

ON SEARCHING FOR SOLUTIONS
OF THE DIOPHANTINE EQUATION $x^3 + y^3 + 2z^3 = n$

KENJI KOYAMA

ABSTRACT. We propose an efficient search algorithm to solve the equation $x^3 + y^3 + 2z^3 = n$ for a fixed value of $n > 0$. By parametrizing $|z|$, this algorithm obtains $|x|$ and $|y|$ (if they exist) by solving a quadratic equation derived from divisors of $2|z|^3 \pm n$. Thanks to the use of several efficient number-theoretic sieves, the new algorithm is much faster on average than previous straightforward algorithms. We performed a computer search for six values of n below 1000 for which no solution had previously been found. We found three new integer solutions for $n = 183, 491$ and 931 in the range of $|z| \leq 5 \cdot 10^7$.

1. INTRODUCTION

Demjanenko [2, 9] proved that every number $n \not\equiv \pm 4 \pmod{9}$ can be expressed as the sum of *four* positive or negative cubes: $x^3 + y^3 + z^3 + w^3 = n$. Recently, Lukes [8] found representations of (x, y, z, w) for all $n \leq 10^7$, including $n \equiv \pm 4 \pmod{9}$. Because representations appear to get easier with increasing size of n , it is most plausible that all numbers can be represented as the sum of four cubes.

Guy mentioned two related open problems in a book entitled “Unsolved problems in number theory” (Problem D5 in [3, 4]). One problem asks if every number $\not\equiv \pm 4 \pmod{9}$ is the sum of *three* positive or negative cubes. The other problem asks if every number is the sum of four cubes with two of them equal. More exactly, does each of the following Diophantine equations have integer solutions:

$$(1) \quad x^3 + y^3 + z^3 = n,$$

$$(2) \quad x^3 + y^3 + 2z^3 = n,$$

where n is a fixed positive integer and x, y and z can be any integers with minus signs allowed? There is no known general criterion to check for the existence of solutions for equation (1) or (2), although there are still many values of n for which no solution has been found. For equation (1), Heath-Brown, Lioen and te Riele [5] presented an efficient search algorithm based on the class number of $Q(\sqrt[3]{n})$. Their algorithm uses the idea of factoring in $Q(\sqrt[3]{n})$. They performed a computer search for six values of n below 50. Koyama, Tsuruoka and Sekigawa [7] proposed a one-dimensional quadratic search algorithm for equation (1) by using the idea of integer factoring in \mathbf{Z} and extending [6]. They performed a computer search for 51 values of n below 1000 for which no solution had previously been found. They

Received by the editor October 7, 1996 and, in revised form, January 18, 1999.

1991 *Mathematics Subject Classification*. Primary 11D25.

Key words and phrases. Diophantine equation, cubic, number-theoretic sieves, search algorithm, computer search.

found eight new integer solutions in the range of $\min(|x|, |y|, |z|) \leq 2 \cdot 10^7$. As a result, there are now 43 values of n below 1000 (and $\not\equiv \pm 4 \pmod{9}$) for which no solution of equation (1) has been found.

In this paper, we focus on equation (2). Equation (2) has several parametric solutions for the special form of n :

$$\begin{aligned}x &= 1 + 3t^3, \quad y = 1 - 3t^3, \quad z = -3t^2, \quad n = 2; \\x &= \lambda^3 + 3t^3, \quad y = \lambda^3 - 3t^3, \quad z = -3\lambda t^2, \quad n = 2\lambda^9; \\x &= \lambda, \quad y = \lambda + 2, \quad z = -\lambda - 1, \quad n = 6\lambda + 6.\end{aligned}$$

In 1994, Guy [4] mentioned that there were 15 values of n below 1000 for which no solution of equation (2) had previously been found:

$$n = 76, 148, 183, 230, 356, 418, 428, 445, 482, 491, 580, 671, 788, 931, 967.$$

In an e-mail message from Cohn to Guy [1], Cohn mentioned that he had found nine new solutions for n among the above 15 values. His solutions (x, y, z, n) with $|x| \leq |y|$ were

$$\begin{aligned}(-21167, -122171, 97135, 76), \\(-14101, 27293, -20617, 230), \\(129521, 1048469, -832693, 356), \\(15961, 91705, -72914, 418), \\(-111433, -117091, 114332, 428), \\(-19178, 150439, -119321, 445), \\(-2254, -11878, 9449, 482), \\(85111, 89845, -87542, 580),\end{aligned}$$

and

$$(380698, 641263, -542246, 967).$$

This left the solutions for six values of n below 1000 to be solved:

$$(3) \quad n = 148, 183, 491, 671, 788, 931.$$

In this paper, we propose an efficient algorithm for finding all solutions of equation (2) in the range of $|z| \leq L$ for the fixed values of n in the above list (3). This algorithm is similar to that in [7] in the sense of a one-dimensional quadratic search method that takes $O(L^2)$ steps. The proposed algorithm obtains $|x|$ and $|y|$ (if they exist) by solving a quadratic equation derived from divisors of $2|z|^3 \pm n$, where $|z|$ is a parameter. Efficiency of this algorithm is improved by several number-theoretic sieves and a primality test. We show the results of a computer search that used this algorithm.

2. OUTLINE OF QUADRATIC SEARCH ALGORITHM

Without loss of generality, we may take

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

The solutions are generally classified into the following three cases:

- Case 0: $\{x \geq 0, y \geq 0, z \geq 0\}$ or $\{x < 0, y \geq 0, z \geq 0\}$,
- Case 1: $\{x \geq 0, y < 0, z \geq 0\}$ or $\{x < 0, y < 0, z \geq 0\}$,
- Case 2: $\{x \geq 0, y \geq 0, z < 0\}$ or $\{x < 0, y \geq 0, z < 0\}$.

In case 0, the constraint $0 < x^3 + y^3 + 2z^3 < 1000$ implies $z \leq 7$. Thus, it is easy to find all solutions for case 0, even if a three-dimensional exhaustive search is done. 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 two parameters, say x and y , was usually done. 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 z . In case 1, we put $X = x, Y = -y, Z = z$, and $A = 2Z^3 - n$, where Z is assumed so that $2Z^3 > n$. In case 2, we put $X = -x, Y = y, Z = -z$, and $A = 2Z^3 + n$. Summarizing case 1 and case 2, we have

$$(4) \quad Y^3 - X^3 = A,$$

where $Y > |X| > 0$ and $A > 0$. Equation (4) can be rewritten as a product of two divisors:

$$(5) \quad (Y - X)(Y^2 + YX + X^2) = A.$$

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

$$(6) \quad Y^2 - CY + \frac{C^2 - D}{3} = 0.$$

Note that $(C^2 - D)/3$ is an integer. The value of $Y (> 0)$ is obtained as one of the roots of equation (6) as

$$(7) \quad Y = \frac{C + \sqrt{Q}}{2}, \quad \text{where } Q = \frac{4D - C^2}{3}.$$

From $X = Y - C$, we have

$$(8) \quad X = \frac{-C + \sqrt{Q}}{2}.$$

Note that Q is a positive integer because $4D \equiv C^2 \pmod{3}$ and $C^2 < 4D$, which inequality is derived as

$$C^2 = Y^2 - 2YX + X^2 < Y^2 - 2YX + X^2 + (\sqrt{3}Y + \sqrt{3}X)^2 = 4Y^2 + 4YX + 4X^2 = 4D.$$

If Q is a square, then Y and X , which are represented by equations (7) and (8), become integers because $\sqrt{Q} \equiv C \pmod{2}$.

3. THE ALGORITHM WITH NUMBER-THEORETIC SIEVES

By parametrizing the positive integer $Z (= |z|)$ in the range $S \leq Z \leq L$, our search algorithm utilizing several properties for number-theoretic sieves is as follows. Hereafter, we write $p^e || N$ if $p^e | N$ and $p^{e+1} \nmid N$.

Input: n, S, L

Output: A solution (x, y, z) of $x^3 + y^3 + 2z^3 = n$ with $S \leq |z| \leq L$ or a message “nonexistence” if there is no solution.

Step 1. Let W_m and $V_m(n)$ be the sets of primes satisfying

$$W_m = \{p_i \mid p_i \equiv 2 \pmod{3}, p_i \leq m\},$$

$$V_m(n) = \{p_i \mid p_i \equiv 1 \pmod{3}, (n/2)^{(p_i-1)/3} \pmod{p_i} = 1, p_i \leq m\}.$$

Collect primes $p_i \in W_m$ and $p_i \in V_m(n)$, where $m = 2L$.

Step 2. Put $Z = S$.

Step 3. Check Z by the values of $n \pmod{7}$ and $n \pmod{9}$ by using properties 1 and 2.

Property 1.

- If $n \equiv 1, 2 \pmod{7}$, then $z \equiv 0, 1, 2, -3 \pmod{7}$.
- If $n \equiv -1, -2 \pmod{7}$, then $z \equiv 0, -1, -2, 3 \pmod{7}$.
- If $n \equiv \pm 3 \pmod{7}$, then $z \equiv \pm 1, \pm 2, \pm 3 \pmod{7}$.

Property 2.

- If $n \equiv 2 \pmod{9}$, then $z \equiv 0, 1 \pmod{3}$.
- If $n \equiv -2 \pmod{9}$, then $z \equiv 0, -1 \pmod{3}$.
- If $n \equiv 3, 4 \pmod{9}$, then $z \equiv 1 \pmod{3}$.
- If $n \equiv -3, -4 \pmod{9}$, then $z \equiv -1 \pmod{3}$.

If Z is appropriate as a solution for case 1, then compute $A_1 = 2Z^3 - n$.

If Z is appropriate as a solution for case 2, then compute $A_2 = 2Z^3 + n$.

If Z is not appropriate for both case 1 and case 2, then go to step 11.

(A is a representative of A_1 and A_2 , and each case is carried out individually from step 4 and step 10.)

Step 4. If A is a prime and $A \not\equiv 1 \pmod{3}$ then go to 11.

If A is a prime and $A \equiv 1 \pmod{3}$

then put $C = 1, D = A$.

if A and $C (= 1)$ satisfy properties 3, 4 and 5,

Property 3. If $n \equiv \pm 4 \pmod{9}$, then

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

$$\text{where } k \equiv \begin{cases} \frac{n+8}{3} \pmod{9} & \text{if } n \equiv 4 \pmod{9}, \\ \frac{n-8}{3} \pmod{9} & \text{if } n \equiv -4 \pmod{9}. \end{cases}$$

Property 4.

- 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 $C \equiv -1, \pm 2 \pmod{5}$.

Property 5.

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

then go to step 10.

else go to step 11.

else

Step 5. Put $B = 2Z, H = 1, F = 1$ and $\tilde{A} = A' = A$.

if $3^e \parallel \tilde{A}$ ($e \geq 1$),

then put $H = 3^h, h = \lceil \frac{e}{3} \rceil, B = \lfloor B/3^h \rfloor, F = 3^{e-h}, \tilde{A} = A' = \tilde{A}/3^e$.

If \tilde{A} is a prime, then go to step 9.

else

Step 6. Find prime factors $p_i \in W_B$ of \tilde{A} by a revised trial division:

Put $H' = 1$.

Do while $\{p_i \leq B \text{ and } H' \not\equiv A' \pmod{3}\}$ or $\{p_i^2 \leq B \text{ and } H' \equiv A' \pmod{3}\}$

if $p_i^{e_i} \parallel \tilde{A}$ ($e_i \geq 1$),
 then if $p_i^{h_i} < B$, where

$$h_i = \begin{cases} \lceil \frac{e_i}{3} \rceil + (1 - (\lceil \frac{e_i}{3} \rceil \bmod 2)) & \text{if } e_i \text{ is odd,} \\ \lceil \frac{e_i}{3} \rceil + (\lceil \frac{e_i}{3} \rceil \bmod 2) & \text{if } e_i \text{ is even.} \end{cases}$$

then put $H' = H' \cdot p_i^{h_i}$, $B = \lfloor B/p_i^{h_i} \rfloor$, $F = F \cdot p_i^{e_i - h_i}$, $\tilde{A} = \tilde{A}/p_i^{e_i}$.
 If \tilde{A} is a prime, then go to step 7.
 else go to step 11.

else
 enddo

Step 7. If $H' \equiv A' \pmod{3}$,
 then $H = H \cdot H'$.
 else go to step 11.

Step 8. If \tilde{A} is a prime, then go to step 9.
 Find prime factors $p_i \in V_B(n)$ of \tilde{A} by a trial division:
Do while $p_i < B$
 if $p_i^{e_i} \parallel \tilde{A}$ ($e_i \geq 1$),
 then put $F = F \cdot p_i^{e_i}$, $\tilde{A} = \tilde{A}/p_i^{e_i}$.
 If \tilde{A} is a prime, then go to step 9.

else
 enddo

Step 9. Let F_j be the j th element among combinations of factors of F .
 Choose candidates of divisors C as $C_j = HF_j$ satisfying properties 3, 4, 5, 6 and 7.

- Property 6.** $C < 2Z$ if $Z \gg n$.
- Property 7.** $C \equiv A \pmod{6}$.

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

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

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

Step 11. Put $Z = Z + 1$. If $Z > L$ then output the message “nonexistence”; otherwise, go to step 3.

Remarks. 1. Step 1 corresponds to a precomputation phase; steps 2 to 11 correspond to the main phase. Only primes in the union of W_m and V_m and the prime 3 can become factors of A . Using these prechosen primes, factoring based on trial and division can be more efficiently carried out in the similar way as [7].

Step 6 and step 8 are the most time-consuming parts of the algorithm. Since the number of primes below β is about $\lfloor \beta/\log \beta \rfloor$ for large β , step 6 requires at most about $\lfloor Z/\log 2Z \rfloor$ divisions and step 8 requires at most about $(1/3) \cdot \lfloor Z/\log 2Z \rfloor$ divisions for each value of Z . Thus, the order of this algorithm is $O(cL^2)$, but the constant term c is very small on average.

2. Size restriction of C mainly saves time for trial division in the algorithm. Since $C^2 < 4D = 4A/C$, we have $C < (4A)^{1/3}$. When $Z \gg n$ such that $n < 1000$, $Z > 100000$, we have $A = 2Z^3 \pm n \approx 2Z^3$, and an upper bound of C is obtained as

$C < (8Z^3)^{1/3} = 2Z$. This inequality implies the above Property 6, and it is used in steps 1, 6, 8 and 9. Note that a naive bigger upper bound of C for equation (2) is $\sqrt{2}Z^{3/2}$ without property 6. For equation (1), a more restricted upper bound such as $0.26X$ for varying parameter X was obtained in [7].

3. Congruence restriction between n and z is also effective for a sieve. For given n , the value of z is restricted as Properties 1 and 2, which are slightly different from those in [7]. We have proven that no other values of the modulus for n except 7 and 9 have the sieve effect of excluding some values of z for a solution [10].

4. The value of h in step 5 and the values of h_i in step 6 are derived from the following properties 8 and 9 for equation (2), which are the same as those for equation (1) in [7].

Property 8. If $3^e \parallel A$ ($e \geq 1$), then $3^f \parallel C$, $3^g \parallel D$, $e = f + g$ and $f \geq \lceil \frac{g}{2} \rceil$. Moreover, if $e \geq 1$, then $e \geq 2$, $f \geq 1$ and $g \geq 1$.

Property 9. Let p be a prime with $p \equiv 2 \pmod{3}$. If $p^e \parallel A$ ($e \geq 1$), then $p^f \parallel C$ ($f \geq 0$), $e = f + 2g$ and $f \geq g$, where g is a nonnegative integer.

Note that the six values of n in the list (3) satisfy $n \equiv \pm 3, \pm 4 \pmod{9}$, then $3 \nmid A$.

Remarks. 5. The final value of H in step 6 is a kernel divisor of C , which is always a factor of C , i.e., $H \mid C$. Note that $H \equiv A \pmod{6}$.

6. The first trial division factoring in steps 5 and 6 is carried out for the prime 3 and primes in W_B . At the beginning, an upper bound of searched primes is put as $B = 2Z$. After prime factors $p_i^{e_i}$ of A satisfying $p_i = 3$ or $p_i \equiv 2 \pmod{3}$ are found, the upper bound of primes for the trial division factoring is dynamically reduced to

$$(9) \quad B = \left\lfloor \frac{2Z}{\prod_i p_i^{h_i}} \right\rfloor,$$

where $1 \leq h_i \leq e_i$. Moreover, during the first trial division by primes in W_B , if $H' \equiv A' \pmod{3}$ for the intermediate value of H' , then \tilde{A} has other even (or zero) prime factors in W_B to satisfy $H' \equiv A' \pmod{3}$ for the final value of H' . Thus, the upper bound of primes for the first trial division is further reduced to \sqrt{B} , where B is defined in (9).

After step 6, the congruence $H' \equiv A' \pmod{3}$ is checked. The passing ratio of this check is about 50%. If the check is successful, the second trial division factoring in step 8 is carried out for primes in $V_B(n)$, where B is the final upper bound of the first trial division factoring.

7. Property 3 shows congruence restriction of C for special values $n \equiv \pm 4 \pmod{9}$. If $n \equiv 4 \pmod{9}$ for equation (2), 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 $n \equiv 4 \pmod{9}$, we have $n \equiv x^3 + y^3 + 2z^3 \equiv (3x - 2) + (3y - 2) + 2(3z - 2) \equiv 3(x + y + 2z) - 8 \pmod{27}$, which implies $x + y + z \equiv \frac{n+8}{3} \pmod{9}$. On the other hand, if $n \equiv -4 \pmod{9}$, 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 $n \equiv -4 \pmod{9}$, we have $n \equiv x^3 + y^3 + 2z^3 \equiv (3x + 2) + (3y + 2) + 2(3z + 2) \equiv 3(x + y + 2z) + 8 \pmod{27}$, which implies $x + y + z \equiv \frac{n-8}{3} \pmod{9}$.

8. Properties 4 and 5 of congruence restriction of C were derived from quadratic residuacity for equation (2), which are the same as those for equation (1) in [7].

9. In steps 4, 5, 6, and 8, the primality of A or \tilde{A} is checked by a fast Rabin test. This introduction of a primality test improves the efficiency by about 20%.

10. 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. For $n = 183$, we found a new solution for case 1. We mention the values of the intermediate variables in the algorithm. Let $2\,090\,532 \leq Z \leq 2\,090\,533$. When $Z = 2\,090\,532$, the information of $\{n \equiv 3 \pmod{9}$ and $Z \equiv 0 \pmod{3}\}$ shows that this value of Z is not a solution for both case 1 and case 2. When $Z = 2\,090\,533$, the information of $\{n \equiv 1 \pmod{7}$ and $Z \equiv -3 \pmod{7}\}$ or $\{n \equiv 3 \pmod{9}$ and $Z \equiv 1 \pmod{3}\}$ shows that this value of Z may be a solution for case 1, and it follows that $A = 2Z^3 - n = 18\,272\,630\,746\,578\,898\,691$. Note that A is not a prime, $A \equiv 2 \pmod{3}$ and an initial upper bound of searched primes is $2 \times 2\,090\,533 = 4\,181\,066$. We apply the trial division factoring of step 6 with primes p_i satisfying $p_i \equiv 2 \pmod{3}$ and $p_i \leq 4\,181\,066$. After learning that A has the factor 17, the upper bound of primes for the trial and division is reduced to $\lfloor \frac{2Z}{17} \rfloor = 245\,945$. For an intermediate value of H' , we have $H' \equiv A' \equiv 2 \pmod{3}$. We confirm that A has no prime factor p_i ($\equiv 2 \pmod{3}$) in the range $17 < p_i \leq 495 = \lfloor \sqrt{245\,945} \rfloor$. Thus, we have $H = H' = 17$.

Next, we apply the trial division factoring of step 8 with primes p_i satisfying $p_i \equiv 1 \pmod{3}$, $(183/2)^{(p_i-1)/3} \equiv 1 \pmod{p_i}$ and $p_i \leq 245\,945$. After learning that A has the factor 19081, step 8 ends with $\lfloor \frac{2Z}{17 \cdot 19081} \rfloor = 12$ and $F = 19081$. Thus, the candidates for divisor C satisfying $A \equiv C \equiv 5 \pmod{6}$ are $\{H, H \cdot F\} = \{17, 324\,377 (= 17 \cdot 19081)\}$. For $C = 17$, Q is not the square of an integer. For $C = 324\,377$, we have $Q = (4D - C^2)/3 = 75\,073\,542\,921\,001$, which is the square of 8664499. Thus, we can compute $X = 4\,170\,061$ and $Y = 4\,494\,438$. Finally, we obtain the solution for $n = 183$ as $(x, y, z) = (4\,170\,061, -4\,494\,438, 2\,090\,533)$.

Computer Search. By using the above search algorithm, we performed a computer search for solutions of equation (2) for the six values of n below 1000 in the list (3). Taking into account our computer's power, we put $L = 5 \cdot 10^7$. The CPU-time on a DEC Alpha Server 2100 computer (4 processors, 250 MHz) is about one month.

We found three new integer solutions as follows:

$$(x, y, z, n) = (4\,170\,061, -4\,494\,438, 2\,090\,533, 183),$$

$$(x, y, z, n) = (13\,476\,659, 13\,584\,908, -13\,531\,000, 491),$$

and

$$(x, y, z, n) = (-6\,942\,368, -23\,115\,371, 18\,510\,883, 931).$$

The remaining three missing values of n below 1000 are 148, 671 and 788.

REFERENCES

- [1] J. H. E. Cohn, private communication (1995).
- [2] V.A. Demjanenko, *On sums of four cubes (Russian)*, Izv.Vyssh.Uchebn. Zaved. Matematika, **1966** no. 5 (54) 64–69. MR **34**:2525
- [3] R. K. Guy, *Unsolved Problems in Number Theory*, First Edition, Springer, New York, 1981. MR **83k**:10002
- [4] R. K. Guy, *Unsolved Problems in Number Theory*, Second Edition, Springer, New York, 1994. MR **96e**:11002

- [5] 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), 235-244. MR **94f**:11132
- [6] K. Koyama, *Tables of solutions of the Diophantine equation $x^3 + y^3 + z^3 = n$* , Math. Comp. **62** (1994), 941-942.
- [7] K. Koyama, Y. Tsuruoka and H. Sekigawa, *On searching for solutions of the Diophantine equation $x^3 + y^3 + z^3 = n$* , Math. Comp. **66** (1997), 841-851. MR **97m**:11041
- [8] R. F. Lukes, private communication (1995).
- [9] L. J. Mordell, *Diophantine Equations*, Academic Press, New York, 1969. MR **40**:2600
- [10] H. Sekigawa and K. Koyama, *Nonexistence conditions of a solution for the congruence $x_1^k + \dots + x_s^k \equiv N \pmod{p^n}$* , to appear in Math. Comp., **68** (1999), 1283-1297. MR **99i**:11024

NTT COMMUNICATION SCIENCE LABORATORIES, 2-4 HIKARIDAI, SEIKA-CHO, SORAKU-GUN, KYOTO 619-02 JAPAN

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