AN EFFECTIVE ESTIMATE FOR THE SUM OF TWO CUBES PROBLEM

SAUNAK BHATTACHARJEE

ABSTRACT. Let $f(x,y) \in \mathbb{Z}[x,y]$ be a cubic form with non-zero discriminant, and for each integer $m \in \mathbb{Z}$, let, $N_f(m) = \#\left\{(x,y) \in \mathbb{Z}^2 : f(x,y) = m\right\}$. In 1983, Silverman proved that $N_f(m) > \Omega\left((\log|m|)^{3/5}\right)$ when $f(x,y) = x^3 + y^3$. In this paper, we obtain an explicit bound for $N_f(m)$, namely, showing that $N_f(m) > 4.2 \times 10^{-6} (\log|m|)^{11/13}$ (holds for infinitely many integers m), when $f(x,y) = x^3 + y^3$.

1. Introduction

Let $f(x,y) \in \mathbb{Z}[x,y]$ be a cubic form with non-zero discriminant, and for each integer $m \in \mathbb{Z}$, define

$$N_f(m) =: \#\left\{(x,y) \in \mathbb{Z}^2 : f(x,y) = m\right\}.$$

It has been a topic of interest to study how large can $N_f(m)$ be. In 1935, Mahler [6] proved that

$$N_f(m) > \Omega\left((\log|m|)^{1/4}\right),$$

i.e., there exists a constant $c > 0$, independent of m, such that for infinitely many integers m,

$$N_f(m) > c\,(\log|m|)^{1/4}.$$

Invoking the theory of height functions, Silverman[1] extended the idea of Mahler (Mordell, Pillai and Chowla[5]). This resulted in an improvement of the exponent from 1/4 to 1/3 and simplification of calculation as well.

More specifically, restricting $f(x,y) = x^3 + y^3$, Silverman proved that,

$$N_f(m) > \Omega\left((\log|m|)^{3/5}\right).$$

In this short note, we are interested in the special case, when $f(x,y) = x^3 + y^3$. Using the methods employed by Silverman and exploiting the properties of canonical height function on elliptic curves, we explicitly capture the implied constant in the formula.

Theorem 1.1. *Let $f(x,y) = x^3 + y^3 \in \mathbb{Z}[x,y]$. Let $m_0 \in \mathbb{Z}$ be a non zero integer. Consider the curve E with homogeneous equation*

$$E : f(x,y) = m_0\, z^3$$

2020 *Mathematics Subject Classification.* 11G50.

with the point $[1,-1,0]$ *defined over* $\mathbb{Q}$. *Using that point as origin, we give* E *the structure of an elliptic curve. Let*

$$r = \operatorname{rank} E(\mathbb{Q})$$

the rank of the Mordell-Weil group of $E/\mathbb{Q}$. *Then the following inequality holds for infinitely many integers* m,

$$N_f(m) > \frac{1}{(9 \times 2^{r+1} - 20)^{r/r+2}(\hat{h}(\bar{P}))^{r/r+2}}(\log|m|)^{r/(r+2)}$$

Where $\hat{h}(\bar{P})$ *denotes the Canonical height of a specified point* $\bar{P}$ *on the elliptic curve* $E' : Y^2 = X^3 - 432m_0^2$, *defined over* $\mathbb{Q}$, *with the base point* $[0,1,0]$ *at infinity.*

As an immediate corollary, we have the following.

Corollary 1.1. *Let* $f(x,y) = x^3 + y^3 \in \mathbb{Z}[x,y]$. *Then the following inequality holds for infinitely many integers* m,

$$N_f(m) > 4.2 \times 10^{-6}(\log|m|)^{11/13}$$

2. **Preliminaries**

We state and develop the necessary tools to prove our main theorem.

Lemma 2.1. *Let there exist integers* x, y, z *and* m_0, *such that* $x^3 + y^3 = m_0 z^3$ *with* $gcd(x,y,z) = 1$, $gcd(12m_0 z, x+y) = d$, *then* $|d| < 3^{1/3} 12 m_0^{5/2} |z|^{1/2}$.

Proof. Let,

$$da = 12m_0 z \text{ and } db = x + y, \text{ where } gcd(a,b) = 1.$$

Now, our aim is to show that,

$$d^2 | 3.12^3 m_0^2 b.$$

Let, p be a prime dividing d and having the maximum power k in d.

We will show that, p^{2k} will always divide $3.12^3 m_0^2 b$.

As, $p^k | d \Rightarrow p^k | 12m_0 z$, we have two possible cases,

$$p^k | 12m_0 \quad \text{or} \quad p|z$$

If $p^k | 12m_0$, then we are done. So, it is enough to show when $p|z$.

We have,

$$x^3 + y^3 = m_0 z^3 \Rightarrow 12^3 m_0^2 (x+y)((x+y)^2 - 3xy) = 12^3 m_0^3 z^3$$

$$\Rightarrow 12^3 m_0^2 b(d^2 b^2 - 3xy) = d^2 a^3$$

$$\Rightarrow d^2 | 3.12^3 m_0^2 bxy$$

now,

$$p|d \Rightarrow p|x + y$$

but,

on the other hand, we have $p|z$ and $gcd(x, y, z) = 1$, which clearly implies $p \nmid xy$.

As we have $d^2|3.12^3 m_0^2 bxy$, the primes dividing d and not dividing xy, should be completely contained in the factorisation of $3.12^3 m_0^2 b$.

Hence,

$$p^{2k}|3.12^3 m_0^2 b \text{ , for all prime } p \text{ dividing } d \Rightarrow d^2|3.12^3 m_0^2 b.$$

$$\Rightarrow |d|^2 \leq 3.12^3 m_0^2 |b| \Rightarrow |d|^3 \leq 3.12^3 m_0^2 |b||d| = 3.12^3 m_0^2 |x+y|$$

$$\Rightarrow |d|^6 \leq (3.12^3 m_0^2)^2 (|x+y|)^2 \leq (3.12^3 m_0^2)^2 |x^3+y^3| = (3.12^3 m_0^2)^2 m_0 |z|^3$$

$$\Rightarrow |d| < 3^{1/3} 12 m_0^{5/2} |z|^{1/2}.$$

□

Next, we state the following result due to Nèron and Tate from [2], which gives the required properties of the canonical height, we are going to apply in the proof of the theorem.

Lemma 2.2. ***(Néron, Tate)*** *Consider the canonical height or Nèron-Tate height denoted by $\hat{h}$ on an elliptic curve $E/\mathbb{Q}$, defined as the following*

$$\hat{h}(P) = \tfrac{1}{2} \lim_{k\to\infty} \left(4^{-k} h_x \left([2^k]P\right)\right) \textit{ where } h_x(P) = \log\left(H\left([x(P), 1]\right)\right) \textit{, then}$$

(a) *For all $P, Q \in E(\overline{\mathbb{Q}})$ we have*
$$\hat{h}(P+Q) + \hat{h}(P-Q) = 2\hat{h}(P) + 2\hat{h}(Q)$$
(parallelogram law).

(b) *For all $P \in E(\overline{\mathbb{Q}})$ and all $m \in \mathbb{Z}$,*
$$\hat{h}([m]P) = m^2 \hat{h}(P).$$

(c) *The canonical height $\hat{h}$ is a quadratic form on E, i.e., $\hat{h}$ is an even function, and the pairing*
$$\langle \cdot, \cdot \rangle : E(\overline{\mathbb{Q}}) \times E(\overline{\mathbb{Q}}) \to \mathbb{R}, \quad \langle P, Q \rangle = \hat{h}(P+Q) - \hat{h}(P) - \hat{h}(Q),$$
is bilinear.

(d) *Let $P \in E(\overline{\mathbb{Q}})$. Then $\hat{h}(P) \geq 0$, and $\hat{h}(P) = 0$ if and only if P is a torsion point.*

(e)
$$\hat{h} = \frac{1}{2} h_x + O(1),$$
where the $O(1)$ depends on E and x.

Proof. See pp. $248 - 251$ [2]. □

Note that, in (e) of Lemma 2.2, the implied constant is not explicit. In 1990, Silverman proved a general result which explicitly determines the constant in terms of the j-invariant and discriminant of the elliptic curve. From [3] we invoke a specific case of this result here.

Lemma 2.3. *Let, $E/\mathbb{Q}$ be an elliptic curve given by the Weierstrass equation*

$$y^2 = x^3 + B \text{ , then for every } P \in E(\bar{\mathbb{Q}})$$

$$-\tfrac{1}{6}h(B) - 1.48 \leq \hat{h}(P) - \tfrac{1}{2}h_x(P) \leq \tfrac{1}{6}h(B) + 1.576$$

Proof. See pp. 726 [3] . □

Once we have the lower bound of $N_f(m)$ in theorem 1.1, the explicit lower bound in corollary 1.1 follows from the existence of a specific elliptic curve of rank 11, which is recently given by Elkies and Rogers in [4]. We state this result as a proposition below.

Proposition 2.1. *The elliptic curve given by the equation*

$$x^3 + y^3 = m_0 z^3 \text{ or the Weierstrass form } Y^2 = X^3 - 432m_0^2$$

where, $m_0 = 1329399805658495217415723 5$ *, has the Mordell-Weil rank* 11*.*

Moreover, $\max\{h_x(P_i) \mid 1 \leq i \leq 11\} = 76.61$ *where* P_i *varies over* 11 *independent points of the Mordell-Weil group.*

Proof. For the construction of this elliptic curve and the list of 11 independent points; see pp. 192-193 [4] . The rest follows by simple computation. □

3. Proof of theorem 1.1 and corollary 1.1

We are given, that the elliptic curve $E/\mathbb{Q}$

$$E : x^3 + y^3 = m_0 z^3$$

with the base point $[1, -1, 0]$ has the Mordell-Weil rank r.

Observe that, any non-torsion point $Q = [x(Q), y(Q), z(Q)] \in E(\mathbb{Q})$ has $z(Q) \neq 0$ as the only point in $E(\mathbb{Q})$ with $z(Q) = 0$ is $Q = [1, -1, 0]$, the identity of the Mordell-Weil group $E(\mathbb{Q})$.

As the rank of $E(\mathbb{Q})$ is r, we can choose r independent points $P_1, ..., P_r$ from the free part of the group $E(\mathbb{Q})$ and for any point $Q \in E(\mathbb{Q})$, we will always write $Q = [x(Q), y(Q), z(Q)]$ with $x(Q), y(Q), z(Q) \in \mathbb{Z}$ and $gcd\,(x(Q), y(Q), z(Q)) = 1$.

Now fix a large positive integer N and for each $n = (n_1, ..., n_r) \in \mathbb{Z}^r$ with $1 \leq n_i \leq N$, consider the sum

$$Q_n = n_1 P_1 + ... + n_r P_r$$

which gives N^r distinct points in $E(\mathbb{Q})$.

Now consider

$$m = m_0 \prod_n z(Q_n)^3,$$

where the product runs over all $r-$tuples $(n_1, ..., n_r)$. Note that, $m \neq 0$ as $z(Q_n) \neq 0$.

Hence for each r-tuple $n' = (n'_1, ..., n'_r)$, the equation $f(x, y) = x^3 + y^3 = m$ has the following integral solution

$$(x, y) = \left(x(Q_{n'}) \prod_{n \neq n'} z(Q_n)^3, y(Q_{n'}) \prod_{n \neq n'} z(Q_n)^3 \right).$$

From this, we immediately get

$$N_f(m) > N^r.$$

Now, we will use the properties of height functions to give an upper bound for m in terms of N. To do this in an explicit manner, we will first transform the elliptic curve $E/\mathbb{Q}$ into it's Weierstrass form and then will proceed by using the explicit properties of the height functions on that Weierstrass form.

Consider the following morphism which takes $E/\mathbb{Q}$ to it's Weierstrass form $E'/\mathbb{Q}$

$$\Phi : E \to E'$$

defined as

$$\Phi([x, y, z]) = \begin{cases} \left[12m_0 \frac{z}{y+x}, 36m_0 \frac{y-x}{y+x}, 1\right], & z \neq 0, \\ [0, 1, 0], & z = 0. \end{cases}$$

where $E' : Y^2 = X^3 - 432\, m_0^2$ denotes the Weierstrass form of $E : x^3 + y^3 = m_0 z^3$.

Note that, Φ induces a group homomorphism $\Phi : E(\mathbb{Q}) \to E'(\mathbb{Q})$ of the corresponding Mordell-Weil groups.

Let $Q_n = [x(Q_n), y(Q_n), z(Q_n)] \in E(\mathbb{Q})$ as above. Then the height (with respect to x) of Q_n under Φ is given by

$$h_x (\Phi(Q_n)) = h (x (\Phi(Q_n))),$$

where $h(x(P) = \log (H ([x(P), 1]))$, H is the height on $\mathbb{P}^1(\mathbb{Q})$ [2, pp. 234].

As $z(Q_n) \neq 0$, we have

$$x (\Phi(Q_n)) = 12m_0 \frac{z(Q_n)}{y(Q_n) + x(Q_n)}$$

for simplicity we will write x, y, z respectively for $x(Q_n), y(Q_n)$ and $z(Q_n)$.

Hence, we can write

$$\begin{aligned} h_x(\Phi(Q_n)) &= \log\left(H\left([12m_0\frac{z}{y+x},1]\right)\right) \\ &= \log\left(H\left([12m_0 z, x+y]\right)\right) \\ &= \log\left(\max\{|\frac{12m_0 z}{d}|,|\frac{x+y}{d}|\}\right) \end{aligned}$$

where, $d = gcd(12m_0 z, x+y)$ and $\log\left(\max\{|\frac{12m_0 z}{d}|,|\frac{x+y}{d}|\}\right) \geq \log\left(\frac{|12m_0 z|}{|d|}\right)$.

So, clearly

$$h_x(\Phi(Q_n)) + \log(|d|) \geq \log(12|m_0|) + \log(|z|).$$

Now, using Lemma 2.1 we have

$$h_x(\Phi(Q_n)) \geq b_{m_0} + \frac{1}{2}\log(|z|)$$

where, b_{m_0} is a constant depending on m_0.

Further, using (e) of Lemma 2.2, we have

$$\log(|z|) \leq 4\hat{h}(\Phi(Q_n)) + c_{m_0}$$

where, c_{m_0} is another constant depending on m_0.

As, $\Phi : E(\mathbb{Q}) \to E'(\mathbb{Q})$ is group homomorphism,

$$\hat{h}(\Phi(Q_n)) = \hat{h}\left(\textstyle\sum_{i=1}^r n_i\Phi(P_i)\right).$$

Now, using (a), (b) and (d) of Lemma 2.2, we have the following estimate for $\hat{h}$.

$$\begin{aligned} \hat{h}(\Phi(Q_n)) &\leq (3\times 2^{r-1}-2)\max\{\hat{h}(n_i\Phi(P_i)) \mid 1\leq i\leq r\} \\ &\leq (3\times 2^{r-1}-2)N^2\max\{\hat{h}(\Phi(P_i)) \mid 1\leq i\leq r\} \end{aligned}$$

For simplicity of notation, write $\max\{\hat{h}(\Phi(P_i)) \mid 1\leq i\leq r\} = \hat{h}(\bar{P})$, $\bar{P} = \Phi(P_i)$ for some i.

Hence, altogether we have

$$\begin{aligned} \log(|z(Q_n)|) &\leq 4(3\times 2^{r-1}-2)N^2\hat{h}(\bar{P}) + c_{m_0} \\ &\leq (3\times 2^{r+1}-7)N^2\hat{h}(\bar{P}) \end{aligned}$$

as we can choose a large N such that $c_{m_0} \leq N^2\hat{h}(\bar{P})$.

Now, we have total N^r points Q_n on $E(\mathbb{Q})$, so for large enough N,

$$\log|m| = 3\sum_n \log|z(Q_n)| + \log(|m_0|) \leq (3^2\times 2^{r+1}-20)N^{r+2}\hat{h}(\bar{P}).$$

So, clearly we have the following estimate

$$N_f(m) > N^r \geq \frac{1}{(9 \times 2^{r+1} - 20)^{r/r+2}(\hat{h}(\bar{P}))^{r/r+2}}(\log |m|)^{r/(r+2)}$$

which concludes the proof of theorem 1.1, because we can choose arbitrarily large N, giving infinitely many choices for m.

The proof of the corollary 1.1 follows by using the elliptic curve of Proposition 2.1 in Theorem 1.1. Observe that, using Lemma 2.3 on the elliptic curve $Y^2 = X^3 - 432m_0^2$ with $m_0 =$ 1329399805658495217415723 5, we have

$$\hat{h}(\bar{P}) \leq 121.767/6 + 76.61/2 + 1.576 = 60.17$$

by putting $r = 11$, we have the required estimate holding for infinitely many integers m

$$N_f(m) > 4.2 \times 10^{-6}(\log |m|)^{11/13}.$$

4. **Concluding remarks**

It will be interesting to know, if a similar explicit bound can be obtained for other cubic forms as well. The key idea is to get a result similar to Lemma 2.1 for a general form, then using the similar methods in this article an explicit bound can be obtained. In our case, for $f(x,y) = x^3 + y^3$, the computation turned out to be much simpler which can be a bit complicated for other forms.

Acknowledgments

I am thankful to Dr. Anup Dixit and Sushant Kala for their invaluable support, guidance and numerous fruitful discussions. I would also like to thank The Institute of Mathematical Sciences, Chennai(HBNI) for supporting my stay as a visiting student.

References

[1] Silverman, J.H., 1983. Integer points on curves of genus 1. *Journal of the London Mathematical Society*, 2(1), pp.1-7.

[2] Silverman, J.H., 2009. *The arithmetic of elliptic curves* (Vol. 106, pp. xx+-513). New York: Springer.

[3] Silverman, J.H., 1990. The difference between the Weil height and the canonical height on elliptic curves. *Mathematics of computation*, 55(192), pp.723-743.

[4] Elkies, N.D. and Rogers, N.F., 2004. Elliptic curves x 3+ y 3= k of high rank. In *Algorithmic Number Theory: 6th International Symposium, ANTS-VI, Burlington*, VT, USA, June 13-18, 2004, Proceedings 6 (pp. 184-193). Springer Berlin Heidelberg.

[5] A. CHOWLA, 1933. Contributions to the analytic theory of numbers (II), *J. Indian Math. Soc*, 20, pp. 120—128.

[6] Mahler, K., 1935. On the lattice points on curves of genus 1. *Proceedings of the London Mathematical Society*, 2(1), pp.431-466.

Indian Institute of Science Education and Research, Tirupati, Andhra Pradesh, India – 517619.
Email address: saunakbhattacharjee@students.iisertirupati.ac.in