ON THE SUM OF TWO SQUARES AND AT MOST K POWERS OF 2

Dan Wang
School of Mathematics and Statistics, Qilu University of Technology (Shandong Academy of Sciences), Jinan, Shandong, China
wangdan-10@hotmail.com

Received: 12/17/19, Revised: 9/1/20, Accepted: 5/20/21, Published: 5/27/21

Abstract

We prove that if there exists an integer subject to some congruence conditions that cannot be expressed as the sum of two squares of integers and at most k powers of $2, k = 3, 4$, then there are infinitely many such integers.

1. Introduction and Main Results

It is well known that there are infinitely many integers that cannot be expressed as the sum of two squares; in particular, this is true for any integer whose prime factorization contains a prime $p \equiv 3(\text{mod } 4)$ to an odd power [2, Theorem 278].

Crocker [1] proved that one can generate an infinitude of integers not expressible as a sum of two squares and at most two powers of 2, if one can show the existence of a single integer $N_0 \equiv 0(\text{mod } 36)$ that cannot be so expressed. Crocker listed 142 congruence conditions on such an N_0 and proveed that the first example must be below $2^{1417} = 3.62 \cdots \times 10^{426}$.

Platt and Trudgian [3] proved that there are infinitely many integers that cannot be expressed as the sum of two squares and at most one power of 2, and also gave a shorter proof that there are infinitely many integers that cannot be expressed as the sum of two squares and at most two powers of 2.

Inspired by these results, we prove that if there exists an integer subject to some congruence conditions that cannot be expressed as the sum of two squares of integers and at most k powers of $2, k = 3, 4$, then there are infinitely many such integers. We shall give the following two theorems.

Theorem 1. *If we can find an integer n satisfying $n \equiv 0 \ (mod\, 90)$, $n \equiv 2 \ (mod\, (2^a - 1)^2), a \geq 3$, which cannot be expressed as the sum of two squares and at most three powers of 2, then there are infinitely many such integers.*

Theorem 2. *If we can find an integer n satisfying $n \equiv 0 \pmod{90}$, $n \equiv 2 \pmod{(2^a + 2^b - 1)^2}$, $a, b \geq 2$, which cannot be expressed as the sum of two squares and at most four powers of 2, then there are infinitely many such integers.*

2. Proofs of Main Results

Lemma 1. *If an integer n cannot be expressed as the sum of two squares, then neither can $2^\alpha n$ for $\alpha \geq 0$.*

Proof. See Lemma 1 of [3]. □

Lemma 2. *If an integer $n \equiv 0 \pmod{18}$ cannot be expressed as the sum of two squares and at most two powers of 2, then neither can $2^\alpha n$ for any integer $\alpha \geq 0$.*

Proof. See Lemma 3 of [3]. □

We now give the proof of Theorem 1.

Proof of Theorem 1. By the hypothesis of Theorem 1, we know that $n, n - 2^a, n - 2^a - 2^b$ and $n - 2^a - 2^b - 2^c$, with $a, b, c \geq 0$, are not the sum of two squares. Next we prove that $2n, 2n - 2^a, 2n - 2^a - 2^b$, and $2n - 2^a - 2^b - 2^c$ with $a, b, c \geq 0$, cannot be expressed as the sum of two squares.

By Lemma 2.1, we know that $2n$ cannot be expressed as the sum of two squares. To prove that $2n - 2^a, a \geq 0$, is not the sum of two squares, by the hypothesis that $n \equiv 0 \pmod{90}$, we have $2n \equiv 0 \pmod 4$ and easily get $2n - 1 \equiv 3 \pmod 4$. By the proof of Lemma 3 of [3], we know that $2n - 1$ cannot be expressed as the sum of two squares. By Lemma 2.1 and the hypothetical conditions that $n - 2^a, a \geq 0$, cannot be expressed as the sum of two squares, we get that $2n - 2^a, a \geq 1$ cannot be expressed as the sum of two squares.

We now show that $2n - 2^a - 2^b, a \geq 0, b \geq 0$, is not the sum of two squares. First, by Lemma 2.1 and the hypothetical conditions that $n - 2^a, n - 2^a - 2^b$, with $a, b \geq 0$, are not the sum of two squares, we obtain that $2n - 2^a - 2^b, a \geq 1, b \geq 1$ and $2n - 2^a - 2^b, a = 0, b = 0$, are not the sum of two squares. Also, when $b = 0, a = 1$, we consider $2n - 3 \equiv 6 \pmod 9$; The only values of $x^2 \pmod 9$ are $0, 1, 4$, and 7, and therefore $2n - 3$ cannot be the sum of two squares.

When $b = 0, a \geq 2$, we consider $2n - 1 - 2^a \equiv 3 \pmod 4$. By the proof of Lemma 3 of Platt and Trudgian [3], we know that $2n - 1$ cannot be expressed as the sum of two squares, and therefore $2n - 2^a - 2^b, a \geq 0, b \geq 0$, cannot be expressed as the sum of two squares.

We next show that $2n - 2^a - 2^b - 2^c, a \geq 0, b \geq 0, c \geq 0$, cannot be the sum of two squares. By Lemma 2.1 and the hypothesis that $n - 2^a - 2^b - 2^c$ with $a, b, c \geq 0$ are not the sum of two squares, we deduce that $2n - 2^a - 2^b - 2^c, a \geq 1, b \geq 1, c \geq 1$,

are not the sum of two squares. When $a = 0, b = 0, c = 0$, i.e, $2n - 3 \equiv 6 \pmod 9$, then by Case 2, we know that $2n - 3$ cannot be the sum of two squares.

When $a \geq 1, b = 0, c = 0$, i.e, $2n - 2 - 2^a$, this case is covered by Lemma 2.1.

When $a \geq 1, b \geq 1, c = 0$, i.e, $2n - 1 - 2^a - 2^b$,, we consider four possibilities as listed in the following array:

$$2n-1-2^a-2^b, a \geq 1, b \geq 1, = \begin{cases} 2n-1-4 \equiv 3 \pmod 4, \text{a} = 1, \text{b} = 1, \\ 2n-1-2^a-2^b \equiv 3 \pmod 4, \text{a} \geq 2, \text{b} \geq 2, \\ 2n-3-2^2, a = 2, b = 1, \\ 2n-3-2^a, \ a \geq 3, b = 1. \end{cases}$$

In the first two subcases, then, by the proof of Lemma 3 of [3], we know that $2n-1$ cannot be expressed as the sum of two squares.

Now consider $2n-7 \equiv 3 \pmod{10}$. The only values of $x^2 \pmod{10}$ are $0, 1, 4, 5, 6$ and 9, and therefore $2n - 7$ cannot be the sum of two squares.

Next we consider the case of $2n-3-2^a, \ a \geq 3$. If $n-2 \equiv 0 \pmod{(2^a-1)^2}$, then $2(n-2)-(2^a-1) \equiv -(2^a-1) \pmod{(2^a-1)^2}$. Since $2^a-1 \equiv 3 \pmod 4$, there exists some q^m, $q \equiv 3 \pmod 4$ prime and m odd, dividing $2^a - 1$, and $\left(\frac{(2^a-1)}{q^m}, q\right) = 1$. Then $2(n-2)-(2^a-1) \equiv -(2^a-1) = -q^m \left(\frac{(2^a-1)}{q^m}\right) \pmod{q^{2m}}$. However, a sum of two squares must be congruent to $q^{m'} m'' \bmod q^{2m}$ for some even m' and $(m'', q) = 1$ when q is a prime such that $q \equiv 3 \pmod 4$, and therefore $2(n-2) - (2^a - 1)$ is not the sum of two squares, namely, $2n - 3 - 2^a, \ a \geq 3$, cannot be the sum of two squares.

Combining Case 1 to Case 3, we prove that if an integer n satisfying $n \equiv 0 \pmod{90}$, $n \equiv 2 \pmod{(2^a-1)^2}, a \geq 3$ cannot be expressed as the sum of two squares and at most three powers of 2, then $2n$ cannot be expressed as the sum of two squares and at most three powers of 2. By iterative method, we complete Theorem 1. □

Proof of Theorem 2. By hypothesis, we know that $n, n-2^a, n-2^a-2^b, n-2^a-2^b-2^c$ and $n-2^a-2^b-2^c-2^d$, with $a, b, c, d \geq 0$, are not the sum of two squares. Next we prove that $2n, 2n-2^a, 2n-2^a-2^b, 2n-2^a-2^b-2^c$, and $2n-2^a-2^b-2^c-2^d$, with $a, b, c, d \geq 0$, cannot be expressed as the sum of two squares.

By Lemma 2.1, we know that $2n, 2n-2^{a+1}$ (where $a \geq 0$), $2n-2^{a+1}-2^{b+1}$ (where $a, b \geq 0$), $2n-2^{a+1}-2^{b+1}-2^{c+1}$ (where $a, b, c \geq 0$), and $2n-2^{a+1}-2^{b+1}-2^{c+1}-2^{d+1}$ (where $a, b, c, d \geq 0$), cannot be expressed as the sum of two squares.

In Theorem 1, we have proved that $2n, 2n-2^a, 2n-2^a-2^b$, and $2n-2^a-2^b-2^c, a, b, c \geq 0$, cannot be expressed as the sum of two squares. Therefore we only prove $2n-2^a-2^b-2^c-2^d$ with $a, b, c, d \geq 0$, cannot be expressed as the sum of two squares.

We consider five possibilities: (i) $a, b, c, d \geq 1$; (ii) $a = b = c = d = 0$; (iii) $a = 1$,

$b = c = d = 0$; (iv) $a, b \geq 1$ and $c = d = 0$; (v) $a = b = c = 1$ and $d = 0$.

For (i), by Lemma 2.1 and the hypothesis that $n-2^a-2^b-2^c-2^d$, with $a, b, c, d \geq 0$, are not the sum of two squares, we know that $2n - 2^a - 2^b - 2^c - 2^d, a, b, c, d \geq 1$, are also not the sum of two squares.

When $a = 0, b = 0, c = 0, d = 0$, i.e, $2n - 4$, then by hypothesis and Lemma 2.1, we know that $2n - 2^{a+1}$(where $a \geq 0$) cannot be expressed as the sum of two squares, and therefore $2n - 4$ cannot be the sum of two squares.

When $a \geq 1, b = 0, c = 0, d = 0$, i.e, $2n - 3 - 2^a$, this case is covered by Case 3 of the proof of Theorem 1.

When $a \geq 1, b \geq 1, c = 0, d = 0$, i.e, $2n - 2 - 2^a - 2^b$, then by hypothesis and Lemma 2.1, we know that $2n - 2^{a+1} - 2^{b+1} - 2^{c+1}$ (where $a, b, c \geq 0$), cannot be expressed as the sum of two squares, and therefore $2n - 2 - 2^a - 2^b$ cannot be the sum of two squares.

When $a \geq 1, b \geq 1, c \geq 1, d = 0$, i.e, $2n - 1 - 2^a - 2^b - 2^c$, we consider four subcases as given in the following array:

$$
\begin{aligned}
& 2n - 1 - 2^a - 2^b - 2^c, a \geq 1, b \geq 1, c \geq 1, \\
= & \begin{cases} 2n - 7(a = 1, b = 1, c = 1), \\ 2n - 5 - 2^a \equiv 3 \pmod 4 (\mathrm{a} \geq 2, \mathrm{b} = 1, \mathrm{c} = 1), \\ 2n - 3 - 2^a - 2^b (a \geq 2, b \geq 2, c = 1), \\ 2n - 1 - 2^a - 2^b - 2^c \equiv 3 \pmod 4 (\mathrm{a} \geq 2, \mathrm{b} \geq 2, \mathrm{c} \geq 2). \end{cases}
\end{aligned}
$$

We consider $2n - 3 - 2^a - 2^b,\ a, b \geq 2$, and let $n - 2 \equiv 0 \pmod{(2^a + 2^b - 1)^2}$. Then $2(n-2) - (2^a + 2^b - 1) \equiv -(2^a + 2^b - 1) \pmod{(2^a + 2^b - 1)^2}$. For $2^a + 2^b - 1 \equiv 3 \pmod 4$, there exists some q^m, $q \equiv 3 \pmod 4$ prime and m odd, dividing $2^a + 2^b - 1$, and $\left(\frac{(2^a+2^b-1)}{q^m}, q\right) = 1$. Then $2(n-2) - (2^a + 2^b - 1) \equiv -(2^a + 2^b - 1) = -q^m \left(\frac{(2^a+2^b-1)}{q^m}\right) \pmod{q^{2m}}$. However, a sum of two squares must be congruent to $q^{m'} m'' \bmod q^{2m}$ for some even m' and $(m'', q) = 1$ when q is a prime such that $q \equiv 3 \pmod 4$. Therefore, $2(n-2) - (2^a + 2^b - 1)$ is not the sum of two squares, namely $2n - 3 - 2^a - 2^b$, a, $b \geq 2$, cannot be the sum of two squares.

Combining all cases, we proved that if an integer n satisfying $n \equiv 0 \pmod{90}$, $n \equiv 2 \pmod{(2^a + 2^b - 1)^2}, a, b \geq 2$ cannot be expressed as the sum of two squares and at most four powers of 2, then $2n$ cannot be expressed as the sum of two squares and at most four powers of 2.

From $n \equiv 2 \pmod{(2^a + 2^b - 1)^2}, a, b \geq 2$, we can easily get $n \equiv 2 \pmod{(2^a - 1)^2}, a \geq 3$, and therefore we only need $n \equiv 2 \pmod{(2^a + 2^b - 1)^2}, a, b \geq 2$. By iterative method, we complete Theorem 2. □

For $k = 5$, using a similar method, we have the following result: if n is an integer satisfying $n \equiv 0 \pmod{90}$, and $n \equiv 2 \pmod{(2^a + 2^b + 2^c - 1)^2}, a, b, c \geq 2$ cannot be expressed as the sum of two squares and at most five powers of 2, then there are

infinitely many such integers. Further, for $k \geq 6$ (but not too large), we may use a similar method to study the problem.

Acknowledgements. The author is very grateful to the reviewers for many valuable suggestions and comments. Many thanks to Timothy Scott Trudgian for many useful discussions and valuable suggestions and the UNSW Study Abroad Research Practicum Program. This work is supported by a scholarship from the China Scholarship Council.

References

[1] R. C. Crocker, On the sum of a prime and two powers of two, *Pacific J. Math.* **36** (1971), 103–107.

[2] G. H. Hardy and E. M. Wright, *An Introduction to the Theory of Numbers, Sixth Edition*, Oxford Univ. Press, Oxford, 2008.

[3] D. Platt and T. Trudgian, On the sum of two squares and at most two powers of 2, *Amer. Math. Monthly.* **124** (2017), 737–740.

[4] T. Foo, On the sum of integers from some multiplicative sets and some powers of integers, *Integers* **18** (2018), Article A27, 5 pp.