MATHEMATICS OF COMPUTATION
Volume 68, Number 227, Pages 1283–1297
S 0025-5718(99)01067-4
Article electronically published on February 24, 1999

NONEXISTENCE CONDITIONS OF A SOLUTION FOR THE CONGRUENCE $x_1^k + \cdots + x_s^k \equiv N \pmod{p^n}$

HIROSHI SEKIGAWA AND KENJI KOYAMA

ABSTRACT. We obtain nonexistence conditions of a solution for of the congruence $x_1^k + \cdots + x_s^k \equiv N \pmod{p^n}$, where $k \geq 2$, $s \geq 2$ and N are integers, and p^n is a prime power. We give nonexistence conditions of the form $(s, N \bmod p^n)$ for $k = 2, 3, 4, 5, 7$, and of the form (s, p^n) for $k = 11, 13, 17, 19$. Furthermore, we complete some tables concerned with Waring's problem in p-adic fields that were computed by Hardy and Littlewood.

1. INTRODUCTION

It is well known that there is no solution to the Diophantine equation $x^3 + y^3 + z^3 = n$ where $n \equiv \pm 4 \pmod 9$ [6]. Furthermore, if $n \equiv 2 \pmod 7$, then there is no solution such that $x \equiv 3, 5, 6 \pmod 7$. In this paper, we consider more general congruences and their conditions for nonexistence of a solution. The analysis and computer search is not only interesting in itself, but is also useful for some number theoretic sieves that efficiently solve some Diophantine equations [5].

Here, we discuss nonexistence conditions of a solution for the following congruence:

$$x_1^k + \cdots + x_s^k \equiv N \pmod{p^n}, \tag{1}$$

where $k \geq 2$, $s \geq 2$ and N are integers, and p^n is a prime power.

As described in Section 4, for a sufficiently large p that depends on k (we can compute the bound), we can completely describe whether there exists a solution for the congruence (1) through theoretical analysis. Therefore, we consider the following problem.

Problem. For a given integer $k \geq 2$, find all integers $s \geq 2$ and prime powers p^n (we are interested in the least n for each pair (s, p)) such that the congruence (1) has no solution for an integer N. In addition, find all the values of $N \bmod p^n$.

After the preliminary Section 2, we consider some special cases in which the nonexistence conditions can be obtained through the theoretical analysis in Section 3. We will show some theoretical results that our search algorithm depends on to obtain all nonexistence conditions in Section 4. Using these results, we describe our search algorithm in Section 5. In Section 6, by theoretical analysis and computer search, we will show the nonexistence conditions of a solution for the

Received by the editor December 1, 1997.
1991 *Mathematics Subject Classification.* Primary 11D79; Secondary 11P05.
Key words and phrases. Congruences, Diophantine equations, solvability, Waring's problem in p-adic fields, computer search.

congruence (1) of the form $(s, N \bmod p^n)$ for $k = 2, 3, 4, 5, 7$, and of the form (s, p^n) for $k = 11, 13, 17, 19$. Finally in Section 7, using the computer search, we consider Waring's problem in p-adic fields; we complete some tables of Hardy and Littlewood, and correct some of their computation errors in [4].

2. Preliminaries

If k is a positive integer and p is a prime we can write $k = p^\tau dl$, where $d = (k, p-1)$ and $p \nmid l$. We write

$$\nu = \begin{cases} \tau+1, & p \text{ odd}, \\ \tau+2, & p=2. \end{cases}$$

If the congruence

$$x_1^k + \cdots + x_s^k \equiv M \pmod{p^\nu} \tag{2}$$

has a primitive solution, then for all positive integers m, the congruence

$$x_1^k + \cdots + x_s^k \equiv M \pmod{p^m}$$

has a primitive solution. This statement follows from the fact that for an integer $a \not\equiv 0 \pmod p$, if the congruence

$$x^k \equiv a \pmod{p^\nu}$$

has a solution, then for all positive integers m, the congruence

$$x^k \equiv a \pmod{p^m} \tag{3}$$

has a solution. Notably, the congruence (3) has a solution for any integer $a \not\equiv 0 \pmod p$ and any positive integer m if and only if $\tau = 0$ and $d = 1$.

The following lemmas are obvious.

Lemma 1. *When $k \geq 2$, then $k \geq \nu$ if and only if $(k,p) \neq (2,2)$. The equality holds if and only if $(k,p) = (4,2)$.*

Lemma 2. *Suppose that $(k,p) \neq (2,2)$, $(4,2)$ and $M \not\equiv 0 \pmod{p^\nu}$. If the congruence (2) has a solution, then it is primitive.*

Lemma 3. *Let p be a prime, $k \geq 2$, and $(k,p) \neq (2,2)$, $(4,2)$. If the congruence*

$$x_1^k + \cdots + x_s^k \equiv 0 \pmod{p^\nu}$$

has no primitive solution, then for any integer $t \not\equiv 0 \pmod p$, the congruence

$$x_1^k + \cdots + x_s^k \equiv p^\nu t \pmod{p^{\nu+1}}$$

has no solution.

3. Nonexistence conditions through theoretical analysis

In this section, we discuss the cases we can treat analytically. First, we can obtain all nonexistence conditions for the following congruence:

$$x_1^k + \cdots + x_s^k \equiv N \pmod{2^n}. \tag{4}$$

Theorem 1.

1. *When k is odd, the congruence $x_1^k + x_2^k = M \pmod{2^m}$ has a primitive solution for any integer M and any positive integer m.*

2. *When k is even, the nonexistence conditions of a solution for the congruence* (4) *are as follows:*
   (a) *If* $k = 2$, *then* $(2, 3 \bmod 4)$, $(3, 7 \bmod 8)$.
   (b) *If* $k = 4$, *then*
$$\begin{aligned}&(2, 3 \bmod 4),\\ &(i, j \bmod 8) \quad \textit{for} \quad 3 \le i \le 6,\ i+1 \le j \le 7,\\ &(i, j \bmod 16) \quad \textit{for} \quad 7 \le i \le 14,\ i+1 \le j \le 15.\end{aligned}$$
   (c) *If* $k \ne 2$, 4, *then*
$$\begin{aligned}&(2, 3 \bmod 4),\\ &(i, j \bmod 2^m) \ \textit{for}\ 3 \le m \le \nu,\ 2^{m-1} - 1 \le i \le 2^m - 2,\\ &\qquad\qquad\qquad\qquad\qquad\qquad i + 1 \le j \le 2^m - 1,\\ &(2^\nu - 1, 2^\nu \bmod 2^{\nu+1}).\end{aligned}$$

Proof. Suppose that k is even (when k is odd, Theorem 1 is clear).

When $k = 2$,
$$(\mathbb{Z}/2^\nu\mathbb{Z})^k = (\mathbb{Z}/8\mathbb{Z})^2 = \{0 \bmod 8,\ 1 \bmod 8,\ 4 \bmod 8\}.$$
Therefore, for $s = 2$, 3 the statement holds. For $s = 4$, we will show that the congruence (4) has a solution for any integer N and any positive integer n. The statement holds for $N \not\equiv 0 \pmod 8$ clearly. For $N \equiv 0 \pmod 8$, put $N = 4^e N'$, where $4 \nmid N'$; then the congruence
$$x_1^2 + x_2^2 + x_3^2 + x_4^2 \equiv N' \pmod 8$$
has a primitive solution, and therefore, for any n, the congruence
$$x_1^2 + x_2^2 + x_3^2 + x_4^2 \equiv N' \pmod{2^n}$$
has a solution $x_i \equiv a_i \pmod{2^n}$. Therefore,
$$(2^e a_1)^2 + (2^e a_2)^2 + (2^e a_3)^2 + (2^e a_4)^2 \equiv N \pmod{2^n},$$
that is, Theorem 1 holds for $k = 2$.

Next we consider the case $k \ne 2$. Note that
$$(\mathbb{Z}/2^\nu\mathbb{Z})^\times \cong \mathbb{Z}/2\mathbb{Z} \oplus \mathbb{Z}/2^\tau\mathbb{Z}$$
and
$$(\mathbb{Z}/2^\nu\mathbb{Z})^k = \{0 \bmod 2^\nu,\ 1 \bmod 2^\nu\}.$$
The latter holds from the former and from $2^k \equiv 0 \pmod{2^\nu}$, which follows from Lemma 1. Therefore, for $s = 2, 3, \ldots, 2^\nu - 2$, Theorem 1 holds.

When $k = 4$, then $2^\nu = 16$. For any integer N and $s = 15$, we will show that the congruence (4) has a solution for all positive integers n. The statement clearly holds for $N \not\equiv 0 \pmod{16}$. For $N \equiv 0 \pmod{16}$, put $N = 16^e N'$, where $16 \nmid N'$; the proof is similar to the case $k = 2$, $s = 4$ and $N \equiv 0 \pmod 8$.

Finally we consider the case $k \ne 2, 4$ and $s = 2^\nu - 1$. When $N \not\equiv 0 \pmod{2^\nu}$, the congruence (4) has a primitive solution for any integer N from Lemma 2; therefore the congruence has a solution for any integer n. When $N \equiv 0 \pmod{2^\nu}$, the congruence has only a trivial solution, and the statement follows from Lemma 3. □

Next, we consider nonexistence conditions of a solution for the congruence
$$x_1^k + \cdots + x_s^k \equiv N \pmod{p^n} \tag{5}$$
for odd primes of p.

Theorem 2. *Let p be an odd prime.*

1. *When $(k, p-1) = p-1$, the nonexistence conditions of a solution for the congruence* (5) *are as follows:*

$$\begin{aligned} &(i, j \bmod p) \text{ for } 2 \le i \le p-2,\ i+1 \le j \le p-1, \\ &(i, j \bmod p^m) \text{ for } 2 \le m \le \nu,\ p^{m-1}-1 \le i \le p^m-2, \\ &\qquad\qquad\qquad\qquad\qquad\qquad i+1 \le j \le p^m-1, \\ &(p^\nu - 1, p^\nu t \bmod p^{\nu+1}) \text{ for } 1 \le t \le p-1. \end{aligned}$$

2. *In the case where $(k, p-1) = (p-1)/2$:*
   (a) *If $(p, \tau) = (3, 0)$, the congruence $x_1^k + x_2^k \equiv M \pmod{3^m}$ has a primitive solution for any integer M and any positive integer m.*
   (b) *If $(p, \tau) \ne (3, 0)$, the nonexistence conditions of a solution for the congruence* (5) *are as follows:*

$$\begin{aligned} &(i, j \bmod p) \text{ for } 2 \le i \le (p-3)/2,\ i+1 \le j \le p-i-1, \\ &(i, j \bmod p^m) \text{ for } 2 \le m \le \nu,\ (p^{m-1}-1)/2 \le i \le (p^m-3)/2, \\ &\qquad\qquad\qquad\qquad\qquad\qquad i+1 \le j \le p^m-i-1. \end{aligned}$$

Proof. Note that $(\mathbb{Z}/p^\nu\mathbb{Z})^\times \cong \mathbb{Z}/(p-1)p^\tau\mathbb{Z}$.

1. When $(k, p-1) = p-1$,

$$(\mathbb{Z}/p^\nu\mathbb{Z})^k = \{0 \bmod p^\nu,\ 1 \bmod p^\nu\}$$

follows from the above fact and from $p^k \equiv 0 \pmod{p^\nu}$. Therefore, for $s = 2, 3, \ldots, p^\nu - 2$, Theorem 2 holds. For $s = p^\nu - 1$, the congruence

$$x_1^k + \cdots + x_s^k \equiv M \pmod{p^\nu}$$

has a solution for any integer M. Therefore, from Lemma 2, for $M \not\equiv 0 \pmod{p^\nu}$, the solution is primitive. For $M \equiv 0 \pmod{p^\nu}$, the above congruence has only a trivial solution, and when $s = p^\nu$, the congruence has a primitive solution. Therefore, the statement holds by Lemma 3.

2. When $(k, p-1) = (p-1)/2$, the proof is similar to the case $(k, p-1) = p-1$ except that

$$(\mathbb{Z}/p^\nu\mathbb{Z})^k = \{0 \bmod p^\nu,\ 1 \bmod p^\nu,\ -1 \bmod p^\nu\},$$

and the congruence

$$x_1^k + x_2^k \equiv 0 \pmod{p^\nu}$$

has a primitive solution.

□

Remark 1. When (a) $p = 2$ or (b) p is odd and $(k, p-1) \ge (p-1)/2$, using Theorems 1 and 2, we can find the minimal s such that the congruence

$$x_1^k + \cdots + x_s^k \equiv M \pmod{p^m}$$

has a primitive solution for any integer M and any positive integer m as follows:

$$\begin{array}{lll}
\text{(a)} & k = 2, & \text{then } 4, \\
 & k = 4, & \text{then } 15, \\
 & k \text{ is even}, \neq 2, 4, & \text{then } 2^{\nu}, \\
 & k \text{ is odd}, & \text{then } 2, \\
\text{(b)} & (k, p-1) = p-1, & \text{then } p^{\nu}, \\
 & (p, \tau) = (3, 0), & \text{then } 2, \\
 & (k, p-1) = (p-1)/2,\ (p, \tau) \neq (3, 0), & \text{then } (p^{\nu} - 1)/2.
\end{array}$$

Hardy and Littlewood obtained these values in [4].

4. Finiteness of search for a fixed k

In this section, we show three kinds of theoretical results that our search algorithm depends on to obtain all nonexistence conditions for the congruence

$$x_1^k + \cdots + x_s^k \equiv N \pmod{p^n}.$$

The first kind of theoretical result shows that for a fixed k we can obtain all nonexistence conditions in a finite number of steps (Theorem 5 and Corollary 2). The second kind is for efficiency (Proposition 1, Lemma 4 and Corollaries 1, 3 and 5). The third kind is for Waring's problem in p-adic integers, which is used in Section 7 (Theorem 6).

First, we observe solutions with modulus p. For $s = 2$, the following famous theorem by Weil [7] clearly shows that the necessary search is finite.

Theorem 3 ([7]). *Let C be a nonsingular projective curve over a finite field $\mathbb{F}_p$. Let L be the number of $\mathbb{F}_p$-rational points, and let g be the genus of C. Then,*

$$|L - p - 1| \leq 2g\sqrt{p}.$$

From Theorem 3, we obtain the following corollary, which is used for the efficient search.

Corollary 1. *Let p be a prime and d be $(k, p-1)$. We write $k = p^{\tau} dl$, where $(p, l) = 1$, and write $d = 2^f d'$, where d' is odd. Put*

$$c = \begin{cases} d & p = 2 \text{ or } p \equiv 1 \pmod{2^{f+1}}, \\ 0 & \text{otherwise}. \end{cases}$$

If p satisfies the inequality

$$p + 1 - c > (dl - 1)(dl - 2)\sqrt{p},$$

then for any integer M the following congruence has a solution:

$$x_1^k + x_2^k \equiv M \pmod{p}. \tag{6}$$

Proof. It is sufficient to prove the case $M \not\equiv 0 \pmod{p}$. Note that the congruence (6) has a solution if and only if the congruence

$$x_1^{dl} + x_2^{dl} \equiv M \pmod{p}$$

has a solution. Apply Theorem 3 to the nonsingular projective curve over $\mathbb{F}_p$ defined by the equation

$$x^{dl} + y^{dl} - Mz^{dl} = 0.$$

The genus of the curve is $(dl-1)(dl-2)/2$. The number of $\mathbb{F}_p$-rational points whose z coordinates are 0 is d, if there exists a nontrivial solution for $x^{dl}+y^{dl}=0$ in $\mathbb{F}_p$, and otherwise 0. Therefore, Corollary 1 follows from the next lemma. □

Lemma 4. *The congruence $x_1^k + x_2^k \equiv 0 \pmod{p}$ has a nontrivial solution if and only if $p=2$ or $p \equiv 1 \pmod{2^{f+1}}$, where $k = 2^f k'$ and k' is odd.*

The following corollary is also derived from Theorem 3, and it gives a computable bound A_k such that for any prime $p > A_k$ and any integer M, the congruence (6) has a solution.

Corollary 2. *Let $k \geq 2$ be an integer and let A_k be*

$$\frac{1}{2}\left((k-1)^2(k-2)^2 + 2(k-1) + (k-1)(k-2)\sqrt{(k-1)^2(k-2)^2+4(k-1)}\right).$$

Then for any prime number $p > A_k$ and for any integer M, the congruence (6) has a solution. The order of magnitude of A_k is k^4.

Proof. In Corollary 1, $c \leq k$ and $dl \leq k$. □

For $s \geq 3$, we can obtain similar results. The following theorem corresponds to Theorem 3 (see [8] for an example).

Theorem 4 ([8]). *Let L be the number of solutions of the congruence*

$$a_1 x_1^{k_1} + \cdots + a_s x_s^{k_s} \equiv 0 \pmod{p},$$

where p does not divide $a_1, \ldots, a_s$. Then

$$|L - p^{s-1}| \leq D(p-1)p^{s/2-1},$$

where $D = \prod_{i=1}^{s}(d_i - 1)$, $d_i = (k_i, p-1)$.

The following two corollaries give conditions when the congruence

$$x_1^k + \cdots + x_s^k \equiv M \pmod{p} \tag{7}$$

has a solution for any integer M; Corollary 3 corresponds to Corollary 1 and Corollary 4 corresponds to Corollary 2.

Corollary 3. *Let $k \geq 2$ and $s \geq 2$ be integers, p be a prime, and d be $(k, p-1)$. If p satisfies the inequality*

$$p^{s/2} > (d-1)^s\left((d-1)p^{1/2}+1\right), \tag{8}$$

then for any integer M, the congruence (7) has a solution.

Proof. It is sufficient to prove this for $M \not\equiv 0 \pmod{p}$. The congruence (7) has a solution if and only if the congruence

$$x_1^k + \cdots + x_s^k - M x_{s+1}^k \equiv 0 \pmod{p} \tag{9}$$

has a solution such that $x_{s+1} \not\equiv 0 \pmod{p}$. From Theorem 4 the number of solutions of the congruence (9) is at least

$$p^s - (d-1)^{s+1}(p-1)p^{(s-1)/2},$$

and that of the congruence (9) such that $x_{s+1} \equiv 0 \pmod{p}$ is at most

$$p^{s-1} + (d-1)^s(p-1)p^{s/2-1},$$

since the latter is equal to the number of solution of the congruence

$$x_1^k + \cdots + x_s^k \equiv 0 \pmod{p}.$$

Therefore, if the following inequality holds, then the congruence (7) has a solution:

$$p^s - (d-1)^{s+1}(p-1)p^{(s-1)/2} > p^{s-1} + (d-1)^s(p-1)p^{s/2-1} \tag{10}$$

Corollary 3 follows from the inequality (10). □

Corollary 4. *Let $k \geq 2$ and $s \geq 3$ be integers, and let*

$$A_k(s) = (k-1)^{2s/(s-1)} k^{2/(s-1)}.$$

Then for any prime number $p \geq A_k(s)$ and for any integer M, the congruence (7) *has a solution.*

Proof. Since $d \leq k$ and $1 < p^{1/2}$, if p satisfies the inequality

$$p^{s/2} \geq (k-1)^s k p^{1/2}, \tag{11}$$

then p satisfies the inequality (8) in Corollary 3. Corollary 4 follows from the inequality (11). □

Remark 2. For small values of k and s, the bound $A_k(s)$ is larger than A_k. The pairs (k, s) such that the inequality $A_k(s) > A_k$ holds are as follows: (a) $(k, 3)$ where $k \geq 2$, (b) $(3, 4)$, $(3, 5)$, $(3, 6)$, $(4, 4)$.

The following two corollaries give conditions when the congruence

$$x_1^k + \cdots + x_s^k \equiv 0 \pmod{p} \tag{12}$$

has a nontrivial zero for an even k; Corollary 5 corresponds to Corollary 1 and Corollary 6 corresponds to Corollary 2.

Corollary 5. *Let $k \geq 2$ be even, $s \geq 3$ be an integer, p be a prime and d be $(k, p-1)$. If p satisfies the inequality*

$$p^{s/2} - (d-1)^s(p-1) > 0,$$

then for any integer M the congruence (12) *has a primitive solution.*

Proof. If the inequality

$$p^{s-1} - (d-1)^s p^{s/2-1} > 0 \tag{13}$$

holds, then the congruence (12) has a nontrivial solution since the number of solutions for this congruence is not less than $p^{s-1} - (d-1)^s(p-1)p^{s/2-1}$. Corollary 5 immediately follows from the inequality (13). □

Corollary 6. *Let $k \geq 2$ be even, $s \geq 3$ be an integer, and let $B_k(s)$ be $(k-1)^{2s/(s-2)}$. Then for any prime number $p \geq B_k(s)$, the congruence* (12) *has a primitive solution.*

Remark 3. The congruence

$$x_1^k + x_2^k + x_3^k \equiv 0 \pmod{p} \tag{14}$$

has a nontrivial solution if and only if the congruence $x_1^k + x_2^k \equiv -1 \pmod{p}$ has a solution. Therefore, if $p > A_k$ then the congruence (14) has a nontrivial solution. The inequality $A_k < B_k(s)$ holds if and only if $k \geq 4$ and $s = 3$, 4.

Next, we are concerned with higher prime powers p^n. Thanks to the fact described in Section 2, we must only examine $n \leq \nu$.

If $s = 2$ and $p|k$, then there exists an integer N such that the congruence has no solution with modulus p^2.

Proposition 1. *Let $k \geq 2$ be an integer. If a prime p divides k, then there exists an integer N such that the congruence*

$$x_1^k + x_2^k \equiv N \pmod{p^2} \tag{15}$$

has no solution.

Proof. It is sufficient to prove that $k = p$. Since $\#\{a^p \mid a \in \mathbb{Z}/p^2\mathbb{Z}\} = p$,

$$\begin{aligned}\#\{a^p + b^p \mid a, b \in \mathbb{Z}/p^2\mathbb{Z}\} \leq \#\{\{a^p, b^p\} \mid a, b \in \mathbb{Z}/p^2\mathbb{Z}\} &= \frac{p^2+p}{2} \\ &< p^2 = \#\mathbb{Z}/p^2\mathbb{Z}.\end{aligned}$$

Therefore, there exists at least one $N \in \mathbb{Z}/p^2\mathbb{Z}$ such that the congruence (15) has no solution. □

With modulus p^n, we need only examine $s < k$, thanks to the next theorem.

Theorem 5 ([4]). *Suppose k is of the form $k = p^\tau dl$, where $d = (k, p-1)$, $p \nmid l$ and p is an odd prime. If $d < (p-1)/2$, then for $s \geq k$ the congruence*

$$x_1^k + \cdots + x_s^k \equiv M \pmod{p^m} \tag{16}$$

has a primitive solution for any integer M and any positive integer m.

Remark 4. Improvements of the form "if $s \geq k^c$ $(c < 1)$ then the congruence has a solution" exist: Birch [1], Dodson [3], Bovey [2], etc. However, their results contain a condition "for all sufficiently large k."

From Corollaries 4, 6 and Remarks 2, 3, we obtain the following theorem, which is a supplement to Theorem 5.

Theorem 6. *Let $k \geq 4$ and $3 \leq s \leq k-1$ be integers, and p be a prime. Then the congruence* (16) *has a primitive solution for any integer M and any positive integer m if the following condition is satisfied, where A_k, $A_k(s)$ and $B_k(s)$ are described as in Corollaries* 2, 4 *and* 6, *respectively.*

1. *When k is odd, then*
   $p > A_k$ *for* $s = 3$,
   $p \geq A_k(s)$ *for* $s \geq 4$.
2. *When k is even, then*
   $p > A_4 = 21 + 12\sqrt{3} = 41.78\ldots$ *for* $(k, s) = (4, 3)$,
   $p \geq B_k(s)$ *for other* (k, s).

Proof. First note that if $p > A_k$ (resp. $p \geq A_k(s)$ or $p \geq B_k(s)$) then $p \nmid k$. Therefore, we need only examine with modulus p whether the congruence has a primitive solution for any integer M.

When k is odd, the congruence has a nontrivial zero even if $s = 2$. Therefore, Theorem 6 follows from Corollary 4 and Remark 2.

When k is even, first we will show that in the range $3 \le s \le k-1$ the inequality $A_k(s) < B_k(s)$, i.e., the inequality

$$\frac{A_k(s)}{B_k(s)} = \left(\frac{k^{s-2}}{(k-1)^s}\right)^{2/(s-1)(s-2)} < 1 \tag{17}$$

holds. But this follows from the following inequalities:

$$\frac{k^{s-2}}{(k-1)^s} = \frac{1}{k^2}\left(1+\frac{1}{k-1}\right)^s \le \frac{1}{k^2}\left(1+\frac{1}{k-1}\right)^{k-1} < \frac{e}{k^2} \le \frac{e}{16} < 1.$$

Therefore, by Corollaries 4, 6 and Remark 3, Theorem 6 holds. □

5. Algorithm

Using the results in Section 4, we will show that for a fixed k, we can obtain all nonexistence conditions for the congruence

$$x_1^k + \cdots + x_s^k \equiv N \pmod{p^n} \tag{18}$$

in a finite number of steps. Note that if $p \nmid k$ and $(k, p-1) = 1$, then the congruence

$$x_1^k + x_2^k \equiv M \pmod{p^m}$$

has a primitive solution for any M and m. Therefore, we only examine primes p such that $p|k$ or $d = (k, p-1) > 1$.

Algorithm (finding all nonexistence conditions).

Input: An integer $k \ge 2$.

Output: All nonexistence conditions for the congruence (18).

1. For $p = 2$ and odd primes p such that $d \ge (p-1)/2$, we completely determine the nonexistence conditions of a solution for the congruence (18) from Theorems 1 and 2.
2. For other primes p, we need only examine $s < k$ from Theorem 5.
   (a) The number of odd primes p that satisfy $p|k$ and $1 \le d < (p-1)/2$ is finite, and it is sufficient to examine whether the congruence (18) has a solution in the range $n \le \nu$ for such a prime p, using Lemmas 3, 4, Proposition 1, and Corollaries 1, 3, 5, or by a computer search.
   (b) There are an infinite number of odd primes p such that $p \nmid k$ and $1 < d < (p-1)/2$, by Dirichlet's Theorem. Since $\nu = 1$ for these p, we need only examine whether the congruence

$$x_1^k + \cdots + x_s^k \equiv N \pmod{p} \tag{19}$$

   has a primitive solution (higher powers of p^n are not necessary).
   For any prime $p > A_k$ and any integer N, the congruence (19) has a solution. When $p \nmid N$ the solution is primitive from Lemma 2.
   Suppose that $p > A_k$ and $p|N$. When $s > 2$ the congruence (19) has a primitive solution (set $x_s = 1$). When $s = 2$ we completely determine whether (19) has a primitive solution from Lemma 4. For primes p where (19) has no primitive solution, we completely determine the values N mod p^2 so that the congruence $x_1^k + x_2^k \equiv N \pmod{p^2}$ has no solution from Lemma 3.
   Therefore, we must only examine $s < k$ and odd primes p that satisfy $p \le A_k$, $p \nmid k$ and $1 < d < (p-1)/2$ to determine whether the congruence (19)

has a primitive solution using Corollaries 3 and 5, or by a computer search.

We illustrate the algorithm when $k = 5$.

Example ($k = 5$)**.** We examine primes p such that $p|5$ or $d = (5, p-1) > 1$; the latter condition is equivalent to $p \equiv 1 \pmod{10}$.

1. Among the above primes, 11 is the only one that satisfies $d \geq (p-1)/2$. From Theorem 2, we completely determine the nonexistence conditions of a solution for the congruence (18).
2. For other primes, we must only examine $s < 5$.
   (a) 5 is the only prime that divides k. Note that $\nu = 2$ for $p = 5$. Since $a^5 \equiv a \pmod 5$ for any a, the congruence (19) has a solution for any $s \geq 2$ and any integer N. When $s = 2$, there exists an integer N such that the congruence
$$x_1^5 + x_2^5 \equiv N \pmod{5^2}$$
   has no solution, by Proposition 1. We search for them and obtain $N \equiv 3$, 4, 5, 9, 10, 12, 13, 15, 16, 20, 21, 22 mod 5^2. When $s = 3$, for the above values N we find that the congruence
$$x_1^5 + x_2^5 + x_3^5 \equiv N \pmod{5^2}$$
   has a primitive solution by a computer search.
   (b) Since the bound A_5 is $76 + 24\sqrt{10} = 151.89\ldots$, the primes we must examine are 31, 41, 61, 71, 101, 131, 151. Since 5 is odd, the congruence
$$x_1^5 + x_2^5 \equiv M \pmod p$$
   has a primitive solution for any integer M and any prime $p > 151$.
   Set $p = 31$ and $s = 2$. The pair $(k, p) = (5, 31)$ does not satisfy the condition in Corollary 1. Therefore, by a computer search, we find that for $N \equiv 3$, 8, 9, 13, 14, 15, 16, 17, 18, 22, 23, 28 mod 31, the congruence
$$x_1^5 + x_2^5 \equiv N \pmod{31}$$
   has no solution. Next set $s = 3$. Since $(k, s, p) = (5, 3, 31)$ does not satisfy the condition in Corollary 3, we must examine whether the congruence
$$x_1^5 + x_2^5 + x_3^5 \equiv N \pmod{31} \tag{20}$$
   has a solution for the above values of N by a computer search. We confirm that for these values of N, the congruence (20) has a primitive solution. Similar procedures are carried out for $p = 41$, 61, 71, 101, 131, 151, and we obtain the results described in Table 2.

6. Tables derived by computer search

Using the algorithm in Section 5, for a fixed k, we obtained the nonexistence conditions of the form $(s, N \bmod p^n)$.

Fortunately, for $k = 2$ and 3, no computer search is necessary.

Case $k = 2$: The bound A_2 is 1. The nonexistence conditions $(s, N \bmod p^n)$ are:

$(2, 3 \bmod 4)$, from Theorem 1,
$(2, pt \bmod p^2)$ for $p \equiv 3 \pmod 4$ and $1 \leq t \leq p-1$, from Lemmas 3 and 4,
$(3, 7 \bmod 8)$, from Theorem 1.

Case $k = 3$: The bound A_3 is $7.46\ldots$. The nonexistence conditions $(s, N \bmod p^n)$ are:

$$
\begin{aligned}
&(2, i \bmod 9), \text{ for } 3 \le i \le 6, \text{ from Theorem 2},\\
&(2, i \bmod 7), \text{ for } i = 3,\ 4, \text{ from Theorem 2},\\
&(3, i \bmod 9), \text{ for } i = 4,\ 5, \text{ from Theorem 2}.
\end{aligned}
$$

For other values of k, we completed tables by computer search. We obtained the nonexistence conditions for $4 \le k \le 10$ and all primes $k \le 47$. To save space, we do not show all of the results; Tables 1, 2 and 3 show the nonexistence conditions $(s, N \bmod p^n)$ for $k = 4$, 5 and 7, respectively. For $k = 7$, integers $N \bmod p^n$ are represented by means of a generator of the cyclic group $((\mathbb{Z}/p^n\mathbb{Z})^\times)^7$ and representatives of the cosets $(\mathbb{Z}/p^n\mathbb{Z})^\times/((\mathbb{Z}/p^n\mathbb{Z})^\times)^7$. For example, the first row means the congruence

$$x_1^7 + x_2^7 \equiv N \pmod{7^2}$$

has no solution for $N \equiv 31^i t \pmod{7^2}$, where $1 \le i \le 6$ and $t = 3$, 9, 27, 43.

Table 4 shows the nonexistence conditions (s, p^n) for $k = 11$, 13, 17, 19. To save space, this table shows only the maximal s for each pair (k, p^n). For example, the row "$k = 11$, $s = 3$, $p^n = 11^2$, 89" means there exist integers N_1 and N_2 such that the congruences

$$
\begin{aligned}
x_1^{11} + \cdots + x_s^{11} &\equiv N_1 \pmod{11^2}\\
x_1^{11} + \cdots + x_s^{11} &\equiv N_2 \pmod{89}
\end{aligned}
$$

have no solution for $s \le 3$.

The computer search was carried out on a DEC Alpha Server 4100/5/400 (400 MHz, 256 MB memory). We show the CPU times for some values of k: less than 0.1 seconds for $k = 7$, approximately 40 seconds for $k = 19$, approximately 20 minutes for $k = 29$, approximately 2 hours for $k = 37$, and approximately 13 hours for $k = 47$.

TABLE 1. Nonexistence conditions $(s, N \bmod p^n)$ for $k = 4$.

s	$N \bmod p^n$
2	7, 8, 11 mod 13
	6, 7, 10, 11 mod 17
	4, 5, 6, 9, 13, 22, 28 mod 29
	$pt \bmod p^2$ $(1 \le t \le p-1)^*$
	$37t \bmod 37^2$ $(1 \le t \le 36)$
3	$29t \bmod 29^2$ $(1 \le t \le 28)$

$*$: $p = 7$, 11, 19, 23, 31.

$A_4 = 41.78\ldots$,

mod 2^n :	see Theorem 1,
mod 3^n, mod 5^n :	see Theorem 2,
mod p^2 for $p \ge 43$, $\equiv 3 \pmod 4$:	see Lemmas 3 and 4,
mod p^2 for $p \ge 53$, $\equiv 5 \pmod 8$:	see Lemmas 3 and 4.

TABLE 2. Nonexistence conditions $(s, N \bmod p^n)$ for $k = 5$.

s	$N \bmod p^n$
2	3, 4, 5, 9, 10, 12, 13, 15, 16, 20, 21, 22 mod 5^2
	3, 8, 9, 13, 14, 15, 16, 17, 18, 22, 23, 28 mod 31
	7, 16, 19, 20, 21, 22, 25, 34 mod 41
	4, 5, 6, 9, 17, 23, 38, 44, 52, 55, 56, 57 mod 61

mod 11^n: see Theorem 2.

TABLE 3. Nonexistence conditions $(s, N \bmod p^n)$ for $k = 7$.

s	$N \bmod p^n$	
	generator of $((\mathbb{Z}/p^n\mathbb{Z})^\times)^7$	representatives of $(\mathbb{Z}/p^n\mathbb{Z})^\times/((\mathbb{Z}/p^n\mathbb{Z})^\times)^7$
2	31 mod 7^2	3, 9, 27, 43 mod 7^2
	12 mod 29	3, 4, 6, 8 mod 29
	37 mod 43	3, 9, 27, 28 mod 43
	14 mod 71	7 mod 71
	40 mod 113	81 mod 113
	28 mod 127	116 mod 127
3	31 mod 7^2	9, 27 mod 7^2
	12 mod 29	8 mod 29
	37 mod 43	27 mod 43

TABLE 4. Nonexistence conditions (s, p^n) for $k = 11, 13, 17, 19$.

k	s	p^n
11	2	199, 331, 353, 419, 463, 617
	3	11^2, 89
	4	67
13	2	13^2, 131, 157, 313, 443, 521, 547, 599, 677, 859, 911, 937, 1171
	4	79
	5	53
17	2	239, 307, 409, 443, 613, 647, 919, 953, 1021, 1123, 1259, 1327, 1361, 1531, 1667
	3	17^2, 137
	5	103
19	2	19^2, 457, 571, 647, 761, 1103, 1217, 1483, 1559, 1597, 1787, 2053, 2129, 2357, 2927
	3	191, 229, 419

mod 23^n for $k = 11$: see Theorem 2.

7. Waring's problem in p-adic fields

Through theoretical analysis and computer search, for several values of k we obtained the nonexistence conditions of a solution for the congruence

$$x_1^k + \cdots + x_s^k \equiv N \pmod{p^n}.$$

These results are closely related to Waring's problem in p-adic fields, namely, the problem of representing any p-adic integer by a sum of s kth powers of p-adic integers. The problem is equivalent to finding a primitive solution of the congruence

$$x_1^k + \cdots + x_s^k \equiv M \pmod{p^\nu} \tag{21}$$

for any rational integer M, except in the case $(k,p) = (4,2)$ (the least s such that any 2-adic integer can be represented as s 4th powers of 2-adic integers is 15, however, the least s such that the congruence (21) has a primitive solution for any rational integer M is 16). We define the number $\Gamma_p(k)$ as the least positive integer s such that the congruence (21) has a primitive solution for all rational integers M. The number $\Gamma(k)$ is defined as $\max\{\Gamma_p(k)\}$, where p runs through all prime numbers.

We utilize the algorithm described in Section 5 for computing $\Gamma(k)$. Obtaining the value of $\Gamma(k)$ is easier than obtaining all nonexistence conditions for k, since the bound, up to which we must examine primes p, decreases whenever we find a prime p such that $\Gamma_q(k) < \Gamma_p(k)$ for all primes $q < p$. Significantly, if we find a prime p such that $\Gamma_p(k) \geq k$ in Step 1, then Step 2 is not necessary, by Theorem 5.

We illustrate how the bound decreases while computing $\Gamma(34)$. In Step 1, the largest value of $\Gamma_p(34)$ is 8 for $p = 2$. Since $8 < k = 34$, by Theorem 6, we must examine whether there exists a prime $p < B_{34}(8) = 11203.93\ldots$ such that $\Gamma_p(34) \geq 9$ using Corollaries 3, 5 or by a computer search. The bound decreases to $B_{34}(10) = 6255.82\ldots$ when we find that $\Gamma_{103}(34) = 10$. Note that we must examine primes $p \leq A_{34} = 115201.99\ldots$ to obtain all nonexistence conditions for $k = 34$.

In [4], Hardy and Littlewood considered the number $\Gamma(k)$; however, their notations were slightly different from ours. Tables 5 and 6 correspond to Tables 1 and 3 in [4], respectively. In the row in Table 5 and in the column in Table 6, "p" refers to the least p such that $\Gamma_p(k) = \Gamma(k)$. There were undecided results (e.g., the entry of $\Gamma(37)$ was "≥ 9") and several errors in [4]. The symbols "$*$" and "†" refer to the undecided results and errors in [4], respectively. It took approximately 6 seconds to obtain Table 5. Note that it took a much longer time to obtain all nonexistence conditions for a single value of k ($k = 29$, as described in Section 6,

Table 5. $\Gamma(k)$ for $3 \leq k \leq 36$ (corresponding to Table 1 in [4]).

k	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18	19
$\Gamma(k)$	4	16	5	9	4	32	13	12	11	16	6	14	15	64	6	27	4
p	3	2	11	3	7	2	3	5	23	2	53	29	31	2	103	3	†191

k	20	21	22	23	24	25	26	27	28	29	30	31	32	33	34	35	36
$\Gamma(k)$	25	24	23	23	32	10	26	40	29	29	31	5	128	33	†10	35	†37
p	5	7	23	47	2	†5	53	3	29	59	31	†373	2	67	103	71	†37

TABLE 6. $\Gamma(k)$ for $37 \le k \le 200$ (corresponding to Table 3 in [4]).

k	$\Gamma(k)$	p	k	$\Gamma(k)$	p	k	$\Gamma(k)$	p	k	$\Gamma(k)$	p
37	*9	149	78	84	13	119	119	239	160	*128	2
38	*9	229	79	*13	317	120	120	241	161	*23	47
39	39	79	80	†64	2	121	*16	727	162	†243	3
40	41	41	81	121	3	122	*21	367	163	*21	653
41	41	83	82	83	83	123	*41	83	164	*83	83
42	49	7	83	83	167	124	*20	373	165	165	331
43	†12	173	84	*49	7	125	125	251	166	167	167
44	44	89	85	*7	1021	126	127	127	167	*5	2339
45	*15	31	86	86	173	127	*21	509	168	168	337
46	47	47	87	*29	59	128	512	2	169	*25	677
47	*10	283	88	89	89	129	†*12	173	170	*20	1021
48	64	2	89	89	179	130	131	131	171	*180	19
49	*13	197	90	90	181	131	131	263	172	173	173
50	†62	5	91	*13	547	132	*67	67	173	173	347
51	51	103	92	*47	47	133	*7	1597	174	174	349
52	53	53	93	*17	373	134	134	269	175	*35	71
53	53	107	94	*18	283	135	135	271	176	†176	353
54	81	3	95	95	191	136	144	17	177	*21	709
55	60	11	96	128	2	137	*17	823	178	179	179
56	56	113	97	*16	389	138	139	139	179	179	359
57	*14	229	98	98	197	139	*18	557	180	181	181
58	59	59	99	99	199	140	140	281	181	*19	1087
59	†5	709	100	125	5	141	141	283	182	*26	53
60	61	61	101	*16	607	142	*19	569	183	183	367
61	*11	367	102	103	103	143	*18	859	184	*47	47
62	*12	373	103	*16	619	144	*73	73	185	*9	149
63	63	127	104	†53	53	145	*29	59	186	186	373
64	256	2	105	105	211	146	146	293	187	*22	1123
65	65	131	106	107	107	147	171	7	188	*22	1129
66	*67	67	107	*15	643	148	149	149	189	189	379
67	*12	269	108	*109	109	149	*8	1193	190	191	191
68	68	137	109	*6	1091	150	151	151	191	191	383
69	69	139	110	121	11	151	*19	907	192	256	2
70	71	71	111	111	223	152	*32	2	193	*21	773
71	*6	569	112	113	113	153	153	307	194	194	389
72	73	73	113	113	227	154	*23	23	195	*65	131
73	*16	293	114	114	229	155	155	311	196	*197	197
74	74	149	115	*23	47	156	169	13	197	*5	3547
75	75	151	116	116	233	157	†*7	1571	198	199	199
76	*16	2	117	*39	79	158	158	317	199	*25	797
77	*14	463	118	†*17	709	159	†53	107	200	200	401

took approximately 20 minutes). The results in Table 6 were obtained in approximately 33 hours. Almost all CPU time was for $k = 167$ and 197 (approximately 9 hours for $k = 167$ and approximately 23 hours for $k = 197$).

Hardy and Littlewood proved that $\Gamma(k) \geq 3$. After declaring they could not prove that $\Gamma(k) \geq 4$, although no case of $\Gamma(k) = 3$ was known, they wrote (p. 539 in [4]):

> We have explored the possibilities $\Gamma(k) = 3$ and $\Gamma(k) = 4$ in the range $2 < k \leq 3000$. Our results are that $\Gamma(k) > 3$ in all cases; and $\Gamma(k) > 4$ except for $k = 2$, 3, 7, 19, for which it is 4, and possibly (but very improbably) for $k = 1163$, 1637, 1861, 1997, 2053.

Therefore, we computed $\Gamma(k)$ for $k = 1163$, 1637, 1861, 1997, 2053. In approximately one minute, we obtained

$$\Gamma_{37217}(1163) = 6, \quad \Gamma_{62207}(1637) = 7, \quad \Gamma_{74441}(1861) = 5,$$
$$\Gamma_{87869}(1997) = 5, \quad \Gamma_{94439}(2053) = 5,$$

where the primes $p = 37217$, 62207, 74441, 87869, 94439 were the least primes satisfying the condition $p \equiv 1 \pmod{k}$ for $k = 1163$, 1637, 1861, 1997, 2053, respectively. That is, $\Gamma(k) \geq 6$, 7, 5, 5, 5 for $k = 1163$, 1637, 1861, 1997, 2053, and we confirmed that $\Gamma(k) > 4$ in the range $19 < k \leq 3000$.

References

1. B. J. Birch, *Waring's problem for* $\mathfrak{p}$*-adic number fields*, Acta Arith. **9** (1964), 169–176. MR **29:**3462
2. J. D. Bovey, *A note on Waring's problem in p-fields*, Acta Arith. **29** (1976), 343–351. MR **58:**21982
3. M. M. Dodson, *On Waring's Problem in p-adic fields*, Acta Arith. **22** (1973), 315–327. MR **49:**2621
4. G. H. Hardy and J. E. Littlewood, *Some problems of 'Partitio Numerorum'* (VIII)*: The number* $\Gamma(k)$ *in Waring's problem*, Proc. London Math. Soc. **28** (1928), 518–542.
5. 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
6. L. J. Mordell, *Diophantine Equations*, Academic Press, New York, 1969. MR **40:**2600
7. A. Weil, *Sur les Courbes Algébriques et les Variétés qui s'en Déduisent*, Hermann, Paris, 1948. MR **10:**262c
8. ———, *Numbers of solutions of equations in finite fields*, Bull. Amer. Math. Soc. **55** (1949), 497–508. MR **10:**592e

NTT Communication Science Laboratories, 2-4 Hikaridai, Seika-cho, Soraku-gun Kyoto 619-0237 Japan

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

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