elliptic curve over the finite field $\mathbf{F_{313}}$: $\mathbf{y^2 = x^3 + 2x + 4}$

Private and Public Key Creation

Alice	Bob
Private Key: Chooses a secret integer **79** Public Key: Computes the point **(123:97:1)** = 79 * (53:25:1) $\in E(F_{313})$	Private Key: Chooses a secret integer **23** Public Key: Computes the point **(75:190:1)** = 23 * (53:25:1) $\in E(F_{313})$

Public Key Exchange

Alice sends **97** to Bob	Bob sends **190** to Alice

Final Private Computations

Alice finds **(75:190:1)** from **190**	Bob finds **(123:97:1)** from **97**
Alice calculates **(225:105:1)** = 79 *(75:190:1)	Bob calculates **(225:105:1)** = 23 * (123:97:1)

The shared secret value is

79 * (75:190:1) = **(225:105:1)** = 23 * (123:97:1)

PRIMALITY TESTING

- Integer factorization uses elliptic curves to break numbers into the multiplication of prime numbers (can be used to check if a number is prime).
- Goldwasser & Kilian (1999) used elliptic curves in their proposal of an algorithm to quickly test the primality of a number.

FERMAT'S LAST THEOREM

- If $n > 2$, then $A^n + B^n = C^n$ has no solution where A, B, and C are positive integers.
- Took over 360 years to be proven officially, done by Andrew Wiles through elliptic curves.
- Number theorist Gerhard Frey found an elliptic equation to represent Fermat's equation, but it had no modular form.
  - Taniyama-Shimura's Conjecture: for every elliptic equation there is a modular form.
- In Wiles' proof, had to also prove Taniyama-Shimura's Conjecture.
  - Wiles work is significant because in his proof of Taniyama-Shimura's conjecture and Fermat's last theorem, he bridged together the gap between several previously disparate areas of mathematics.

REFERENCES

Allenbaugh, M. H. (2001). The enduring and revolutionary impact of Pierre de Fermat's last theorem. In N. Schlager & J. Lauer (Eds.) *Science and its times: Under the social significance of scientific discovery*, (Vol. 3, pp. 259-262).

Desmos Graphing Calculator. (2011, June 30). Retrieved March 28, 2024, from Desmos: https://www.desmos.com/calculator

Goldwasser, S. & Killian, J. (1999). Primality testing using elliptic curves. *Journal of ACM, 46*(4), 450-472.

Hoffstein, J., Pipher, J., & Silverman, J. H. (2008). *An Introduction to Mathematical Cryptography*. Springer Science+Business Media.

SageMath, the Sage Mathematics Software System (Version 10.1), The Sage Developers, 2023, https://www.sagemath.org.

Washington, L. C. (2008). *Elliptic curves, number theory and cryptography*. Chapman & Hall/CRC.

ACKNOWLEDGEMENTS

We would like to thank the Choose Ohio First Math Cohort of Cleveland State University for providing us the opportunity to engage in the exploration of elliptic curves. We would also like to give a special thanks to Dr. Galetto as our advisor for providing us his time and the necessary resources to complete this research project.