MATHEMATICS OF COMPUTATION
Volume 76, Number 259, July 2007, Pages 1683–1690
S 0025-5718(07)01947-3
Article electronically published on March 14, 2007

NEW INTEGER REPRESENTATIONS AS THE SUM OF THREE CUBES

MICHAEL BECK, ERIC PINE, WAYNE TARRANT, AND KIM YARBROUGH JENSEN

ABSTRACT. We describe a new algorithm for finding integer solutions to $x^3 + y^3 + z^3 = k$ for specific values of k. We use this to find representations for values of k for which no solution was previously known, including $k = 30$ and $k = 52$.

1. INTRODUCTION

The table below lists the new solutions we found using the method described in this article.

TABLE 1. Solutions to the equation $x^3 + y^3 + z^3 = k$

k	(x, y, z)	*Date*
30	(-283059965, -2218888517, 2220422932)	7/10/99
52	(60702901317, 23961292454, -61922712865)	2/6/00
195	(-2238006277, -5087472163, 5227922915)	12/30/99
588	(-3650204951, -5097345554, 5657478787)	5/23/00

For a given positive k, we wish to find integers x, y, z satisfying

$$x^3 + y^3 + z^3 = k. \tag{1}$$

Note that for $k \equiv \pm 4 \pmod 9$ there are no solutions since, for any integer x, $x^3 \equiv 0, 1, -1 \pmod 9$. After searching for solutions where all of $|x|, |y|, |z|$ are relatively small with respect to the size of k, we then focus on solutions where at least one of $|x|, |y|, |z|$ is large. In this case, x, y, z cannot all be the same sign, so suppose z is of different sign from x and y. By letting $T = |x + y|$ we notice that T divides $x^3 + y^3 = k - z^3$. Then for a given T, z must satisfy

$$z^3 \equiv k \pmod T. \tag{2}$$

These ideas have been used in earlier searches, for example, see [2] and [4]. We were able to impose another condition on z, namely that either $-T < z < -T/2$ or $T/2 < z < T$. Therefore, each solution for z to (2) modulo T yields at most one possible *integer* z. Moreover, fixing such an integer z also determines the integer values for x and y if they exist for the particular value of T.

Received by the editor February 7, 2002 and, in revised form, October 8, 2005.
2000 *Mathematics Subject Classification.* Primary 11D25; Secondary 11Y50, 11N36.

2. Previous results

The question as to which integers are expressible as a sum of three integer cubes is over 150 years old. The first known reference to this problem is found in S. Ryley's article in the Ladies' Diary in 1825 [17], in which he gives a parametrization of rational solutions x, y, z to $x^3 + y^3 + z^3 = k$, for $k \in \mathbf{Z}$, namely,

$$x = \frac{(9d^6 - 30k^2d^3 + k^4)(3d^3 + k^2) + 72k^4d^3}{6kd(3d^3 + k^2)^2}$$
$$y = \frac{30k^2d^3 - 9d^6 - k^4}{6kd(3d^3 + k^2)}$$
$$z = \frac{18kd^5 - 6k^3d^2}{(3d^3 + k^2)^2}.$$

In 1908, A.S. Werebrusov found the following parametrization of x, y, and z when $k = 2$ [15]:

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

In 1936, Mahler [13] discovered a parametric solution for $k = 1$:

$$(9t^4)^3 + (3t - 9t^4)^3 + (1 - 9t^3)^3 = 1.$$

Mordell proved in 1942 [15] that for any other k a parametric solution with rational coefficients must have degree at least 5.

In 1954, Miller and Woollett discovered explicit representations for 69 values of k between 1 and 100. Their search exhausted the region $\{|x|, |y|, |z| \leq 3164\}$ [14].

In 1963 Gardiner, Lazarus, and Stein looked at the equation $x^3 + y^3 = z^3 - k$ in the range $0 \leq x \leq y \leq 2^{16}$, where $0 < z - x \leq 2^{16}$ and $0 < |k| \leq 999$. Their search left only 70 values of k between 1 and 1000 without a known representation including eight values less than 100 [6].

In 1992, the first solution for $k = 39$ was found. Heath-Brown, Lioen, and te Riele [8] determined that $39 = 134476^3 + 117367^3 + (-159380)^3$ with the rather deep algorithm of Heath-Brown [7]. This algorithm involved searching for solutions for a specific value of k using the class number of $\mathbf{Q}(\sqrt[3]{k})$ to eliminate values of x, y, z which would not yield a solution.

In 1994, Koyama used modern computers to expand the search region to $\{|x|, |y|, |z| < 2^{21}\}$, and successfully found first solutions for 16 integers between 100 and 1000 [9].

Also in 1994, Conn and Vaserstein chose specific values of k to target, and then used relations implied by each chosen value to limit the number of triples (x, y, z) searched. In so doing, they found first representations for 84 and 960. Their paper also lists a solution for each $k < 100$ for which a representation was known [4].

Next, in 1995, Bremner [2] devised an algorithm which uses elliptic curve arguments to narrow the search space. He discovered a solution for 75 (and thus a solution for 600), leaving only five values less than 100 for which no solution was known. Lukes then extended this search method to also find the first representations for each of the values 110, 435, and 478 [12].

In 1997, Koyama, Tsuruoka, and Sekigawa [10] used a new algorithm to find first solutions for five more values between 100 and 1000 as well as independently finding the same solution for 75 that Bremner found. Their method proceeded by taking x to be the smallest of the three variables in absolute value, and letting this

be the parameter by introducing the variable $A = X^3 - k$, where $X = x$, if $x > 0$, or $A = X^3 + k$, where $X = -x$, if $x \leq 0$.

Also in the same paper, the authors discuss the complexity of the above algorithms. To find solutions with $|x|, |y|, |z| \leq N$, the Heath-Brown algorithm has a running time of $c_k N(\log(N))^{O(1)}$, for a fixed value of k. The running time for each of the other algorithms is $O(N^2)$. Of these, the method of [10] fixes a value of k, while the others search for solutions over a range of values of k.

In an August 1999 email, Elkies informed us that Bernstein had implemented the method he had suggested in [5], and found solutions for 11 new values of k, including the same solution for $k = 30$ that we had found.

The values of $k < 1000$, where $k \not\equiv \pm 4 \pmod 9$, for which no representation is yet known are listed in Table 2 at the end of this article.

3. Algorithm and running time

The algorithm described searches for integer solutions to (1) up to a search bound N, for a fixed value of k. In the next section we explain the various conditions on the special cases in the first two steps, and show that the algorithm will find any solution to (1) with $|x + y| < N$ as described below. To ease notation, we begin with the following definition:

$$B_k = \frac{3 + \sqrt{12k - 3}}{6}. \tag{3}$$

Before beginning the search for general solutions, we first check two special cases:

1) $|x|,|y|,|z| \leq B_k$,
2) $k = 3xyz$ with $x + y + z = 0$.

We then begin the general case in which x, y, z cannot all be the same sign. Without loss of generality, assume z is of different sign from x and y, and thus $|z| > B_k$. Let $T = |x + y|$ and notice that T divides $x^3 + y^3 = k - z^3$. Therefore, given T, z must satisfy $z^3 \equiv k \pmod T$. Moreover, by Theorem 4.1, of the next section, z must also satisfy either $-T < z < -T/2$ or $T/2 < z < T$, leaving at most one integer z for each modulo T solution for z. This also determines the sign of $s = x + y = \pm T$. To check if this z and s pair allows an integer solution to (1), we rewrite this main equation as:

$$s^2 - 3xy = \frac{k - z^3}{s}.$$

Substituting $y = s - x$ and solving for x, we see that the following expression for x must be an integer:

$$x = \frac{3s \pm \sqrt{-3s^2 - 12(z^3 - k)/s}}{6}.$$

3.1. The Algorithm.

Step 1: Search for solutions to $x^3 + y^3 + z^3 = k$ with $\max\{|x|, |y|, |z|\} \leq B_k$.

Step 2: When $3|k$, search for solutions to $k = x^3 + y^3 + z^3 = 3xyz$ where $x + y + z = 0$. Since $k > 0$, it must be that $x, y < 0$ and $z > 0$. Thus for each distinct factorization of $k/3$ as xyz, simply test if both $x + y + z = 0$ and $x^3 + y^3 + z^3 = k$.

Repeat steps 3-5 for values of $T < N$, beginning with $T = 2$.

Step 3: Find all solutions z of $z^3 = k \pmod{T}$ using, for example, the algorithm given in [1].

Step 4: For each of the cube roots modulo T found in the previous step, the corresponding integer solution must lie in the range $T/2 < |z| < T$. Fix one of the values of z found in step 3. If $T/2 < z < T$, then we leave z unchanged and so $s = -T$. If $0 < z < T/2$, we replace z with $z - T$ and thus $s = T$.

Step 5: Let $D = -3s^2 - 12(z^3 - k)/s$ and check that:

1) $D = d^2$ for $d \in \mathbf{Z}$,
2) $3|d$,
3) $3s \equiv \pm d \pmod{6}$.

If all of these conditions hold, then we have an integer triple (x, y, z) with $x^3 + y^3 + z^3 = k$.

To continue, return to step 4 with the next possible z value given by step 3. When all cube roots of k modulo T have been checked, increment T by 1 and return to step 3.

3.2. **Running Time.** The expected number of bit operations required for this algorithm to check all values of $|x + y| = T \leq N$ is $N(\log(N))^{O(1)}$, so long as $N > k$. The algorithm can be split into two parts. In the first, factor the numbers $1 \leq T \leq N$ by sieving with the primes $p \leq \sqrt{N}$. For each such prime there are at most N/p steps, hence the total number of steps is $O(N \log\log(N))$. Each value of T has at most one prime factor $p > \sqrt{N}$, so accounting for these takes $O(N)$ steps. The total number of steps for factoring the integers T is then $O(N \log\log(N))$. Accounting for the size of N, the number of bit operations is therefore $N(\log N)^{O(1)}$.

The second part of the algorithm involves finding modular cube roots, and testing if each leads to a solution. To calculate modular cube roots modulo T, use the factorization given above and first calculate cube roots modulo the prime factors of T. The Chinese Remainder Theorem then yields cube roots modulo T. The expected running time of finding all cube roots modulo a prime $p \leq N$ can be bounded by $O((\log N)^3)$ bit operations (see [1]). Extending this to the prime power dividing T gives the same order. Let $\omega(T)$ be the number of distinct prime powers dividing T. To calculate inverses modulo p^a of T/p^a for each $p^a \parallel T$ using Euclid's Algorithm takes $O(\omega(T)\log(N))$ steps. For each $p^a \parallel T$ there are at most three cube roots of k modulo p^a, so the number of steps required to check all of them for a particular T is $O(\omega(T)\log(N) + 3^{\omega(T)})$. Summing this for values of $T \leq N$ gives $O\left(N(\log N)^2\right)$ (see [19]). Thus the number of expected bit operations of this second part and hence the algorithm is $N(\log(N))^{O(1)}$. Note that to check for solutions with $x, y, z < N$ we need only to check values of $T \leq 2N$, and hence the running time is of the same order.

4. Verifying the algorithm

In this section we show that the algorithm presented will, for a fixed value of k, find any solution to (1) with $|x+y| < N$, with x and y as described in the previous section. The main result of this section is:

Theorem 4.1. *Fix a positive integer $k \not\equiv \pm 4 \pmod{9}$. Suppose integers x, y, and z satisfy $x^3 + y^3 + z^3 = k$, where x and y are of different sign than z, and $|z| > B_k$. Then letting $s = x + y$ and $T = |s|$ we have either*

i) $3xyz = k$ *with* $x + y + z = 0$, *or*
ii) $T/2 < |z| < T$.

In the proof of Theorem 4.1 we will use the following lemma:

Lemma 4.2. *Fix a positive integer* k *and an arbitrary integer* z. *Suppose real numbers* x *and* y *have different sign from* z, *with* $|x| \leq |y|$, *and let* $s = x + y$. *Then under the constraint* $x^3 + y^3 + z^3 - k = 0$ *the quotient* s/z *achieves a minimum when* $x = y$.

Proof. Let $f(x, y) = (x + y)/z$ and $g(x, y) = x^3 + y^3 + z^3 - k$. Using Lagrange Multipliers to find the critical points of $f(x, y)$ under the constraint of $g(x, y)$, we know that for some real λ,

$$\frac{1}{z} = 3\lambda x^2 \quad \text{and} \quad \frac{1}{z} = 3\lambda y^2.$$

So, $x = \pm y$. Yet by construction x and y have the same sign, hence the only critical point is when $x = y$.

The minimum may also occur when the partials of g equal 0. The two possibilities for this are $x = 0$ or $y = 0$. Notice that these two conditions are equivalent by renaming variables. Therefore, to show that the critical point yields the minimum for $f(x, y)$ under our constraint, we simply compare values of $f(x, y)$ at the critical point and at $x = 0$.

If $x = y$, then $2y^3 = k - z^3$ and

$$s/z = 2y/z = \sqrt[3]{4}\sqrt[3]{k/z^3 - 1}. \tag{4}$$

If $x = 0$, we have $s/z = y/z = \sqrt[3]{k/z^3 - 1}$. Since $k < |z|^3$, indeed the minimum occurs when $x = y$. □

We can now prove the main theroem.

Proof of Theorem 4.1. First we will let z be fixed but arbitrary. Since

$$\min(s/z)_{\{x,y\in\mathbf{Z}\}} \geq \min(s/z)_{\{x,y\in\mathbf{R}\}},$$

we can apply Lemma 4.2 noting that $|z|^3 > k$:

$$s/z \geq \sqrt[3]{4}\sqrt[3]{k/z^3 - 1} > \sqrt[3]{4}\sqrt[3]{-2} = -2,$$

so, $|z| > T/2$.

For the other inequality we note that since z has the opposite sign from x and y, we have $s/z < 0$. But,

$$\left(\frac{x + y}{z}\right)^3 = \frac{x^3 + y^3}{z^3} + \frac{3xy(x + y)}{z^3} \leq \frac{x^3 + y^3}{z^3} = k/z^3 - 1,$$

so then,

$$s/z \leq \sqrt[3]{k/z^3 - 1}. \tag{5}$$

The proof then naturally splits into two cases.
Case 1: $x, y, s, k \geq 0$ and $z < 0$.
Since $k/z^3 < 0$, using (5) we see that $|z| < T$.
Case 2: $z, k > 0$ and $x, y, s \leq 0$.

In this case $k/z^3 > 0$, so we do not get the bound immediately as above. From (5) we have $T \geq |\sqrt[3]{k-z^3}|$. If $T = |z|$, then $k = x^3 + y^3 + z^3 = 3xyz$ with $x + y + z = 0$, satisfying condition (i) of the theorem.

Otherwise, if $|z| > T$, then since T and $|z|$ are integers, we would have $|\sqrt[3]{k-z^3}| \leq |z| - 1$, that is, $\sqrt[3]{k-z^3} + z \geq 1$. This is equivalent to the inequality $3z^2 - 3z + (1-k) \leq 0$, which is false since $z > B_k$. Thus $|z| < T$, completing Case 2, and hence the theorem. □

In order to use Theorem 4.1, we must determine when $|z| > B_k$. The following lemma shows that unless $|x|, |y|, |z|$ are all small, this is indeed true.

Lemma 4.3. *Let k be a fixed positive integer. Suppose that x, y, z are integers so that $x^3 + y^3 + z^3 = k$, with $max\{|x|, |y|, |z|\} > B_k$. Then one of x, y, z must be of different sign from the other two. Moreover, if we let z be the one with different sign, then $|z| > B_k$.*

Proof. By expanding out the expression (3) for B_k, we see that $k \geq 1$ implies $B_k^3 \geq k$. Therefore, not all of x, y, z can be non-negative. By relabeling if necessary, let z have different sign from x and y.

Without loss of generality, we will assume that $|x| \leq |y|$. If $|z| > B_k$, then the lemma holds trivially. So, suppose $|z| \leq B_k$, but $|y| > B_k$.

We split into two cases, depending on the sign of z and derive a contradiction for each. If $z > 0$ and $x, y \leq 0$, then $x^3 + y^3 + z^3 \leq y^3 + z^3 < 0$. But since $k > 0$, this is a contradiction.

Now suppose that $z < 0$ and $x, y \geq 0$. Certainly, if $0 < |z| \leq |x| \leq |y|$, then $x^3 + y^3 + z^3 \geq y^3 > k$. So we can further suppose that $0 \leq |x| < |z| \leq B_k < |y|$. In this case,

$$\begin{aligned} x^3 + y^3 + z^3 - k &\geq 0^3 + (\lfloor B_k \rfloor + 1)^3 + (-\lfloor B_k \rfloor)^3 - k \\ &= 3(\lfloor B_k \rfloor)^2 + 3(\lfloor B_k \rfloor) + 1 - k \\ &> 3(B_k - 1)^2 + 3(B_k - 1) + (1 - k) = 0. \end{aligned}$$

Hence, $x^3 + y^3 + z^3 > k$, which again is a contradiction. □

5. Practical considerations

In practice, the basic algorithm described in Section 3 can be improved. The following optimizations were added when the algorithm was implemented.

(1) Suppose for a particular T value, there is a prime $p|T$ for which k is not a cube modulo p, then k is also not a cube modulo T. This allows us to skip any value of T having a prime factor p for which k is not a cube modulo p.
(2) A similar argument can be made for primes dividing k. Suppose that a prime $p \parallel k$, and $p^2|T$, then $p \parallel (k - s(s^2 - 3xy)) = z^3$, which is impossible. So, for primes $p \parallel k$, we can exclude T for which $p^2|T$ from consideration. This idea can be extended to the case where $p^r \parallel k$ and $p^{r+1}|T$ if $r \not\equiv 0 \pmod 3$.
(3) We pre-computed a cube root modulo p for all primes $p \equiv 1 \pmod 3$ up to some bound B. This ensures that for $T < B^2$ we will need to calculate a cube root modulo p at most once for each T. (That is, only for the prime divisor $p \equiv 1 \pmod 3$ of T which is greater than B, if such a factor exists).

6. Results

Our original implementation of the algorithm was written in Magma. It was with this version of the code that the solution for $k = 30$ was found. In order to increase portability, reduce the memory footprint, and increase the speed of the program, we wrote a version in C, using the gmp arbitrary precision arithmetic library. The rest of the results were found using this second version of the program. The bulk of the calculations were carried out on a 400 MHz Sun Ultra Enterprise 3000. Checking 1,000,000 values for T of size 10^{10} required approximately 60 seconds on this machine for the C version and 90 seconds for the original Magma version.

We searched for a solution for each of the integers less than 1000 which are not congruent to 4 or 5 modulo 9 and for which no solution was known. The search found representations for four new values of k, which are listed in Table 1 at the beginning of the article. Current search bounds for the other such values of $k < 1000$ are given in the table below. No integer solution to $x^3 + y^3 + z^3 = k$ for these values of k were found with an associated T-value smaller than the bound indicated.

Table 2. Search bounds on T for $k < 1000$

k	T
33	10^{12}
42	6.5×10^{11}
74	1.5×10^{11}
156, 165, 318, 366, 390, 420, 534, 564, 579, 609, 627, 633, 732, 758, 786, 789, 795, 834, 894, 903, 906, 921, 948, 975	10^{10}

Acknowledgments

The authors would like to thank Andrew Granville and Carl Pomerance for their help in developing the algorithm and simplifying the arguments in this article, and the referee for providing valuable suggestions concerning its organization. We would also like to thank Red Alford, and remember him for all that he did to inspire students to study computational aspects of number theory.

References

1. Eric Bach and Jeffrey Shallit, Algorithmic number theory (1996), 160–161. MR1406794 (97e:11157)
2. Andrew Bremner, *On sums of three cubes,* Canadian Mathematical Society Conference Proceedings **15** (1995), 87–91. MR1353923 (96g:11024)
3. J.W.S. Cassels, *A Note on the Diophantine Equation* $x^3 + y^3 + z^3 = 3$*,* Mathematics of Computation **44** (1985), 265. MR0771049 (86d:11021)
4. W. Conn and L.N. Vaserstein, *On Sums of Three Integral Cubes,* Contemporary Mathematics **166** (1994), 285–294. MR1284068 (95g:11128)
5. Noam Elkies, <elkies@abel.math.harvard.edu> "x^3 + y^3 + z^3 = d," 9 July 1996, <nmbrthry@listserv.nodak.edu> via <http://listserv.nodak.edu/archives/nmbrthry.html>.
6. V.L. Gardiner, R.B. Lazarus, and P.R. Stein, *Solutions of the Diophantine Equation* $x^3+y^3 = z^3 - d$*,* Mathematics of Computation **18** (1964), 408–413. MR0175843 (31:119)

7. D.R. Heath-Brown, *Searching for Solutions of* $x^3 + y^3 + z^3 = k$*,* Seminaire de Theorie des Nombres, (1989–1990), 71–76. MR1476729 (98f:11025)
8. 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,* Mathematics of Computation **61** (1993), 235–244. MR1202610 (94f:11132)
9. Kenji Koyama, *Tables of solutions of the Diophantine equation* $x^3+y^3+z^3 = n$*,* Mathematics of Computation **62** (1994), 941–942.
10. Kenji Koyama, Yukio Tsuruoka, and Hiroshi Sekigawa, *On Searching for Solutions of the Diophantine Equation* $x^3 + y^3 + z^3 = n$*,* Mathematics of Computation **66** (1997), 841–851. MR1401942 (97m:11041)
11. D.H. Lehmer, *On the Diophantine Equation* $x^3 + y^3 + z^3 = 1$*,* Journal of the London Mathematical Society **31** (1956), 275–280. MR0078397 (17:1187c)
12. Richard F. Lukes, *A Very Fast Electronic Number Sieve,* University of Manitoba doctoral thesis, 1995.
13. Kurt Mahler, *Note On Hypothesis K of Hardy and Littlewood,* Journal of the London Mathematical Society **11** (1936), 136–138.
14. J.C.P. Miller and M.F.C. Woollett, *Solution of the Diophantine Equation* $x^3 + y^3 + z^3 = k$*,* Journal of the London Mathematical Society **30** (1955), 101–110. MR0067916 (16:797e)
15. L.J. Mordell, *On Sums of Three Cubes,* Journal of the London Mathematical Society **17** (1942), 139–144. MR0007761 (4:189d)
16. L.J. Mordell, *On an Infinity of Integer Solutions of* $ax^3 + ay^3 + bz^3 = bc^3$*,* Journal of the London Mathematical Society **30** (1955), 111–113. MR0067917 (16:798a)
17. S. Ryley, The Ladies' Diary **122** (1825), 35.
18. Manny Scarowsky and Abraham Boyarsky, *A Note on the Diophantine Equation* $x^n + y^n + z^n = 3$*,* Mathematics of Computation **42** (1984), 235–237. MR0726000 (85c:11029)
19. Gerald Tenenbaum, Introduction to analytic and probablistic number theory (1995), 200–202. MR1342300 (97e:11005b)
20. R.C. Vaughan, *A new iterative method in Waring's problem,* Acta Mathematica **162** (1989), 1–71. MR0981199 (90c:11072)

Department of Mathematics, University of Georgia, Athens, Georgia 30602
E-mail address: mbeck@math.uga.edu

Department of Mathematics, University of Georgia, Athens, Georgia 30602
E-mail address: epine@math.uga.edu

Department of Mathematics, University of Georgia, Athens, Georgia 30602

Department of Mathematics, University of Georgia, Athens, Georgia 30602