Sums of Integer Cubes

Samir Siksek[a,1]

[a] Mathematics Institute, University of Warwick, CV4 7AL , United Kingdom

This manuscript was compiled on March 8, 2021

??

In 1956 Mordell (1) wrote

> “I do not know anything about the integer solutions of $X^3 + Y^3 + Z^3 = 3$ beyond the existence of the four sets $(1, 1, 1)$, $(4, 4, -5)$, etc.; and it must be very difficult indeed to find out anything about any other solutions. One may wonder if the problem of finding other solutions is comparable in difficulty with that of finding when an assigned sequence, e.g. 123456789, occurs in the decimal expansion of π.”

Over 60 years later, in a shocking computational breakthrough (2), another solution has just been found by Booker and Sutherland,

$$569936821221962380720^3 + (-569936821113563493509)^3 + (-472715493453327032)^3 = 3. \qquad [1]$$

Booker and Sutherland also consider the more general question of expressing a positive integer k as the sum of three integer cubes:

$$X^3 + Y^3 + Z^3 = k, \qquad X,\ Y,\ Z \in \mathbb{Z}. \qquad [2]$$

Any integer cube has to 0 or $\pm 1 \pmod 9$. It follows easily from this that Eq. (2) has no solutions for $k \equiv 4$ or $5 \pmod 9$. But what of other values k? There are no obvious bounds on the sizes of X, Y, Z, and it is natural to wonder, beyond the mere existence of solutions, whether there are finitely or infinitely many solutions. In 1954, at the behest of Mordell, Miller and Woollett (3) conducted one of the earliest mathematical experiments to be carried out on a computer. They programmed the EDSAC (*Electronic Delay Storage Automatic Calculator*) at Cambridge to search for solutions to Eq. (2) in the range $0 \le k \le 100$ and $|Z| \le |Y| \le |X| \le 3164$, and obtained a total of 436 solutions. In fact, solutions were found for all $k \not\equiv 4, 5 \pmod 9$ in the range except for

$$k = 30,\ 33,\ 39,\ 42,\ 52,\ 74,\ 75,\ 84,\ 87. \qquad [3]$$

In a review of (3), Lehmer (Mathematical Reviews [MR0067916]) took the small number of solutions as an indication that Eq. (2) has only finitely many solutions for some values of $k \not\equiv 4, 5 \pmod 9$. In 1964 a more ambitious search was carried by Gardiner, Lazarus and Stein (4) which considered solutions to Eq. (2) in the larger range $k \le 1000$ and $0 < X \le Y \le 2^{16}$. Of the outstanding values of k in the tables of Miller and Woolett, they only found a solution for $k = 87$ (see Table 1). Based on this disappointing outcome, Gardiner et al. expressed the opinion that it is unlikely that all of the missing values will turn out to be expressible as sums of three cubes, and that it would be of interest to attempt a proof that $k = 30$ cannot be so expressed.

In 1992, and contrary to the mounting evidence of computational disappointments, Heath-Brown (5) conjectured that Eq. (2) has infinitely many solutions for every $k \not\equiv 4, 5 \pmod 9$. He went much further by conjecturing an asymptotic formula for the number of solutions. Fix k and let $B > 0$. Write $N(B)$ for the number of solutions to Eq. (2) belonging to the box

$$\max\{|X|, |Y|, |Z|\} \ \le\ B. \qquad [4]$$

Heath-Brown conjectured that

$$N(B) \ \sim\ \frac{1}{9} \cdot \frac{\Gamma(1/3)^2}{\Gamma(2/3)} \left(\prod_{p \text{ prime}} \sigma_p \right) \cdot \log B. \qquad [5]$$

Here, the σ_p are given by

$$\sigma_p \ =\ \lim_{e \to \infty} \frac{\#\{(X, Y, Z) \pmod{p^e} \ :\ X^3 + Y^3 + Z^3 \equiv k \pmod{p^e}\}}{p^{2e}},$$

and interpreted as ‘p-adic densities’ of solutions to Eq. (2). Heath-Brown’s conjecture is motivated by the Hardy–Littlewood circle method, which can be rigorously used to prove such asymptotic formulae for the number of solutions when one is dealing

There are no competing interests associated with this work.

[1] Samir Siksek. E-mail: samir.siksekgmail.com

k	(X,Y,Z)	noted by	year
30	$(2220422932, -283059965, -2218888517)$	Beck, Pine, Tarrant, and Yarbrough Jensen (6) (and independently, unpublished) Bernstein	1999
33	$(8866128975287528, -8778405442862239, -2736111468807040)$	Booker (7)	2019
39	$(134476, 117367, -159380)$	Heath-Brown, Lioen and te Riele (8)	1993
42	$(-80538738812075974, 80435758145817515, 12602123297335631)$	Booker and Sutherland (2)	2021
52	$(60702901317, 23961292454, -61922712865)$	Beck, Pine, Tarrant, and Yarbrough Jensen (6)	2000
74	$(-284650292555885, 66229832190556, 283450105697727)$	Huisman (9)	2016
75	$(4381159, 435203083, -435203231)$	Bremner (10)	1993
84	$(41639611, -41531726, -8241191)$	Conn and Vaserstein (11)	1994
87	$(4271, -4126, -1972)$	Gardiner, Lazarus and Stein (4)	1964

Table 1. Solutions to Eq. (2) **for** k **belonging to the list** Eq. (3)**.**

with a much larger number of variables. The logarithmic growth in the number of solutions predicted by Heath-Brown's Eq. (5) provided an explanation for the failures of early searches to find new solutions for $k = 3$ and any solutions for $k = 30, 33, 42, \ldots$.

The problems of eliminating the gaps and extending the tables to all $k \le 1000$, and also of finding other solutions for $k = 3$, attracted the attention of many mathematicians over the past few decades, both professional and amateur. For the nine values of k left outstanding by Miller and Woollett, the eventual outcome is summarized in Table 1. Thanks to these efforts, and especially to the most recent work of Booker and Sutherland, we now have solutions for all $k \le 100$ not of the form $k \not\equiv \pm 4 \pmod 9$. Although we do not yet have enough data to provide accurate experimental confirmation for Heath-Brown's Eq. (5), Booker and Sutherland have generated enough to be able to experimentally verify a version of the conjecture averaged over many values of k. The computational successes are partly the result of better hardware, and distributed computing [*], but more importantly they are the result of the development of vastly better algorithms for searching for solutions. To search for solutions to Eq. (2) in the box specified by Eq. (4), the early algorithms had a running time of roughly $O(B^2)$. We highlight two algorithms that are substantially better, and that have been historically significant for Eq. (2).

One of these two algorithms is due to Elkies (12). Suppose one is interested in finding solutions (X, Y, Z) to Eq. (2) where $|Z|$ is very large compared to k. Then $(X/Z, Y/Z)$ is a rational point that is *close* to lying on the curve $x^3 + y^3 + 1 = 0$. Elkies' algorithm subdivides the real locus of the curve $x^3 + y^3 + 1 = 0$ into tiny arcs that can be thought of as roughly approximable by tiny line segments. The algorithm then translates the problem of finding rational points that almost lie on the tiny arc into the problem of finding a short vectors in a lattice. The latter "short vector problem" has a standard solution thanks to the algorithms of Fincke and Pohst. One advantage of Elkies' algorithm over earlier approaches is that it can deal with a range values of k simultaneously, instead of focusing on one value of k at a time. Elkies algorithm was implemented in 1999 by Daniel Bernstein and yielded many new solutions for $k \le 1000$, including one for $k = 30$.

The other historically significant algorithm is based on an approach that was initially suggested by Heath-Brown (13), and successively refined by many including Heath-Brown et al. (8), Beck et al (6), Booker (7), and Booker and Sutherland (7). Fix k, and let $d = X + Y$ where (X, Y, Z) is a solution to Eq. (2). Then $Z^3 \equiv k \pmod d$. Moreover, taking $X = d - Y$ in Eq. (2), gives a quadratic equation for Y in terms of d and Z, and the discriminant of this equation must be a square. This approach yields two constraints on Z,

$$Z^3 \equiv k \pmod d, \qquad 3d \cdot (4(k - Z^3) - d^3) \;=\; \text{square}. \tag{6}$$

These dual constraints are very strong, but the algorithmic difficulty lies in exploiting them efficiently. One bottle-neck is computing the cube roots of k modulo each of a large range of values of d. Rather than running through the values of d consecutively, Booker (7) runs through the values of d by their prime factorization. Computing cube roots modulo prime powers is relatively fast, and then the Chinese Remainder Theorem can be applied to compute the cube roots of k modulo d once one knows the cube roots of k modulo the prime power factors. Booker points out that the method in fact finds all solutions in the region

$$\min\{|X|, |Y|, |Z|\} \;\le\; B$$

in $O(B \log\log B \log\log\log B)$ arithmetic operations and table look-ups. In essence the added efficiency is partially the result of a time-space trade-off. One remarkable aspect of the algorithm is that the time dependence is on the smallest unknown and not the largest, and it does yield solutions where one of the three cubes is substantially smaller than the other two, as in Eq. (1). An significant improvement in (2), exploiting an idea originally due to Cassels, is the systematic use of cubic reciprocity to obtain congruence restrictions on the solutions. Indeed, one can rewrite Eq. (2) as

$$(X + Y)(X + \zeta Y)(X + \bar{\zeta} Y) = k - Z^3, \qquad \zeta = \frac{-1 + \sqrt{-3}}{2}.$$

It follows that k is a cubic residue modulo $X + \zeta Y$, and cubic reciprocity then gives congruence restrictions on the solution modulo a certain divisor of $27k$. For example, for $k = 3$, the restriction on the solution is $X \equiv Y \equiv Z \pmod 9$.

[*] Indeed, Booker and Sutherland ran their computations on Charity Engine's global compute grid of 500,000 volunteer PCs.

Although there is now ample evidence that Eq. (2) has solutions for each $k \not\equiv 4, 5 \pmod 9$, a proof does seem to be out of reach. We point out that even the apparently easier problem of showing that for every k the equation

$$X^3 + Y^3 + Z^3 + W^3 = k, \qquad X,\ Y, Z\ , W \in \mathbb{Z} \qquad [7]$$

has a solution is still open. In 1966, using clever polynomial identities, Dem'janenko (14) has shown that Eq. (7) has a solution for $k \not\equiv 4, 5 \pmod 9$. However, unlike Eq. (2), there is no obstruction to Eq. (7) having solutions modulo 9 when $k \equiv 4, 5 \pmod 9$. The question of showing that Eq. (7) has solutions for $k \equiv 4, 5 \pmod 9$ does seem out of reach too.

ACKNOWLEDGMENTS. Siksek is supported by the Engineering and Physical Sciences Research Council grant *Moduli of Elliptic curves and Classical Diophantine Problems* (EP/S031537/1).

1. LJ Mordell, On the integer solutions of the equation $x^2 + y^2 + z^2 + 2xyz = n$. *J. Lond. Math. Soc.* **s1-28**, 500–510 (1953).
2. A Booker, A Sutherland, On a question of mordell. *Proc. Natl. Acad. Sci.* **XXX**, 1–12 (2021).
3. JCP Miller, MFC Woollett, Solutions of the diophantine equation: $x^3 + y^3 + z^3 = k$. *J. Lond. Math. Soc.* **s1-30**, 101–110 (1955).
4. VL Gardiner, RB Lazarus, PR Stein, Solutions of the diophantine equation $x^3 + y^3 = z^3 - d$. *Math. Comp.* **18**, 408–413 (1964).
5. DR Heath-Brown, The density of zeros of forms for which weak approximation fails. *Math. Comp.* **59**, 613–623 (1992).
6. M Beck, E Pine, W Tarrant, K Yarbrough Jensen, New integer representations as the sum of three cubes. *Math. Comp.* **76**, 1683–1690 (2007).
7. AR Booker, Cracking the problem with 33. *Res. Number Theory* **5**, Paper No. 26, 6 (2019).
8. DR Heath-Brown, WM Lioen, HJJ te Riele, On solving the Diophantine equation $x^3 + y^3 + z^3 = k$ on a vector computer. *Math. Comp.* **61**, 235–244 (1993).
9. SG Huisman, Newer sums of three cubes (accessed on march 8, 2021) (2016).
10. A Bremner, On sums of three cubes in *Number theory (Halifax, NS, 1994)*, CMS Conf. Proc. (Amer. Math. Soc., Providence, RI) Vol. 15, pp. 87–91 (1995).
11. W Conn, LN Vaserstein, On sums of three integral cubes in *The Rademacher legacy to mathematics (University Park, PA, 1992)*, Contemp. Math. (Amer. Math. Soc., Providence, RI) Vol. 166, pp. 285–294 (1994).
12. ND Elkies, Rational points near curves and small nonzero $|x^3 - y^2|$ via lattice reduction in *Algorithmic number theory (Leiden, 2000)*, Lecture Notes in Comput. Sci. (Springer, Berlin) Vol. 1838, pp. 33–63 (2000).
13. DR Heath-Brown, Searching for solutions of $x^3 + y^3 + z^3 = k$ in *Séminaire de Théorie des Nombres, Paris, 1989–90*, Progr. Math. (Birkhäuser Boston, Boston, MA) Vol. 102, pp. 71–76 (1992).
14. VA Dem'janenko, Sums of four cubes. *Izv. Vysš. Učebn. Zaved. Matematika* **1966**, 64–69 (1966).