TOKYO J. MATH.
VOL. 13, No. 2, 1990

On the Equation $s(1^k+2^k+\cdots+x^k)+r=by^z$

Hiroyuki KANO

Keio University

(Communicated by Y. Ito)

§1. Introduction.

We consider the equation

$$s(1^k+2^k+\cdots+x^k)+r=by^z \tag{1}$$

where b, s, r, and k are integer constants and investigate the conditions under which we can assert that the equation has only finitely many solutions in integers $x>0$, $y\geqq 2$, and $z\geqq 2$.

This was proved by K. Győry, R. Tijdeman and M. Voorhoeve [4] in the case $b\neq 0$, $k>0$, $s=1$, and r arbitrary, provided that $k\notin\{1, 3, 5\}$. They also stated the same condition when s is a certain squarefree odd integer.

B. Brindza [2] proved the assertion in the case when s is squarefree and $z\notin\{1, 2, 3, 4, 6\}$ or if s is odd and $k\notin\{1, 2, 3, 5\}$.

In this paper, we obtain new conditions on k, r, and s which allow us to show that (1) has only finitely many solutions in integers $x>0$, $|y|\geqq 2$, and $z\geqq 2$.

§2. Results.

For an integer $n\neq 0$ and a prime p, there exists an integer $m\geqq 0$ for which $p^m \| n$. Then we put $\nu_p(n)=m$ and define, for a nonzero rational number $\alpha=m/n$ with $m, n\in \boldsymbol{Z}$,

$$\nu_p(\alpha)=\nu_p(m)-\nu_p(n)$$

which depends only on α. Also we write $\operatorname{num}\alpha=m$ and $\operatorname{den}\alpha=n$ for a rational number $\alpha=m/n$ with $m, n\in \boldsymbol{Z}$, $n>0$, and $(m, n)=1$, where (m, n) denotes the greatest common divisor of m and n.

THEOREM. *For given integers $b\neq 0$, $r\neq 0$, $s\neq 0$, and $k>0$, the equation*

Received January 31, 1990

(1) *has only finitely many solutions in integers* $x>0$, y *with* $|y|\geqq 2$, *and* $z\geqq 2$, *provided that* k, r, *and* s *satisfy one of the following conditions*;

I) $k\equiv 0 \pmod 2$, $\nu_2(s/r)\leqq 0$,

II) $k\equiv 0 \pmod 2$, $\nu_2(s/r)=2$,

III) $k=2^h$ $(h\in \boldsymbol{N})$, $\nu_2(s/r)=1$,

IV) $k\equiv 3 \pmod 4$, $\nu_2(s/(r(k+1)))\neq k+1$.

REMARK 1. Each condition in Theorem is equivalent to the following statement: If $(s, r)=1$,

I) k is even and s is odd,

II) k is even and $s\equiv 4 \pmod 8$,

III) k is a power of 2 and $s\equiv 2 \pmod 4$,

IV) $k\equiv 3 \pmod 4$ and $\mathrm{num}(s/(k+1))\not\equiv 2^{k+1} \pmod{2^{k+2}}$.

If $(s, r)\neq 1$, s should be replaced by $s/(s, r)$.

REMARK 2. In Theorem we assumed $r\neq 0$. If $r=0$, one can deduce from Theorem 2 in [4] that the equation (1) has only finitely many solutions in integers $x>0$, y with $|y|\geqq 2$, and $z\geqq 2$ provided that $k\notin \{1, 3, 5\}$.

COROLLARY 1. *Let* $b\neq 0$, r, $s\neq 0$, *and* $k>0$ *be given integers. If* s *is odd and* $k\notin\{1, 3, 5\}$, *the equation* (1) *has only finitely many solutions in integers* $x>0$, y *with* $|y|\geqq 2$, *and* $z\geqq 2$.

REMARK 3. If s is odd but $k\in\{1, 3, 5\}$, the equation (1) may have infinitely many solutions in integers $x>0$, $y\geqq 2$, and $z\geqq 2$, under some conditions for b and r; for instance when $s=1$, $k\in\{1, 3, 5\}$, $b=1$, and $r=0$ (cf. [5]).

COROLLARY 2. *For given integers* a, $b\neq 0$, $k>0$, r, *and* $s\neq 0$, *each of the equations*

$$s\{a^k+(a+1)^k+\cdots+x^k\}+r=by^z \qquad (x\geqq a,\ |y|\geqq 2,\ z\geqq 2) \tag{2}$$

and

$$s\{x^k+(x+1)^k+\cdots+a^k\}+r=by^z \qquad (x\leqq a,\ |y|\geqq 2,\ z\geqq 2) \tag{3}$$

has only finitely many solutions in integers x, y, *and* z, *provided that* k *and* s *satisfy one of the following conditions*;

V) $k\equiv 0 \pmod 2$, $s\equiv 1 \pmod 2$,

VI) $k>3$, $k\equiv 3 \pmod 4$, $s\not\equiv 0 \pmod{2^{k+3}}$.

§ 3. Lemmas.

The left-hand side of (1) can be written as

$$\frac{s}{k+1}\{B_{k+1}(x+1)-B_{k+1}\}+r ,$$

where B_i is the Bernoulli number defined by

$$\frac{z}{e^z-1}=\sum_{i=0}^{\infty}\frac{B_i z^i}{i!}$$

and $B_k(x)$ is the Bernoulli polynomial given by

$$B_k(x)=\sum_{i=0}^{k}\binom{k}{i}B_i x^{k-i} .$$

We remark that $B_0=1$, $B_1=-1/2$, $B_i=0$ for odd $i>1$, and

$$B_k(1-x)=(-1)^k B_k(x) , \tag{4}$$

$$B_k'(x)=kB_{k-1}(x) . \tag{5}$$

LEMMA 1 (von Stadt-Clausen's theorem).

$$\operatorname{den} B_{2i}=\prod_{p-1|2i} p \qquad (i\geqq 1) .$$

In particular, $\operatorname{den} B_{2i}$ *is squarefree and* $2 \,\|\, \operatorname{den} B_{2i}$.

LEMMA 2 (K. Győry, R. Tijdeman, and M. Voorhoeve [4] Lemma 1 and Lemma 2). *Let* $P(x)\in \boldsymbol{Q}[x]$ *be a polynomial having at least three simple zeros, and let* $b\neq 0$ *be an integer. Then the equation*

$$P(x)=by^z$$

has only finitely many solutions in integers $x>0$, y *with* $|y|\geqq 2$, *and* $z\geqq 2$.

§ 4. Proofs.

PROOF OF THEOREM. By Lemma 2 we have only to prove that the equation in x,

$$\frac{s}{k+1}\{B_{k+1}(x+1)-B_{k+1}\}+r=0 ,$$

has at least three simple roots. Since the number of the roots as well as their multiplicity of an algebraic equation is not varied by replacing x by a linear polynomial, we have

$$S\{B_{k+1}(x)-B_{k+1}\}+R=0\ , \tag{6}$$

where $S=s/g$, $R=r(k+1)/g$ with $g=(s, r(k+1))$, so that $(S, R)=1$. Furthermore, denoting by d the least common multiple of the denominators of the coefficients appearing in the polynomial on the left-hand side of (6), we have

$$\begin{aligned} P(x) &:= d(k+1)g^{-1}[s\{1^k+2^k+\cdots+(x-1)^k\}+r] \\ &= dS\{B_{k+1}(x)-B_{k+1}\}+dR \\ &= dS\sum_{i=0}^{k}\binom{k+1}{i}B_i x^{k+1-i}+dR \\ &= dS\left\{x^{k+1}-\frac{k+1}{2}x^k+\sum_{i=1}^{k/2}\binom{k+1}{2i}B_{2i}x^{k+1-2i}\right\}+dR=0\ . \end{aligned} \tag{7}$$

Here $P(x)\in \boldsymbol{Z}[x]$ is a primitive polynomial, because of the choice of d and $(S, R)=1$. We note that d is squarefree, $(d, S)=1$, d is odd when S is even, and d is even when S is odd and k is even. We also remark that $\nu_2(S/R)=\nu_2(s/(r(k+1)))$ and that $\nu_2(S/R)=\nu_2(s/r)$ when k is even. Hence in Theorem we may replace $\nu_2(s/r)$ and $\nu_2(s/(r(k+1)))$ by $\nu_2(S/R)$. In what follows, we shall prove that $P(x)=0$ has at least three simple roots. The proof will be divided into four cases I), II), III), and IV).

Case I). k is even and $\nu_2(S/R)\leqq 0$. The last inequality implies that S is odd, since $(S, R)=1$. It follows from (7) that

$$\begin{aligned} P(x)+xP'(x) &= dS\cdot(k+2)x^{k+1}-\frac{1}{2}dS\cdot(k+1)^2x^k \\ &\quad +\sum_{i=1}^{k/2} ds\binom{k+1}{2i}B_{2i}\cdot(k+2-2i)x^{k+1-2i}+dR\ . \end{aligned} \tag{8}$$

Here $2\,\|\,d$, and $ds\binom{k+1}{2i}B_{2i}\in \boldsymbol{Z}$, and so

$$dS\cdot(k+2)\equiv 0 \pmod 2\ , \qquad -\frac{1}{2}dS\cdot(k+1)^2\equiv 1 \pmod 2\ ,$$

$$dS\binom{k+1}{2i}B_{2i}\cdot(k+2-2i)\equiv 0 \pmod 2\ , \qquad dR\equiv 0 \pmod 2\ .$$

Therefore we have

$$P(x)+xP'(x)\equiv x^k \pmod 2\ . \tag{9}$$

Since $\deg P(x)=k+1\geqq 3$, we have only to prove that $P(x)=0$ has no multiple root. Suppose that $P(x)=0$ has a multiple root. Then there exists a non-constant polynomial $Q(x)\in \boldsymbol{Z}[x]$ such that

$$\{Q(x)\}^2 \mid P(x) , \qquad Q(x) \mid P'(x) \tag{10}$$

and so

$$Q(x) \mid P(x)+xP'(x) .$$

Hence we have by (9) and (10)

$$Q(x)\equiv x^m \pmod 2 , \qquad P'(x)\equiv x^m R(x) \pmod 2 \tag{11}$$

for some integer $m\geqq 0$ and some polynomial $R(x)\in \boldsymbol{Z}[x]$. Here we find

$$P'(0)\equiv 1 \pmod 2 ,$$

since $P'(0)=dS\cdot(k+1)B_k$ with $2\,\|\,d$, S odd, k even, and $\operatorname{den} B_k$ is even; so that (11) implies $m=0$. Hence we have $Q(x)\equiv 1 \pmod 2$, and so we may write

$$Q(x)=2S(x)+1 , \qquad S(x)\in \boldsymbol{Z}[x] .$$

Noticing that neither $Q(x)$ nor $S(x)$ is a constant and that $\{2S(x)+1\}^2 \mid P(x)$ by (10), the leading coefficient dS of $P(x)$ is divisible by 4, which is a contradiction.

Case II). k is even and $\nu_2(S/R)=2$. The last equality implies that R and d are odd, since $(S, R)=1$. We also note that $dS\binom{k+1}{i}B_i\equiv 0 \pmod 2$, since $2\,\|\,\operatorname{den} B_i$ by Lemma 1. Hence we have by (7),

$$P(x)\equiv 1 \pmod 2 . \tag{12}$$

Since $\deg P(x)\geqq 3$, we have only to prove that $P(x)=0$ has no multiple root. Suppose that $P(x)=0$ has a multiple root. Then there exist a non-constant polynomial $Q(x)\in \boldsymbol{Z}[x]$ and a polynomial $R(x)\in \boldsymbol{Z}[x]$ such that

$$P(x)=\{Q(x)\}^2 R(x) .$$

Since $\deg P(x)$ is odd, $\deg R(x)$ is odd, and so $R(x)$ is not a constant. Noticing that $Q(x)$, $R(x) \mid P(x)$, we have by (12)

$$Q(x)\equiv 1 \pmod 2 , \qquad R(x)\equiv 1 \pmod 2 ,$$

and so we may write

$$Q(x)=2S(x)+1\ ,\qquad R(x)=2T(x)+1\ ,$$

where $S(x)$, $T(x)\in \boldsymbol{Z}[x]$. Hence we get

$$P(x)=\{2S(x)+1\}^2\{2T(x)+1\}\ ,$$

where neither $S(x)$ nor $T(x)$ is a constant. Therefore the leading coefficient dS of $P(x)$ is divisible by 8, which is a contradiction.

Case III). $k=2^h$ ($h\in \boldsymbol{N}$) and $\nu_2(S/R)=1$. The last equality implies that R and d are odd since $(S, R)=1$. As in the Case I), we have (8). Noticing that k is even, $2\|S$, and $dS\binom{k+1}{2i}B_{2i}\in \boldsymbol{Z}$, we find

$$dS\cdot(k+2)\equiv 0 \pmod 2\ ,\qquad -\frac{1}{2}dS\cdot(k+1)^2\equiv 1 \pmod 2\ ,$$

$$dS\binom{k+1}{2i}B_{2i}\cdot(k+2-2i)\equiv 0 \pmod 2\ ,\qquad dR\equiv 1 \pmod 2\ .$$

Therefore it follows from (8) with $k=2^h$ that

$$P(x)+xP'(x)\equiv x^k+1\equiv(x+1)^k \pmod 2\ . \tag{13}$$

We will show that $P(x)=0$ has no multiple root. Suppose that $P(x)=0$ has a multiple root. Then there exists a non-constant polynomial $Q(x)\in \boldsymbol{Z}[x]$ such that

$$\{Q(x)\}^2\mid P(x)\ ,\qquad Q(x)\mid P'(x)\ ,$$

and so

$$Q(x)\mid P(x)+xP'(x)\ .$$

Hence it follows from (13) that

$$Q(x)\equiv(x+1)^m \pmod 2\ ,\qquad P(x)\equiv(x+1)^{2m}R(x) \pmod 2 \tag{14}$$

for some integer $m\geqq 0$ and polynomial $R(x)\in \boldsymbol{Z}[x]$. But we have by (7)

$$P(3)=d(k+1)S\cdot(1+2^k)+dR\ ,$$

so that

$$P(3)\equiv 1 \pmod 2$$

since d and R are odd and S is even. On the other hand, we have by (14)

$$P(3)\equiv 4^{2m}R(3) \pmod 2\ .$$

Thus we get $m=0$, and hence (14) gives $Q(x)\equiv 1 \pmod 2$. Therefore, as in the Case I), we find $4 \mid dS$, which is a contradiction.

Case IV). $k\equiv 3 \pmod 4$ and $(d, S)=(S, R)=1$. It follows from (5) and (8) that

$$P'(x)=dS\cdot(k+1)B_k(x) .$$

Since k is odd, we can show, by the same way as in the proof of Theorem 2 in [4], that the equation $B_k(x)=0$ as well as $P'(x)=0$ has no multiple root. Hence the multiplicity of a root of $P(x)=0$ is at most 2. Thus we can write

$$P(x)=\{Q(x)\}^2R(x) , \tag{15}$$

where $Q(x)$, $R(x)\in \boldsymbol{Z}[x]$ have only simple zeros and no common zeros. It is enough to prove that

$$\deg R(x)\geqq 3 .$$

For this we prove first that

$$P\left(\frac{1}{2}\right)\neq 0 . \tag{16}$$

If S is odd, it is easily seen that $2^{k+1}P(1/2)$ is odd for odd d and $2^kP(1/2)$ is odd for even d; and hence (16) holds for odd S. If S is even, then d and R are odd. We put $S=\nu_2(S)S'$, where S' is odd, so that $2dS'\binom{k+1}{i}B_i\in \boldsymbol{Z}$. We note that $\nu_2(S/R)=\nu_2(S)\neq k+1$ by IV). If $\nu_2(S)<k+1$,

$$2^{k+1-\nu_2(S)}P\left(\frac{1}{2}\right)=dS'-(k+1)dS'+2\sum_{i=2}^{k}2dS'\binom{k+1}{i}B_i2^{i-2}+2^{k+1-\nu_2(S)}dR$$

is odd. Similarly $P(1/2)$ is odd when $\nu_2(s)>k+1$. Hence (16) holds also for even S.

Now it follows from (4) and (7) with odd k that

$$P(1-x)=P(x) .$$

Hence the roots of $P(x)=0$ are located symmetrically about $x=1/2$, and the multiplicity of the corresponding roots are equal. The same is true for the roots of $Q(x)=0$. By (16) we get $\deg Q(x)\equiv 0 \pmod 2$, so that $\deg\{Q(x)\}^2\equiv 0 \pmod 4$. Hence we find by (15)

$$\deg R(x)\equiv \deg P(x)=k+1\equiv 0 \pmod 4 .$$

Thus it is sufficient to prove that $R(x)$ is not a constant. Suppose that $R(x)$ is a constant, say $c\neq 0$. Then we may write

$$P(x)=c\{Q(x)\}^2 \tag{17}$$

where $\deg Q(x)=(k+1)/2$. Recalling that every term of $P(x)$ of odd degree not greater than $(k+1)/2$ is zero and $P(0)\neq 0$, we can prove by comparing the coefficients of the both sides of (17), that every term of odd degree of $Q(x)$ and also that of $P(x)$ is zero, which contradicts the fact that the coefficient of x^k of $P(x)$, where k is odd, is different from zero. The proof of our Theorem is now complete.

PROOF OF COROLLARY 1. By the result of B. Brindza [2] mentioned in the introduction, we have only to prove the statement when $k=2$. Thus if $r\neq 0$, Corollary 1 follows from Case I) in Theorem. The case of $r=0$ is already discussed in Remark 2.

PROOF OF COROLLARY 2. The conditions V) and VI) are special cases of I) and IV) in Theorem respectively. Equation (2) has a specific form of (1) with suitable modified r. (3) is reduced to (2) by multiplying the both sides by $(-1)^k$.

I would like to express my thanks to Professor Iekata Shiokawa for his valuable advice concerning the paper.

References

[1] Z. I. BOREVICH and I. R. SHAFAREVICH, *Number Theory*, 2nd. ed., Academic Press, 1967.

[2] B. BRINDZA, On some generalizations of the diophantine equation $1^k+2^k+\cdots+x^k=y^z$, Acta Arith., **44** (1984), 99–107.

[3] K. DILCHER, On a diophantine equation involving quadratic characters, Compositio Math., **57** (1986), 383–403.

[4] K. GYŐRY, R. TIJDEMAN and M. VOORHOEVE, On the equation $1^k+2^k+\cdots+x^k=y^z$, Acta Arith., **37** (1980), 233–240.

[5] J. J. SCHÄFFER, The equation $1^p+2^p+3^p+\cdots+n^p=m^q$, Acta Math., **95** (1956), 155–189.

[6] T. N. SHOREY, A. J. VAN DER POORTEN, R. TIJDEMAN and A. SCHINZEL, Applications of the Gel'fond-Baker method to Diophantine equations, *Transcendence Theory: Advances and Applications*, Academic Press, 1979, 59–77.

[7] J. URBANOWICZ, On the equation $f(1)1^k+f(2)2^k+\cdots+f(x)x^k+R(x)=by^z$, Acta Arith., **51** (1988), 349–368.

Present Address:
DEPARTMENT OF MATHEMATICS, FACULTY OF SCIENCE AND TECHNOLOGY, KEIO UNIVERSITY
HIYOSHI, KOHOKU-KU, YOKOHAMA 223, JAPAN