

INTEGERS AS SUMS OF THREE CUBES

Gary Walsh

gwalsh@uottawa.ca

Tutte Institute and
Dept. Math. University of Ottawa
Ottawa, Ontario, Canada

University of Debrecen Number Theory Seminar
March 25, 2022

Dedicated to Richard Guy



HISTORICAL BACKGROUND

Are all numbers which are not of the form $9n \pm 4$ the sum of *three* cubes? From the list of unknowns given in the second edition, Andrew Bremner has deleted 75 and 600; Conn & Vaserstein 84; Richard Lukes 110, 435 and 478; Kenyi Koyama 444, 501, 618, 912 and 969. Don Reble quoted $30 = 2220422932^3 - 283059965^3 - 2218888517^3$ and the website <http://www.asahi-net.or.jp/~KC2H-MSM/mathland/math04/cube01.htm> which implies that only 25 remain:

33 42 52 74 114 156 165 318 366 390 420 564 579
627 633 732 758 789 795 894 906 921 933 948 975

Noam Elkies sent 462 and many smaller representations of earlier unknowns, and he wrote

... is the representation $12 = 9730705^3 - 9019406^3 - 5725013^3$ known? Miller & Woolett found only $12 = 10^3 + 7^3 - 11^3$ and asked about the existence of further solutions, of which the above is the first. Likewise for $2 = 1214928^3 + 3480205^3 - 3528875^3$, the first instance not accounted for by the identity $2 = (6t^3 + 1)^3 - (6t^3 - 1)^3 - (6t^2)^3$.

The equation $3 = x^3 + y^3 + z^3$ has the solutions $(1, 1, 1)$ and $(4, 4, -5)$. Are there any others?

FIGURE: How Richard Guy controls people's lives
(p. 232 from UPINT.v3-2004)

HISTORICAL BACKGROUND

BEATS THE WORLD AT MATHEMATICS



LEWIS J. MORDEL

Lewis J. Mordel, High School Graduate, Wins Scholarship in Cambridge Over Competitors from Many Countries.

Lewis J. Mordel, a graduate of the Central High School, brought additional honor to his alma mater yesterday, when he was awarded a three-year scholarship in mathematics by St. John's College, Cambridge, England.

Mordel went to Cambridge with nothing but High School training and competed against graduates of schools and colleges in every part of the world. The examinations were open to all competitors, but for the first time a High School graduate was entered against college men. His entry created laughter instead of serious consideration, but at the conclusion of the examinations, which lasted four days, he stood No. 1 of 220 applicants, with an average of a 'trifle below 300.'

At the Central High School Mordel's ability along mathematical lines was regarded by the members of the faculty as phenomenal. In his Sophomore year he had completed the mathematical course provided for the four-year course and during his last two years in the school he took up the higher mathematics.

To support himself he devoted seven hours of every day to coaching his fellow-students and on one occasion stayed at a blackboard for four-and-a-half hours in an endeavor to pull a student through an examination. And the examination was passed. At the end of his Senior year he devoted his time to coaching, having no examinations to take, and in this manner earned enough money to take him to England.

He is now aiming to cover his three years' work sufficiently well to entitle him to a fellowship for four additional years.

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*.

FIGURE: Mordell's original question, *J. London Math. Soc.* 1953

HISTORICAL BACKGROUND

J.C.P. Miller (Cambridge) and
M.F.C. Woollett (Royal Aeronautical Establishment) **1953-54**

Mordell suggested a computer search for solutions ($k = 3$).

Miller and Woollett searched for integer solutions to

$$x^3 + y^3 + z^3 = k,$$

with $0 \leq k \leq 100$, $|z| \leq |y| \leq |x| \leq 3164$.

No sol'ns for $k \in \{24, 30, 33, 39, 42, 52, 74, 75, 80, 84, 87, 96\}$.

All sol'ns found for $k = 2$ satisfy
 $(x, y, z) = (6t^3 + 1, -6t^3 + 1, -6t^2)$.

HISTORICAL BACKGROUND

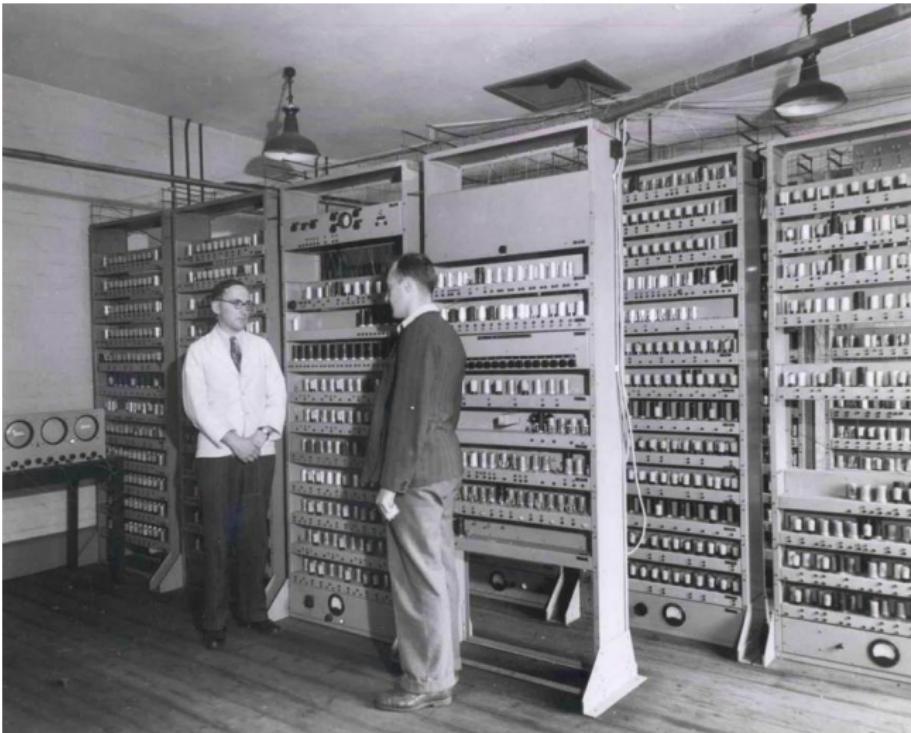


FIGURE: The Electronic Delay Storage Automatic Calculator, 1953-54

V.L. Gardiner, R.B. Lazarus, P.R. Stein (1961-63):
extended the Miller-Woollett search for $|x|$ up to 65536.

- Suggested to Stein (Los Alamos) by **Chowla** (UC-Boulder) (for $k = 3$) in 1961.
- Search was performed in 1963 on the IBM 7030 STRETCH computer at the Los Alamos Research Lab.
- For the unsolved $k \leq 100$, solutions found only for $k = 87$ and $k = 96$.

HISTORICAL BACKGROUND

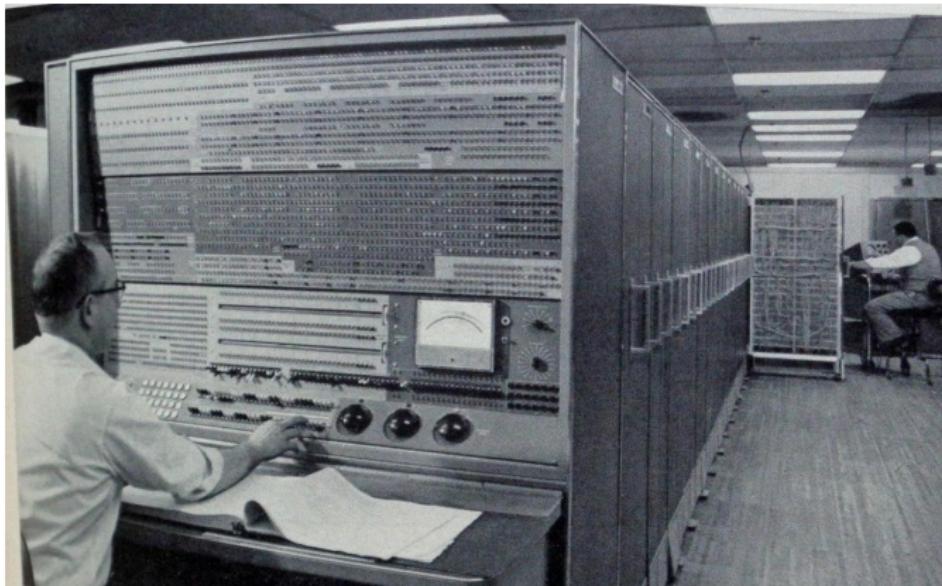


FIGURE: Los Alamos IBM 7030 STRETCH Computer, 1963

HISTORICAL BACKGROUND

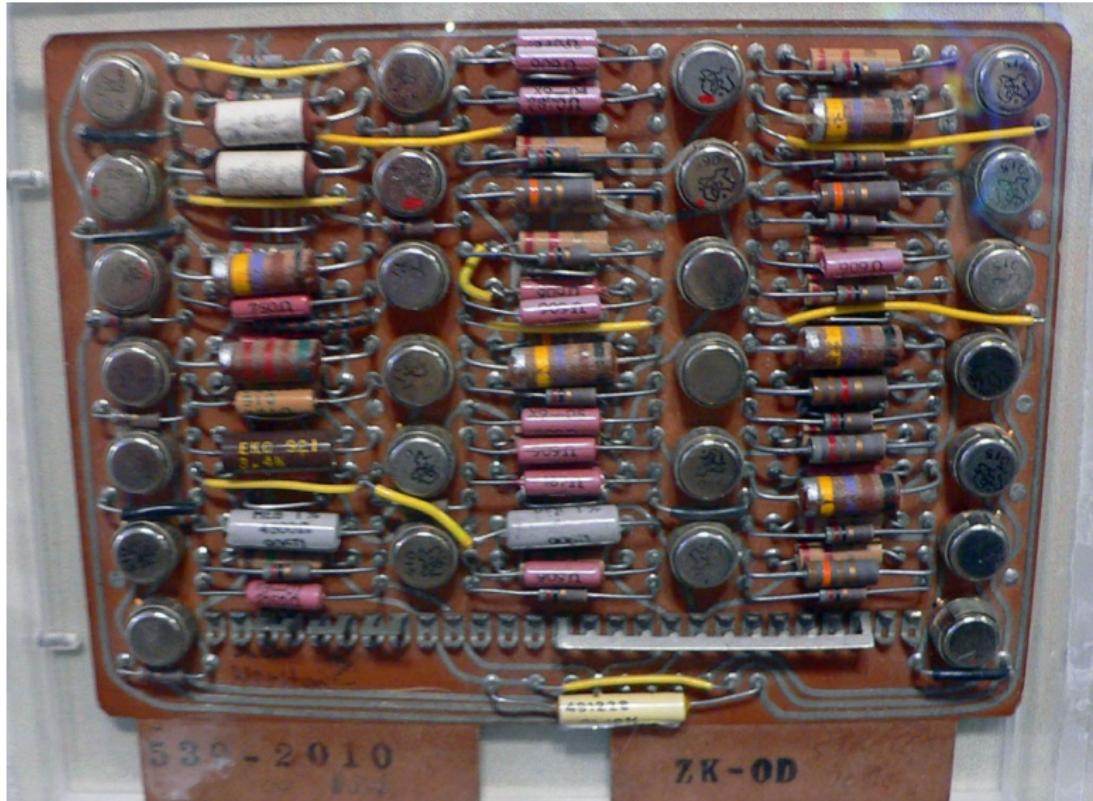


FIGURE: An IBM 7030 STRETCH circuit board

D.R. Heath-Brown, W.M. Lioen, H.J.J. te Riele (1993):

Implementation on a vector computer, increasing the search space to $|z| \leq |y| \leq |x| \leq 10^8$.

Found solutions for $k \in \{24, 80, 84\}$ and for $k = 2$, a solution not in the Miller-Woollett family:

$$3528875^3 - 3480205^3 - 1214928^3 = -2.$$

Still unsolved at this point: $k \in \{30, 33, 39, 42, 52, 74, 75\}$.

HISTORICAL BACKGROUND

Bremner (1994) rewrites the main equation as

$$(y + t)^3 - y^3 = z^3 + k$$

in the hope that a solution exists with $|t|$ small.

Putting $(X, Y) = ((12tz)^3, 72yt + 36t^2)$, the pair (X, Y) satisfy

$$Y^2 = X^3 - 432t^6 + 12^3kt^3.$$

For $k = 75$, there is an integral point of exactly the correct form for $t = -148$:

$$(X, Y) = (7780938384, 686353676466816).$$

$$453203231^3 - 453203083^3 - 4381159^3 = -75.$$

Other contributors: K. Koyama, D. Bernstein, N. Elkies, S. Huisman <https://math.mit.edu/drew/huisman.txt>

HISTORICAL BACKGROUND

References

1. [▲] ^{■■■} Davenport, H. (1939), "On Waring's problem for cubes", *Acta Mathematica*, **71**: 123–143, doi:10.1007/BF02547752 
2. [▲] ^{■■■} Mochizuki, Yu. (2007), "On Euler's hypothetical proof", *Mathematical Notes*, **82** (3): 352–356, doi:10.1134/S0001443607090088, MR 2364600 
3. [▲] ^{■■■} Mahler, Kurt (1936), "Note on Hypothesis K of Hardy and Littlewood", *Journal of the London Mathematical Society*, **11** (2): 136–138, doi:10.1112/jlms/s1-11.2.136g, MR 1547619
4. [▲] ^{■■■} Veretenskiy, A. S. (1968), "О биографии", $x^3 + y^3 + z^3 = 2u^3$ (on the equation $x^3 + y^3 + z^3 = 2u^3$), *Математический Сборник* (in Russian), **26** (4): 622–624, JFM 39.0259.02 
5. [▲] ^{■■■} ^{■■■■} Mordell, L.J. (1942), "On sums of three cubes", *Journal of the London Mathematical Society*, Second Series, **17** (3): 139–144, doi:10.1112/jlms/s1-17.3.139g, MR 00077619 
6. [▲] ^{■■■} Avagyan, Armen, Dallakyan, Gurgen (2018), "A new method in the problem of three cubes", *Journal of Computational Mathematics*, **5** (3): 45–56, arXiv:1802.06776 
7. [▲] ^{■■■} ^{■■■■} Heath-Brown, D.R., Lloren, W.M., te Riele, H. J. (1993), "On solving the Diophantine equation $x^3 + y^3 + z^3 = k$ on a vector computer", *Mathematics of Computation*, **61** (203): 235–244, Bibcode:1993Mca..61.235Hg, doi:10.2307/2152950 
8. [▲] ^{■■■} Mordell, L.J. (1953), "On the integer solutions of the equation $x^3 + y^3 + z^3 + 2xyz = n$ ", *Journal of the London Mathematical Society*, Second Series, **28**: 500–510, doi:10.1112/jlms/s1-28.4.501g, MR 0056619 
9. [▲] The equality mod 9 of numbers whose cubes sum to 3 was credited to J. W. S. Cassels by Mordell (1953), but its proof was not published until Cassels, J. W. S. (1965), "A note on the Diophantine equation $x^3 + y^3 + z^3 = k$ ", *Mathematics of Computation*, **44** (169): 265–268, doi:10.2307/20078119, JSTOR 20078119, MR 0771049 
10. [▲] ^{■■■} Miller, J. C. P., Woollett, M. F. C. (1955), "Solutions of the Diophantine equation $x^3 + y^3 + z^3 = k$ ", *Journal of the London Mathematical Society*, Second Series, **30**: 101–110, doi:10.1112/jlms/s1-30.1.101g, MR 0067916 
14. [▲] ^{■■■} Koyama, Kenji, Tsuruoka, Yukio, Sekigawa, Hiroshi (1997), "On searching for solutions of the Diophantine equation $x^3 + y^3 + z^3 = n$ ", *Mathematics of Computation*, **66** (218): 841–851, doi:10.1090/S0025-5718-97-00330-2 
15. [▲] ^{■■■} Elkies, Noam D. (2000), "Rational points near curves and small nonzero $|x^3 - y^3|$ via lattice reduction", *Algorithmic number theory* (Leiden, 2000), Lecture Notes in Computer Science, vol. 1838, Berlin, pp. 33–63, arXiv:math/0005139, doi:10.1007/10722028_20, MR 1805986 
16. [▲] ^{■■■} ^{■■■■} Baćk, Michael, Pine, Eric, Tarrant, Wayne, Yarborough Jansen, Kim (2007), "New integer representations as the sum of three cubes", *Mathematics of Computation*, **76** (259): 1683–1690, doi:10.1090/S0025-5718-07-01947-3, MR 2399759 
17. [▲] ^{■■■} ^{■■■■} Elsenhans, Andreas-Stephan, Jörg (2009), "New sums of three cubes", *Mathematics of Computation*, **78** (265): 1227–1230, doi:10.1090/S0025-5718-08-02166-6 
18. [▲] ^{■■■} ^{■■■■} Huisman, Sander G. (2016), "Newer sums of three cubes", arXiv:1604.07746 
19. [▲] ^{■■■} Booker, Andrew R. (2019), "Cracking the problem with 33", *Research in Number Theory*, **5** (26), doi:10.1007/s40993-019-0162-4, MR 3985560 
20. [▲] ^{■■■} ^{■■■■} Heath-Brown, D.R., Lloren, W.M., te Riele, H.J.J. (1993), "On solving the Diophantine equation $x^3 + y^3 + z^3 = k$ on a vector computer", *Mathematics of Computation*, **61** (203): 235–244, Bibcode:1993Mca..61.235Hg, doi:10.2307/2152950 
21. [▲] ^{■■■} ^{■■■■} Booker, Andrew R., Sutherland, Andrew V. (2020), "On a question of Mordell", arXiv:2007.01209 
22. [▲] ^{■■■} ^{■■■■} Lu, Donna (September 18, 2019), "Mathematicians find a completely new way to write the number 37", *New Scientist* 
23. [▲] ^{■■■} ^{■■■■} Haran, Brady (September 24, 2019), "3 is the sum of 3 cubes", *Numberphile* 
24. [▲] ^{■■■} Houston, Robin (September 6, 2019), "Is 42 the answer to the question 'What is 10038738812075974'?", *Plus* 
25. [▲] ^{■■■} ^{■■■■} Haran, Brady (November 6, 2015), "The uncracked problem with 33", *Numberphile* 
26. [▲] ^{■■■} ^{■■■■} Haran, Brady (May 31, 2016), "74 is cracked", *Numberphile* 
32. [▲] ^{■■■} ^{■■■■} ^{■■■■■} Sum of three cubes for 42 finally solved – using real life planetary computer, University of Bristol, September 6, 2019 
33. [▲] ^{■■■} ^{■■■■} ^{■■■■■} Miller, Sandi (September 10, 2019), "The answer to life, the universe, and everything: Mathematician finds a solution to the 65-year-old problem of three cubes", *Quanta Magazine* 
34. [▲] ^{■■■} ^{■■■■} ^{■■■■■} Lu, Donna (September 6, 2019), "Mathematicians crack elusive puzzle involving the number 42", *New Scientist* 
35. [▲] ^{■■■} ^{■■■■} ^{■■■■■} Delahaye, Jean-Paul (September 20, 2020), "For Math Fans: A Hitchhiker's Guide to the Number 42", *Scientific American* 
36. [▲] ^{■■■} ^{■■■■} ^{■■■■■} Grossman, David (September 6, 2019), "After 65 Years, Supercomputers Finally Solve This Unsolvable Math Problem", *Popular Mechanics* 
37. [▲] ^{■■■} ^{■■■■} ^{■■■■■} Quach, Kathanya (September 7, 2019), "Finally! A solution to 42 – The Answer to the Ultimate Question of Life, The Universe, and Everything?", *The Register* 
38. [▲] ^{■■■} ^{■■■■} ^{■■■■■} "Mathproblem um die Zahl 42 geknackt", *Der Zeit*, September 16, 2019 
39. [▲] ^{■■■} ^{■■■■} ^{■■■■■} "Das Mathproblem um die Zahl 42 ist geknackt", *Der Tagesspiegel*, September 16, 2019 
40. [▲] ^{■■■} ^{■■■■} ^{■■■■■} Krivmaki, Antti (September 18, 2019), "Matematiikkaan voikaa lisäksellä tuottaa vähän kavuton luvun 42", *Helsingin Sanomat* 
41. [▲] ^{■■■} ^{■■■■} ^{■■■■■} "Mathproblem um die 42 geknackt", *Der Spiegel*, September 16, 2019 
42. [▲] ^{■■■} ^{■■■■} ^{■■■■■} "Why the number 42 is the answer to life, the universe and everything", *New Zealand Herald*, September 9, 2019 
43. [▲] ^{■■■} ^{■■■■} ^{■■■■■} Firaqz, Kabir (September 20, 2019), "Explained: How a 65-year-old maths problem was solved", *Indian Express* 
44. [▲] ^{■■■} ^{■■■■} ^{■■■■■} Taschner, Klaus (September 15, 2019), "Endlich! Das Rätsel um die Zahl 42 ist gelöst!", *Der Standard* 
45. [▲] ^{■■■} ^{■■■■} ^{■■■■■} Matemáticos resuelven el enigma del número 42 planteado hace 65 años", *Las Provincias*, September 18, 2019 
46. [▲] ^{■■■} ^{■■■■} ^{■■■■■} Waerstad, Lars (October 19, 2019), "Supermaskin har løst over 60 år gammel tallgås", *Nettavisen* 
47. [▲] ^{■■■} ^{■■■■} ^{■■■■■} "A fast resolved problem can lead to a batâl of cap matematičilor temp de 65 de ani. A fast nevoie de 1 milion de ore de procesare", *Dg24*, September 16, 2019 
48. [▲] ^{■■■} ^{■■■■} ^{■■■■■} Paul, Fernanda (September 12, 2019), "Enigma da soma de 3 cubos: matemáticos encontram a solução final después de 65", *El Diario Vasco* 
53. [▲] ^{■■■} ^{■■■■} ^{■■■■■} Jesus Poblacion, Alfonso (October 3, 2019), "Matemáticos encuentran una nueva forma de llegar al número 37", *El Diario Vasco* 
54. [▲] ^{■■■} ^{■■■■} ^{■■■■■} Horner, Patrick (November 5, 2019), "Why the Sum of Three Cubes Is a Hard Math Problem", *Quanta Magazine* 
55. [▲] ^{■■■} ^{■■■■} ^{■■■■■} D'Souza, Dilip (November 28, 2019), "Waste not, there's a third way to make cubes", *LiveMint* 
56. [▲] ^{■■■} ^{■■■■} ^{■■■■■} Booker, Andrew R. (July 4, 2020), "33 and all that", *Algorithmic Number Theory Symposium* 
57. [▲] ^{■■■} ^{■■■■} ^{■■■■■} Heath-Brown, D. R. (1992), "The density of zeros of forms for which weak approximation fails", *Mathematics of Computation*, **59** (200): 613–623, doi:10.1090/s0025-5718-1992-1168305-6 
58. [▲] ^{■■■} ^{■■■■} ^{■■■■■} Poonen, Bjorn (2008), "Undecidability in number theory", *PDF*, Notices of the American Mathematical Society, **55** (3): 344–350, MR 2382621 
59. [▲] ^{■■■} ^{■■■■} ^{■■■■■} Dickson, Leonard Eugene (1920), *History of the Theory of Numbers*, Vol. II: *Diphantine Analysis*, Carnegie Institution of Washington, p. 717 
60. [▲] ^{■■■} ^{■■■■} ^{■■■■■} Balog, Antal, Bröden, Jörg (1995), "Sums of three cubes in three linked three-progressions", *Journal für die Reine und Angewandte Mathematik*, **1995** (466): 45–85, doi:10.1515/crll.1995.466.45gk, MR 1353314 
61. [▲] ^{■■■} ^{■■■■} ^{■■■■■} Deshoulieres, Jean-Marc, Hemerick, François, Landreau, Bernard (2006), "On the density of sums of three cubes", in Hess, Florian, Pauli, Sebastian, Pohst, Michael (eds.), *Algorithmic Number Theory*, 7th International Symposium, ANTS-VII, Berlin, Germany, July 23–28, 2006, Proceedings, Lecture Notes in Computer Science, vol. 4076, Berlin, Springer, pp. 141–155, doi:10.1007/11792068_11g, MR 2292521 
62. [▲] ^{■■■} ^{■■■■} ^{■■■■■} Wooley, Trevor D. (1995), "Breaking classical convexity in Waring's problem: sums of cubes and quasi-diagonal behaviour", *PDF*, *Inventiones Mathematicae*, **122** (3): 421–451, doi:10.1007/BF01231451, hdl:2027.42/46568, MR 1359596 
63. [▲] ^{■■■} ^{■■■■} ^{■■■■■} Wooley, Trevor D. (2000), "Sums of three cubes", *Mathematika*, **47** (1–2): 53–61 (2002), doi:10.1112/S002557930015710g, hdl:2027.42/152941 
64. [▲] ^{■■■} ^{■■■■} ^{■■■■■} Wooley, Trevor D. (2015), "Sums of three cubes, III", *Acta* 

Booker and Sutherland - 2019

The answer to Mordell's question is YES.

$$x = 569936821221962380720$$

$$y = 569936821113563493509$$

$$z = 472715493453327032$$

then

$$x^3 - y^3 - z^3 = 3.$$

SOME EYE-POPPING EXAMPLES

Booker - 2019

$$x = 8866128975287528$$

$$y = 8778405442862239$$

$$z = 2736111468807040$$

then

$$x^3 - y^3 - z^3 = 33.$$

Booker and Sutherland - 2021

$$x = 80538738812075974$$

$$y = 80435758145817515$$

$$z = 12602123297335631$$

then

$$x^3 - y^3 - z^3 = -42.$$

A simple observation

$$x^3 + y^3 + z^3 = k \quad (|z| < |y| < |x|)$$

with k small (typically) forces $|x| \approx |y|$.

As Bremner did, rewrite (1) as

$$x^3 - y^3 = z^3 + k,$$

and focus on $t = x - y$.

A simple observation continued

Define $t = x - y$, then t is a divisor of

$$x^3 - y^3 = z^3 + k = N_{\mathbb{Q}(k^{1/3})/\mathbb{Q}}(z + k^{1/3}).$$

"Ideally" then,

$$t = N_{\mathbb{Q}(k^{1/3})/\mathbb{Q}}(\alpha) = a^3 + b^3k + c^3k^2 - 3kabc,$$

for some $\alpha = a + bk^{1/3} + ck^{2/3} \in \mathbb{Z}[k^{1/3}]$.

(t can be used to compute z by modular cube roots and lifting, and then x, y by the quadratic formula.)

Integral Basis

For k square-free, $\{1, k^{1/3}, k^{2/3}\}$ is an integral basis.

Class Number

Cheat. I can explain!

Large Search Range

Reduction to searching over b and c only.
(recall $\alpha = a + b \cdot k^{1/3} + c \cdot k^{2/3}$)

OVERCOMING NON-UNIQUE FACTORIZATION

Although t may be a product of primes that split in $\mathbb{Z}[k^{1/3}]$, it may not be a norm.

At best, provably, t^h is a norm, where h is the class number.

Experiments show that l/t is a norm for some very small factor l .

N.T.Z. Sardari (2018):

(GRH) The least prime in an ideal class $\leq h_K^2 \log(D_K)$.

Consequence: for each $\alpha = a + bk^{1/3} + ck^{2/3}$, $N = N_{K/\mathbb{Q}}(\alpha)$, we test

$$t = N / \gcd(N, l)$$

for small $1 \leq l \leq \text{BOUND}$. (currently using $\text{BOUND} = 5$)

REDUCING THE SEARCH SPACE

If

$$t = a^3 + b^3k + c^3k^2 - 3kabc$$

and $|c|$ is large enough wrt t , then

$$|t/c^3| = |(a/c)^3 + (b/c)^3k + k^2 - 3k(a/c)(b/c)|$$

is small, and a/c *may be* close to the* real root, say λ , of

$$P(X) = X^3 - 3k(b/c)X + (k(b/c)^3 + k^2),$$

and $a \approx c\lambda$.

In fact: $a \approx c\lambda \approx -bk^{1/3} - ck^{2/3}$.

- Create α by looping over certain ranges for b, c

$$\alpha = a + bk^{1/3} + ck^{2/3}$$

(a is chosen in a small interval containing $-bk^{1/3} - ck^{2/3}$)

- compute the value N of the norm form

$$N = a^3 + b^3k + c^3k^2 - 3kabc$$

- 'try' $t = N/\gcd(N, l)$ over small integers $l \geq 1$

(i.e. use t, k to compute z by modular cube roots and lifting, and then hope the quadratic formula gives x, y from z, t).

PRELIMINARY EXAMPLES

Example 1: $k = 2$, $h = \text{class number} = 1$

$$2 = (6t^3 + 1)^3 - (6t^3 - 1)^3 - (6t^2)^3.$$

Guy asked for solutions not in this family.

$$(x, y, z) = (3528875, 3480205, 1214928)$$

(te Riele and Heath-Brown, ≈ 30 hours cpu time in 1990)

$t = 48670$ and

$$t = N_{\mathbb{Q}(2^{1/3})/\mathbb{Q}}(-2 + 23 \cdot 2^{1/3} + 17 \cdot 2^{2/3})$$

$$(z_1 = 46848 = 2^{1/3} \pmod{t}, \text{ and } z = z_1 + 24 \cdot t).$$

PRELIMINARY EXAMPLES

Example 2: $k = 7, h = 3$

Small solution: $(x, y, z) = (2, 0, 1)$.

Larger solution:

$$(x, y, z) = (17136136, 13010655, 14144042)$$

produced in the following way:

A small search eventually gives

$$\alpha = -395 + 196 \cdot 7^{1/3} + 18 \cdot 7^{2/3},$$

$$N = N(\alpha) = 20627405.$$

The method ‘tries’ $t = N/5 = 4125481$ and succeeds in producing x, y, z .

Example 2': $k = 7, h = 3$ Even larger solution:

$$(x, y, z) = (8940123359, 6427544172, 7657432774)$$

arising from

$$\alpha = 142 + 685 \cdot 7^{1/3} - 60 \cdot 7^{2/3}.$$

EXAMPLE: $k = 74$, $h = 3$

Sander Huisman, 2016: $x^3 - y^3 - z^3 = -74$, where (x, y, z)

$$= (284650292555885, 283450105697727, 66229832190556)$$

$t = x - y = 1200186858158 \neq N_{K/\mathbb{Q}}(\gamma)$ for any $\gamma \in \mathcal{O}$, **but**
 $2t = N_{K/\mathbb{Q}}(a + b \cdot 74^{1/3} + c \cdot 74^{2/3})$ for (a, b, c) in

$$\{(-56994, -20860, 8205), (33454, 7214, 2039), \\ (8592, -7232, 1295), (213402, 51340, 12137), \\ (49068, -3020, -2041), (4498468, 1071596, 255239), \\ (1830228, 435940, 103799), (10218, -3854, 539), \\ (113820, -39256, 2895)\}$$

Example 3: $k = 74$, $h = 3$ (a, b, c) $\text{floor}(-b \cdot 74^{1/3} - c \cdot 74^{2/3})$

$(-56994, -20860, 8205)$	-57044	$(**)$
$(33454, 7214, 2039)$	-66225	
$(8592, -7232, 1295)$	7536	
$(213402, 51340, 12137)$	429469	
$(49068, -3020, -2041)$	48653	$(*)$
$(4498468, 1071596, 255239)$	8997770	
$(1830228, 435940, 103799)$	-3659786	
$(10218, -3854, 539)$	6679	
$(113820, -39256, 2895)$	113782	$(**)$

Point: Search space for a is almost completely eliminated!

Example 4: $k = 109$ ($h = 3$)

Searching $\alpha = a + b \cdot 109^{1/3} + c \cdot 109^{2/3}$ can give very erratic and unpredictable results. Here we search with $|a|, |b|, |c| < 100$.

$\alpha = -56 - 16 \cdot 109^{1/3} + 90 \cdot 109^{2/3}$ gives the solution
 $(X, Y, Z) = (5, -2, -2)$,

$\alpha = -5 + 48 \cdot 109^{1/3} + 29 \cdot 109^{2/3}$ gives the solution
 $(X, Y, Z) = (-576, 514, 381)$.

HOWEVER, $\alpha = -7 + 64 \cdot 109^{1/3} + 8 \cdot 109^{2/3}$
gives the solution

$(X, Y, Z) = (-69946755, 44275762, 63448236)$.

Example 5: $k = 33$, $h = 1$

$$x = 8866128975287528, y = 8778405442862239$$

$$z = 2736111468807040, t = x - y = 87723532425289$$

$$t = N_{\mathbb{Q}(33^{1/3})/\mathbb{Q}}(102406 + 255182 \cdot 33^{1/3} - 89507 \cdot 33^{2/3})$$

Note: $-255182 \cdot 33^{1/3} + 89507 \cdot 33^{2/3} = 102367.7373\dots$

Cost: $b: \approx 5 \cdot 10^5$, $c: \approx 2 \cdot 10^5$, $a: \approx 10^2$, lift factor (31): ≈ 50
Total Search Space $\approx 5 \cdot 10^{14}$ (Booker took about 10^{16})

BOOKER-SUTHERLAND EXAMPLES

Example 6: $k = 42$, $h = 3$

$$x = 80538738812075974, y = 80435758145817515$$

$$z = 12602123297335631, t = x - y = 102980666258459$$

t is **not** a norm, however

$$2t = N_{\mathbb{Q}(42^{1/3})/\mathbb{Q}}(-473180 - 76667 \cdot 42^{1/3} + 61231 \cdot 42^{2/3})$$

$$\text{Note: } 76667 \cdot 42^{1/3} - 61231 \cdot 42^{2/3} = -473343.0184\dots$$

Cost: $b: \approx 2 \cdot 10^5$, $c: \approx 2 \cdot 10^5$, $a: \approx 5 \cdot 10^2$, lift factor
 $(122): \approx 10^2$

Total Search Space $\approx 2 \cdot 10^{15}$ (B and S took about 10^{18})

MORDELL'S QUESTION $k = 3$ ($h = 1$)

$$x = 569936821221962380720$$

$$y = 569936821113563493509$$

$$z = 472715493453327032$$

then

$$x^3 - y^3 - z^3 = 3. \quad (\text{Booker and Sutherland, 2019})$$

In this case, $t = x - y = 108398887211$.

$t = N(\alpha)$ with $\alpha = a + b \cdot 3^{1/3} + c \cdot 3^{2/3}$ and (a, b, c) one of

$(5603, 1612, 1156), (-2386, -143, 2432), (3824, -2135, 992)$.

Two problems arise: approximation and lifting.

$$(s = (z - z_1)/t = 4360888)$$

A VARIATION USING ELLIPTIC CURVES

The factorization (recall $t = N_{K/\mathbb{Q}}(a + b\alpha + c\alpha^2)$)

$$(a + b\alpha + c\alpha^2)(d + e\alpha + f\alpha^2) = z + \alpha$$

gives

$$d = \frac{1}{t}(z(a^2 - kbc) + (kb^2 - kac))$$

$$e = \frac{1}{t}(z(kc^2 - ac) + (a^2 - kbc))$$

$$f = \frac{1}{t}(z(b^2 - ac) + (kc^2 - ab)).$$

Put $z = z_1 + ts$ with $z_1 \equiv -(kb^2 - kac)(a^2 - 3bc)^{-1} \pmod{t}$,

to get ‘cubic in s = quadratic in Y ’:

$$N_{K/\mathbb{Q}}(d + e\alpha + f\alpha^2) = d^3 + ke^3 + k^2f^3 - 3kdef = 3Y^2 + 3Yt + t^2.$$

A VARIATION USING ELLIPTIC CURVES

Point: Let $r = 6Y + 3t$, then (s, r) is an integral point on

$$r^2 = A_0s^3 + A_1s^2 + A_2s + A_3,$$

with $A_i = A_i(a, b, c)$ ($i = 1, 2, 3$).

$$k = 3 : t = 108398887211 = N_{K/\mathbb{Q}}(5603 + 1612\alpha + 1156\alpha^2),$$

$$d = 25803193s + 20709780, \quad e = -5023028s - 4031509,$$

$$f = -3878524s - 3112924.$$

and $s = 4360888$ is the x -coordinate of an integral point on

$$\begin{aligned} r^2 = & 141003824982997192302252s^3 \\ & + 339511260630207004599744s^2 \\ & + 272493544314871871456256s \\ & + 37650633287640319405761. \end{aligned}$$

THE COST

Booker and Sutherland: "Several hundred core-years".

The method above

Time to find an (a, b, c) curve with **one** computable integral point) \times (cost to find that point on the curve)

Search in the cube $0 \leq a, b, c < 10^4$, and test the x -coordinates up to 10^7 . (c is the outer loop)

time $\approx (10^4)^3 \times .0025$ seconds with **hyperellratpoints** (M. Stoll)

Expected time: 80 core years.

Actual time to find the solution: ≈ 9.16 core-years!

(3.5 days on a 1000-core dedicated machine)

