Congruences between Logarithms of Heegner Points

Kevin Wu, Eric Shen
Mentored by Dr. Daniel Kriz

October 15, 2022
MIT PRIMES Conference

Elliptic Curves

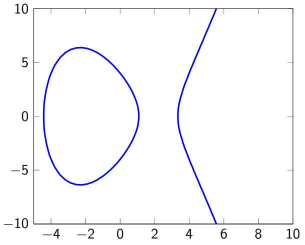
Definition

A cubic curve in normal form is an equation of the form

$$y^2 = f(x) = x^3 + ax^2 + bx + c.$$

When the roots of f are distinct, we call this an *elliptic curve*.

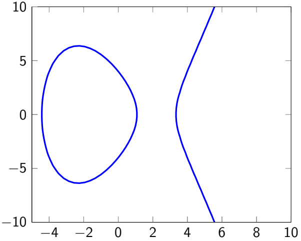
For example, $y^2 = x^3 - 16x + 16$ defines the following valid elliptic curve.



Integral Points

Theorem (Baker, Siegel)

The number of $\mathbb{Z}$-points on an elliptic curve is finite, moreover the coordinates of the points are bounded in terms of the coefficients of the curve.



For example, in our curve $y^2 = x^3 - 16x + 16$, the set of integer points is $(\pm 4, \pm 4), (0, \pm 4), (1, \pm 1), (8, \pm 20), (24, \pm 116)$. There isn't much structure here.

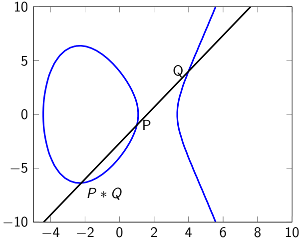
Given a curve E, a rational point $P \in E(\mathbb{Q})$ is a point (x, y) where $x, y \in \mathbb{Q}$.

Group Structure

Definition

Given any two rational points P, Q on an elliptic curve E, define $P * Q$ as the third point that the line through P, Q intersects E at.

It turns out that if P, Q are rational points, then $P * Q$ is also rational.



For example, on our curve $y^2 = x^3 - 16x + 16$, if $P = (1, -1), Q = (4, 4)$ then $P * Q = \left(-\frac{20}{9}, -\frac{172}{27}\right)$.
Notice that $*$ is commutative since swapping P, Q doesn't change the line through them.

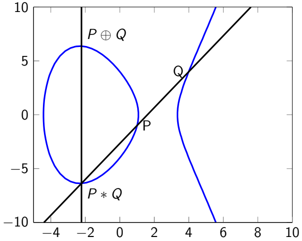
Group Structure (cont.)

Definition

Let $\mathcal{O}$ be a point at infinity along E and define

$$P \oplus Q := \mathcal{O} * (P * Q).$$

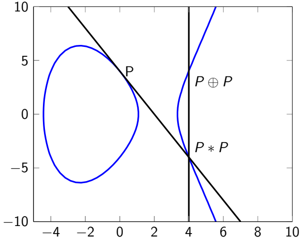
The set of rational points on E including $\mathcal{O}$ with operation $\oplus$ form the group of the elliptic curve.



Continuing from the last slide,
$P = (1, -1)$, $Q = (4, 4)$, so we can compute
$P \oplus Q = \left(-\frac{20}{9}, \frac{172}{27}\right)$.
As $*$ is commutative $\oplus$ is also commutative.

Doubling Points

We can add points to themselves, we just take the line through P, P to be the line tangent to the curve at P.



For example, taking our curve $y^2 = x^3 - 16x + 16$, with point $P = (0, 4)$, then the tangent line at P is $y = 4 - 2x$.

Ranks of Elliptic Curves

Theorem (Mordell)

The group of the elliptic curve is finitely generated: we can say $E(\mathbb{Q}) \cong \mathbb{Z}_{q_1} \times \mathbb{Z}_{q_2} \times \cdots \times \mathbb{Z}_{q_n} \times \mathbb{Z}^r$ for some positive integers $q_1, \cdots, q_n, r$. We define the Mordell-Weil rank of the curve as r.

The torsion subgroup $E(\mathbb{Q})_{tors}$ is the subgroup of points that have finite order, so we can write

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

Theorems of Mazur and Nagell-Lutz let us compute the torsion subgroup easily, so knowing the Mordell-Weil rank of the curve is enough to know the group of the curve.

Birch and Swinnerton-Dyer Conjecture

The L-function of the elliptic curve is defined as

$$L_E(s) = \sum_{n=1}^{\infty} a_n n^{-s}$$

where a_n encodes data about the number of points on the curve over finite fields, which satisfies a certain functional equation (F.E.).
Then we define the analytic rank as

$$r_{an} = \mathrm{ord}_{s=1} L(E, s),$$

the order of vanishing at the point of symmetry of the F.E.

Birch and Swinnerton-Dyer Conjecture

Conjecture (Birch and Swinnerton-Dyer)

The analytic and Mordell-Weil rank are the same.

Currently, the Mordell-Weil rank is “hard” to compute while the analytic rank is (in theory) simpler, amounting to showing the value of a particular function is nonzero, so this conjecture ineffectively solves elliptic curves.

Formal Group

We can parameterize the curve using a coordinate z such that there are Laurent series

$$x, y \in \mathbb{Z}[a, b, c][\![z]\!]$$

such that $P(z) = (x(z), y(z)) \in E$.
Using this, we can find a power series $F(x, y)$ satisfying the equation

$$P(z_1) \oplus P(z_2) = P(F(z_1, z_2)).$$

We call F the formal group law of the elliptic curve.

Formal Logarithm

Definition

The formal logarithm is the integral of the invariant differential:

$$\log_{\mathcal{F}}(T) = \int F_X(0, T)^{-1} dT.$$

The formal logarithm is an isomorphism mapping a formal group to the additive group, that is

$$\log_{\mathcal{F}}(F(A, B)) = \log_{\mathcal{F}}(A) + \log_{\mathcal{F}}(B).$$

The formal logarithm detects torsion points: a point is torsion if and only if its formal logarithm converges to 0 over the p-adic integers.

Main result

Theorem

Let E, E' be elliptic curves over $\mathbb{Q}$ with conductors N, N'. Suppose $E[p^r] \cong E'[p^r]$.
Then letting P be the Heegner point of conductor 1 when p is split in K, conductor p^2 when p is inert in K and conductor p when p is ramified in K, we have

$$\left(\tilde{L}_p(E,1) \prod_{\ell | NN'/M} L_\ell(E,1)\right) \cdot \log_{\hat{E}}(P_E)$$
$$\equiv \pm \left(\tilde{L}_p(E,1) \prod_{\ell | NN'/M} L_\ell(E',1)\right) \cdot \log_{\hat{E}'}(P_{E'}) \pmod{p^r}.$$

Application

Definition

Given an elliptic curve $E : y^2 = f(x)$ then the quadratic twist by d is

$$E^d : dy^2 = f(x).$$

Theorem

Let N be the conductor of E. Suppose $E' = E^d$ where $(N, d) = 1$. Then

$$\tilde{L}_2(E,1) \cdot \left(\prod_{\ell | d} L_\ell(E,1) \right) \cdot \log_{\hat{E}}(P_E) \equiv \tilde{L}_2(E',1) \cdot \log_{\hat{E}'}(P_{E'}) \pmod{2}.$$

Moreover, if they aren't congruent to 0, then BSD holds for E, E^d.

We use this theorem to "propagate BSD". By showing the left hand side is nonzero mod 2, we can show a whole quadratic twist family satisfies BSD.

Acknowledgments

We would like to thank:

- Our mentor, Dr. Daniel Kriz, for teaching us the theory of elliptic curves, guiding us through the project, and offering valuable advice.
- Prof. Etingof, Dr. Gerovitch, Dr. Khovanova, and the MIT PRIMES-USA program for making this research possible.

References

J. H. Silverman, *The Arithmetic of Elliptic Curves*. Graduate Texts in Mathematics. Springer New York, 2nd edition, 2009.

J. H. Silverman and J. T. Tate, *Rational Points on Elliptic Curves*. Undergraduate Texts in Mathematics. Springer, Cham, 2nd edition, 2015.

B. Gross, D. Zagier, *Heegner points and derivatives of L-series*, Invent. Math., 84(2): 225-320, 1986.

T. Honda, *Formal groups and zeta functions*. Osaka J. Math., 5 (1968), 199–213.

V. Kolyvagin, *Euler systems*, in: The Grothendieck Festschift (Vol. II), P. Cartier et al., eds., Prog. in Math 87, Boston: Birkhäuser (1990) 435-483.