MATHEMATICS OF COMPUTATION
Volume 66, Number 218, April 1997, Pages 841–851
S 0025-5718(97)00830-2

ON SEARCHING FOR SOLUTIONS OF THE DIOPHANTINE EQUATION $x^3 + y^3 + z^3 = n$

KENJI KOYAMA, YUKIO TSURUOKA, AND HIROSHI SEKIGAWA

Abstract. We propose a new search algorithm to solve the equation $x^3+y^3+z^3 = n$ for a fixed value of $n > 0$. By parametrizing $|x| = \min(|x|, |y|, |z|)$, this algorithm obtains $|y|$ and $|z|$ (if they exist) by solving a quadratic equation derived from divisors of $|x|^3 \pm n$. By using several efficient number-theoretic sieves, the new algorithm is much faster on average than previous straightforward algorithms. We performed a computer search for 51 values of n below 1000 (except $n \equiv \pm 4 \pmod 9$) for which no solution has previously been found. We found eight new integer solutions for $n = 75$, 435, 444, 501, 600, 618, 912, and 969 in the range of $|x| \leq 2 \cdot 10^7$.

1. Introduction

Consider the Diophantine equation

$$x^3 + y^3 + z^3 = n, \tag{1}$$

where n is a fixed positive integer and x, y and z can be any integers with minus signs allowed [4, 12, 15]. Note that there are no solutions of equation (1) when $n \equiv \pm 4 \pmod 9$ because $a^3 \equiv 0, \pm 1 \pmod 9$ for any integer a. There is no known general criterion for excluding any other values of n, although there are still many values of n for which no solution has been found.

In finding all solutions for a *range* of values of n with $\max(|x|, |y|, |z|) \leq U$, a straightforward two-dimensional algorithm [3, 8, 11] takes $O(U^2)$ steps. In [8], a computer search based on this algorithm in the range of $\max(|x|, |y|, |z|) \leq 2\,097\,151$ $(= 2^{21} - 1)$, $0 < n < 1000$, was discussed. This range included the ones chosen in [3] and [11]. All 5418 solutions found were deposited into the UMT file of the American Mathematical Society. In particular, the search found solutions for 17 values of n for which no solutions had been found before: $n =$ 39, 143, 180, 231, 312, 321, 367, 439, 462, 516, 542, 556, 660, 663, 754, 777, and 870. Recently, Koyama [9] extended a computer search to the range of $\max(|x|, |y|, |z|) \leq 3\,414\,387$, $0 < n < 1000$, on a CRAY-2 computer. He found other solutions for $n = 439$ as $(-869\,418,\ -2\,281\,057,\ 2\,322\,404)$ and for $n = 462$ as $(1\,612\,555,\ 2\,598\,019,\ -2\,790\,488)$ in differing ranges of [8] and [9]. Conn and Vaserstein [2] presented a search method by parametrizing another variable related to $(x,\ y,\ z)$ for a fixed value of n. They carried out a computer search in the range of $0 < n < 100$ on a Sun 4 and a Next workstation. Although they

Received by the editor November 13, 1995 and, in revised form, February 14, 1996.
1991 *Mathematics Subject Classification.* Primary 11D25.
Key words and phrases. Diophantine equation, cubic, number-theoretic sieves, search algorithm, computer search.

missed some solutions, they found solutions for $n = 39$ and 84. In particular, a solution for $n = 84$ was found as $(-8\,241\,191,\ -41\,531\,726,\ 41\,639\,611)$ beyond the range of [9]. Heath-Brown, Lioen and te Riele [6] presented a new algorithm based on the class number of $Q(\sqrt[3]{n})$ for solving equation (1) with a fixed value of n. Their algorithm takes $O(c_0\,U\ \log\ U)$ steps to find all solutions in the range of $\max(|x|,\ |y|,\ |z|) \leq U$, where the constant c_0 depends on n. They did numerical experiments for $n = 2,\ 3,\ 20,\ 30,\ 39,$ and 42 over an extended range on a CYBER 205 vector computer [6, 13]. According to recent private communications among Vaserstein, te Riele and Koyama, it appears that the solution $(117\,367,\ 134\,476,\ -159\,380)$ for $n = 39$ was independently found by these three groups in 1991. In early 1995, Jagy [7] presented a search method by parametrizing $r = x + y + z$ for a fixed value of n. He found a solution for $n = 478$ as $(-1\,368\,722,\ -13\,434\,503, 13\,439\,237)$. With these recent results included, there are 51 values of n below 1000 (and $\not\equiv \pm 4 \bmod 9$) for which no solution has been found:

$$
n = \begin{array}{rrrrrrrrrr}
30, & 33, & 42, & 52, & 74, & 75, & 110, & 114, & 156, & 165, \\
195, & 290, & 318, & 366, & 390, & 420, & 435, & 444, & 452, & 501, \\
530, & 534, & 564, & 579, & 588, & 600, & 606, & 609, & 618, & 627, \\
633, & 732, & 735, & 758, & 767, & 786, & 789, & 795, & 830, & 834, \\
861, & 894, & 903, & 906, & 912, & 921, & 933, & 948, & 964, & 969, \\
975. & & & & & & & & &
\end{array} \tag{2}
$$

In this paper, in order to find all solutions in the range of $\min(|x|,\ |y|,\ |z|) \leq L$ for a *fixed* value of n in the above list, we propose a new search algorithm that takes $O(c\,L^2)$ steps. The constant c depends on n, and the computational complexity is much smaller than that of previous straightforward algorithms [3, 8, 11]. This improved efficiency is achieved by several number-theoretic sieves in the algorithm. We show the results of a computer search that used this algorithm.

2. Outline of new search algorithm

Without loss of generality, we may take

$$|x| \leq |y| \leq |z|.$$

The solutions are generally classified into the following three cases:

Case 0 : $x \geq 0,\ y \geq 0,\ z \geq 0,$

Case 1 : $x > 0,\ y > 0,\ z < 0,$

Case 2 : $x \leq 0,\ y < 0,\ z > 0.$

In case 0, the constraint $0 < x^3 + y^3 + z^3 < 1000$ implies $z \leq 9$. Thus, it is easy to find all solutions for case 0, even if a three-dimensional exhaustive search is done, that is to say, $x,\ y,\ z$ vary independently. In order to find all solutions for case 1 and case 2 over a *range* of values of n, a two-dimensional exhaustive search with parameters y and z was done in [3, 8, 9, 11]. In order to find all solutions for case 1 and case 2 with a *fixed* value of n, we propose a one-dimensional exhaustive search with one parameter x. In case 1, we put $X = x$, $Y = y$, $Z = -z$, and $A = X^3 - n$, where X is assumed so that $X^3 > n$. In case 2, we put $X = -x$, $Y = -y$, $Z = z$, and $A = X^3 + n$. Summarizing case 1 and case 2, we have

$$Z^3 - Y^3 = A, \tag{3}$$

where $Z > Y > 0$ and $A > 0$. Equation (3) can be rewritten as a product of two divisors

$$(Z - Y)(Z^2 + ZY + Y^2) = A. \tag{4}$$

Let $C = Z - Y$ and $D = Z^2 + ZY + Y^2$. For given values of X and n, we compute A. By factorizing A, we obtain candidates for the pair of divisors C and D such that $A = CD$. By substituting $Z = C + Y$ into $D = Z^2 + ZY + Y^2$, we get

$$Y^2 + CY + \frac{C^2 - D}{3} = 0. \tag{5}$$

Note that $(C^2 - D)/3$ is an integer. The value of Y (> 0) is obtained as one of the roots of equation (5) as

$$Y = \frac{-C + \sqrt{Q}}{2}, \quad \text{where } Q = \frac{4D - C^2}{3}. \tag{6}$$

From $Z = C + Y$, we have

$$Z = \frac{C + \sqrt{Q}}{2}. \tag{7}$$

Note that Q is a positive integer because $C^2 = Z^2 - 2ZY + Y^2 < Z^2 + ZY + Y^2 = D$ and $4D \equiv C^2 \pmod 3$. If Q is a square, then Y and Z, which are represented by equations (6) and (7), become integers because $\sqrt{Q} \equiv C \pmod 2$.

3. Properties of sieves and their effect

To execute the above procedure, several sieves based on the following properties can be applied.

3.1. **Congruence restriction between n and x.** If $a = 1, 2, -3$, then $a^3 \equiv 1 \pmod 7$. If $a = -1, -2, 3$, then $a^3 \equiv -1 \pmod 7$. Since $a^3 \equiv 0, \pm 1 \pmod 7$ for any integer a, we have $Z^3 - Y^3 \equiv 0, \pm 1, \pm 2 \pmod 7$. Recall that

$$Z^3 - Y^3 = X^3 \pm n = \begin{cases} x^3 - n & \text{for case 1,} \\ -x^3 + n & \text{for case 2.} \end{cases}$$

Therefore, if $n \equiv \pm 3 \pmod 7$, then $x^3 \not\equiv 0 \pmod 7$. If $n \equiv 2, 3 \pmod 7$, then $x^3 \not\equiv -1 \pmod 7$. If $n \equiv -2, -3 \pmod 7$, then $x^3 \not\equiv 1 \pmod 7$. Thus, for given n, the value of x is restricted as follows:

Property 1.

- *If* $n \equiv 2 \pmod 7$, *then* $x \equiv 0,\ 1,\ 2,\ -3 \pmod 7$.
- *If* $n \equiv -2 \pmod 7$, *then* $x \equiv 0,\ -1,\ -2,\ 3 \pmod 7$.
- *If* $n \equiv 3 \pmod 7$, *then* $x \equiv 1,\ 2,\ -3 \pmod 7$.
- *If* $n \equiv -3 \pmod 7$, *then* $x \equiv -1,\ -2,\ 3 \pmod 7$.

If $n \equiv \pm 2 \pmod 7$, then the passing ratio for X in this sieve is $4/7$. If $n \equiv \pm 3 \pmod 7$, then the passing ratio for X in this sieve is $3/7$. Among the 51 values of n in the list (2), there are 21 values of n satisfying $n \equiv \pm 2 \pmod 7$ and 20 values of n satisfying $n \equiv \pm 3 \pmod 7$.

Since $a^3 \equiv 0, \pm 1 \pmod 9$ for any integer a, we have $Z^3 - Y^3 \equiv 0, \pm 1, \pm 2 \pmod 9$. It is well known that if $n \equiv \pm 4 \pmod 9$, there is no solution. Note that for

$b = 0, \pm 1$, congruence $x^3 \equiv b \pmod{9}$ is equivalent to congruence $x \equiv b \pmod{3}$. For given n such that $n \equiv \pm 2, \pm 3 \pmod{9}$, the value of x is similarly restricted as follows:

Property 2.

- *If* $n \equiv 2 \pmod 9$*, then* $x \equiv 0,\ 1 \pmod 3$.
- *If* $n \equiv -2 \pmod 9$*, then* $x \equiv 0,\ -1 \pmod 3$.
- *If* $n \equiv 3 \pmod 9$*, then* $x \equiv 1 \pmod 3$.
- *If* $n \equiv -3 \pmod 9$*, then* $x \equiv -1 \pmod 3$.

If $n \equiv \pm 2 \pmod{9}$, then the passing ratio for X in this sieve is $2/3$. If $n \equiv \pm 3 \pmod{9}$, then the passing ratio for X in this sieve is $1/3$. Among the 51 values of n in the list (2), there are eight values of n satisfying $n \equiv \pm 2 \pmod{9}$ and 41 values of n satisfying $n \equiv \pm 3 \pmod{9}$. We have proven that no other values of modulus for n except 7 and 9 have the sieve effect of excluding some values of x for a solution [14].

3.2. **Factor restriction of A based on cubic residuacity.**

A prime p is a factor of A $(= X^3 \pm n)$ if and only if $X^3 \equiv \mp n \pmod{p}$. Thus, for given n, the factors of A are restricted as follows:

Property 3. *Let p be a prime. If n is a cubic nonresidue modulo p, then A $(= X^3 \pm n)$ does not have the factor p. When $p \equiv 2 \pmod 3$, all values of n are cubic residues modulo p. When $p \equiv 1 \pmod 3$, n is a cubic residue modulo p if and only if $n^{\frac{p-1}{3}} \equiv 1,\ 0 \pmod p$.*

In advance, for fixed n, we can easily pick primes p satisfying cubic residuacity (i.e., there is a solution X for $X^3 \equiv \pm n \pmod{p}$) from all primes below a certain limit. Let W_m be the set of primes satisfying $p \equiv 2 \pmod{3}$ and $p \leq m$. Let $V_m(n)$ be the set of primes satisfying $p \equiv 1 \pmod{3}$, $n^{\frac{p-1}{3}} \equiv 1,\ 0 \pmod{p}$, and $p \leq m$. Let $P_m(n)$ be the set of the union of W_m and $V_m(n)$ that includes the prime 3. Note that $|P_m(n)| = |W_m| + |V_m(n)| + 1$, where $|\cdot|$ means the cardinality of a set. For example, there are 348 513 primes below 5 000 000, giving us $|W_{5\,000\,000}| = 174\,322$. Table 1 shows $|V_m(n)|$ and $|P_m(n)|$ for several values of n and $m = 5\,000\,000$. From Table 1, we can observe that $|P_m(n)|$ is about 66.7% of the number of all primes (=348 513). Using these prechosen primes, factoring based on trial and division can be more efficiently carried out.

TABLE 1. Number of primes satisfying cubic residuacity below m $(= 5\,000\,000)$

n	30	33	42	52	74	75
$\lvert V_m(n)\rvert$	58 145	58 079	57 912	58 097	58 124	58 064
$\lvert P_m(n)\rvert$	232 468	232 402	232 235	232 420	232 447	232 387

3.3. **Factor restriction between A and C.**

We obtain the following theorem about the relationship of factors of A and C. Hereafter, we denote $p^e || N$ if $p^e | N$ and $p^{e+1} \nmid N$ for integer N and prime p.

Theorem 1. *Let p be a prime with $p \equiv 2 \pmod 3$. If $p^e || A$ $(e \geq 1)$, and $p^f || C$ $(f \geq 0)$, then $e = f + 2g$ and $f \geq g$, where g is a nonnegative integer.*

Proof. Let $\omega = \frac{-1+\sqrt{-3}}{2}$. A prime satisfying $p \equiv 2 \pmod 3$ is a prime element in $\mathbf{Z}[\omega]$. Note that $A = Z^3 - Y^3 = (Z-Y)(Z-\omega Y)(Z-\omega^2 Y)$, where $C = Z - Y$ and $D = (Z-\omega Y)(Z-\omega^2 Y)$. Assume that $Z - \omega Y = p^a \cdot D_1$ and $Z - \omega^2 Y = p^b \cdot D_2$, where $p \nmid D_1,\ p \nmid D_2,\ a \geq 0$ and $b \geq 0$. For any integers $k,\ Y$ and Z, we have

$$k|(Z-\omega Y) \Longleftrightarrow [k|Z \text{ and } k|Y] \Longleftrightarrow k|(Z-\omega^2 Y).$$

Putting $k = p^a$ and $k = p^b$ into the above relation, we have $a = b$, which is denoted by g. Thus, $p^{2g}||D$, which implies $e = f + 2g$. Furthermore, $p^g|(Z-Y)$, that is, $p^g|C$. Thus, $f \geq g$. □

As a result of this theorem, divisor C is restricted as:

Property 4. *Let p be a prime with $p \equiv 2 \pmod 3$. Assume that $p^e||A$, where $e \geq 1$. Then $p^h|C$ and $p^f||C$, where*

$$h = \begin{cases} \lceil \frac{e}{3} \rceil + (1 - (\lceil \frac{e}{3} \rceil \bmod 2)) & \text{if } e \text{ is odd,} \\ \lceil \frac{e}{3} \rceil + (\lceil \frac{e}{3} \rceil \bmod 2) & \text{if } e \text{ is even,} \end{cases} \tag{8}$$

$h \leq f \leq e$ and $f - h$ is even.

For example, if $e = 1, 3$, then $p|C$. If $e = 5, 7, 9$, then $p^3|C$. If $e = 2, 4, 6$, then $p^2|C$. If $e = 8, 10, 12$, then $p^4|C$. If $e = 3$, then either $f = 1$ or $f = 3$. Property 4 is effective in determining the candidates for divisor C from the combination of prime factors of A. Note that, even if a prime factor p of A with $p \equiv 1 \pmod 3$ is found, we cannot determine whether it is a factor of C or not. For the prime factor 3, we obtain the following theorem.

Theorem 2. *Assume that $3^e||A,\ 3^f||C$ and $3^g||D$. Then $e = f + g$ and $f \geq \lceil \frac{g}{2} \rceil$. Moreover, if $e > 0$, then $e \geq 2,\ f \geq 1$ and $g \geq 1$.*

Proof. Let $\omega = \frac{-1+\sqrt{-3}}{2}$ and $\pi = 1 - \omega$. For $Z, Y \in \mathbf{Z}$, if $\pi^a||(Z-\omega Y)$ and $\pi^b||(Z-\omega^2 Y)$, then $a = b$, which is denoted by g. Note that for $N \in \mathbf{Z}$, if $\pi^k||N$, then k is even. Since $3 = -\omega^2\pi^2$, we have $3^k||N \Longleftrightarrow \pi^{2k}||N$ for $N \in \mathbf{Z}$. If $\pi^{2\ell}||Y$, then $g = \min(2f, 2\ell+1)$ because $Z - \omega Y = C + \pi Y$ and $\pi^{2f}||C$. Thus, we have $2f \geq g$ and $f \geq \lceil \frac{g}{2} \rceil$. Since $C^2 \equiv D \pmod 3$, we have $3|C \Longleftrightarrow 3|D$. □

Note that if $3|A$, then $3^2|A$, $3|C$ and $3|D$. By means of Theorem 2, divisor C is restricted as:

Property 5. *If $3^e||A$ and $e \geq 1$, then $3^h|C$, where $h = \lceil \frac{e}{3} \rceil$.*

For example, if $e = 2, 3$, then $h = 1$. If $e = 4, 5, 6$, then $h = 2$. Note that from Property 2, if $n \equiv \pm 2, \pm 3 \pmod 9$, then $3 \nmid A$. Among the 51 values of n in the list (2), there are two values of n satisfying $n \equiv \pm 1 \pmod 9$ for which A may have a factor of 3.

3.4. **Size restriction of C.** Since $C^2 < D = A/C$, we have $C < A^{1/3}$. When $X \gg n$ such that $n < 1\,000$, $X > 100\,000$, we have $A = X^3 \pm n \approx X^3$ and a weak upper bound of C is obtained as $C < X$. Furthermore, since $Z < 2^{1/3}Y$ and $Z > 2^{1/3}X$ if $X \gg n$, a stricter upper bound of C is evaluated in a term of X as:

$$C \approx \frac{X^3}{Y^2 + YZ + Z^2} < \frac{X^3}{Z^2(1 + 2^{-1/3} + 2^{-2/3})} < \frac{X}{1 + 2^{1/3} + 2^{2/3}} \approx 0.2599X.$$

This inequality implies the following property.

Property 6. $C < 0.26X$.

The combination of Properties 4, 5 and 6 is effective in finding prime factors of A, more exactly, prime factors of C. At the beginning of trial division factoring, an upper bound of searched primes is put as $B = \lfloor 0.26X \rfloor$. After prime factors $p_k^{e_k}$ of A satisfying $p_k = 3$ or $p_k \equiv 2 \pmod 3$ are found, the upper bound of primes for trial division factoring is dynamically reduced to $B = \left\lfloor \frac{0.26X}{\prod_k p_k^{h_k}} \right\rfloor$. The final upper bound B depends on the distribution of prime factors of pseudo-random values of A.

3.5. **Congruence restriction between A and C.** If $C \not\equiv 0 \pmod 3$, then $D \equiv 1 \pmod 3$. If $C \not\equiv 0 \pmod 2$, then $D \equiv 1 \pmod 2$. Thus, the following congruences of A and C for a particular modulus hold.

Property 7. $C \equiv A \pmod 6$*, that is,* $C \equiv A \pmod 2$ *and* $C \equiv A \pmod 3$.

The relationship $C \equiv A \pmod 6$ is effective in checking the appropriateness of pairs of C and D. Furthermore, by combining Properties 4, 5, 6 and 7, a kernel divisor of C, which is denoted by H, can be computed and has a congruence relationship with A as shown in the following theorem.

Theorem 3. *Let* $p_1 = 3$. *Let* p_k $(k \geq 2)$ *be a prime satisfying* $p_k \equiv 2 \pmod 3$, $p_k < p_{k+1}$ *and* $p_k < \lfloor 0.26X \rfloor$. *Assume that* $p_k^{e_k} || A$, $e_k \geq 0$ $(k = 1, 2, 3, \ldots)$. *Let* H *be defined as*

$$H = \prod_{k=1}^{\ell} p_k^{h_k},$$

where ℓ *is the maximum integer satisfying* $H < \lfloor 0.26X \rfloor$, *and*

$$h_k = \begin{cases} \lceil \frac{e_1}{3} \rceil & \textit{if } 3^{e_1} || A, \\ \lceil \frac{e_k}{3} \rceil + (1 - (\lceil \frac{e_k}{3} \rceil \bmod 2)) & \textit{if } p_k^{e_k} || A,\ k \geq 2 \textit{ and } e_k \textit{ is odd}, \\ \lceil \frac{e_k}{3} \rceil + (\lceil \frac{e_k}{3} \rceil \bmod 2) & \textit{if } p_k^{e_k} || A,\ k \geq 2 \textit{ and } e_k \textit{ is even}. \end{cases}$$

Then, $H | C$ *and* $H \equiv A \pmod 6$.

Proof. It is clear that $H|C$ because of Properties 4 and 5. Since $H \equiv C \pmod 6$ and $C \equiv A \pmod 6$, we have $H \equiv A \pmod 6$. □

If $p_k \nmid A$ for all primes $p_k \in W_m$, $m = \lfloor 0.26X \rfloor$, then $H = 1$. In Theorem 3, H is generally defined and discussed; however, when $2|A$, the congruence $H \equiv A \pmod 2$ always holds. When $3|A$, the congruence $H \equiv A \pmod 3$ always holds. When the factor 3 is excluded from A and H, the following property can be used as a sieve before checking each candidate of C.

Property 8. *Let* $H = 3^h H'$, $3 \nmid H'$, $A = 3^e A'$ *and* $3 \nmid A'$. *Then* $H' \equiv A' \pmod 3$.

In this sieve, two cases such that $\{H' \equiv 1 \pmod 3$ and $A' \equiv 2 \pmod 3\}$ and $\{H' \equiv 2 \pmod 3$ and $A' \equiv 1 \pmod 3\}$ are rejected, and two other cases such that $\{H' \equiv A' \equiv 1 \pmod 3\}$ and $\{H' \equiv A' \equiv 2 \pmod 3\}$ are accepted. From an extensive computer experiment, we can observe that the passing ratio for X to satisfy $H' \equiv A' \pmod 3$ is about 50% . Note that, even if $H = 1$, the passing ratio for X to satisfy $H' \equiv A' \pmod 3$ is also about 50% .

In our search algorithm, the first trial division factoring is carried out for the prime 3 and primes $\in W_B$, then congruence $H' \equiv A' \pmod 3$ is checked. If the check is successful, then the second trial division factoring is carried out for primes $\in V_B(n)$, where B is the final upper bound of the first trial division factoring. Next, the candidates of C are computed from a combination of these factoring results.

3.6. **Congruence restriction between C and n.** The value of C is more restrictive for special values of n. We can extend the result that was analyzed for $n = 30$ in [13]. If $n \equiv 3 \pmod 9$, then $x \equiv y \equiv z \equiv 1 \pmod 3$. If $a \equiv 1 \pmod 3$, then $a^3 - 3a + 2 \equiv (a-1)^2(a+2) \equiv 0 \pmod{27}$. Thus, when $n \equiv 3 \pmod 9$, we have $n \equiv x^3 + y^3 + z^3 \equiv (3x-2) + (3y-2) + (3z-2) \equiv 3(x+y+z) - 6 \pmod{27}$, which implies $x + y + z \equiv 2 + \frac{n}{3} \pmod 9$. On the ohter hand, if $n \equiv -3 \pmod 9$, then $x \equiv y \equiv z \equiv -1 \pmod 3$. If $a \equiv -1 \pmod 3$, then $a^3 - 3a - 2 \equiv (a+1)^2(a-2) \equiv 0 \pmod{27}$. Thus, when $n \equiv -3 \pmod 9$, we have $n \equiv x^3 + y^3 + z^3 \equiv (3x+2) + (3y+2) + (3z+2) \equiv 3(x+y+z) + 6 \pmod{27}$, which implies $x + y + z \equiv -2 + \frac{n}{3} \pmod 9$. These congruences imply the following property.

Property 9. *If $n \equiv \pm 3 \pmod 9$, then*

$$C \equiv \begin{cases} X - k \pmod 9 & \textit{for case 1,} \\ X + k \pmod 9 & \textit{for case 2,} \end{cases}$$

where

$$k \equiv \begin{cases} 2 + \frac{n}{3} \pmod 9 & \textit{if } n \equiv 3 \pmod 9, \\ -2 + \frac{n}{3} \pmod 9 & \textit{if } n \equiv -3 \pmod 9. \end{cases}$$

If $n \equiv \pm 3 \pmod 9$, then this sieve modulo 9 can be used in addition to the sieve modulo 6. There are 41 values of n satisfying $n \equiv \pm 3 \pmod 9$ in the list (2). They include the case for $n = 30$, which is the smallest in the list (2) and said in [4, Probl. D5] to be the most interesting.

3.7. **Congruence restriction of C based on quadratic residuacity.** If an integer b is a quadratic nonresidue modulo p for some prime p, then b is not a square. This relationship of quadratic residuacity can be applied for choosing an appropriate value of C. An application of several primes, say $p = 5,\ 7$, seems to be practically effective. Recall $Q = (4D - C^2)/3$ is a square if there is a solution for equation (1). When $p = 5$, pairs of (A, C) modulo 5 such that $(-2,\ 1), (-1,\ 2), (1,\ -2)$ and $(2,\ -1)$ imply the quadratic nonresidue condition $Q^{\frac{p-1}{2}} = Q^2 \equiv -1 \pmod 5$. Thus, the value of C is restricted by the value of A modulo 5 as follows.

Property 10.

- *If $A \equiv 1 \pmod 5$, then $C \equiv \pm 1,\ 2 \pmod 5$.*
- *If $A \equiv -1 \pmod 5$, then $C \equiv \pm 1,\ -2 \pmod 5$.*
- *If $A \equiv 2 \pmod 5$, then $C \equiv 1,\ \pm 2 \pmod 5$.*
- *If $A \equiv -2 \pmod 5$, then $C \equiv -1, \pm 2 \pmod 5$.*

The characteristic that $A \equiv 0 \pmod 5$ implies $C \equiv 0 \pmod 5$ is common to Property 4. If $A \not\equiv 0 \pmod 5$, then the passing ratio for C in this sieve is $3/5$.

A similar restriction is obtained for another prime, $p = 7$. Recall $A \not\equiv \pm 3 \pmod 7$. When $A \equiv \pm 2 \pmod 7$, the value of Q is always a quadratic residue modulo 7. Pairs of (A, C) modulo 7 such that $(-1,\ 1), (-1,\ 2), (1,\ 3), (-1,\ -3), (1,\ -2)$, and $(1,\ -1)$ imply the quadratic nonresidue condition $Q^{\frac{p-1}{2}} = Q^3 \equiv -1 \pmod 7$. Thus, the value of C is restricted by the value of A modulo 7 as follows.

Property 11.

- *If* $A \equiv 1 \pmod 7$*, then* $C \equiv 1,\ 2,\ -3 \pmod 7$.
- *If* $A \equiv -1 \pmod 7$*, then* $C \equiv -1,\ -2,\ 3 \pmod 7$.

The sieve based on Property 11 is effective except for n with $n \equiv \pm 3$ (mod 7) because $A \equiv \pm 1$ (mod 7) if and only if $(n, x^3) \equiv (\pm 2, \pm 1),\ (\pm 1, 0)$, and $(0, \pm 1)$ (mod 7). If $A \equiv \pm 1$ (mod 7), then the passing ratio for C in this sieve is 3/7.

4. The algorithm with number-theoretic sieves

By parametrizing the positive integer X in the range of $S \le X \le L$, our search algorithm utilizing all of the above properties is as follows.

Input: n, S, L

Output: A solution (x, y, z) of $x^3 + y^3 + z^3 = n$ with $S \le \min(|x|, |y|, |z|) \le L$ or a message "nonexistence" if there is no solution.

step 1: Let W_m and $V_m(n)$ be the sets of primes satisfying

$$W_m = \{p_i \,|\, p_i \equiv 2 \pmod 3),\ p_i \le m\},$$

$V_m(n) = \{p_i \,|\, p_i \equiv 1 \pmod 3),\ n^{(p_i-1)/3} \bmod p_i = \{0, 1\},\ p_i \le m\}$.
Collect primes $p_i \in W_m$ and $p_i \in V_m(n)$, where $m = \lfloor 0.26L \rfloor$.

step 2: Put $X = S$.

step 3: Check X by the values of n mod 7 and n mod 9 by using Properties 1 and 2.
If X is not appropriate as a solution **then** go to step 11 **endif**.

step 4: Compute $A = X^3 \pm n$
(A is a representative of $A_1 = X^3 - n$ and $A_2 = X^3 + n$).

step 5: Let $B = \lfloor 0.26X \rfloor,\ H = 1$ and $F = 1$.
If $3^e || A$ $(e \ge 1)$ **then** put $H = 3^h,\ B = \lfloor B/3^h \rfloor,\ F = 3^{e-h}$ **endif**.

step 6: Find prime factors $p_i \in W_B$ of A by a revised trial division:
Do while $p_i \le B$
  if $p_i^{e_i} || A$ $(e_i \ge 1)$
  then if $p_i^{h_i} < B$
    then put $H = H \cdot p_i^{h_i},\ B = \lfloor B/p_i^{h_i} \rfloor,\ F = F \cdot p_i^{e_i - h_i}$
    else go to step 11 **endif**
  endif
enddo.

step 7: Let $H' = H/3^h$ $(h \ge 0)$ and $A' = A/3^e$ $(e \ge 0)$.
If $H' \not\equiv A'$ (mod 3) **then** go to step 11 **endif**.

step 8: Find prime factors $p_i \in V_B(n)$ of A by a trial division:
Do while $p_i < B$
  if $p_i^{e_i} || A$ $(e_i \ge 1)$ **then** put $F = F \cdot p_i^{e_i}$ **endif**
enddo.

step 9: By using the information of the factors H and F of A, choose divisor C_j as $C_j = HF_j$ satisfying Properties 6, 7, 9, 10, and 11, where F_j is the jth element among combinations of factors of F.
Compute another divisor $D_j = A/C_j$ from each C_j.

step 10: **If** $Q_j = (4D_j - C_j^2)/3$ is a square for the candidate pair $(C_j,\ D_j)$ **then** compute

$$Y = \frac{-C_j + \sqrt{Q_j}}{2}, \quad Z = \frac{C_j + \sqrt{Q_j}}{2}.$$

Output (x, y, z) transformed from (X, Y, Z) according to either case 1 or case 2 **endif**.

step 11: Put $X = X + 1$.
If $X > L$ **then** output the message "nonexistence"
else go to step 3 **endif**.

Remarks.

- Step 1 corresponds to a precomputation phase; steps 2 to 11 correspond to the main phase. Step 6 and step 8 are the most time-consuming parts of the algorithm. Since the number of primes below β is about $\lfloor \beta / \log \beta \rfloor$, step 6 and step 8 require at most $0.667 \cdot \lfloor 0.26X / \log 0.26X \rfloor$ divisions for each value of X. Thus, the order of this algorithm is $O(c\,L^2)$, but the constant term c is very small on average.
- If A has no prime factors less than $0.26X$, then $C_1 = 1$ and $D_1 = A$.
- The square root $\sqrt{Q}$ is quickly computed in floating-point arithmetic and the value is rounded to the nearest integer. By squaring this integer, the squareness of Q is checked.

Numerical Example. When $n = 501$, we found a new solution for case 2. We mention the values of the intermediate variables in the algorithm. Let $19\,895\,058 \le X \le 19\,895\,059$. When $X = 19\,895\,058$, the information of $\{n \equiv -3 \pmod 9$ and $X \equiv 0 \pmod 3\}$ shows that this value of X is not a solution for both case 1 and case 2. When $X = 19\,895\,059$, the information of $\{n \equiv -3 \pmod 7$ and $X \equiv 2 \pmod 7\}$ or $\{n \equiv -3 \pmod 9$ and $X \equiv 1 \pmod 3\}$ shows that this value of X is not a solution for case 1. This value of X may be a solution for case 2, and it follows that $A = X^3 + n = 7\,874\,730\,401\,134\,188\,690\,880$. Note that $\lfloor 0.26 \times 19\,895\,059 \rfloor = 5\,172\,715$. We apply trial division factoring of step 6 with primes p_i satisfying $p_i \equiv 2 \pmod 3$ and $p_i \le 5\,172\,715$. After knowing that A has the factor 2^6, the upper bound of primes for the trial and division is reduced to $\lfloor \frac{0.26X}{2^2} \rfloor = 1\,293\,178$. Moreover, after knowing that A has the factor 5, the upper bound is reduced to $\lfloor \frac{0.26X}{2^2 \cdot 5} \rfloor = 258\,635$. After finding that A has the factor $169\,553$, step 6 ends with $\lfloor \frac{0.26X}{2^2 \cdot 5 \cdot 169553} \rfloor = 1$. Thus, we have $F = 2^4$ and $H = H' = 2^2 \cdot 5 \cdot 169\,553 = 3\,391\,060$, which holds $H' \equiv A' (= A) \equiv 1 \pmod 3$. Since the reduced upper bound becomes one, we do not need the trial division factoring of step 8 with primes p_i satisfying $p_i \equiv 1 \pmod 3$ and $501^{(p_i - 1)/3} \equiv 0, 1 \pmod{p_i}$. Note that, although A has factors 181 and $6\,073$ below $5\,172\,715$, they are not included into the factors of F. Thus, the candidates for divisor C satisfying the exponent restiction and $A \equiv C \equiv 4 \pmod 6$ are $\{H,\ H \cdot 2^2,\ H \cdot 2^4\}$. Among these candidates, only $3\,391\,060 (= H)$ satisfies $C < 0.26X$. For $C = 3\,391\,060$, we have $Q = (4D - C^2)/3 = 3\,092\,437\,844\,334\,864$, which is a square of $55\,609\,692$. Thus, we can compute $Y = 26\,109\,316$ and $Z = 29\,500\,376$. Finally, we obtain the solution for $n = 501$ as $(-19\,895\,059,\ -26\,109\,316,\ 29\,500\,376)$.

5. Computer search and its results

By using the search algorithm mentioned in §4, we performed a computer search for solutions of equation (1) for the 51 values of n below 1000 in the list (2). The range of the search was determined as follows. The ratio Z/X is maximal when $Z - Y = 1$ and $X \gg n$, which imply

$$X \approx (Z^2 + ZY + Y^2)^{1/3} \approx (3Z^2)^{1/3} = 3^{1/3} Z^{2/3} \approx 1.442 Z^{2/3}.$$

The ratio Z/X is minimal when $X \approx 2^{-1/3} Z \approx 0.7937Z$. As a result, the range of X is represented in terms of Z as

$$1.442 Z^{2/3} < X < 0.7937Z.$$

In [9], a search for all solutions in the range of $\max(|x|, |y|, |z|) = Z \leq 3\,414\,387$ was done. That is to say, a complete search for all solutions in the range of $X \leq \lfloor 3^{1/3} \cdot 3\,414\,387^{2/3} \rfloor = 32\,702$ and a partial search for solutions in the range of $32\,702 < X \leq \lfloor 2^{-1/3} \cdot 3\,414\,387 \rfloor = 2\,710\,000$; a search for solutions in the range of $2\,710\,000 < X$ was not done.

Our new search algorithm parametrizes a positive integer X that is in the range of $S \leq X \leq L$, where $\min(|x|, |y|, |z|) = X$. To keep a continuous and exhaustive search going, we put $S = 32702$. Taking into account our computer's power, we put $L = 2 \cdot 10^7$. The CPU-time on a DEC Alpha Server 2100 computer (4 processors, 190 MHz) was about 4 months.

We found eight new integer solutions for $n = 75$, 435, 444, 501, 600, 618, 912, and 969 as shown in Table 2. Note that the solution (x', y', z') for $n = 600$ is derived from the solution (x, y, z) for $n = 75$ because $600 = 75 \cdot 2^3$ and $(x', y', z') = (2x, 2y, 2z)$. Since our search algorithm is deterministic and exhaustive, we can also confirm that there is no solution for 43 values of n below 1000 exempting the above eight values of n in the range of $|x| \leq 2 \cdot 10^7$.

Quite recently, a referee informed us of the related work [1, 5, 10]. Bremner [1, 5] presented a search method by parametrizing $m = y + z$ and x to find solutions for a fixed value of n. It appears that he and we independently found solutions for $n = 75$ (and $n = 600$). By using Bremner's search method, Lukes [10] found a new solution for $n = 110$ as $(109\,938\,919,\ 16\,540\,290\,030,\ -16\,540\,291\,649)$ and another solution for $n = 435$ as $(-981\,038\,126,\ -509\,795\,654\,285,\ 509\,795\,655\,496)$. These solutions were found beyond the range of our search. As a result, there are 42 values of n below 1000 (exempting $n \equiv \pm 4 \pmod 9$) for which no solutions have been found.

Table 2. New solutions

x	y	z	n
4 381 159	435 203 083	−435 203 231	75
−2 058 260	−5 434 196	5 530 891	435
3 460 795	14 820 289	−14 882 930	444
−19 895 059	−26 109 316	29 500 376	501
8 762 318	870 406 166	−870 406 462	600
5 368 580	15 435 275	−15 648 793	618
−14 232 281	−55 648 340	55 956 937	912
1 319 606	17 395 148	−17 397 679	969

Acknowledgement

We wish to thank Kiyoshi Shirayanagi for his valuable comments, which helped improve our manuscript. We would also like to thank the referee for his valuable comments and bringing the recent work [1, 5, 10] to our attention.

References

1. A. Bremner, *On sums of three cubes*, Canadian Math. Soc. Conf. Proc. **15** (1995), 87-91. MR **96g:**11024
2. B. Conn and L. Vaserstein, *On sums of three integral cubes*, Contemp. Math. **166** (1994), 285-294. MR **95g:**11128
3. V. L. Gardiner, R. B. Lazarus and P. R. Stein, *Solutions of the Diophantine equation* $x^3+y^3 = z^3 - d$, Math. Comp. **18** (1964), 408-413. MR **31:**119
4. R. K. Guy, *Unsolved Problems in Number Theory*, First Edition, Springer, New York, 1981. MR **83k:**10002
5. R. K. Guy, *Unsolved Problems in Number Theory*, Second Edition, Springer, New York, 1994. MR **96e:**11002
6. 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 processor*, Math. Comp. **61** (1993), 235-244. MR **94f:**11132
7. W. C. Jagy, *Progress report*, private communication, January 1995.
8. K. Koyama, *Tables of solutions of the Diophantine equation* $x^3 + y^3 + z^3 = n$, Math. Comp. **62** (1994), 941-942.
9. K. Koyama, *On the solutions of the Diophantine equation* $x^3 + y^3 + z^3 = n$, Trans. of Inst. of Electronics, Information and Communication Engineers (IEICE in Japan), Vol.E78-A, No. 3 (1995), 444-449.
10. R. F. Lukes, *A very fast electronic number sieve*, Ph. D. Thesis, Univ. of Manitoba (1995).
11. 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 **16:**797e
12. L. J. Mordell, *Diophantine Equations*, Academic Press, New York, 1969. MR **40:**2600
13. H. J. J. te Riele and J. van de Lune, *Computational number theory at CWI in 1979-1994*, CWI Quarterly, Vol.7, No.4 (1994). MR **96g:**11147
14. H. Sekigawa and K. Koyama, *Existence condition of solutions of congruence* $x^n + y^n \equiv m \pmod{p^e}$, in preparation.
15. W. Scarowsky and A. Boyarsky, *A note on the Diophantine equation* $x^n + y^n + z^n = 3$, Math. Comp. **42** (1984), 235-237. MR **85c:**11029

NTT Communication Science Laboratories, 2-2 Hikaridai, Seika-cho, Soraku-gun, Kyoto 619-02 Japan

E-mail address: koyama@cslab.kecl.ntt.jp

E-mail address: tsuruoka@cslab.kecl.ntt.jp

E-mail address: sekigawa@cslab.kecl.ntt.jp