ON A QUESTION OF MORDELL

ANDREW R. BOOKER AND ANDREW V. SUTHERLAND

Abstract. We make several improvements to methods for finding integer solutions to \( x^3 + y^3 + z^3 = k \) for small values of \( k \). We implemented these improvements on Charity Engine’s global compute grid of 500,000 volunteer PCs and found new representations for several values of \( k \), including \( k = 3 \) and \( k = 42 \). This completes the search begun by Miller and Woollett in 1954 and resolves a challenge posed by Mordell in 1953.

"I think the problem, to be quite honest with you, is that you've never actually known what the question is." – Deep Thought

1. Introduction

Let \( k \) be an integer with \( k \not\equiv \pm 4 \pmod{9} \). Heath-Brown [HB92] has conjectured that there are infinitely many triples \((x, y, z)\) \( \in \mathbb{Z}^3 \) such that

\[
(1.1) \quad x^3 + y^3 + z^3 = k.
\]

Interest in this Diophantine equation goes back at least to Mordell [Mor53], who asked whether there are any solutions to (1.1) for \( k = 3 \) other than permutations of \((1, 1, 1)\) and \((4, 4, -5)\). The following year, Miller and Woollett [MW55] used the EDSAC at Cambridge to run the first in a long line of computer searches attempting to answer Mordell’s question, and also expanded the search to all positive \( k \leq 100 \).

In this paper we build on the approach of the first author in [ Boo19 ] , and find the following new solutions to (1.1):

\[
569936821221962380720^3 \left( -56993682113563493509 \right)^3 \left( -47271493453327032 \right)^3 = 3,
\]
\[
(-80538738812075974)^3 + 80435758145817515^3 + 12602123297335631^3 = 42,
\]
\[
(-3854955232171884)^3 + 383344975542639445^3 + 98422560467622814^3 = 165,
\]
\[
(-7492425935610397)^3 + 72054089679353378^3 + 35961979615356503^3 = 906.
\]

In particular, we answer Mordell’s question and complete Miller and Woollett’s search by finding at least one solution to (1.1) for all \( k \leq 100 \) for which there are no local obstructions.

The algorithm used in [ Boo19 ] is a refinement of an approach originally suggested in [ HBLTR93 ], which is based on the following observation. Let us first assume that \( |x| > |y| > |z| \) and define

\[
d := |x + y|.
\]

Then \( d \) is nonzero, and the solutions to (1.1) are precisely the triples \((x, y, z)\) for which \( z \) is a cube root of \( k \) modulo \( d \) and the integer

\[
(1.2) \quad \Delta(d, z) := 3d(4|k - z^3| - d^3)
\]

is a perfect square.

Solutions that do not satisfy \( |x| > |y| > |z| \) can be efficiently found by other means: after a suitable permutation either \( x = -y \) and \( z \) is a cube root of \( k \), or \( y = z \) and we seek a solution to the Thue equation \( x^3 + 2y^3 = k \). If we also assume \( |z| > \sqrt{k} \) then we must have \( 0 < d < \alpha|z| \), where \( \alpha = \sqrt[3]{2} - 1 \approx 0.25992 \). Solutions with \( |z| \leq \sqrt{k} \) are easily found by solving \( x^3 + y^3 = k - z^3 \) for each fixed \( z \) with \( |z| \leq \sqrt{k} \).
This leads to an algorithm that searches for solutions with $|z| \leq B$ by enumerating positive integers $d \leq \alpha B$, and for each such $d$, determining the residue classes of all cube roots of $k$ modulo $d$ and searching the corresponding arithmetic progressions for values of $z \in [-B, B]$ that make $\Delta(d, z)$ a square. With suitable optimizations, including sieving arithmetic progressions to quickly rule out integers that are not squares modulo primes in a suitably chosen set, this leads to an algorithm that requires only $O(B(\log \log B)(\log \log \log B))$ operations on integers in $[0, B]$ for any fixed value of $k$. An attractive feature of this algorithm is that it finds all solutions with $\min\{|x|, |y|, |z|\} \leq B$, even those for which $\max\{|x|, |y|, |z|\}$ may be much larger than $B$ (note that this is the case in our solution for $k = 3$).

This algorithm was used in [Boo19] to find solutions for $k = 33$ and $k = 795$, leaving only the following eleven $k \leq 1000$ unresolved:

\[(1.3)\] 42, 114, 165, 390, 579, 627, 633, 732, 906, 921, 975.

The search in [Boo19] also ruled out any solutions for these $k$ with $\min\{|x|, |y|, |z|\} \leq 10^{16}$.

Here we make several practical improvements to this method in [Boo19] that allow us to find a new solution for $k = 3$ as well as three of the outstanding $k$ listed above.

- Instead of a single parameter $B$ bounding $|z| \leq B$ and $0 < d \leq \alpha B$, we use independent bounds $d_{\text{max}}$ on $d$ and $z_{\text{max}}$ on $|z|$, whose ratio we optimize via an analysis of the expected distribution of $|z|/d$; this typically leads to a $z_{\text{max}}/d_{\text{max}}$ ratio that is 10 to 20 times larger than the ratio $1/\alpha \approx 3.847332$ used in [Boo19].
- Rather than explicitly representing a potentially large set of sieved arithmetic progressions containing candidate values of $z$ for a given $d$, we implicitly represent them as intersections of arithmetic progressions modulo the prime power factors of $d$ and auxiliary primes. This both improves the running time and reduces the memory footprint of the algorithm, allowing for much larger values of $|z|$.
- We dynamically optimize the choice of auxiliary primes used for sieving based on the values of $k$ and $d$; when $d$ is much smaller than $z_{\text{max}}$ this can reduce the number of candidate values of $z$ by several orders of magnitude.
- We exploit 3-adic and cubic reciprocity constraints for all $k \equiv \pm 3 \pmod{9}$; for the values of $k$ listed in (1.3) this reduces the average number of $z$ we need to check for a given value of $d$ by a factor of between 2 and 4 compared to the congruence constraints used in [Boo19], which did not use cubic reciprocity for $k \neq 3$.

Along the way we compute to high precision the expected density of solutions to (1.1) conjectured by Heath-Brown [HB92], and compare it with the numerical data compiled by Huisman [Hui16] for $k \in [3, 1000]$ and $\max\{|x|, |y|, |z|\} \leq 10^{15}$. The data strongly support Heath-Brown’s conjecture that (1.1) has infinitely many solutions for all $k \neq \pm 4 \pmod{9}$.

Acknowledgments. We are extremely grateful to Charity Engine for providing the computational resources used for this project, and in particular to Mark McAndrew, Matthew Blumberg, and Rytis Slatkevičius, who were responsible for running these computations on the Charity Engine compute grid.

We thank Roger Heath-Brown for several stimulating discussions; in particular, his conversation with Booker in the Nettle and Rye on 27 February 2019 informed the analysis presented in Section 4.

Sutherland also acknowledges the support of the Simons Foundation (award 550033).
2. Density computations

In this section we study Heath-Brown’s conjecture in detail. In particular, we explain how to compute the conjectured density of solutions to high precision and compare the results with available numerical data. We further study the densities of divisors $d \mid z^3 - k$ and arithmetic progressions $z (\text{mod } d)$ that occur in our algorithm, which informs the choice of parameters used in our computations.

Let $k$ be a cubefree integer with $k \geq 3$ and $k \not\equiv \pm 4 \pmod{9}$. Define $K = \mathbb{Q}(\sqrt[3]{k})$ and $F = \mathbb{Q}(\sqrt[3]{-3})$, and let $\mathfrak{o}_K$ and $\mathfrak{o}_F$ be their respective rings of integers. We have $\mathfrak{o}_F = \mathbb{Z}[\zeta_6]$, where $\zeta_6 = \frac{1+\sqrt[3]{-3}}{2}$ is a generator of the unit group $\mathfrak{o}_F^\times$. Also, $\text{Disc}(F) = -3$ and $\text{Disc}(K) = -3f^2$, where, by [Har17, Lemma 2.1],

$$f = \left( \prod_{p \mid k} p \right) \cdot \begin{cases} 1 & \text{if } k \equiv \pm 1 \pmod{9}, \\ 3 & \text{otherwise.} \end{cases}$$

We define two modular forms related to $F$ and $K$. First, let $f_1$ be the modular form of weight 1 and level $|\text{Disc}(K)|$ such that

$$\zeta_K(s) = \zeta(s)L(s, f_1).$$

It follows from the ramification description in [Har17, §2.1] that rational primes $p$ decompose into prime ideals of $\mathfrak{o}_K$ as follows (subscripts denote inertia degrees):

$$p\mathfrak{o}_K = \begin{cases} \mathfrak{p}_1\mathfrak{p}_2 & \text{if } p \equiv 2 \pmod{3} \text{ and } p \nmid k; \\ \mathfrak{p}_1\mathfrak{p}_2\mathfrak{p}_3 & \text{if } p \equiv 1 \pmod{3} \text{ and } p \nmid k \text{ and } k \equiv a \pmod{p}; \\ \mathfrak{p}_3 & \text{if } p \equiv 1 \pmod{3} \text{ and } p \nmid k \text{ and } k \equiv -a \pmod{p}; \\ \mathfrak{p}_1^2 & \text{if } p = 3 \text{ and } k \equiv \pm 1 \pmod{9}; \\ \mathfrak{p}_1^3 & \text{otherwise.} \end{cases}$$

From this data we find that the local Euler factor of $L(s, f_1)$ at $p$ is

$$L_p(s, f_1) = \frac{1}{1 - c_p(k)p^{-s} + \left( \frac{\text{Disc}(K)}{p} \right)p^{-2s}},$$

where

$$c_p(k) = \begin{cases} 2 & \text{if } p \nmid k \text{ and } p \equiv 1 \pmod{3} \text{ and } k^{3(p-1)/3} \equiv 1 \pmod{p}, \\ -1 & \text{if } p \nmid k \text{ and } p \equiv 1 \pmod{3} \text{ and } k^{3(p-1)/3} \equiv -1 \pmod{p}, \\ 1 & \text{if } p = 3 \text{ and } k \equiv \pm 1 \pmod{9}, \\ 0 & \text{otherwise.} \end{cases}$$

Now let $\sigma : F \to \mathbb{C}$ be the unique embedding for which we have $\Im(\sqrt[3]{-3}) > 0$. Let $\chi_f : (\mathfrak{o}_F/3\mathfrak{o}_F)^\times \to \mathbb{C}^\times$ be the character defined by $\chi_f(\zeta_6 + 3\mathfrak{o}_F) = \sigma(\zeta_6^{-1})$, and define $\chi_\infty(z) = \sigma(z)/|\sigma(z)|$. Let $\chi$ be the Grössencharakter of $F$ defined by

$$\chi(\alpha\mathfrak{o}_F) = \begin{cases} \chi_\infty(\alpha)\chi_f(\alpha + 3\mathfrak{o}_F) & \text{if } \alpha \in \mathfrak{o}_F \setminus \sqrt[3]{-3}\mathfrak{o}_F, \\ 0 & \text{if } \alpha \in \sqrt[3]{-3}\mathfrak{o}_F. \end{cases}$$

By automorphic induction, there is a holomorphic newform $f_2$ of weight 2 and level $|\text{Disc}(F)|N(3\mathfrak{o}_F) = 27$ such that $L(s, f_2) = L(s - \frac{1}{2}, \chi)$.

Given a prime $p \equiv 1 \pmod{3}$, let $a_p$ denote the unique integer for which $a_p \equiv 1 \pmod{3}$ and $4p = a_p^2 + 27b^2$ for some $b \in \mathbb{Z}_{\geq 0}$. Put $\alpha = \frac{a_p + 3b\sqrt[3]{-3}}{2}$ and $p = \alpha\mathfrak{o}_F$, so that $p\mathfrak{o}_F = \overline{p}\mathfrak{o}_F$. 
We have
\[
\alpha + 1 = \frac{a_p + 2 + 3b\sqrt{-3}}{2} = 3 \left( \frac{a_p + 2}{3} + b\sqrt{-3} \right) \in 3\mathcal{O}_F,
\]
so \(\chi_f(\alpha) = \chi_f(-1) = -1\). Thus, \(\chi(p) = -\frac{\sigma(\alpha)}{\sqrt{p}}\) and \(\chi(\overline{p}) = -\frac{\sigma(\alpha)}{\sqrt{p}}\), so the Euler factor of \(L(s, f_2)\) at \(p\) (in algebraic normalization) is
\[
\frac{1}{(1 - \chi(p)p^{\frac{1}{2}-s})(1 - \chi(\overline{p})p^{\frac{1}{2}-s})} = \frac{1}{1 + a_pp^{-s} + p^{1-2s}}.
\]
For a prime \(p \equiv 2 \pmod{3}\), we have \(\chi(p\mathcal{O}_F) = \chi(\infty)(p) = \chi_f(-1) = -1\), so the corresponding Euler factor is
\[
\frac{1}{1 - \chi(p\mathcal{O}_F)N(p\mathcal{O}_F)^{\frac{1}{2}-s}} = \frac{1}{1 + p^{1-2s}}.
\]
Finally, \(\chi(\sqrt{-3}) = 0\), so the Euler factor at \(p = 3\) is 1.

In summary, if we extend the definition of \(a_p\) so that \(a_p = 0\) for \(p \nmid 3\), then the Euler factor of \(L(s, f_2)\) at \(p\) is
\[
L_p(s, f_2) = \frac{1}{1 + a_pp^{-s} + \left(\frac{2}{p}\right)p^{1-2s}}.
\]

2.1. Solution density. Define
\[
\sigma_p := \lim_{e \to \infty} \frac{\#\{(x, y, z) \pmod{p^e} : x^3 + y^3 + z^3 \equiv k \pmod{p^e}\}}{p^{2e}}.
\]
Then, as calculated by Heath-Brown [HB92], we have
\[
\sigma_p = \begin{cases} 
1 + \frac{3\pi(k)}{p} - \frac{a_p}{p^2} & \text{if } p \nmid 3k, \\
1 + \frac{(p-1)a_{p^2}-1}{p^2} & \text{if } p | k \text{ and } p \neq 3, \\
\frac{1}{3}\#\{(x, y, z) \pmod{3} : x^3 + y^3 + z^3 \equiv k \pmod{9}\} & \text{if } p = 3.
\end{cases}
\]

Next, let \(h : \mathbb{R}^3 \to \mathbb{R}_{\geq 0}\) be a height function that is continuous, symmetric in its inputs, and which satisfies
- \(h(x, y, z) > 0\) when \(x^3 + y^3 + z^3 = 0\) and \(xyz \neq 0\),
- \(h(\lambda x, \lambda y, \lambda z) = |\lambda|h(x, y, z)\) for any \(\lambda \in \mathbb{R}^\times\).

The real density of solutions to \(x^3 + y^3 + z^3 = 0\) with height in the interval \(\mathcal{H} := [H_1, H_2]\) can then be computed as follows. For \(\varepsilon > 0\) define
\[
S(\varepsilon) := \left\{(x, y, z) \in \mathbb{R}^3 : h(x, y, z) \in \mathcal{H}, |x^3 + y^3 + z^3| \leq \varepsilon \right\},
\]
\[
T(\varepsilon) := \left\{(x, y, z) \in \mathbb{R}^3 : x \geq y \geq z \geq 0, h(x, -y, -z) \in \mathcal{H}, |x^3 - y^3 - z^3| \leq \varepsilon \right\},
\]
so that \(\text{vol}(S(\varepsilon)) = 12 \text{vol}(T(\varepsilon))\) for all \(\varepsilon > 0\). We may then compute
\[
\lim_{\varepsilon \to 0^+} (2\varepsilon)^{-1} \text{vol}(S(\varepsilon)) = 12 \lim_{\varepsilon \to 0^+} (2\varepsilon)^{-1} \text{vol}(T(\varepsilon)) \\
= 12 \int_0^\infty \int_0^\infty 1_{h(\sqrt[3]{y^3+z^3},-y,-z) \in \mathcal{H}} \frac{dy}{3(y^3+z^3)^{2/3}} \, dz \\
= 4 \int_1^\infty \int_1^\infty 1_{z h(\sqrt[3]{t^3+1},-t,-1) \in \mathcal{H}} \frac{dt}{(t^3+1)^{2/3}} \, dz \\
= 4 \int_1^\infty \int_1^\infty H_2(h(\sqrt[3]{t^3+1},-t,-1)) \frac{dz}{z (t^3+1)^{2/3}} = \sigma_\infty \log \frac{H_2}{H_1},
\]

(2.1)

where \(\sigma_\infty = 4 \int_1^\infty (t^3+1)^{-2/3} \, dt = \frac{2 \pi^2}{3 \Gamma(\frac{1}{3})^3}\).

Heath-Brown conjectures that the number \(n(B)\) of solutions to (1.1), up to permutation, satisfying \(\max\{|x|, |y|, |z|\} \leq B\) is asymptotic to

\[
e(B) := \rho_{sol} \log B \quad \text{as} \quad B \to \infty, \quad \text{where} \quad \rho_{sol} := \frac{1}{6} \sigma_\infty \prod_p \sigma_p.
\]

As shown above, the real density does not depend on the precise choice of the height function \(h\). We thus conjecture that the same asymptotic density applies to the solutions satisfying \(h(x, y, z) \leq B\) for any similar choice of \(h\), including, for example,

\[
\min\{|x|, |y|, |z|\}, \quad |xyz|^{\frac{1}{3}}, \quad \text{and} \quad d = \min\{|x+y|, |x+z|, |y+z|\}.
\]

Let us now define

\[
r_p := \frac{\sigma_p}{L_p(1, f_1)^3 L_p(2, f_2)L_p(2, f_1)^{-6} \zeta_p(2)^{-6} L_p(2, (\frac{2}{3}))^{-3}},
\]

where

\[
\zeta_p(s) = \frac{1}{1-p^{-s}} \quad \text{and} \quad L_p(s, (\frac{2}{3})) = \frac{1}{1-(\frac{2}{3})^{p^{-s}}}.
\]

A straightforward calculation shows that

\[
r_p = 1 - \frac{3a_p c_p(k) + O(1)}{p^3}.
\]

Since \(-a_p c_p(k)\) is the coefficient of \(p^{-s}\) in the Rankin–Selberg \(L\)-function \(L(s, f_1 \boxtimes f_2)\), we expect square-root cancellation in the product \(\prod_p r_p\); under GRH, for large \(X\) we have

\[
(2.2) \quad \prod_p \sigma_p = (1 + O(X^{-2} \log X)) L(1, f_1)^3 L(2, f_2)L(2, f_1)^{-6} \zeta(2)^{-6} L(2, (\frac{2}{3}))^{-3} \prod_{p \leq X} r_p.
\]

2.1.1. Testing Heath-Brown’s conjecture. Applying (2.2) with \(X = 10^9\) allows us to compute the solution densities \(\rho_{sol}\) to roughly 18 digits of precision for all cubefree \(k \leq 1000\). To evaluate the \(L\)-functions, we used the extensive functionality for that purpose in \textsc{PARI/GP} [Par19]. Since our goal is merely to gather some statistics, we content ourselves with a heuristic estimate of the error in this computation, though it could be rigorously certified with more work. Some examples are shown in Table [1].

We compared Huisman’s data set to an average form of Heath-Brown’s conjecture, as follows. For an integer \(K \geq 3\), define

\[
N_K(B) := \# \{(k, x, y, z) \in \mathbb{Z}^4 : x^3+y^3+z^3 = k \text{ cubefree}, 3 \leq k \leq K, \, |z| \leq |y| \leq |x| \leq B\}
\]
Table 1. Selected $\rho_{\text{sol}}$ and $\lceil \exp(1/\rho_{\text{sol}}) \rceil = \min \{ B \in \mathbb{Z} : e^{(B)} \geq 1 \}$ values for $k \leq 1000$, including the ten smallest $\rho_{\text{sol}}$ and all $k$ with $n(10^{15}) = 0$. 

Figure 1. Scatter plot of $N_{1000}(B)$ as a function of $B \in [19^{7.5}, 10^{15}]$ based on Huisman’s dataset [Hui16], compared to the line $\rho_{1000} \log(B) + C$. 

| $k$ | $\rho_{\text{sol}}$ | $\lceil \exp(1/\rho_{\text{sol}}) \rceil$ | $B = 10^5$ | $B = 10^{10}$ | $B = 10^{15}$ |
|-----|-----------------|----------------|------------|--------------|----------------|
|     |                 |                | $e(B)$ | $n(B)$ | $e(B)$ | $n(B)$ | $e(B)$ | $n(B)$ |
| 858 | 0.028504        | 1723846985902459 | 0.328 | 1 | 0.656 | 2 | 0.984 | 2 |
| 276 | 0.031854        | 43031002119138  | 0.367 | 1 | 0.733 | 1 | 1.100 | 2 |
| 390 | 0.032935        | 15358736844736  | 0.379 | 0 | 0.758 | 0 | 1.138 | 0 |
| 516 | 0.033062        | 13665771588173  | 0.381 | 0 | 0.761 | 1 | 1.142 | 1 |
| 663 | 0.033196        | 12097471960974  | 0.382 | 0 | 0.764 | 1 | 1.147 | 1 |
| 975 | 0.038722        | 164297126902    | 0.446 | 0 | 0.892 | 0 | 1.337 | 0 |
| 165 | 0.039636        | 90602378809     | 0.456 | 0 | 0.913 | 0 | 1.369 | 0 |
| 555 | 0.042706        | 14770444441     | 0.492 | 1 | 0.983 | 2 | 1.475 | 2 |
| 921 | 0.044142        | 6895540744      | 0.508 | 0 | 1.016 | 0 | 1.525 | 0 |
| 348 | 0.044632        | 5378175303      | 0.514 | 2 | 1.028 | 2 | 1.542 | 3 |
| 906 | 0.049745        | 537442063       | 0.573 | 0 | 1.145 | 0 | 1.718 | 0 |
| 579 | 0.050838        | 348939959       | 0.585 | 0 | 1.171 | 0 | 1.756 | 0 |
| 114 | 0.058459        | 26853609        | 0.673 | 0 | 1.346 | 0 | 2.019 | 0 |
| 3  | 0.061052        | 12858612        | 0.703 | 2 | 1.406 | 2 | 2.109 | 2 |
| 732 | 0.063137        | 7561540         | 0.727 | 0 | 1.454 | 0 | 2.181 | 0 |
| 633 | 0.079660        | 283059          | 0.917 | 0 | 1.834 | 0 | 2.751 | 0 |
| 33  | 0.088833        | 77422           | 1.023 | 0 | 2.045 | 0 | 3.068 | 0 |
| 795 | 0.089491        | 71273           | 1.030 | 0 | 2.061 | 0 | 3.091 | 0 |
| 42  | 0.113449        | 6732            | 1.306 | 0 | 2.612 | 0 | 3.918 | 0 |
| 627 | 0.129565        | 2249            | 1.492 | 0 | 2.983 | 0 | 4.475 | 0 |
and

$$\rho_K := \sum_{k \in \mathbb{Z} \cap [3, K]} \rho_{sol}(k).$$

Then Heath-Brown’s conjecture implies that for fixed $K$, we have $N_K(B) \sim \rho_K \log B$ as $B \to \infty$. The plot in Figure 1 compares $N_{1000}(B)$ for $B \in [10^{7.5}, 10^{15}]$, computed from Huisman’s data [Hui16], with $\rho_{1000} \log B + C$, where $\rho_{1000} \approx 363.869$ and $C \approx -679.4$ was chosen to minimize the mean square difference.

Out of 6256 points, the two plots never differ by more than 42, which gives strong evidence for Heath-Brown’s conjecture, at least on average over $k$.

2.2. Divisor and arithmetic progression densities. In this section we assume that $k \equiv \pm 3 \pmod{9}$ and derive estimates for the density of arithmetic progressions arising from cube roots of $k$ modulo $d$. Define

$$\delta_d := \begin{cases} 1 & \text{if } \exists z \in \mathbb{Z} \text{ s.t. } z^3 \equiv k \pmod{d} \text{ and } \ord_p(d) \in \{0, \ord_p(k/3)\} \forall p \mid k; \\ 0 & \text{otherwise}, \end{cases}$$

and

$$F(s) := \sum_{d=1}^{\infty} \frac{\delta_d}{d^s}.$$

By [Boo19] Lemma, we need only consider those $d$ for which $\delta_d = 1$.

For $p \nmid k$ and $e > 0$, we have $\delta_p = \frac{e_p(k)+2-(\frac{1}{3})}{3}$, so that $F(s) = \prod_p F_p(s)$, where

$$F_p(s) := \begin{cases} \left( 1 - \frac{e_p(k)+2-(\frac{1}{3})}{3p^s} \right)^{-1} & \text{if } p \nmid k; \\ 1 + p^{-\ord_p(k)s} & \text{if } p \mid \frac{k}{3}; \\ 1 & \text{if } p = 3. \end{cases}$$

For $p \nmid k$, the local factor $\frac{F_p(s)^3L_p(s, \chi)}{\zeta_p(1)^2L_p(1, \chi)}$ is $1 + O(p^{-3s})$. Therefore, $F(s)^3$ has meromorphic continuation to $\Re(s) > \frac{1}{2}$, with a pole of order 2 at $s = 1$ and no other poles in the region $\{s \in \mathbb{C} : \Re(s) \geq 1\}$. By [Kat15] Theorem 3.1, it follows that

$$\sum_{d \leq d_{\max}} \delta_d \sim \rho_{\text{div}} \frac{d_{\max}}{\sqrt{\log d_{\max}}}$$

as $d_{\max} \to \infty$, where $\rho_{\text{div}} := \frac{(\lim_{s \to 1} F(s)^3(s-1)^2)^{\frac{1}{3}}}{\Gamma(\frac{2}{3})}$. In turn, we have

$$\lim_{s \to 1} F(s)^3(s-1)^2 = \left( 1 + O(X^{-2}) \right) \frac{L(1, f_2)}{L(1, \chi)} \prod_{p \leq X} \frac{L_p^3(1, (\chi))}{\zeta_p(1)^2L_p(1, f_1)}.$$

Let us now define

$$G(s) := \sum_{d=1}^{\infty} \frac{\delta_d r_d(k)}{d^s}, \quad \text{where } r_d(k) = \# \{ z \pmod{d} : z^3 \equiv k \pmod{d} \}.$$

Then $G(s) = \prod_p G_p(s)$, where

$$G_p(s) := \begin{cases} 1 + \frac{1 + e_p(k)}{p^{s-1}} & \text{if } p \nmid k; \\ 1 + p^{(1-s)\ord_p(k)-1} & \text{if } p \mid \frac{k}{3}; \\ 1 & \text{if } p = 3. \end{cases}$$
For \( p \nmid k \) we have \( \sum_{d \leq d_{\text{max}}} \delta_p d(k) \sim \rho_{\text{ap}} d_{\text{max}} \) as \( d_{\text{max}} \to \infty \), where \( \rho_{\text{ap}} := \lim_{s \to 1} G(s)(s-1) \).

In turn, we have

\[
\rho_{\text{ap}} = \left(1 + O(X^{-2})\right) \frac{L(1, f_1)}{L(2, f_1)\zeta(2)} \prod_{p \leq X} \frac{G_p(1)L_p(2, f_1)\zeta_p(2)}{L_p(1, f_1)\zeta_p(1)}.
\]

Table 2 lists estimates \( \rho_{\text{ap}} d_{\text{max}} \) for the number \( \pi_{\text{ap}}(d_{\text{max}}) \) of arithmetic progressions modulo \( d \leq d_{\text{max}} \), as well as estimates \( \rho_{\text{div}} d_{\text{max}} / \sqrt[3]{\log d_{\text{max}}} \) for the number \( \pi_{\text{div}}(d_{\text{max}}) \) of admissible \( d \leq d_{\text{max}} \), along with the ratios of these quantities.

| \( k \) | \( \rho_{\text{ap}} d_{\text{max}} \) | \( \pi_{\text{ap}}(d_{\text{max}}) \) | \( \frac{\rho_{\text{div}} d_{\text{max}}}{\sqrt[3]{\log d_{\text{max}}} \rho_{\text{div}}} \) | \( \pi_{\text{div}}(d_{\text{max}}) \) | \( \frac{\rho_{\text{ap}}}{\rho_{\text{div}}} \frac{\sqrt[3]{\log d_{\text{max}}}}{\pi_{\text{ap}}(d_{\text{max}})} \frac{\pi_{\text{ap}}(d_{\text{max}})}{\pi_{\text{div}}(d_{\text{max}})} \) |
|-----|-----------------|-----------------|-----------------|-----------------|-----------------|
| 3   | 476709082386    | 22148041530     | 222316170600    | 2.152           | 2.144           |
| 42  | 439262042312    | 194525166395    | 195034114314    | 2.258           | 2.252           |
| 114 | 346031225026    | 169944552313    | 169697769695    | 2.036           | 2.039           |
| 165 | 398768628911    | 201824011013    | 201648107384    | 1.976           | 1.978           |
| 390 | 361424750258    | 17041108873     | 170119932464    | 2.121           | 2.125           |
| 579 | 467532879762    | 220746986113    | 221627128720    | 2.118           | 2.110           |
| 627 | 544308148137    | 238234806279    | 240026258762    | 2.285           | 2.268           |
| 633 | 510771397972    | 227368579096    | 228697959163    | 2.246           | 2.233           |
| 732 | 396862883985    | 145013347786    | 145167910326    | 2.737           | 2.734           |
| 906 | 353110285004    | 16612860358     | 165813813631    | 2.126           | 2.130           |
| 921 | 420143131383    | 212693499876    | 212924474063    | 1.975           | 1.973           |
| 975 | 461977372770    | 194140103965    | 194481735572    | 2.380           | 2.375           |

Table 2. Comparison of estimated and actual counts of arithmetic progressions modulo \( d \leq d_{\text{max}} = 10^{12} \) for various \( k \) of interest.

Remark 2.1. As can be seen in Table 2, the average number of arithmetic progressions modulo \( d \leq d_{\text{max}} \) is strikingly small; even for \( d_{\text{max}} = 10^{24} \), which is well beyond the feasible range, the average is around 3 and never above 3.5 for the \( k \) listed in Table 2.

Remark 2.2. For any fixed choice of the ratio \( R = z_{\text{max}}/d_{\text{max}} \), the total running time of our algorithm is roughly proportional to \( \rho_{\text{ap}} d_{\text{max}} \). The constant of proportionality can be estimated by running the algorithm on a suitable sample of \( d \leq d_{\text{max}} \). These estimates allow us to efficiently manage resource allocation in large distributed computations; see Section 5 for details.

3. CUBIC RECIPROCITY

In [Cas85], Cassels used cubic reciprocity to prove that whenever \( x, y, z \in \mathbb{Z} \) satisfy \( x^3 + y^3 + z^3 = 3 \) we must have \( x \equiv y \equiv z \pmod{9} \). For fixed \( d = |x+y| \) it follows that \( z \) is determined modulo 81. Colliot-Thélène and Wittenberg [CTW12] later recast this phenomenon in terms of Brauer–Manin obstructions, and showed that for any \( k \), the solutions to (1.1) are always forbidden for some residue classes globally but not locally. In this section we extend Cassels’ analysis to all cubefree \( k \equiv \pm 3 \pmod{9} \), and derive

\[^1\text{Thus strong approximation fails for (1.1), but this is never enough to forbid the existence of integer solutions outright, i.e. there is no Brauer–Manin obstruction.}\]
constraints on the residue class of \( z \) (mod \( q \)) for a certain modulus \( q \mid 27k \). We assume throughout that \( k \equiv 3 \epsilon \) (mod 9) for a fixed \( \epsilon \in \{ \pm 1 \} \).

Given \( \alpha, \beta \in \mathcal{O}_F \) with \( \beta \notin \sqrt{-3}\mathcal{O}_F \), let \( \left( \frac{a}{\beta} \right)_3 \) be the cubic residue symbol, as defined in [IR90, Ch. 9]. Put \( \zeta_3 = \frac{-1+\sqrt{-3}}{2} \in \mathcal{O}_F \). For integers \( x, y \) satisfying \( x \equiv y \equiv \epsilon \) (mod 3), define
\[
\chi_k(x, y) := \sigma(\zeta_3)^{(y-x)/3} \left( \frac{\zeta_3 x + \zeta_3^{-1} y}{k/3} \right)_3.
\]

Note that \( \chi_k(x, y) \) depends only on the residue classes of \( x, y \) (mod 3\( k \)).

**Definition 3.1.** We say that a pair \((d, z) \in \mathbb{Z}^2\) is *admissible* if there exist \( x, y \in \mathbb{Z} \) satisfying the following conditions:

1. \( x + y \equiv -\epsilon \left( \frac{4}{3} \right) d \) (mod 27\( k \));
2. \( x^3 + y^3 + z^3 \equiv k \) (mod 81\( k \));
3. \( \{\chi_k(x, y), \chi_k(x, z), \chi_k(y, z)\} \subseteq \{0, 1\} \).

Note that this definition depends only on the residue classes of \( d, z \) (mod 27\( k \)).

**Lemma 3.2.** Let \((x, y, z) \in \mathbb{Z}^3\) be a solution to (1.1), and set \( d = |x+y| \). Then \((d, z)\) is admissible.

**Proof.** Since every cube is congruent to 0 or ±1 (mod 9), we have \( x \equiv y \equiv z \equiv \epsilon \) (mod 3), so that \( x + y \equiv -\epsilon \equiv -\epsilon \left( \frac{4}{3} \right) d \) (mod 3). As \( d = |x+y| \), it follows that \( x+y = -\epsilon \left( \frac{4}{3} \right) d \), so condition (1) of the definition is satisfied. Condition (2) then follows directly from equation (1.1).

Now let \( \gamma := \epsilon(\zeta_3 x + \zeta_3^{-1} y) = -\epsilon y + \epsilon(x-y)\zeta_3 \).

By [IR90, Ch. 9, Ex. 19], we have
\[
\chi_k(x, y) = \sigma(\zeta_3)^{(y-x)/3} \left( \frac{\zeta_3 x + \zeta_3^{-1} y}{k/3} \right)_3 = \left( \frac{3}{\gamma} \right)_3 \left( \frac{\epsilon \gamma}{k/3} \right)_3 = \left( \frac{-3 \epsilon}{\gamma} \right)_3 \left( \frac{\gamma}{-\epsilon k/3} \right)_3,
\]
where the last equality follows from the fact that \((\alpha/\beta)_3\) depends only on the ideal \( \beta \mathcal{O}_F \) and \((\pm \epsilon/\beta)_3 = ((\pm \epsilon)^3/\beta)_3 = 1 \). By cubic reciprocity [IR90, Ch. 9, Ex. 20], this equals
\[
\left( \frac{-3 \epsilon}{\gamma} \right)_3 \left( \frac{-\epsilon k/3}{\gamma} \right)_3 = \left( \frac{k}{\gamma} \right)_3.
\]
Noting that \( x^3 + y^3 = (x+y)\gamma^3 \), we have \( k \equiv z^3 \) (mod \( \gamma \mathcal{O}_F \)), whence
\[
\chi_k(x, y) = \left( \frac{z^3}{\gamma} \right)_3 \in \{0, 1\}.
\]

Finally, by symmetry we also have \( \chi_k(x, z), \chi_k(y, z) \in \{0, 1\} \). □

**Lemma 3.3.** Let \( q := 27k \prod_{p \mid k, \text{ord}_p(k)=2} p^{-1} \prod_{p=2 \text{ or } e_p(2)=-1} p^{-1} \) and let \( d, z, z' \in \mathbb{Z} \) satisfy \( z' \equiv z \) (mod \( q \)). Then \((d, z)\) is admissible iff \((d, z')\) is admissible.

**Proof.** Suppose that \((d, z)\) is admissible. Let \( p \) be a prime divisor of \( 27k/q \), and consider \( z' \equiv z \) (mod \( 27k/p \)). By the Chinese remainder theorem it suffices to show that \((d, z')\) is admissible in this case.
Set \( a = (z' - z)/p \), so that \( z' = z + ap \). Let \( x, y \) be integers satisfying the conditions in Definition 3.1. Set \( x' = x + bp, y' = y - bp \) for some \( b \in 27kp^{-2}\mathbb{Z} \). Then
\[
(x')^3 + (y')^3 + (z')^3 \equiv x^3 + y^3 + z^3 + 3p[a^2z^2 - b(x^2 - y^2)] \equiv 3p[a^2z^2 - b(x^2 - y^2)] \pmod{p^2}.
\]

If \( p \mid (x^2 - y^2) \) and \( p \nmid (x + y) \) then we have \( x \equiv y \pmod{p} \), \( p > 2 \) and \( p \nmid x \). Thus \( 2x^3 + z^3 \equiv 0 \pmod{p} \), so that \( 2 \equiv (-z/x)^3 \pmod{p} \). This contradicts the assumption that \( 2 \) is a cubic non-residue modulo \( p \), so we must have \( p \nmid (x^2 - y^2) \) or \( p \mid (x + y) \).

If \( p \nmid (x^2 - y^2) \) then we may choose \( b \) so that \( b(x^2 - y^2) \equiv az^2 \pmod{p} \), while if \( p \mid (x + y) \) then \( p \mid z \) and any choice of \( b \) suffices. It follows that
\[
(x')^3 + (y')^3 + (z')^3 \equiv k \pmod{81k}.
\]
Moreover, we have \( \chi_k(x', y') = \chi_k(x, y), \chi_k(x', z') = \chi_k(x, z) \) and \( \chi_k(y', z') = \chi_k(y, z) \), by inspection. Thus \( (d, z') \) is admissible, as desired.

Thus, the definition of admissibility factors through \( \mathbb{Z}/27k\mathbb{Z} \times \mathbb{Z}/q\mathbb{Z} \).

**Example 3.4.** The following table shows the average density of admissible residues \( z \pmod{q} \) among all locally permitted residues, the ratio

\[
\frac{\sum_{d \pmod{27k}} \#\{z \pmod{q} : (d, z) \text{ is admissible}\}}{\sum_{d \pmod{27k}} \#\{z \pmod{q} : \exists x \pmod{q} \text{ s.t. } x^3 + (d - x)^3 + z^3 \equiv k \pmod{3q}\}}
\]

for a few \( k \) of interest:

| \( k \)   | 3     | 33    | 42    | 114   | 633   |
|--------|-------|-------|-------|-------|-------|
| density| 0.250 | 0.590 | 0.970 | 0.962 | 0.585 |

Although the improvement is modest for some \( k \), those cases still benefit from imposing local constraints \( \pmod{q} \), some of which were not used in [Boo19]; in particular, passing from mod 9 solutions to mod 81 solutions reduces the density by a factor of 4/9.

### 3.1. Algorithm

Let \( k \equiv 3 \pmod{9} \) be a positive integer, and for each positive integer \( m \), let
\[
C(m) := \{z + m\mathbb{Z} : z^3 \equiv k \pmod{m}\} \subseteq \mathbb{Z}/m\mathbb{Z}
\]
denote the set of cube roots of \( k \) modulo \( m \). Let \( P \) be the set of primes \( p \nmid k \) for which \( \#C(p) > 0 \); for \( p \in P \) we then have \( \#C(p) = 3 \) if \( p \equiv 1 \pmod{3} \) and \( \#C(p) = 1 \) otherwise.

Let \( A \) be a set of small auxiliary primes \( p \nmid k \) whose product exceeds \( d_{\max}z_{\max} \); in practical computations we may take \( A \) to be the primes \( p < 256 \) not dividing \( k \). Let \( s := \epsilon (\frac{4}{3}) \), so that any solution to (1.1) with \( d = |x + y| \) has \( \text{sgn} \ z = s \), and for positive integers \( d \) and primes \( p \nmid dk \) define
\[
S_d(p) := \left\{ z + p\mathbb{Z} : 3d(4s(z^3 - k) - d^3) \equiv \square (\pmod{p}) \right\}
\]
if \( p > 2 \),
\[
\{k + d + 2\mathbb{Z}\}
\]
if \( p = 2 \).

Finally, let \( c_1 > c_0 > 1 \) and \( c_2 > 1 \) denote integers that we will choose to optimize performance (typically \( c_0 \approx 4, c_1 \approx 50, \) and \( c_2 \approx 6 \)), and let \( q \) be the divisor of \( 27k \) defined in Lemma 3.3.

**Algorithm 3.5.** Given \( k, d_{\max}, z_{\max} \in \mathbb{Z}_{>0} \) with \( k \equiv 3 \pmod{9} \), enumerate all pairs \((d, z) \in \mathbb{Z}^2 \) for which there exist \((x, y, z) \in \mathbb{Z}^3 \) satisfying (1.1) with \( |x| > |y| > |z| \), \( \sqrt{k} < |z| \leq z_{\max} \), and \( |x + y| = d \leq d_{\max} \) as follows:

Recursively enumerate all positive integers \( d_0 = p_1^{e_1} \cdots p_n^{e_n} \leq d_{\max} \), where \( p_1 > \cdots > p_n \) are primes in \( P \) and \( e_i \in \mathbb{Z}_{>0} \). For each such \( d_0 \) do the following:
1. For each positive divisor $d_1$ of $k/3$ with $\gcd(d_1, k/d_1) = 1$, set $d := d_0d_1$ and let $A_d(q)$ be the set of $z + q\mathbb{Z}$ for which $(d, z)$ is admissible.

2. Set $a := 1$, and if $c_1d_0 < z_{\text{max}}$ then order the $p \nmid d$ in $\mathbb{A}$ by $\log \#S_d(p) / \log p$, and while $c_0d_0pa < z_{\text{max}}$ replace $a$ by $pa$, where $p$ is the next prime in the ordering.

3. Let $b$ be the product of $c_2$ primes $p \in A$ not dividing $da$, chosen either using the ordering computed in the previous step or a fixed order.

4. Set $m := d_0ga$, and let $\mathcal{Z}(m)$ be the subset of $\mathbb{Z}/m\mathbb{Z}$ that is identified with $C(p_{e_1}^{n_1}) \times \cdots \times C(p_{e_n}^{n_n}) \times A_d(q) \times \prod_{p|\mu} S_d(p)$ via the Chinese remainder theorem. Let

$$
\mathcal{Z}(m, s, z_{\text{max}}) := \{z \in \mathbb{Z} : z + m\mathbb{Z} \in \mathcal{Z}(m), \ sgn z = s, \ \text{and} \ |z| \leq z_{\text{max}}\}.
$$

For each $z \in \mathcal{Z}(m, s, z_{\text{max}})$, if $z + p\mathbb{Z}$ lies in $S_d(p)$ for all $p \mid b$, check if $\Delta(d, z)$ is square, and if so output the pair $(d, z)$.

**Remarks 3.6.** The following remarks apply to the implementation of Algorithm [3.5]

- The algorithm can be easily parallelized by restricting the range of $p_1$ and, for very small values of $p_1$, fixing $p_1$ and restricting the range of $p_2$.
- The recursive enumeration of $d_0 = p_1^{e_1} \cdots p_n^{e_n}$ ensures that typically only the value of $p_n^{e_n}$ changes from one $d_0$ to the next, allowing the product $C(p_1^{e_1}) \times \cdots \times C(p_n^{e_n})$ to be updated incrementally rather than recomputed for each $d_0$.
- The sets $C(p^e)$ are precomputed for each $p \in P$ with $p \leq \sqrt{d_{\text{max}}}$, as are the sets $A_d(q)$ for each $d \in \{1, \ldots, q - 1\}$ not divisible by 3, and the sets $S_d(p)$ for each $p \in A$ and $d \in \{1, \ldots, p - 1\}$. This allows the sets $\mathcal{Z}(m)$ to be enumerated quickly.
- The sets $\mathcal{Z}(m)$ are never stored in memory; they are enumerated via an explicit application of the Chinese remainder theorem.
- For $p \in A$ the precomputed sets $S_d(p)$ for $d \in \{1, \ldots, p - 1\}$ are also stored as bitmaps, as are Cartesian products of pairs of these sets and certain triples; this facilitates testing if $z + p\mathbb{Z}$ lies in $S_d(p)$ for $p \mid b$.

**Example 3.7.** For $k = 33$ and $d = 5$ we have $\mathcal{C}(d) = \{2\}$ and sgn $z = +1$. For $z_{\text{max}} = 10^{16}$ this leaves $2 \times 10^{15}$ candidate pairs $(5, z)$ to check. We have $A_d(q) = 14$ with $q = 891$, which reduces this to approximately $3.143 \times 10^{13}$. The table below shows the benefit of including additional primes $p \mid a$.

| $p \mid a$ | #$S_d(p)$ | #$\mathcal{Z}(m)$ | $m$ | #$\mathcal{Z}(m, s, z_{\text{max}})$ |
|---|---|---|---|---|
| – | – | 14 | 4455 | 3.143 $\times 10^{13}$ |
| 2 | 1 | 14 | 8910 | 1.571 $\times 10^{13}$ |
| 7 | 1 | 14 | 62370 | 2.245 $\times 10^{12}$ |
| 13 | 3 | 14 | 810810 | 5.180 $\times 10^{11}$ |
| 17 | 9 | 378 | 13783770 | 2.742 $\times 10^{11}$ |
| 23 | 12 | 4536 | 317026710 | 1.431 $\times 10^{11}$ |
| 29 | 15 | 68040 | 9193774590 | 7.401 $\times 10^{10}$ |
| 43 | 19 | 1292760 | 395332307370 | 3.270 $\times 10^{10}$ |
| 67 | 27 | 34904520 | 26487264593790 | 1.318 $\times 10^{10}$ |
| 103 | 43 | 1500894360 | 2728188253160370 | 5.501 $\times 10^{9}$ |

The net gain is a factor of more than 363541 over the naïve approach; we gain a factor of about 63 from cubic reciprocity and local constraints mod $q$, and a factor of about 5712
Given a large solution (of the Huisman data set with 10 hypothesis, we plotted the cumulative distribution of $R$. Hence, for any $d$ small, we need to consider for small values of $d$ a negligible proportion of the total computation.

Remark 3.8. With CRT enumeration, we avoid the need to store the sets $Z(m)$, analogs of which were explicitly constructed in [Boo19]. This greatly reduces the memory required when $d$ is small. In this way, we no longer rely on computations of integral points on the elliptic curve defined by (1.2) to rule out very small values of $d$. Nevertheless, we note that one can improve on the integral point search carried out in [Boo19], using a trick of Bremner [Bre95] to pass to a 3-isogenous curve. Using this approach we were able to unconditionally rule out any solutions to (1.1) with $d \leq 100$ for the $k$ listed in (1.3), and with $d \leq 20,000$ assuming the GRH. It is thus now possible to rigorously certify (under GRH) Bremner’s heuristic search of the same region in 1995.

4. HEURISTICS

In this section we present a heuristic analysis of the distribution of solutions to (1.1) for a fixed $k$. We then use this to optimize the choice of the ratio $R := z_{max}/d_{max}$.

From (2.1) we see that on $V = \{ (x, y, z) \in \mathbb{R}^3 : x^3 + y^3 + z^3 = k, \ |x| \geq |y| \geq |z| \}$, the projective point $[x : y : z] \in \mathbb{P}^2(\mathbb{R})$ lies close to the Fermat curve $x^3 + y^3 + z^3 = 0$. We conjecture that for fixed $k$, the ratios $y/z$ are distributed as above, i.e. the proportion of points (ordered by any height function as in (2.1) with $y/z \in [t_1, t_2]$ is approximately (4.1).

Let’s assume that this is the case and work out the distribution of $r := \frac{y}{x+y}$ for $(x, y, z) \in V$. We have

$$- \frac{y}{x} = \frac{2r^3 + 1 - \sqrt{12r^3 - 3}}{2(r^3 - 1)} \quad \text{and} \quad - \frac{z}{x} = \frac{r(\sqrt{12r^3 - 3} - 3)}{2(r^3 - 1)},$$

so that

$$t := \frac{y}{z} = \frac{\sqrt{12r^3 - 3} - 3}{6r} \quad \text{and} \quad (t^3 + 1)^{-2/3} \frac{dt}{dr} = \frac{3}{4r^3 - 1}.$$ 

Hence, for any $R \geq \alpha^{-1}$ we have

$$\Pr[r \leq R] = 1 - \Pr[r > R] = 1 - 4\sigma^{-1}_\infty \int_R^\infty \sqrt{\frac{3}{4r^3 - 1}} \ dr = 1 - cK(R),$$

where $c = 4\sqrt{3}\sigma^{-1}_\infty = 6\sqrt{3}\Gamma(2/3)\Gamma(1/3)^2 = 1.96084321968938583\ldots$ and

$$K(R) := \int_R^\infty \frac{dr}{\sqrt{4r^3 - 1}} = R^{-1/2} \sum_{j=0}^{\infty} \frac{(j-\frac{1}{2})}{1 + 6j} (4R^3)^{-j}.$$ 

Thus, the values of $1 - cK(r)$ should be uniformly distributed on $[0, 1]$. To test this hypothesis, we plotted the cumulative distribution of $1 - cK(-z/(x+y))$ over the points of the Huisman data set with $10^{7.5} < |x| \leq 10^{15}$ versus that of a uniform random variable; see Figure 2.

Example 4.1. For our solution to $x^3 + y^3 + z^3 = 3$ we have

$$r \approx 4.36 \times 10^6 \quad \text{and} \quad cK(r) \approx 9.39 \times 10^{-4},$$
so this solution was an approximately 1-in-1000 event. This is also reflected by the fact that the solution is highly skewed, with $x$ and $y$ much larger than $z$.

We use the above to optimize the choice of $R = z_{\text{max}}/d_{\text{max}}$ as follows. We assume that a given divisor $d \in \mathbb{Z}_{>0}$ occurs with probability $\kappa_d/d$, where $\kappa_d$ is an arithmetic factor (depending on $k$) encoding the local solubility, in such a way that

$$\sum_{d \leq x} \kappa_d = \rho x + O(x/\log^2 x), \quad \text{for some constant } \rho > 0.$$

By partial summation it follows that there exists $C$ such that

$$\sum_{d \leq x} \frac{\kappa_d}{d} \log x + C + o(1) \quad \text{and} \quad \sum_{d \leq x} \kappa_d f(d) = (\rho + o(1)) \int_0^x f(u) \, du \quad \text{as } x \to \infty,$$

for any monotonically decreasing function $f$ satisfying $f(u) \asymp u^{-s}$ for some $s \in (0, 1)$. In turn, we expect to find $z$ corresponding to $d \leq d_{\text{max}}$ with probability $1 - cK(z_{\text{max}}/d)$. Hence, the number of solutions that we expect to find is

$$\sum_{d \leq d_{\text{max}}} \frac{\kappa_d}{d} \left(1 - cK\left(\frac{z_{\text{max}}}{d}\right)\right) = \rho \log d_{\text{max}} + C + o(1) - (\rho + o(1))c \int_0^{d_{\text{max}}} K\left(\frac{z_{\text{max}}}{u}\right) \frac{du}{u}.$$

Taking $d_{\text{max}} = \alpha z_{\text{max}}$ recovers Heath-Brown’s conjecture, provided that $\rho = \rho_{\text{sol}}$.

Next, suppose that the total running time is $T(d_{\text{max}}, z_{\text{max}})$, and let $T_d$ and $T_z$ denote its partial derivatives. Let $d_{\text{max}}$ be defined implicitly in terms of $R = z_{\text{max}}/d_{\text{max}}$ so that
Differentiating with respect to $R$ so that 

$$ T(d_{\text{max}}, Rd_{\text{max}}) = \text{constant}. $$

We seek to maximize the expected solution count, which to leading order is 

$$ \rho \log d_{\text{max}} + C - \rho c \int_{R}^{\infty} K(r) \frac{dr}{r}. $$

Differentiating with respect to $R$, we have 

$$ T_d(d_{\text{max}}, Rd_{\text{max}}) \frac{\partial d_{\text{max}}}{\partial R} + T_z(d_{\text{max}}, Rd_{\text{max}}) \left( d_{\text{max}} + R \frac{\partial d_{\text{max}}}{\partial R} \right) = 0. $$

From Table 3 we can see that for $k = 3$ and various values of $R$ and $d_{\text{max}}$.

| $R$ | $d_{\text{max}}$ | $z_{\text{max}}$ | $T_d$ | $T_z$ | $T_d/T_z$ | $C_R$ |
|-----|----------------|----------------|------|------|---------|-------|
| 32  | $2^{25}$      | $2^{40}$      | 2.804 $\times 10^{-08}$ | 2.359 $\times 10^{-10}$ | 118.9  | 60.3  |
| 32  | $2^{20}$      | $2^{45}$      | 2.738 $\times 10^{-08}$ | 2.247 $\times 10^{-10}$ | 121.8  | 60.3  |
| 32  | $2^{25}$      | $2^{50}$      | 2.922 $\times 10^{-08}$ | 2.175 $\times 10^{-10}$ | 134.4  | 60.3  |
| 32  | $2^{50}$      | $2^{55}$      | 3.113 $\times 10^{-08}$ | 2.150 $\times 10^{-10}$ | 144.8  | 60.3  |
| 32  | $2^{55}$      | $2^{60}$      | 3.678 $\times 10^{-08}$ | 2.100 $\times 10^{-10}$ | 175.2  | 60.3  |
| 64  | $2^{25}$      | $2^{41}$      | 3.140 $\times 10^{-08}$ | 1.813 $\times 10^{-10}$ | 173.2  | 197.1 |
| 64  | $2^{40}$      | $2^{46}$      | 2.771 $\times 10^{-08}$ | 1.730 $\times 10^{-10}$ | 160.2  | 197.1 |
| 64  | $2^{45}$      | $2^{51}$      | 3.112 $\times 10^{-08}$ | 1.613 $\times 10^{-10}$ | 192.9  | 197.1 |
| 64  | $2^{50}$      | $2^{56}$      | 3.187 $\times 10^{-08}$ | 1.506 $\times 10^{-10}$ | 211.6  | 197.1 |
| 64  | $2^{55}$      | $2^{61}$      | 3.862 $\times 10^{-08}$ | 1.612 $\times 10^{-10}$ | 239.6  | 197.1 |
| 128 | $2^{25}$      | $2^{42}$      | 3.749 $\times 10^{-08}$ | 1.238 $\times 10^{-10}$ | 302.8  | 618.5 |
| 128 | $2^{40}$      | $2^{47}$      | 3.407 $\times 10^{-08}$ | 1.216 $\times 10^{-10}$ | 280.2  | 618.5 |
| 128 | $2^{45}$      | $2^{52}$      | 3.826 $\times 10^{-08}$ | 1.530 $\times 10^{-10}$ | 250.1  | 618.5 |
| 128 | $2^{50}$      | $2^{57}$      | 3.768 $\times 10^{-08}$ | 1.185 $\times 10^{-10}$ | 318.0  | 618.5 |
| 128 | $2^{55}$      | $2^{62}$      | 4.096 $\times 10^{-08}$ | 1.091 $\times 10^{-10}$ | 375.4  | 618.5 |

Table 3. $T_d/T_z$ vs $C_R$ for various values of $d_{\text{max}}$ and $R = z_{\text{max}}/d_{\text{max}}$ for $k = 3$. 
5. Computational results

5.1. Implementation. We implemented the algorithm described in Section 3.1 using the gcc C compiler [GCC19] and the primesieve library for fast prime enumeration [Wal19]. We parallelized by partitioning the set of primes \( p \leq d_{\text{max}} \) into sub-intervals \([p_{\text{min}}, p_{\text{max}}]\) of suitable size, with the work distributed across jobs that checked all the \((d, z)\) candidates with the largest prime factor \( p_1 \mid d \) lying in the assigned interval. Each job was run on a separate machine, with local parallelism achieved by distributing the \( p_1 \) across available cores (and for small values of \( p_1 \) also distributing the \( p_2 \)), as noted in Remarks 3.6. When choosing the number of jobs and the sizes of the intervals \([p_{\text{min}}, p_{\text{max}}]\) we use the \( \rho_{\text{ap}} \) density estimates derived in Section 2.1, as noted in Remark 2.2.

We used a standard Tonelli–Shanks approach to computing cube roots modulo primes; this involves computing a discrete logarithm in the 3-Sylow subgroup of \((\mathbb{Z}/p\mathbb{Z})^\times\), using \( O(1) \) group operations on average, and \( O(1) \) exponentiations. Hensel lifting was used to compute cube roots modulo prime powers; these were precomputed and cached for all prime powers up to \( \min\{p_{\text{max}}, \sqrt{d_{\text{max}}}\} \). For the the values of \( d_{\text{max}} \) that we used, this precomputation typically takes just a few seconds and the cache size is well under one gigabyte. We use Montgomery representation [Mon85] for performing arithmetic in \((\mathbb{Z}/p\mathbb{Z})^\times\), but switch to standard integer representation and use Barrett reduction [Bar87] during CRT enumeration of cube roots of \( k \) modulo \( d \), and when sieving arithmetic progressions via auxiliary primes.

For the \( k \) of interest, the sets \( A_d(q) \) giving constraints modulo the integer \( q \) defined in Lemma 3.3 for admissible pairs \((d, z)\) were precomputed and cached; again this takes only a few seconds for the largest values of \( k \). In order to avoid using arithmetic progressions of modulus larger than \( z_{\text{max}} \) we project these constraints to residue classes modulo a suitably chosen divisor of \( q \) when \( qd > z_{\text{max}} \).

For the computations run on Charity Engine’s compute grid we used the cygwin dynamic link library [Cyg19] to create a Microsoft Windows executable.

5.2. Computations. In September 2019 we ran computations for the eleven unresolved \( k \leq 1000 \) listed in (1.3) on Charity Engine’s crowd-sourced compute grid consisting of approximately 500,000 personal computers. For this initial search we used \( z_{\text{max}} = 10^{17} \) and \( d_{\text{max}} = \alpha z_{\text{max}} \) to search for all solutions to (1) with \( \min\{|x|, |y|, |z|\} \leq 10^{17} \). This search yielded the solutions for \( k = 42, k = 165, \) and \( k = 906 \) listed in the introduction. We then ran a search for \( k = 3 \) using \( z_{\text{max}} = 10^{18} \) and \( d_{\text{max}} = \alpha z_{\text{max}}/9 \) and found the solution for \( k = 3 \) listed in the introduction. These computations involved a total of several hundred core-years but were completed in just a few weeks (it is difficult to give more precise estimates of the computational costs due to variations in processor speeds and resource availability in a crowd-sourced computation).

Remark 5.1. While in principle these searches rule out the existence of any solutions that were not found, we are reluctant to make any unconditional claims. Despite putting in place measures to detect failures, including counting the primes that were enumerated (these counts can be efficiently verified after the fact), there is always the possibility of undetected hardware or software errors, especially on a large network of personal computers that typically do not have error correcting memory.

In order to verify the minimality of the solution we found for \( k = 3 \), we ran a separate verification using \( z_{\text{max}} = 472715493453327032 \), equal to the absolute value of the \( z \) in our solution, and \( d_{\text{max}} = \alpha z_{\text{max}} \). This search was run on Google’s Compute Engine [Goo19] and found no solutions other than those already known. These computations were run
on 8-core (16-vCPU) instances equipped with Intel Xeon processors in the Sandybridge, Haswell, and Broadwell families running at 2.0GHz or 2.2GHz. Using 155,579 nodes the computation took less than 4 hours and used approximately 120 core-years. We detected errors in 5 of the 155,579 runs which were corrected upon re-running the computations. Barring the existence of any undetected errors, these computations rule out any smaller solutions for \( k = 3 \) other than those we now know.

To assess the benefit of the theoretical and algorithmic improvements introduced here, we searched for solutions to \( k = 33 \) using \( R = 64 \), which is close to the optimal choice for \( d_{\text{max}} \) in the range \([2^{20}, 2^{50}]\). The general search strategy we envision is to start with a value of \( d_{\text{max}} \) for which all solutions with \(|z| \leq Rd_{\text{max}}\) are known, where \( R \) is chosen optimally for \( d_{\text{max}} \). One would then successively double \( d_{\text{max}} \), adjusting \( R \) as necessary, and run a search using \( z_{\text{max}} = Rd_{\text{max}} \). If one takes care to avoid checking the same admissible \((d, z)\) twice, the total time is approximately equal to a single complete search using the final values of \( d_{\text{max}} \) and \( R \) (one expects \( R \) to be increasing). The first \( d_{\text{max}} = 2^n \) sufficient to find a solution for \( k = 33 \) with this strategy is \( d_{\text{max}} = 2^{47} \), for which we choose \( R = 64 \), yielding \( z_{\text{max}} = 2^{93} \). Using 2.8GHz Intel processors in the Skylake family, this search finds the known solution for \( k = 33 \) in 107 core-days. The search in [Boo19] using \( z_{\text{max}} = 10^{16} \) and \( d_{\text{max}} = \alpha z_{\text{max}} \) took 3145 core-days running mostly on 2.6GHz Intel processors in the Sandybridge family. After adjusting for the difference in processor speeds and \( z_{\text{max}} \) values, our new approach finds the first solution for \( k = 33 \) approximately 25 times faster.

In the future we hope to use this strategy to search for solutions for the eight \( k \leq 1000 \) that remain unresolved.

**References**

[Bar87] Paul Barrett, *Implementing the Rivest Shamir and Adleman public key encryption algorithm on a standard digital signal processor*, Advances in cryptology—CRYPTO ’86 (Santa Barbara, Calif., 1986), Lecture Notes in Comput. Sci., vol. 263, Springer, Berlin, 1987, pp. 311–323. MR 907099

[Boo19] Andrew R. Booker, *Cracking the problem with 33*, Res. Number Theory 5 (2019), no. 3, Art. 26, 6. MR 3983550

[Bre95] Andrew Brenner, *On sums of three cubes*, Number theory (Halifax, NS, 1994), CMS Conf. Proc., vol. 15, Amer. Math. Soc., Providence, RI, 1995, pp. 87–91. MR 1353923

[Cas85] J. W. S. Cassels, *A note on the Diophantine equation \( x^3 + y^3 + z^3 = 3 \)*, Math. Comp. 44 (1985), no. 169, 265–266. MR 771049

[CTW12] Jean-Louis Colliot-Thélène and Olivier Wittenberg, *Groupe de Brauer et points entiers de deux familles de surfaces cubiques affines*, Amer. J. Math. 134 (2012), no. 5, 1303–1327. MR 2975237

[Cyg19] The Cygwin Authors, *Cygwin*, 2019, https://cygwin.com.

[GCC19] The GCC Team, *GCC: The GNU Ccompiler Collection*, 7.4.0 ed., 2019, https://gcc.gnu.org.

[Goo19] Google LLC, *Google Compute Engine documentation*, 2019, https://cloud.google.com/compute/docs/.

[Har17] Robert Harron, *The shapes of pure cubic fields*, Proc. Amer. Math. Soc. 145 (2017), no. 2, 509–524. MR 3577857

[HB92] D. R. Heath-Brown, *The density of zeros of forms for which weak approximation fails*, Math. Comp. 59 (1992), no. 200, 613–623. MR 1146835

[HBLtR93] D. R. Heath-Brown, W. M. Lioen, and H. J. J. te Riele, *On solving the Diophantine equation \( x^3+y^3+z^3 = k \) on a vector computer*, Math. Comp. 61 (1993), no. 203, 235–244. MR 1202610

[Hui16] Sander G. Huisman, *Newer sums of three cubes*, arXiv:1604.07746 2016.

[IR90] Kenneth Ireland and Michael Rosen, *A classical introduction to modern number theory*, second ed., Graduate Texts in Mathematics, vol. 84, Springer-Verlag, New York, 1990. MR 1070716
[Kat15] Ryo Kato, *A remark on the Wiener-Ikehara Tauberian theorem*, Comment. Math. Univ. St. Pauli 64 (2015), no. 1, 47–58. MR 3410120

[Mon85] Peter L. Montgomery, *Modular multiplication without trial division*, Math. Comp. 44 (1985), no. 170, 519–521. MR 777282

[Mor53] L. J. Mordell, *On the integer solutions of the equation $x^2 + y^2 + z^2 + 2xyz = n$*, J. London Math. Soc. 28 (1953), 500–510. MR 0056619

[MW55] J. C. P. Miller and M. F. C. Woollett, *Solutions of the Diophantine equation $x^3 + y^3 + z^3 = k$*, J. London Math. Soc. 30 (1955), 101–110. MR 0067916

[Par19] The PARI Group, Univ. Bordeaux, *PARI/GP version 2.11.2*, 2019, available from [http://pari.math.u-bordeaux.fr/](http://pari.math.u-bordeaux.fr/)

[Wall19] Kim Walisch, *primesieve*, 2019, [https://primesieve.org](https://primesieve.org)

School of Mathematics, University of Bristol, Woodland Road, Bristol, BS8 1UG, UK

*E-mail address:* andrew.booker@bristol.ac.uk

Department of Mathematics, Massachusetts Institute of Technology, 77 Mass. Ave., Cambridge, MA 02139, USA

*E-mail address:* drew@math.mit.edu