UPPER BOUNDS FOR MORDELL EQUATIONS

NAVVYE ANAND

1. Introduction

Mordell equations are celebrated equations within number theory and elliptic curves. They were named after *Louis Mordell*, an American-born British mathematician, known for pioneering research in number theory. Mordell's work in this area was revolutionary as it marked the beginning of systematic study of the rational points on elliptic curves, a field that has since become a cornerstone of modern number theory. His findings led to the development of what is now known as the Mordell-Weil theorem, which states that the group of rational points on an elliptic curve over a number field is finitely generated. This theorem was a major breakthrough and laid the groundwork for further research by other mathematicians, including André Weil and John Tate. The study of Mordell equations is not just a theoretical pursuit, but it has practical applications in areas such as cryptography, particularly in the creation of elliptic curve cryptography (ECC). In this expository paper, we'll cover some properties of Mordell Equations, as well as some interesting upper bounds to the number of integral solutions of Mordell Equations. We will go over some of the recent developments in the field as well.

Definition 1.1. The *Mordell Equations* are elliptic curves of the form $y^2 = x^3 + k$ where k is an integer.

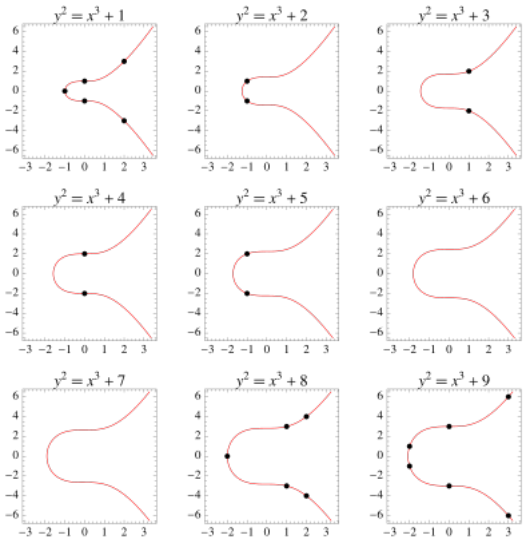

Figure 1. Graphs of Mordell Equations

2. Theorems of Mordell and Thue

The Mordell-Weil Theorem is a very important theorem in the the field of algebraic number theory. It states that the number of *rational* solutions to elliptic curves is finitely generated, which means that there exists a finite set of group generators for the group of rational points on an elliptic curve. Naturally, the question arises: What about integral solutions? The question of whether a Mordell equation could have infinitely many integer solutions was an interesting one in the early 20th century. However, impressive work by both Axel Thue and Louis Mordell proved that a Mordell equation can only have finitely many integral solutions.

Theorem 2.1. *Every Mordell Equation has only finitely many integer solutions*

2.1. **Relating binary cubic forms and Mordell equations.** A brief sketch of the proof is given for brevity. We wish to establish a connection between the binary cubic forms and Mordell Equations. Consider,

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

to 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 $Z[x, y]$ under the action of both SL_2 and GL_2. In order to see this, we describe the Hessian of the F to be $H = H_F(x, y)$

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

and 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

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

and $d_1 = -3bcd + 2c^3 + ad^2$. Crucially for our arguments, these covariants satisfy the linear relation (defined as a syzygy by Hilbert)

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

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

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

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 as in (2.1) 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

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

In summary, there exists a direct correspondence between the set of the integral solutions of binary cubic forms, and the set of integral solutions of Mordell equations. Therefore, if we prove that every binary cubic form $F(x, y) = r$ has finitely many solutions, then we have essentially proven that every Mordell equation has finitely many solutions. We now give another brief sketch for the **Thue–Siegel–Roth theorem**, which states precisely that every binary cubic form has finitely many solutions.

Roth's theorem is a very important theorem in diophantine approximation of algebraic numbers. It states that algebraic numbers cannot have many rational number approximations that are *very good*. The definition of *very good* has evolved over time, and was defined by many different mathematicians such as Axel Thue (1909), Carl Ludwig Siegel (1921), Freeman Dyson (1947), and Klaus Roth (1955).

The theorem states that for any algebraic number α has an approximation exponent equal to 2. In other words, for any $\epsilon > 0$, then there exist only finitely many co-prime integers p and q such that the inequality

$$\left|\alpha - \frac{p}{q}\right| < \frac{1}{q^{2+\epsilon}}$$

holds.

This proof technique involves the creation of an auxiliary multivariate polynomial, which is defined with a large number of variables dependent on ϵ. The technique leads to a contradiction when faced with an excessive number of good approximations. To apply this method, one identifies several rational approximations of a specific irrational algebraic number. Each of these rational approximations is then used as input for a distinct variable in the function's defining expression. This approach is particularly effective in demonstrating contradictions in the context of algebraic number approximations.

An interesting extension of the theorem is we consider a constant in the original expression. If α is a real algebraic number of degree n, $n \geq 2$ then there is a constant $c > 0$ such that for any rational number p/q, $q > 0$

$$\left|\alpha - \frac{p}{q}\right| > \frac{c}{q^n}.$$

It is clearly enough to assume $|\alpha - p/q| \leq 1$. By the mean value theorem $f(p/q) = f(\alpha) - f(p/q) \leq |\alpha - p/q|\, A$ where $f(x) \in \mathbb{Z}[x]$ is irreducible, $f(\alpha) = 0$, and $A = \sup |f'(x)|$, $|x - \alpha| \leq 1$. But since α is not rational $f(p/q) \neq 0$ and $|f(p/q)| \geq 1/q^n$. This completes the proof. ■

3. Bounding using Binary Forms

In this section, we utilize the close relation between binary cubic forms and Mordell equations to bound the number of integral solutions. The proofs of these results is beyond the scope of the paper, but can be accessed in the bibliography.

Theorem 3.1. *If $F(x, y)$ is a homogeneous cubic polynomial with integral coefficients for which $F(x, 1)$ has at least two distinct complex roots, then the equation*

$$F(x, y) = 1$$

possesses at most 10 solutions in integers x and y.

Theorem 3.2. *If $F(x, y)$ is a homogeneous cubic polynomial with integral coeffcients and nonzero discriminant and m is a nonzero integer, then the equation*

$$F(x, y) = m$$

possesses at most $10 \times 3^{\omega(m)}$ solutions in coprime integers x and y. Here, $\omega(m)$ denotes the number of distinct prime factors of m.

Additionally, a result of the flavour of 3.1 leads, via an argument of Mordell to additional bounds for the number of solutions of Mordell's equation:

Theorem 3.3. *If k is a nonzero integer, then the equation*

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

has at most $10h_3(-108k)$ solutions in integers x and y, where $h_3(-108k)$ is the class number of binary cubic forms of discriminant k.

We note, if $\epsilon > 0$, one may show that

$$h_3(-108k) \ll |k|^{1/2+\epsilon}$$

which yields us to the next portion of the paper: Hall's conjecture.

4. Hall's Conjecture

Hall's conjecture is an open question, on the differences between perfect squares and perfect cubes. It asserts that a perfect square y^2 and a perfect cube x^3 that are not equal must lie a *substantial* distance apart. Substantial in this context is defined in terms of $\sqrt{x}$. Originally, the conjecture stated that $|y^2 - x^3| > C\sqrt{|x|}$ for a fixed constant C. Hall suggested that the constant C could be taken as 0.2, which was in line with the computations of his era. However, an increase in computation power has yielded us with a better upper bound on C. For example, in 1998, Noam Elkies found the current record holder for C, for which compatibility with Hall's conjecture would require C to be less than $.0214 \approx 1/50$, roughly 10 times smaller than the original choice of $1/5$ that Hall suggested. The original, strong, form of the conjecture with exponent $1/2$ has never been disproven, although it is no longer believed to be true and the term Hall's conjecture now generally means the version with the constant $C(\epsilon)$ which is a constant dependent on the ϵ. The weak form of Hall's conjecture, which states that $|y^2 - x^3| > C(\epsilon)x^{0.5-\epsilon}$ was proven in 1980.

The following table gives the 25 solutions of $0 < |k| < x^{1/2}$ with $x < 10^{18}$ where $k = x^3 - y^2$ and $r = \dfrac{x^{1/2}}{|k|}$.

#	k	x	r
1	1641843	5853886516781223	46.60
2	30032270	38115991067861271	6.50
3	-1090	28187351	4.87
4	-193234265	810574762403977064	4.66
5	-17	5234	4.26
6	-225	720114	3.77
7	-24	8158	3.76
8	307	939787	3.16
9	207	367806	2.93
10	-28024	3790689201	2.20
11	-117073	65589428378	2.19
12	-4401169	53197086958290	1.66
13	105077952	23415546067124892	1.46
14	-1	2	1.41
15	-497218657	471477085999389882	1.38
16	-14668	384242766	1.34
17	-14857	390620082	1.33
18	-87002345	12813608766102806	1.30
19	2767769	12438517260105	1.27
20	-8569	110781386	1.23
21	5190544	35495694227489	1.15
22	-11492	154319269	1.08
23	-618	421351	1.05
24	548147655	322001299796379844	1.04
25	-297	93844	1.03

Table 1. Table of Hall Equation Parameters

Clearly, work done in Hall's conjecture shows that the number of integral solutions can be asymptotically be bounded by an exponent of $x^{\frac{1}{2}}$, but also shows that a tighter bound can be achieved.

4.1. **Finding Good Examples of Hall's Conjecture.**

Definition 4.1. We define good examples of Hall's conjecture to be examples where $0 < |y^2 - x^3| < x^{\frac{1}{2}}$.

An interesting algorithm, with verification of it's proof, is given below.

Definition 4.2. Let q, p, x, and y be real numbers. Define the following functions:

$$\begin{aligned} B(q,p,x) &= p^2 - q^2x, \\ C(q,p,x,y) &= p^3 - 3pq^2x + 2q^3y, \\ F(q,p,x,y) &= 4pC - 3B^2, \\ H(q,p,x,y) &= 9FB - 8C^2. \end{aligned}$$

where x, y, p, q are positive integers. The algorithm is based on the four polynomials given by the definition above. The values of these polynomials will be small when (x, y) is a good example and $\frac{p}{q}$ is the approximation to $x^{1/2}$ given by the next theorem.

Theorem 4.3. *Let (x, y) be a good example. Then, there exist $p, q, Q \in \mathbb{N}$ and $\delta \in \mathbb{R}$ such that (i) $p = qx^{1/2}(1+\delta)$, (ii) $0 < q < x^{1/6} < Q$ and (iii) $\frac{1}{qx^{1/2}(Q+q)} < |\delta| < \frac{1}{qx^{1/2}Q}$.*

Proof. Proof. We know that p and q are co-prime. Now we note that $x^{1/2}$ is an irrational number when (x, y) is a good example. (If $x^{1/2}$ is a natural number, then (x, y) will not be a good example as $x^3 - y^2 = 0$. But $x^{1/2}$ is either a natural number or an irrational number. Thus, $x^{1/2}$ is irrational.) Let $a_0, a_1, a_2, \ldots$ be the coefficients for the continued fraction for $x^{1/2}$, that is

$$x^{1/2} = \lim_{n\to\infty} [a_0; a_1, \ldots, a_n].$$

The list of coefficients will be infinite as $x^{1/2}$ is irrational. Let h_i and k_i be, respectively, the nominator and the denominator of the convergent $[a_0; a_1, \ldots, a_i]$, that is $\frac{h_i}{k_i} = [a_0; a_1, \ldots, a_i]$. Then, for any $i \in \mathbb{N}$, we have

$$\frac{1}{k_i\left(k_i + k_{i+1}\right)} < \left|\frac{h_i}{k_i} - x^{1/2}\right| < \frac{1}{k_i k_{i+1}}$$

and $k_i < k_{i+1}$. Now, pick the least j such that $k_{j+1} > x^{1/6}$. Let $q = k_j$, let $p = h_j$ and let $Q = k_{j+1}$. Then, we have

$$\frac{1}{q(q+Q)} < \left|\frac{p}{q} - x^{1/2}\right| < \frac{1}{qQ}$$

where $q < x^{1/6} < Q$ (we cannot have $q = x^{1/6}$ as $x^{1/6} \notin \mathbb{N}$). Next, let δ be the real number such that $p = qx^{1/2}(1+\delta)$. Then, we have

$$\frac{1}{q(q+Q)} < \left|\frac{qx^{1/2}(1+\delta)}{q} - x^{1/2}\right| < \frac{1}{qQ}.$$

Thus

$$\frac{1}{qx^{1/2}(q+Q)} < |\delta| < \frac{1}{qx^{1/2}Q}.$$

Note that p and q are co-prime since h_j and k_j are co-prime for any convergent $\frac{h_j}{k_j}$. ∎

5. Modern Work

Modern work in the field of bounding the number of integral points on an elliptic curve has been carried out by academic stalwarts such as Akshay Venkatesh, Manjul Bhargava etc. A brief description of some of their results, as well as some of their approaches is given in this section.

5.1. **Helgott, Venkatesh, Bhargava.** The study of elliptic curves over number fields is a rich area of inquiry, particularly concerning the set $E(K, S)$ of S-integral points on an elliptic curve E defined over a number field K, where S is a finite set of places of K. Helfgott and Venkatesh seek to establish bounds for the cardinality of $E(K, S)$. Embedding the Mordell–Weil lattice $E(K)$, modulo torsion, into $\mathbb{R}^{\mathrm{rank}(E(K))}$, aligns the canonical height with the square of the Euclidean norm. By viewing $E(K, S)$ as a subset of $E(K)$, Helfgott

and Venkatesh note that the points of $E(K,S)$ exhibit a propensity for separation, a notion that can be traced back to earlier work of Silverman and Gross.

Helfgott and Venkatesh propose a novel approach to bounding $E(K,S)$ by invoking the best sphere-packing results given by Kabatjanskii and Levenshtein, thereby improving upon previous bounds on elliptic curves. This method, however, is noted to have a significant drawback: its sensitivity to the rank of the Mordell-Weil lattice, which becomes problematic when considering problems like 3-torsion in quadratic class groups.

To circumvent this limitation, Helfgott and Venkatesh explore the geometry of high-dimensional Euclidean spaces, where certain packing problems exhibit a weak dependence on the dimension. This is exemplified by the work of Kabatiansky and Levenshtein, which provides an upper bound for the packing problem that grows with the angle α when $\theta = \frac{\pi}{2} - \alpha$. The important aspect here, is that α grows sublinearly. Adopting this geometric insight, Helfgott and Venkatesh introduce a sophisticated slicing technique for $E(K,S)$, optimizing the separation angle to significantly lower the bound per slice. This involves partitioning $E(K,S)$ into fibers of the reduction map to $E(\mathbb{F}_p)$, with the prime p serving as a tunable parameter. The continuous dependency of the results on the separation angle leads to the discovery that an angle of 90° is suboptimal within the interval [60°, 90°]. Thus, Helfgott and Venkatesh are able to refine their approach and achieve bounds that surpass those obtained using canonical height analogues and other traditional methods, breaking through the $h_3(D) \ll D^{1/2}$ barrier. The techniques developed herein are not confined to elliptic curves but can also be extended to curves of higher genus. Helfgott and Venkatesh reference further discussions which demonstrate improvements on the exponent $\frac{2}{d}$ found in the work of Heath-Brown and Elkies , underscoring the potential for these methods to enhance the understanding of rational and integer points on curves.

Bhargava, Shankar, Taniguchi, Thorne, Tsimerman, and Zhao improved upon this bound to prove that

$$N(E) < O_\epsilon(|\mathrm{Disc}(E)|^{0.1117\ldots+\epsilon})$$

where $N(E)$ is the number integral points on an elliptic curve.

5.2. **Alpoge and Ho.** Let $A, B \in \mathbb{Z}$ satisfy $\Delta_{A,B} := -16\left(4A^3 + 16B^2\right) \neq 0$. If $\mathcal{E}_{A,B}$ is the affine integral model $y^2 = x^3 + Ax + B$ of the associated elliptic curve $E_{A,B}$ over $\mathbb{Q}$, then the number of solutions $(x,y) \in \mathbb{Z}^2$ to $y^2 = x^3 + Ax + B$ is

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

where $v_p(n)$ is the greatest nonnegative integer such that $p^{v_p(n)} \mid n$. Considering the fact that the number of primes dividing n has maximal order $O((\log n)/\log\log n)$ and normal order $O(\log\log n)$, this bound considerably improves upon the one mentioned earlier. It is interesting to note that many people now believe that there exists an absolute constant $c > 0$ such that $\mathrm{rank}\left(E_{A,B}\right) < c$, so the rank contribution to this bound is widely believed to be negligible. The **Helfgott-Venkatesh bound**

$$N(E) < e^{O\left(\omega\left(\Delta_{A,B}\right)\right)} 1.33^{\mathrm{rank}\left(E_{A,B}\right)} \left(\log\left|\Delta_{A,B}\right|\right)^2.$$

where, $\omega(n)$ is the number of distinct prime factors of n, might be stronger than Alpöge and Ho's, depending on the prime factorization of $\Delta_{A,B}$. We can now take their minimum:

$$\ll \min \left\{ 2^{\operatorname{rank}\left(E_{A,B}\right)} \prod_{p^2 \mid \Delta_{A,B}} \min \left(4 \left\lfloor \frac{v_p\left(\Delta_{A,B}\right)}{2} \right\rfloor + 1, 7^{2^7} \right), \right.$$
$$\left. e^{O\left(\omega\left(\Delta_{A,B}\right)\right)} 1.33^{\operatorname{rank}\left(E_{A,B}\right)} \left(\log \left|\Delta_{A,B}\right|\right)^2 \right\}$$

6. Conclusion

In conclusion, we looked at Mordell equations, and discussed various upper and lower bounds for the same. The field of algebraic number theory will be forever indebted to Louis Mordell for founding the study of these beautiful elliptic curves.

References

[1] Avanesov, E.T. The representation of numbers by binary cubic forms of positive discriminant (Russian). *Acta Arith.* 14 (1967/68), 13–25. MR 37:1312

[2] Avanesov, E.T. A bound for the number of representations by a special class of binary cubic forms of positive discriminant (Russian). *Acta Arith.* 20 (1972), 17–31. MR 45:6759

[3] Ayad, M. Automorphismes d'une forme binaire cubique et représentation d'entiers. *C.R. Acad. Sc. Paris* 299 (1984), 959–962. MR 86e:11028

[4] Baker, A. Contributions to the theory of Diophantine equations. I. On the representation of integers by binary forms. *Philos. Trans. Roy. Soc. London Ser. A* 263 (1967/1968), 173–191. MR 37:4005

[5] Baker, A. and Wüstholz, G. Logarithmic forms and group varieties. *J. Reine Angew. Math.* 442 (1993), 19–62. MR 94i:11050

[6] Baulin, V.I. On an indeterminate equation of the third degree with least positive discriminant (Russian). *Tul'sk Gos. Ped. Inst. Ucen. Zap. Fiz. Math. Nauk. Vip.* 7 (1960), 138–170. MR 33:7298

[7] Belabas, K. A fast algorithm to compute cubic fields. *Math. Comp.* 66 (1997), 1213–1237. MR 97m:11159

[8] Belabas, K. and Cohen, H. Binary cubic forms and cubic number fields. Proceedings Organic Mathematics Workshop, Vancouver 1995 (*CMS Conference Proceedings* 20, 1997), 175–204. MR 98j:11084

[9] Belabas, K. and Cohen, H. Binary cubic forms and cubic number fields. *Proceedings of a Conference in Honor of A.O.L. Atkin*, 1995 (AMS/IP Studies in Advanced Mathematics 7, 1998), 191–219. MR 98m:11027

[10] Bennett, M.A. Simultaneous rational approximation to binomial functions. *Trans. Amer. Math. Soc.* 348 (1996)

[11] Helfgott, H. A., & Venkatesh, A. Integral points on elliptic curves and 3-torsion in class groups. *arXiv preprint arXiv:math/0405180* (2005).

[12] Alpöge, L., & Ho, W. The second moment of the number of integral points on elliptic curves is bounded. *arXiv preprint arXiv:1807.03761* (2022).

Email address: navvyeanand@gmail.com