On Bounds and Diophantine Properties of Elliptic Curves

Navvye Anand

October 17, 2024

Introduction to Elliptic Curves

- Elliptic curves are ubiquitous in number theory!
- They are smooth, projective curves of genus one, usually of the form $y^2 = x^3 + Ax + B$.
- These curves arise naturally in the study of Diophantine equations, particularly those concerning rational points, where they help answer questions about the existence and structure of solutions.
- Elliptic curves are crucial to major results such as Fermat's Last Theorem, which was proven using insights from elliptic curves and modular forms.
- Moreover, elliptic curves have applications in cryptography, particularly in elliptic curve cryptography (ECC), where their group structure provides a secure foundation for encryption algorithms due to the difficulty of the elliptic curve discrete logarithm problem.

More about Elliptic Curves!

- Elliptic curves also play a role in the Birch and Swinnerton-Dyer Conjecture, one of the Millennium Prize Problems, which connects the rank of an elliptic curve (the number of independent rational points) with the behavior of its associated L-function.
- The Hasse-Weil L-function $L(s, V)$ is attached to an algebraic variety V defined over a number field K. It is constructed using the local zeta functions $Z(V_{\mathfrak{p}}, t)$, which correspond to the reductions of V at prime ideals $\mathfrak{p}$ of the ring of integers $\mathcal{O}_K$ of K.
- For simplicity, consider the case of an elliptic curve E defined over a number field K. The Hasse-Weil L-function of E, denoted $L(s, E/K)$, is formally defined by an Euler product over the prime ideals $\mathfrak{p}$ of K:

$$L(s, E/K) = \prod_{\mathfrak{p}} L_{\mathfrak{p}}(s, E),$$

Mordell Curves

- Mordell equations, are a subset of elliptic curves and take the form $E := y^2 = x^3 + k$, with $k \in \mathbb{Z}$.
- Named after Louis Mordell, an American-born British mathematician, known for his pioneering research in number theory.
- These curves were closely studied by Louis Mordell, from the point of view of determining their integer points. He showed that every Mordell curve contains only finitely many integer points (x, y).
- The finite nature of $N(E)$ for Mordell equations invites a natural inquiry into the precise determination of these solutions.
- Examples of work done include Hall's conjecture, which states that $y^2 - x^3 \geq C\sqrt{|x|}$ for an absolute constant C.
- The modern version of Hall's conjecture posits that $y^2 - x^3 \geq C(\varepsilon) \cdot x^{\frac{1}{2}-\varepsilon}$ for any $\epsilon > 0$ and a constant $C(\varepsilon)$ dependent solely on ε.

Siegel's Theorem

- Siegel's theorem says that for a smooth algebraic curve C of genus g defined over a number field K, presented in an affine space in a given coordinate system, there are only finitely many points on C with coordinates in the ring of integers O of K, provided $g > 0$.
- This well known result of Siegel implies that the number of solutions of Mordell equation is finite.

Note

Broadly, the genus of a curve is the number of handles added to a sphere, or the number of holes in a surface. A sphere has genus $g = 0$. A torus has genus $g = 1$. A double toroid (below) has genus $g = 2$.

Some Solutions of Elliptic Curves

Value of k	Number of Integral Points	Points
-1	1	$(1, 0)$
-2	2	$(3, 5)$, $(3, -5)$
-8	1	$(2, 0)$
-13	2	$(17, 70)$, $(17, -70)$
-15	2	$(4, 7)$, $(4, -7)$
-18	2	$(3, 3)$, $(3, -3)$
-19	2	$(7, 18)$, $(7, -18)$
-20	2	$(6, 14)$, $(6, -14)$
-23	2	$(3, 2)$, $(3, -2)$
-25	2	$(5, 10)$, $(5, -10)$
-27	1	$(3, 0)$

Table: Table of Solutions for $k < 0$

Some More Solutions

Value of k	Number of Integral Points	Points
2	2	$(-1,-1)$, $(-1,1)$
3	2	$(1,-2)$, $(1,2)$
4	2	$(0,-2)$, $(0,2)$
5	2	$(-1,-2)$, $(-1,2)$
10	2	$(-1,-3)$, $(-1,3)$
16	2	$(0,-4)$, $(0,4)$

Table: Table of Solutions for $k > 0$

Main Question

Which Mordell curves of the form $y^2 = x^3 + k$ have exactly $|k|$ integral solutions?

Problems Faced

Before we delve into the paper, we provide a brief description of the state of the art bounds regarding elliptic curves.

- Helfgott and Venkatesh proposed a novel approach to bounding $E(K, S)$ by invoking the best sphere-packing results given by Kabatjanskii and Levenshtein, and thereby improved upon previous bounds on elliptic curves, breaking the $N(E) = O(|\mathrm{Disc(E)}|^{0.5})$ barrier.
- Bhargava et al improved upon this bound and proved

$$N(E) = O(|\mathrm{Disc}(E)|^{0.1117...+\epsilon}).$$

- Alpoge and Ho proved that

$$N(E) = O\left(2^{\mathrm{rank}(E_{A,B})} \prod_{p^2|\Delta_{A,B}} \min\left(4\left\lfloor \frac{\nu_p\left(\Delta_{A,B}\right)}{2} \right\rfloor + 1, 7^{2^7}\right)\right)$$

- However, the aforementioned bounds don't allow us to explicitly compute all k such that $N(E) = |k|$. Therefore, we turn our attention to binary cubic forms!

Tools Used

- In order to prove the statements above, we rely heavily on the connection between binary cubic forms and Mordell curves.
- The main theorem is proved by bounding the number of integral points on a Mordell curve by the 3-part of the class number of the quadratic field $\mathbb{Q}(\sqrt{k})$, denoted by $h_3(k)$, and then bounding the class number of the quadratic field using the explicit version of Dirichlet's class number formula.
- Additionally, we also find explicit bounds for the number of integral points on well defined twists of elliptic curve, and parameterized families of elliptic curves. We improve the state of the art lower bound for number of integral solutions for families of Mordell curves by exploiting this very relation.

Finitely Many Cases

Theorem

There exist only finitely many elliptic curves $E : y^2 = x^3 + k$ such that $N(E) \geq |k|$.

Proof.

- The discriminant of an elliptic curve $y^2 = x^3 + ax + k$ is $\mathrm{Disc}(E) := -16(4a^3 + 27k^2)$. Now, since $a = 0$, the discriminant is simply $\mathrm{Disc}(E) = -432k^2$.
- As demonstrated by Bhargava et al, the number of integral points for any elliptic curve E over $\mathbb{Q}$ in Weierstrass form with integral coefficients is at most $O_\varepsilon\left(|\mathrm{Disc}(E)|^{0.1117+\varepsilon}\right)$.
- Now, $N(E) = O_\varepsilon\left(|-432k^2|^{0.1117+\varepsilon}\right)$. Clearly, $\lim_{k\to\infty} \frac{|k|}{N(E)} = \infty$. Hence there are only finitely many cases where $N(E) \geq |k|$ and hence only finitely many cases where $N(E) = |k|$.

Introduction to Binary Cubic Forms

- A binary cubic form is a homogeneous polynomial of degree 3.
- It is often represented as:

$$F(x, y) = ax^3 + 3bx^2y + 3cxy^2 + dy^3$$

- Let $\mathcal{C}_1(x, y) = (a_1, b_1, c_1, d_1)$ and $\mathcal{C}(x, y) = (a, b, c, d)$ be integral binary cubic forms.
- The forms $\mathcal{C}_1$ and $\mathcal{C}$ are said to be equivalent, written as $\mathcal{C}_1 \sim \mathcal{C}$, if there exists a matrix $M \in GL_2(\mathbb{Z})$ such that the equation:

$$\mathcal{C}_1(x_1, y_1) = \mathcal{C}(x, y) \circ M$$

holds.

- The general linear group of order 2 in integers is defined as

$$GL(2, \mathbb{Z}) := \left\{ \begin{pmatrix} a & b \\ c & d \end{pmatrix} \middle| \, a, b, c, d \in \mathbb{Z}, ad - bc \neq 0 \right\}$$

Binary Cubic Forms are Cool!

- Boris Delone and Dmitry Faddeev showed that binary cubic forms with integer coefficients can be used to parametrize orders in cubic fields.
- Let K be a number field defined by a root θ of the polynomial $x^3 + px^2 + qx + r$ with $p, q, r \in \mathbb{Z}$ such that there exists an integral basis of the form $(1, \theta, \frac{(\theta^2+t\theta+u)}{f})$ with $t, u, f \in \mathbb{Z}$ and $f = [\mathbb{Z}_K : \mathbb{Z}[\theta]]$
- Then we choose $\alpha = \theta$ and $\beta = (\theta^2 + t\theta + u)/f$.
- Now, we have explicitly

$$\begin{aligned} F_B(x, y) = & \frac{t^3 - 2t^2p + t(q + p^2) + r - pq}{f^2}x^3 \\ & + \frac{-3t^2 + 4tp - (p^2 + q)}{f} \cdot x^2y \\ & + (3t - 2p)xy^2 - fy^3 \end{aligned}$$

- Fun fact! There are infinitely many acceptable binary cubic forms.

Main Theorems

Theorem

There exists a correspondence between the set of integral solutions $S_k = \{(X_1, Y_1), \ldots, (X_{N_k}, Y_{N_k})\}$ *for the Mordell equation* $Y^2 = X^3 + k$ *and the set* T_k *of triples* (F, x, y) *where* F *is a binary cubic form of the shape* $ax^3 + 3bx^2y + 3cxy^2 + dy^3$ *with discriminant* $-108k$ *and with integers* x, y *satisfying* $F(x, y) = 1$.

Theorem

Furthermore, there exists a bijection between T_k *and* S_k *under the actions of* $SL_2(\mathbb{Z})$ *and* $GL_2(\mathbb{Z})$.

Proof of Main Theorems

Let

$$F = F(x, y) = ax^3 + 3bx^2y + 3cxy^2 + dy^3$$

be a binary cubic form with the discriminant

$$D_F = -27(a^2d^2 - 6abcd - 3b^2c^2 + 4ac^3 + 4b^3d)$$

We observe the fact that the set of the binary cubic forms of the shape F is closed within the larger set of binary cubic forms of the set $\mathbb{Z}[x, y]$ under the action of both SL_2 and GL_2. Now, describe the Hessian of the F to be

$$H = H_F(x, y) = -\frac{1}{4}\left(\frac{\partial^2 F}{\partial x^2}\frac{\partial^2 F}{\partial y^2} - \left(\frac{\partial^2 F}{\partial x \partial y}\right)^2\right)$$

Define the Jacobian determinant of F and H, a cubic form $G = G_F$ defined as

$$G = G_F(x, y) = \frac{\partial F}{\partial x}\frac{\partial H}{\partial y} - \frac{\partial F}{\partial y}\frac{\partial H}{\partial x}.$$

Proof of Main Theorems

Define the Jacobian determinant of F and H, a cubic form $G = G_F$ defined as

$$G = G_F(x, y) = \frac{\partial F}{\partial x}\frac{\partial H}{\partial y} - \frac{\partial F}{\partial y}\frac{\partial H}{\partial x}.$$

Now, we have

$$H/9 = \left(b^2 - ac\right)x^2 + (bc - ad)xy + \left(c^2 - bd\right)y^2$$

and

$$G/27 = a_1x^3 + 3b_1x^2y + 3c_1xy^2 + d_1y^3,$$

where

$$a_1 = -a^2d+3abc-2b^3, \quad b_1 = -b^2c-abd+2ac^2, \quad c_1 = bc^2-2b^2d+acd,$$

These covariants satisfy the syzygy

$$4H(x, y)^3 = G(x, y)^2 + 27DF(x, y)^2.$$

Defining $D_1 = D/27, H_1 = H/9$ and $G_1 = G/27$, we get

$$4H_1(x, y)^3 = G_1(x, y)^2 + D_1F(x, y)^2.$$

Proof Continued

We note that if (x_0, y_0) satisfies the equation $F(x_0, y_0) = 1$ and $D_1 \equiv 0 \pmod 4$ then necessarily $G_1(x_0, y_0) \equiv 0 \pmod 2$. We may therefore conclude that $Y^2 = X^3 + k$, where

$$X = H_1(x_0, y_0), \quad Y = \frac{G_1(x_0, y_0)}{2} \quad \text{and} \quad k = -\frac{D_1}{4} = -\frac{D}{108}.$$

It follows that, to a given triple (F, x_0, y_0), where F is a cubic form of the shape $ax^3 + 3bx^2y + 3cxy^2 + dy^3$ with discriminant $-108k$, and x_0, y_0 are integers for which $F(x_0, y_0) = 1$, we can associate an integral point on the Mordell equation $Y^2 = X^3 + k$. The converse of this can be proven easily by taking the covariants of the factors to be

$$X = \frac{G_1(1,0)}{2} = \frac{G(1,0)}{54} \text{ and } Y = H_1(1,0) = \frac{H(1,0)}{9}$$

The proof of bijection between T_k and S_k under the action of $GL_2(\mathbb{Z})$ and $SL_2(\mathbb{Z})$ is achieved by constructing a contradiction.

To Reiterate

- There exists a bijective correspondence between integral solutions (X, Y) of the Mordell equation $Y^2 = X^3 + k$ and triples (F, x, y), where F is a binary cubic form with discriminant $-108k$, and (x, y) are integers satisfying $F(x, y) = 1$.
- This correspondence allows us to translate problems about Mordell equation solutions into problems about binary cubic forms, and vice versa, potentially simplifying certain analyses.
- The correspondence preserves algebraic structures, providing a powerful tool for studying properties of Mordell equation solutions, such as their finiteness in certain cases.

Explicit Bounds for Mordell Curves

Theorem

If k is a nonzero integer, then the equation

$$y^2 = x^3 + k$$

has at most $10h_3(-108k)$ solutions in integers x, y where $h_3(-108k)$ is the class number of the binary cubic forms with discriminant $-108k$, which is also referred to as the 3-part of class number of the quadratic field $\mathbb{Q}(\sqrt{-108k}) = \mathbb{Q}(\sqrt{-3k})$.

Note

The class number of a binary quadratic form $h(d)$ is the number of equivalence classes of binary quadratic forms with discriminant d.

Intermediary Lemmas

Lemma (Scholz Reflection Formula)

$h_3(-3k) \leq h_3(k) + 1$

Lemma (Dirichlet's Class Number Formula)

$$h(k) = \begin{cases} \dfrac{w\sqrt{|k|}}{2\pi} L(1,x), & \text{if } k < 0; \\ \dfrac{\sqrt{k}}{\ln \varepsilon} L(1,x), & \text{if } k > 0. \end{cases}$$

where w is the number of automorphisms of quadratic forms of discriminant k, ε is the fundamental unit of the quadratic field $\mathbb{Q}(\sqrt{k})$, and $L(1,\chi)$ is the Dirichlet L function $\sum_{n=1}^{\infty} \frac{\chi(n)}{n}$.

Dirichlet's Class Number Formula and $L-$ Function

Let $h(d)$ for the number of equivalence classes of quadratic forms with discriminant d. Let $\chi = \left(\frac{d}{m}\right)$ be the Kronecker symbol. Then χ is a Dirichlet character. Write $L(s, \chi)$ for the Dirichlet L-series based on χ. For $d > 0$, let $t > 0, u > 0$ be the solution to the Pell equation $t^2 - du^2 = 4$ for which u is smallest, and write

$$\varepsilon = \frac{1}{2}(t + u\sqrt{d})$$

(Then ε is either a fundamental unit of the real quadratic field $\mathbb{Q}(\sqrt{d})$ or the square of a fundamental unit.) For $d < 0$, write w for the number of automorphisms of quadratic forms of discriminant d. Then, Dirichlet showed that

$$h(d) = \begin{cases} \frac{w\sqrt{|d|}}{2\pi} L(1, \chi), & d < 0 \\ \frac{\sqrt{d}}{2 \ln \varepsilon} L(1, \chi), & d > 0. \end{cases}$$

More Intermediary Lemmas

- Now in order to achieve effective bounds, we shall divide k into two cases, $k > 0$ and $k < 0$.
- Let us define Δ to be the discriminant of a real quadratic field $\mathbb{Q}(\sqrt{k})$ such that $\Delta = \begin{cases} k & \text{if } k \equiv 1 \pmod 4 \\ 4k & \text{if } k \not\equiv 1 \pmod 4 \end{cases}$.
- Now, Maohua Le (Zhanjiang) proved that for any $k \in \mathbb{N}$, where k is square-free, we have $h(k) \leq \left\lfloor \frac{\sqrt{\Delta}}{2} \right\rfloor$.
- Now for imaginary quadratic fields, the case is a bit trickier, but luckily, we utilize a combination of bounds to achieve our desired result. We begin by noting that

$$w = \begin{cases} 2 & \text{when } k < -4 \\ 4 & \text{when } k = 4 \\ 6 & \text{when } k = -3 \end{cases} \implies h(k) = \frac{|k|^{1/2} L(1, \chi)}{\pi} \text{ for } k < -4.$$

Explicit Bound Bashing

Theorem (Louboutin)

Let χ be a Dirichlet character modulo q with conductor f. Then, if χ is even

$$|L(1,\chi)| \leq \frac{1}{2}\log f + c_1 \quad \textit{with} \quad c_1 = \left(2 + \gamma - \frac{\log(4\pi)}{2}\right) = 0.023\ldots$$

and if χ is odd, then

$$|L(1,\chi)| \leq \frac{1}{2}\log f + c_2 \quad \textit{with} \quad c_2 = \frac{(2 + \gamma - \log\pi)}{2} = 0.716.$$

Note

For a Dirichlet character χ modulo q, the conductor f is the smallest divisor of q such that $\chi(n)$ depends only on $n \pmod f$ for all n coprime to q. Trivially, we have $f \leq q$.

More Explicit Bound Bashing

- Replacing f with q in the above-mentioned bound, we get

$$L(1,\chi) \leq \begin{cases} \frac{1}{2}\log q + 0.023 & \text{if } \chi \text{ is even,} \\ \frac{1}{2}\log q + 0.716 & \text{if } \chi \text{ is odd.} \end{cases}$$

- Now, since $h_3(-3k) \leq h_3(k) + 1 \leq h(k) + 1$ and

$$h(k) \leq \frac{|k|^{1/2}}{\pi}(0.5\log|k| + 0.716),$$

we have

$$h_3(-3k) \leq \frac{|k|^{1/2}}{\pi}(0.5\log|k| + 0.716) + 1$$

$$N(E) \leq 10\left(\frac{|k|^{1/2}}{\pi}(0.5\log|k| + 0.716) + 1\right).$$

- But since we want $N(E) = |k|$, we must have

$$|k| \leq 10\left(\frac{|k|^{1/2}}{\pi}(0.5\log|k| + 0.716) + 1\right) \implies k \leq 116$$

Final Result

Theorem (Final Result!)

- ***Including the point at infinity:*** *there are precisely three curves for which* $N(E) = |k|$*. These correspond to the cases* $k = 3, 8, 17$*.*
- ***Excluding the point at infinity:*** *there are precisely four curves for which* $N(E) = |k|$*, corresponding to the cases* $k = -1, -2, -4, 2$*.*

Corollary (Final Result!)

- ***Excluding the point at infinity:*** *there is no curve for which* $N(E) = |2k|$*.*
- ***Including the point at infinity:*** *there is only one curve for which* $N(E) = |2k|$*, corresponding to the case* $k = -1$

Misc Results

We also proved some miscellaneous results!

Explicit Bounds on Twists of Elliptic Curves

We begin by defining an elliptic curve $E : y^2 = x^3 + Ax + B$, with discriminant $\Delta = -16(4A^3 + 27B^2) > 0$ and roots $e_1 < e_2 < e_3$. Now, let Ω_E denote the real period of E such that

$$\Omega_E = \int \frac{\mathrm{d}x}{y} = \int \frac{\mathrm{d}x}{\sqrt{x^3 + Ax + B}} \quad \text{where } y > 0.$$

For $n \in \mathbb{Z}^+$, let $E_n : y^2 = x^3 + n^2Ax + n^3B$ be the quadratic twist on E. Finally, let $\nu_E(n)$ denote the number of integral points on $E_n^*(\mathbb{Z})$, a subset of $E_N(\mathbb{Z})$ with $\gcd(x, n) = 1$, such that

$$\nu_E(n) = \#\left\{(x, y) \in \mathbb{Z}^2;\, y^2 = x^3 + An^2x + Bn^3 \text{ where } \gcd(n, x) = 1\right\}.$$

Explicit Bounds on Twists of Elliptic Curves

Theorem

Let there be an elliptic curve E over $\mathbb{R}$ with discriminant $\Delta > 0$, which is isomorphic to the Legendre normal form

$$E(\lambda) = x(x-1)(x-\lambda)$$

for some λ such that $0 < \lambda < 1$, then

$$\lim_{N\to\infty} \frac{1}{\sqrt{N}} \sum_{n\leq N} \nu_E(N) \leq \frac{(|\Delta|^{1/2} - 1) \cdot (0.5 \log|\Delta| + 0.716)}{4\,\mathrm{L}\left(1, \sqrt{1-\lambda}\right)}$$

where $\mathrm{L}\,(a,b)$ is the logarithmic mean of (a,b),

$$\mathrm{L}\,(a,b) = \frac{b-a}{\ln b - \ln a}.$$

Results for Another Family of Elliptic Curves

Theorem

Let $t \neq 2$ be an integer such that the fundamental unit ω of the quadratic field $\mathbb{Q}\left(\sqrt{t^2+4}\right)$ is $\frac{\left(t+\sqrt{t^2+4}\right)}{2}$. Then, the elliptic curve $E := y^2 = (t^2+4)x^4 - 4$ has exactly one integral point. When $t = 2$, the elliptic curve has exactly two integral points.