Values of certain binary partition function represented by sum of three squares

Maciej Ulas (joint work with Bartosz Sobolewski)

Institute of Mathematics, Jagiellonian University, Kraków, Poland

Online Number Theory Seminar, September 14th, 2022

Short plan of the presentation

- Introduction and motivation

Short plan of the presentation

- Introduction and motivation
- The equation $b(n) = x^2 + y^2 + z^2$

Short plan of the presentation

- Introduction and motivation
- The equation $b(n) = x^2 + y^2 + z^2$
- The equation $b_3(n) = x^2 + y^2 + z^2$

Short plan of the presentation

- Introduction and motivation
- The equation $b(n) = x^2 + y^2 + z^2$
- The equation $b_3(n) = x^2 + y^2 + z^2$
- The equation $b_{2^k-1}(n) = x^2 + y^2 + z^2$ for $k \geq 3$

Short plan of the presentation

- Introduction and motivation
- The equation $b(n) = x^2 + y^2 + z^2$
- The equation $b_3(n) = x^2 + y^2 + z^2$
- The equation $b_{2^k-1}(n) = x^2 + y^2 + z^2$ for $k \geq 3$
- Computational results, questions, problems and conjectures

Introduction and motivation

In 1798 Legendre proved that if N is a positive integer and

$$N = x^2 + y^2 + z^2$$

for some $x, y, z \in \mathbb{Z}$, then N is not of the form $4^k(8s + 7)$ for $k, s \in \mathbb{N}$. In particular, the natural density of the set of integers which can not be represented by sum of three squares is equal to $1/6$.

In 1798 Legendre proved that if N is a positive integer and

$$N = x^2 + y^2 + z^2$$

for some $x, y, z \in \mathbb{Z}$, then N is not of the form $4^k(8s+7)$ for $k, s \in \mathbb{N}$. In particular, the natural density of the set of integers which can not be represented by sum of three squares is equal to $1/6$.

This rises an interesting question whether, for a given sequence of integers $(u_n)_{n\in\mathbb{N}}$, there are infinitely many solutions of the Diophantine equation

$$u_n = x^2 + y^2 + z^2. \tag{1}$$

It is clear to characterize the solutions of (1) it is necessary to have a good understanding of the 2-adic behavior, or to be more precise the 2-adic valuation, of the terms of the sequence $(u_n)_{n\in\mathbb{N}}$.

Especially interesting is the case, when u_n has a combinatorial meaning. The equation (1) with $u_n = \binom{2n}{n}$ was investigated by Granville and Zhu. They characterized those $n \in \mathbb{N}$ such that (1) has a solution in x, y, z. The obtained characterization is equivalent with the existence of certain patterns in (unique) binary expansion of n.

Especially interesting is the case, when u_n has a combinatorial meaning. The equation (1) with $u_n = \binom{2n}{n}$ was investigated by Granville and Zhu. They characterized those $n \in \mathbb{N}$ such that (1) has a solution in x, y, z. The obtained characterization is equivalent with the existence of certain patterns in (unique) binary expansion of n.

In particular, the set of integers n, for which $\binom{2n}{n}$ can be represented as a sum of three squares, has asymptotic density $7/8$ in the set of all natural number. The cited authors obtained also characterization of those n such that (1) with $u_n = n!$ has no solutions. A different approach, via automatic sequences, to this problem was presented by Deshouillers and Luca. They showed that if

$$S = \{n : \ n! \neq x^2 + y^2 + z^2\}$$

then

$$S(x) = \#\{n \leq x : \ n \in S\} = \frac{7}{8}x + O(x^{2/3}).$$

Especially interesting is the case, when u_n has a combinatorial meaning. The equation (1) with $u_n = \binom{2n}{n}$ was investigated by Granville and Zhu. They characterized those $n \in \mathbb{N}$ such that (1) has a solution in x, y, z. The obtained characterization is equivalent with the existence of certain patterns in (unique) binary expansion of n.

In particular, the set of integers n, for which $\binom{2n}{n}$ can be represented as a sum of three squares, has asymptotic density $7/8$ in the set of all natural number. The cited authors obtained also characterization of those n such that (1) with $u_n = n!$ has no solutions. A different approach, via automatic sequences, to this problem was presented by Deshouillers and Luca. They showed that if

$$S = \{n : \ n! \neq x^2 + y^2 + z^2\}$$

then

$$S(x) = \#\{n \leq x : \ n \in S\} = \frac{7}{8}x + O(x^{2/3}).$$

This result was improved by Hajdu and Papp to

$$S(x) = 7/8x + O(x^{1/2}\log^2 x)$$

and recently by Burns to $S(x) = 7/8x + O(x^{1/2})$.

We follow the same line of research and consider first the equation (1) with $u_n = b(n)$ being binary partition function. More precisely, let $b(n)$ counts the number of partitions of n with parts being powers of two. For example, $b(4) = 4$ because

$$4 = 2^2 = 2 + 2 = 1 + 1 + 2 = 1 + 1 + 1 + 1$$

are all possible representations of 4 as a sum of powers of two. The sequence $(b(n))_{n\in\mathbb{N}}$ was already introduced by Euler.

We follow the same line of research and consider first the equation (1) with $u_n = b(n)$ being binary partition function. More precisely, let $b(n)$ counts the number of partitions of n with parts being powers of two. For example, $b(4) = 4$ because

$$4 = 2^2 = 2 + 2 = 1 + 1 + 2 = 1 + 1 + 1 + 1$$

are all possible representations of 4 as a sum of powers of two. The sequence $(b(n))_{n\in\mathbb{N}}$ was already introduced by Euler.

Recall that the ordinary generating function of the sequence $(b(n))_{n\in\mathbb{N}}$ has the form

$$B(x) = \prod_{n=0}^{\infty} \frac{1}{1 - x^{2^n}} = \sum_{n=0}^{\infty} b(n)x^n.$$

As a consequence we see that $B(x)$ satisfies the functional equation $(1 - x)B(x) = B(x^2)$. Comparing coefficients on both sides we get that the sequence $(b(n))_{n\in\mathbb{N}}$ satisfies the recurrence: $b(0) = b(1) = 1$ and

$$b(2n) = b(2n - 1) + b(n), \quad b(2n + 1) = b(2n).$$

The corresponding series

$$T(x) = \frac{1}{B(x)} = \prod_{n=0}^{\infty}\left(1 - x^{2^n}\right) = \sum_{n=0}^{\infty} t_n x^n$$

is the ordinary generating function for the famous Prouhet-Thue-Morse sequence $(t_n)_{n\in\mathbb{N}}$ (the PTM seqence for short). Recall that $t_n = (-1)^{s_2(n)}$, where $s_2(n)$ is the number of 1's in the unique expansion of n in base 2. Equivalently, we have $t_0 = 1$ and

$$t_{2n} = t_n, \quad t_{2n+1} = -t_n, \quad n \geq 0.$$

The corresponding series

$$T(x) = \frac{1}{B(x)} = \prod_{n=0}^{\infty}\left(1 - x^{2^n}\right) = \sum_{n=0}^{\infty} t_n x^n$$

is the ordinary generating function for the famous Prouhet-Thue-Morse sequence $(t_n)_{n\in\mathbb{N}}$ (the PTM seqence for short). Recall that $t_n = (-1)^{s_2(n)}$, where $s_2(n)$ is the number of 1's in the unique expansion of n in base 2. Equivalently, we have $t_0 = 1$ and

$$t_{2n} = t_n, \quad t_{2n+1} = -t_n, \quad n \geq 0.$$

Moreover, for $n \geq 2$, the 2-adic valuation of $b(n)$ is equal to

$$\nu_2(b(n)) = \frac{1}{2}|t_n - 2t_{n-1} + t_{n-2}|.$$

In particular, if $n \geq 2$, then $\nu_2(b(n)) \in \{1, 2\}$ or to be more precise,

$$b(n) \equiv 0 \pmod{4} \iff \nu_2(n) \equiv 0 \pmod{2} \textit{ or } \nu_2(n-1) \equiv 0 \pmod{2}. \quad (2)$$

For $m \in \mathbb{N}_+$ we define $b_m(n)$ as a convolution of m copies of $b(n)$. More precisely,

$$b_m(n) = \sum_{i_1+\ldots+i_m=n} b(i_1)\cdots b(i_m).$$

Note that $b_1(n) = b(n)$. The number $b_m(n)$ has also a combinatorial interpretation. Indeed, $b_m(n)$ is the number of binary partitions of n, where each part has one of m possible colors.

For $m \in \mathbb{N}_+$ we define $b_m(n)$ as a convolution of m copies of $b(n)$. More precisely,

$$b_m(n) = \sum_{i_1+\ldots+i_m=n} b(i_1)\cdots b(i_m).$$

Note that $b_1(n) = b(n)$. The number $b_m(n)$ has also a combinatorial interpretation. Indeed, $b_m(n)$ is the number of binary partitions of n, where each part has one of m possible colors.

It is proved that for $m = 2^k - 1$ the 2-adic valuation of $b_m(n) \in \{1, 2\}$ for $n \geq 2^k$. More precisely, we have the following.

Theorem 1

Let $k \in \mathbb{N}_+$. For $n, i \in \mathbb{N}$ such that $i < 2^{k+2}$ we have

$$\nu_2(b_{2^k-1}(2^{k+2}n + i)) = \begin{cases} \nu_2(b(8n)) & \text{if } 0 \leq i < 2^k, \\ 1 & \text{if } 2^k \leq i < 2^{k+1}, \\ 2 & \text{if } 2^{k+1} \leq i < 3 \cdot 2^k, \\ 1 & \text{if } 3 \cdot 2^{k+1} \leq i < 2^{k+2}. \end{cases}$$

In particular, $\nu_2(b_{2^k-1}(n)) \in \{0, 1, 2\}$ and $\nu_2(b_{2^k-1}(n)) = 0$ if and only if $n < 2^k$.

The case $m = 1$

Let

$$S_m := \{n \in \mathbb{N} : \ b_m(n) \neq x^2 + y^2 + z^2\}.$$

The case $m = 1$

Let

$$S_m := \{n \in \mathbb{N} : \ b_m(n) \neq x^2 + y^2 + z^2\}.$$

We start with the characterization of the set S_1.

The case $m = 1$

Let

$$S_m := \{n \in \mathbb{N} : \ b_m(n) \neq x^2 + y^2 + z^2\}.$$

We start with the characterization of the set S_1.

From Gauss-Legendre's theorem and 2-adic properties of $b(n)$ we need to understand the behaviour of the sequence $b(n) \pmod{32}$. From the equality $b(2n+1) = b(2n)$ it is enough to consider $b(2n) \pmod{32}$. We thus put $u(n) := b(2n)$ and observe that

$$u(2n) = u(2n-1) + u(n), \quad u(2n+1) = u(2n-1) + 2u(n). \qquad (3)$$

Proposition 2

For all $n > 0$ we have

$$\nu_2(u(n)) = \begin{cases} 1 & \text{if } \nu_2(n) \equiv 0 \pmod{2}, \\ 2 & \text{if } \nu_2(n) \equiv 1 \pmod{2}. \end{cases}$$

Proposition 2

For all $n > 0$ we have

$$\nu_2(u(n)) = \begin{cases} 1 & \text{if } \nu_2(n) \equiv 0 \pmod{2}, \\ 2 & \text{if } \nu_2(n) \equiv 1 \pmod{2}. \end{cases}$$

Lemma 3

For each $k, n \in \mathbb{N}$ we have

$$u(2^{2k+1}(2n+1)) \equiv u(2(2n+1)) \pmod{32}.$$

Proposition 2

For all $n > 0$ we have

$$\nu_2(u(n)) = \begin{cases} 1 & \textit{if } \nu_2(n) \equiv 0 \pmod 2, \\ 2 & \textit{if } \nu_2(n) \equiv 1 \pmod 2. \end{cases}$$

Lemma 3

For each $k, n \in \mathbb{N}$ we have

$$u(2^{2k+1}(2n+1)) \equiv u(2(2n+1)) \pmod{32}.$$

Proof: This is a simple consequence of the Gupta-Rödseth result concerning the behaviour of $\nu_2(b(4n) - b(n))$. The cited result implies that

$$b(2^{s+2}n) \equiv b(2^s n) \pmod{2^{\mu(s)}},$$

where $\mu(s) = \lfloor \frac{3s+4}{2} \rfloor$. Replacing s by $2k$ and $b(2^{s+2}n)$ by $u(2^{s+1}n)$, and noting that $\mu(2k) \geq 5$ for $k \in \mathbb{N}_+$ we get the statement of our lemma. $\square$

Theorem 4

Let

$$j(n) = \frac{u(4n+2)}{4} \mod 8,$$
$$k(n) = \frac{u(2n+1)}{2} \mod 8.$$

Then the sequences $(j(n))_{n\in\mathbb{N}}$ *and* $(k(n))_{n\in\mathbb{N}}$ *are 2-automatic. More precisely, for all* $n \in \mathbb{N}$ *we have*

$$j(2n) = 4 - 3t_n, \tag{4}$$
$$j(2n+1) = 4 + t_n, \tag{5}$$

and

$$k(2n) = 4 - 3t_n,\ k(2n+1) = 4 - t_n,$$

where t_n *is the* n *term in the PTM sequence.*

Theorem 4

Let

$$j(n) = \frac{u(4n+2)}{4} \mod 8,$$
$$k(n) = \frac{u(2n+1)}{2} \mod 8.$$

Then the sequences $(j(n))_{n\in\mathbb{N}}$ *and* $(k(n))_{n\in\mathbb{N}}$ *are 2-automatic. More precisely, for all* $n \in \mathbb{N}$ *we have*

$$j(2n) = 4 - 3t_n, \quad (4)$$
$$j(2n+1) = 4 + t_n, \quad (5)$$

and

$$k(2n) = 4 - 3t_n, \; k(2n+1) = 4 - t_n,$$

where t_n *is the n term in the PTM sequence.*

Proof: The proof uses a careful examination of the bahaviour of $u(n) \pmod{32}$.

Let us put $T_n = (1 - t_n)/2 \in \{0, 1\}$ and recall that

$$\mathcal{A} = \{n \in \mathbb{N} : \ T_n = 1\} = \{2m + T_m : \ m \in \mathbb{N}\},$$
$$\mathcal{E} = \{n \in \mathbb{N} : \ T_n = 0\} = \{2m + 1 - T_m : \ m \in \mathbb{N}\}.$$

Let us put $T_n = (1 - t_n)/2 \in \{0, 1\}$ and recall that

$$\mathcal{A} = \{n \in \mathbb{N} : \ T_n = 1\} = \{2m + T_m : \ m \in \mathbb{N}\},$$
$$\mathcal{E} = \{n \in \mathbb{N} : \ T_n = 0\} = \{2m + 1 - T_m : \ m \in \mathbb{N}\}.$$

Theorem 5

For each $a \in \{1, 3, 5, 7\}$ let $\mathbf{c}_a = (c_a(m))_{m\in\mathbb{N}}$ be the increasing sequence such that

$$\{n \in \mathbb{N} : \ j(n) = a\} = \{c_a(m) : \ m \in \mathbb{N}\}.$$

Then the sequence $\mathbf{c}_a$ is 2-regular. More precisely, we have

$$c_1(m) = 4m - t_m + 1,$$
$$c_3(m) = 4m + t_m + 2,$$
$$c_5(m) = 4m - t_m + 2,$$
$$c_7(m) = 4m + t_m + 1.$$

It is easy to see that each of the above sequences from the statement of the theorem is increasing. In order to prove that $j(n) = a$ if and only if $n = c_a(m)$ for some $m \in \mathbb{N}$, we restate Theorem 4 in the following way:

$$j(n) = \begin{cases} 1 & \text{if } 2 \mid n \text{ and } T_n = 0, \\ 3 & \text{if } 2 \nmid n \text{ and } T_n = 0, \\ 5 & \text{if } 2 \nmid n \text{ and } T_n = 1, \\ 7 & \text{if } 2 \mid n \text{ and } T_n = 1. \end{cases}$$

It is easy to see that each of the above sequences from the statement of the theorem is increasing. In order to prove that $j(n) = a$ if and only if $n = c_a(m)$ for some $m \in \mathbb{N}$, we restate Theorem 4 in the following way:

$$j(n) = \begin{cases} 1 & \text{if } 2 \mid n \text{ and } T_n = 0, \\ 3 & \text{if } 2 \nmid n \text{ and } T_n = 0, \\ 5 & \text{if } 2 \nmid n \text{ and } T_n = 1, \\ 7 & \text{if } 2 \mid n \text{ and } T_n = 1. \end{cases}$$

If $j(n) = 1$, then $2 \mid n$ and $n = 2k + T_k$ for some $k \in \mathbb{N}$. This implies $T_k = 0$, and thus $k = 2m + T_m$ for some $n \in \mathbb{N}$. As a result, we get $n = 4m + 2T_m = 4m - t_m + 1$. Conversely, if n is of this form, then $j(n) = 1$ so we get the claim for $a = 1$.

It is easy to see that each of the above sequences from the statement of the theorem is increasing. In order to prove that $j(n) = a$ if and only if $n = c_a(m)$ for some $m \in \mathbb{N}$, we restate Theorem 4 in the following way:

$$j(n) = \begin{cases} 1 & \text{if } 2 \mid n \text{ and } T_n = 0, \\ 3 & \text{if } 2 \nmid n \text{ and } T_n = 0, \\ 5 & \text{if } 2 \nmid n \text{ and } T_n = 1, \\ 7 & \text{if } 2 \mid n \text{ and } T_n = 1. \end{cases}$$

If $j(n) = 1$, then $2 \mid n$ and $n = 2k + T_k$ for some $k \in \mathbb{N}$. This implies $T_k = 0$, and thus $k = 2m + T_m$ for some $n \in \mathbb{N}$. As a result, we get $n = 4m + 2T_m = 4m - t_m + 1$. Conversely, if n is of this form, then $j(n) = 1$ so we get the claim for $a = 1$.

The proof for $a = 3, 5, 7$ is similar.

Corollary 6

The number $b(2n)$ *is not a sum of three squares if and only if*

$$n = 2^{2k-1}(8s + 2t_s + 3)$$

for some $k, s \in \mathbb{N}_+$.

Corollary 6

The number $b(2n)$ is not a sum of three squares if and only if

$$n = 2^{2k-1}(8s + 2t_s + 3)$$

for some $k, s \in \mathbb{N}_+$.

Proof: If $b(2n) \notin S$ then necessarily $\nu_2(b(2n)) = \nu_2(u(n)) = 2$. Thus $\nu_2(n)$ is odd, say $n = 2^{2k-1}(2m+1)$ for some $k \in \mathbb{N}_+$ and $m \in \mathbb{N}$. To get the result, we need to calculate $\frac{u(2^{2k-1}(2m+1))}{4} \pmod{8}$. From Lemma 3 it is enough to consider the case $k = 1$, i.e., investigate the sequence $(j(m))_{m\in\mathbb{N}}$. More precisely, $u(2(2m+1))/4$ is not a sum of three squares if and only if $j(m) = 7$.

Corollary 6

The number $b(2n)$ is not a sum of three squares if and only if

$$n = 2^{2k-1}(8s + 2t_s + 3)$$

for some $k, s \in \mathbb{N}_+$.

Proof: If $b(2n) \notin S$ then necessarily $\nu_2(b(2n)) = \nu_2(u(n)) = 2$. Thus $\nu_2(n)$ is odd, say $n = 2^{2k-1}(2m+1)$ for some $k \in \mathbb{N}_+$ and $m \in \mathbb{N}$. To get the result, we need to calculate $\frac{u(2^{2k-1}(2m+1))}{4} \pmod{8}$. From Lemma 3 it is enough to consider the case $k = 1$, i.e., investigate the sequence $(j(m))_{m\in\mathbb{N}}$. More precisely, $u(2(2m+1))/4$ is not a sum of three squares if and only if $j(m) = 7$.

From Theorem 5 we know that $j(m) = 7$ if and only if $m = 4s + t_s + 1$ for some $s \in \mathbb{N}$. We thus get that for each $k \in \mathbb{N}$ we have

$$u(2^{2k-1}(8s + 2t_s + 3)) \equiv u(2(8s + 2t_s + 3)) \equiv 7 \pmod{8}$$

for each $k \in \mathbb{N}_+$ and $s \in \mathbb{N}$, and hence the result.

The case $m = 3$

To get required characterization of S_3, we need to understand of the behaviour of $b_3(16n+i) \pmod{32}$ for $i = 0, 1, 2, 3, 8, 9, 10, 11$.

The case $m = 3$

To get required characterization of S_3, we need to understand of the behaviour of $b_3(16n+i) \mod 32$ for $i = 0, 1, 2, 3, 8, 9, 10, 11$.

Lemma 7

The following congruences holds:

$$b_3(8n+i+4) \equiv 2(2i+1+4(-1)^n)t_n \pmod{32},$$
$$b_3(32n+i) \equiv b_3(8n+i) \pmod{64},\ \ i = 0, 1, 2, 3, 4$$
$$b_3(8(2n+1)+i) \equiv 4(3+3i-i^2-2(-1)^{n+i})t_n \pmod{32}$$
$$\equiv \begin{cases} 4(3-2(-1)^n)t_n \pmod{32} & \textit{if } i = 0, \\ 4(5+2(-1)^n)t_n \pmod{32} & \textit{if } i = 1, \\ 4(5-2(-1)^n)t_n \pmod{32} & \textit{if } i = 2, \\ 4(3+2(-1)^n)t_n \pmod{32} & \textit{if } i = 3. \end{cases}$$

In particular, for each $k \in \mathbb{N}_+$ and $i \in \{0, 1, 2, 3\}$, we have

$$b_3(2^{2k}(2n+1)+i) \equiv 2 \pmod{4},$$
$$b_3(2^{2k+1}(2n+1)+i) \equiv b_3(8(2n+1)+i) \pmod{32},$$

Theorem 8

We have that $n \in S_3$ *if and only if*

$$n = 2^{2k+1}\left(8p + 2\left\lfloor \frac{i}{2} \right\rfloor + 3 + 2(-1)^i t_p\right) + i$$

for some $i \in \{0, 1, 2, 3\}$ *and* $k \in \mathbb{N}_+$, $p \in \mathbb{N}$.

Theorem 8

We have that $n \in S_3$ *if and only if*

$$n = 2^{2k+1}\left(8p + 2\left\lfloor \frac{i}{2} \right\rfloor + 3 + 2(-1)^i t_p\right) + i$$

for some $i \in \{0, 1, 2, 3\}$ *and* $k \in \mathbb{N}_+$, $p \in \mathbb{N}$.

Proof: From the characterization of the 2-adic valuation of $b_3(n)$ and Lemma 7 we know that if $n \in S_3$, then necessary we have $n \pmod{16} \in \{0, 1, 2, 3, 8, 9, 10, 11\}$. Then we use case by case analysis and get the result. $\square$

The case $m = 2^k - 1, k \geq 3$

To analyze the general case we express $(b_{2^k-1}(n))_{n\in\mathbb{N}}$ as the convolution of $(b_{2^k}(n))_{n\in\mathbb{N}}$ and the PTM sequence, and use the following lemma.

Lemma 9

For all $k, n \in \mathbb{N}$ we have

$$b_{2^k}(n) \equiv \binom{2^k}{n} + 2^{k+1}\binom{2^k-2}{n-2} \pmod{2^{k+2}}.$$

The case $m = 2^k - 1$, $k \geq 3$

To analyze the general case we express $(b_{2^k-1}(n))_{n\in\mathbb{N}}$ as the convolution of $(b_{2^k}(n))_{n\in\mathbb{N}}$ and the PTM sequence, and use the following lemma.

Lemma 9

For all $k, n \in \mathbb{N}$ we have

$$b_{2^k}(n) \equiv \binom{2^k}{n} + 2^{k+1}\binom{2^k-2}{n-2} \pmod{2^{k+2}}.$$

We split our reasoning into two parts: $n < 2^k$ and $n \geq 2^k$. Starting with the simpler case $n < 2^k$, we have $\nu_2(b_{2^k-1}(n)) = 0$. It is thus sufficient for our purposes to describe $b_{2^k-1}(n)$ modulo 8.

Proposition 10

Let $k \geq 3$ and $n < 2^k$. Then

$$b_{2^k-1}(n) \equiv t_n \cdot \begin{cases} 1 \pmod 8 & \text{if } 0 \leq n < 2^{k-2}, \\ 5 \pmod 8 & \text{if } 2^{k-2} \leq n < 2^{k-1}, \\ 7 \pmod 8 & \text{if } 2^{k-1} \leq n < 3\cdot 2^{k-2}, \\ 3 \pmod 8 & \text{if } 3\cdot 2^{k-2} \leq n < 2^k. \end{cases}$$

As an immediate corollary, we can describe $n < 2^k$ such that $b_{2^k-1}(n)$ is (not) a sum of three squares.

Corollary 11

Let $k \geq 3$ and $n < 2^k$. Then $b_{2^k-1}(n)$ is not a sum of three squares of integers if and only if one of the following cases holds:

- $0 \leq n < 2^{k-2}$ *and* $t_n = -1$;
- $2^{k-1} \leq n < 3 \cdot 2^{k-2}$ *and* $t_n = 1$.

As an immediate corollary, we can describe $n < 2^k$ such that $b_{2^k-1}(n)$ is (not) a sum of three squares.

Corollary 11

Let $k \geq 3$ and $n < 2^k$. Then $b_{2^k-1}(n)$ is not a sum of three squares of integers if and only if one of the following cases holds:

- $0 \leq n < 2^{k-2}$ *and* $t_n = -1$*;*
- $2^{k-1} \leq n < 3 \cdot 2^{k-2}$ *and* $t_n = 1$*.*

We move on to the case $n \geq 2^k$. This time we have $\nu_2(b_{2^k-1}(n)) \in \{1, 2\}$ by Theorem 1, which means that we need to consider $b_{2^k-1}(n)$ modulo 32.

Lemma 12

1. *For all $k, n \in \mathbb{N}$ such that $n \leq 2^k$ we have*

$$\nu_2\left(\binom{2^k}{n}\right) = k - \nu_2(n). \tag{6}$$

2. *For all $m, n \in \mathbb{N}$ we have*

$$\binom{2m}{2n} \equiv \binom{m}{n} \pmod{2^{\nu_2(m)+1}}. \tag{7}$$

We are now ready to describe $b_{2^k-1}(n)$ modulo 32 for $n \geq 2^k$. This time, the characterization involves two terms of the PTM sequence.

Theorem 13

Fix $k, i, j \in \mathbb{N}$ such that $k \geq 3$, $i < 8$, and $j < 2^{k-3}$. Then for all $m \geq 1$ we have

$$b_{2^k-1}(2^k m + 2^{k-3} i + j) \equiv t_j(c_i t_m + d_i t_{m-1}) \pmod{32},$$

where the coefficients c_i, d_i do not depend on k and are given in Table 1.

i	0	1	2	3	4	5	6	7
c_i	1	7	3	5	9	-1	3	5
d_i	-5	-3	1	-9	-5	-3	-7	-1

Table: *The coefficients c_i, d_i.*

Proof: Consider first the case $k \geq 4$. By Lemma 9 we have

$$b_{2^k-1}(n) = \sum_{l=0}^{n} b_{2^k}(l) t_{n-l} \equiv \sum_{l=0}^{n} \binom{2^k}{l} t_{n-l} \pmod{32}.$$

Proof: Consider first the case $k \geq 4$. By Lemma 9 we have

$$b_{2^k-1}(n) = \sum_{l=0}^{n} b_{2^k}(l) t_{n-l} \equiv \sum_{l=0}^{n} \binom{2^k}{l} t_{n-l} \pmod{32}.$$

Now, by (6), the binomial coefficients with $v_2(l) < k-4$ vanish modulo 32. Hence, assuming that $n \geq 2^k$, the above sum simplifies to

$$b_{2^k-1}(n) \equiv \sum_{l=0}^{16} \binom{2^k}{2^{k-4}l} t_{n-2^{k-4}l} \equiv \sum_{l=0}^{16} \binom{16}{l} t_{n-2^{k-4}l} \pmod{32},$$

where the second congruence follows from (7).

Proof: Consider first the case $k \geq 4$. By Lemma 9 we have

$$b_{2^k-1}(n) = \sum_{l=0}^{n} b_{2^k}(l) t_{n-l} \equiv \sum_{l=0}^{n} \binom{2^k}{l} t_{n-l} \pmod{32}.$$

Now, by (6), the binomial coefficients with $v_2(l) < k-4$ vanish modulo 32. Hence, assuming that $n \geq 2^k$, the above sum simplifies to

$$b_{2^k-1}(n) \equiv \sum_{l=0}^{16} \binom{2^k}{2^{k-4}l} t_{n-2^{k-4}l} \equiv \sum_{l=0}^{16} \binom{16}{l} t_{n-2^{k-4}l} \pmod{32},$$

where the second congruence follows from (7).

Furthermore, we can get rid of the terms with j odd, since there is an even number of them and they are all congruent to 16 modulo 32. Therefore, we get the congruence

$$b_{2^k-1}(n) \equiv \sum_{l=0}^{8} \binom{16}{2l} t_{n-2^{k-3}l} \pmod{32}.$$

In order to simplify the right-hand side, consider b_{2^k-1} at indices of the form given in the statement, namely $n = 2^k m + 2^{k-3} i + j$, where $m \geq 1$, $0 \leq i < 8$, and $0 \leq j < 2^{k-3}$.

By the recurrences defining the Thue–Morse sequence, we get

$$t(2^k m+2^{k-3}i+j-2^{k-3}l) = t(j)t(8m+i-l) = t(j)\cdot\begin{cases} t_n t_{i-l} & \text{if } l \le i, \\ -t_{n-1}t_{l-i} & \text{if } l > i. \end{cases}$$

By the recurrences defining the Thue–Morse sequence, we get

$$t(2^k m+2^{k-3}i+j-2^{k-3}l) = t(j)t(8m+i-l) = t(j)\cdot\begin{cases} t_n t_{i-l} & \text{if } l \leq i, \\ -t_{n-1}t_{l-i} & \text{if } l > i. \end{cases}$$

Hence, the claimed formula holds with the coefficients

$$c_i = \sum_{l=0}^{i} \binom{16}{2l} t_{i-l},$$
$$d_i = -\sum_{l=i+1}^{8} \binom{16}{2l} t_{l-i},$$

and a direct computation (modulo 32) gives their values as in Table 1.

Using this result, we can determine the indices $n \geq 2^k$ such that $b_{2^k-1}(n)$ is not a sum of three squares. The description turns out to be surprisingly simple in the sense that it does not require distinguishing cases for n modulo 2^k (unlike Theorem 13).

Using this result, we can determine the indices $n \geq 2^k$ such that $b_{2^k-1}(n)$ is not a sum of three squares. The description turns out to be surprisingly simple in the sense that it does not require distinguishing cases for n modulo 2^k (unlike Theorem 13).

Corollary 14

For each $k \geq 3$ and $n \geq 2^k$ the term $b_{2^k-1}(n)$ is not a sum of three squares of integers if and only if $t_n = t_{n-2^k} = 1$. Equivalently, n is of the form

$$n = 2^k m + l,$$

where $l, j \in \mathbb{N}$ are such that $t_m = t_l$, $\nu_2(m) \equiv 1 \pmod 2$ and $0 \leq l < 2^k$.

Using this result, we can determine the indices $n \geq 2^k$ such that $b_{2^k-1}(n)$ is not a sum of three squares. The description turns out to be surprisingly simple in the sense that it does not require distinguishing cases for n modulo 2^k (unlike Theorem 13).

Corollary 14

For each $k \geq 3$ and $n \geq 2^k$ the term $b_{2^k-1}(n)$ is not a sum of three squares of integers if and only if $t_n = t_{n-2^k} = 1$. Equivalently, n is of the form

$$n = 2^k m + l,$$

where $l, j \in \mathbb{N}$ are such that $t_m = t_l$, $\nu_2(m) \equiv 1 \pmod 2$ and $0 \leq l < 2^k$.

Let $n = 2^k m + 2^{k-3} i + j$ as in Theorem 13. Observe that $c_i + d_i = -4t_i$, while $c_i - d_i$ is not divisible by 4. Hence, the term $b_{2^k-1}(2^k m + 2^{k-3} i + j)$ is not a sum of three squares if and only if

$$t_m = t_{m-1} = t_i t_j,$$

which after multiplying both sides by $t_i t_j$ gives precisely the first part of the statement. The second part follows immediately by writing $l = 2^{k-3} i + j$ and observing that $t_m = (-1)^{\nu_2(m)+1} t_{m-1}$.

Counting the solutions

For real $x \geq 0$ and $m \in \mathbb{N}_+$ let

$$S_m(x) = S_m \cap [0, x] = \#\{n \leq x : b_m(n) \text{ is not a sum of three squares}\}.$$

Counting the solutions

For real $x \geq 0$ and $m \in \mathbb{N}_+$ let

$$S_m(x) = S_m \cap [0, x] = \#\{n \leq x : b_m(n) \text{ is not a sum of three squares}\}.$$

Using the descriptions of the sets S_{2^k-1} obtained in the previous sections for various k it is easy to check that

$$S_{2^k-1}(x) = d_k x + O(\log x),$$

where $d_1 = d_2 = 1/12$ and $d_k = 1/6$ for $k \geq 3$.

For real $x \geq 0$ and $m \in \mathbb{N}_+$ let

$$S_m(x) = S_m \cap [0, x] = \#\{n \leq x : b_m(n) \text{ is not a sum of three squares}\}.$$

Using the descriptions of the sets S_{2^k-1} obtained in the previous sections for various k it is easy to check that

$$S_{2^k-1}(x) = d_k x + O(\log x),$$

where $d_1 = d_2 = 1/12$ and $d_k = 1/6$ for $k \geq 3$.

In the following three results we provide more precise bounds for $S_{2^k-1}(x) - d_k x$ in the case $k = 1, k = 2$ and $k \geq 3$, respectively. In particular, each lower and upper bound is of the form $C_1 \log_2 x + C_2$, where the constant C_1 is optimal.

Theorem 15

For every $x \geq 1$ *we have*

$$-2 < S_1(x) - \frac{x}{12} < \frac{1}{2}\log_2 x.$$

In particular, the natural density of the set S_1 *in* $\mathbb{N}$ *exists and is equal to*

$$\lim_{x\to+\infty} \frac{S_1(x)}{x} = \frac{1}{12}.$$

Moreover, there exists an increasing sequence $(m_k)_{k\in\mathbb{N}} \subset \mathbb{N}$ *such that*

$$S_1(m_l) - \frac{m_l}{12} \sim \frac{1}{2}\log_2 m_l.$$

Proof: For $x \in \mathbb{R}$ define

$$P(x) = \#\{s \in \mathbb{N} : 8s + 2t_s + 3 \leq x\}, \quad Q(x) = \sum_{k=0} P\left(\frac{x}{4^k}\right).$$

Proof: For $x \in \mathbb{R}$ define

$$P(x) = \#\{s \in \mathbb{N} : 8s + 2t_s + 3 \leq x\}, \quad Q(x) = \sum_{k=0} P\left(\frac{x}{4^k}\right).$$

We have that that $Q\left(\frac{x}{2}\right) = \#\{n \leq x : b(2n) \in S\}$, hence by the relation $b(2n+1) = b(2n)$, we get

$$S(x) = Q\left(\frac{x}{4}\right) + Q\left(\frac{x-1}{4}\right).$$

For $m \in \mathbb{N}$ and $i = 0, 1, 2, 3$ we have the recurrence relations

$$Q(4m+i) = Q(m) + P(4m+i).$$

Proof: For $x \in \mathbb{R}$ define

$$P(x) = \#\{s \in \mathbb{N} : 8s + 2t_s + 3 \leq x\}, \quad Q(x) = \sum_{k=0} P\left(\frac{x}{4^k}\right).$$

We have that that $Q\left(\frac{x}{2}\right) = \#\{n \leq x : b(2n) \in S\}$, hence by the relation $b(2n+1) = b(2n)$, we get

$$S(x) = Q\left(\frac{x}{4}\right) + Q\left(\frac{x-1}{4}\right).$$

For $m \in \mathbb{N}$ and $i = 0, 1, 2, 3$ we have the recurrence relations

$$Q(4m + i) = Q(m) + P(4m + i).$$

Also, for $i < 8$ we have

$$P(8m + i) = m + \begin{cases} 0 & \text{if } i = 0, \\ T_m & \text{if } i = 1, 2, 3, 4, \\ 1 & \text{if } i = 5, 6, 7. \end{cases}$$

Put

$$R(x) = Q(x) - \frac{x}{6}.$$

We will prove by induction on length $L(m)$ of binary expansion of $m \in \mathbb{N}_+$ that

$$-\frac{2}{3} \leq R(m) \leq \frac{1}{4}\lfloor \log_2 m \rfloor - \frac{1}{6}. \tag{8}$$

Direct computation shows that our claim holds for $L(m) \leq 5$. Now let $L(m) \geq 6$. It is sufficient to prove that there exists $n \in \mathbb{N}_+$ with $L(n) = L(m) - 2$ such that

$$0 \leq R(m) - R(n) \leq \frac{1}{2}.$$

This is indeed the case, as shown by the following set of identities (ordered according to the residue class modulo 8):

$$
\begin{aligned}
R(8n) &= R(2n), \\
R(16n+1) &= R(4n+1), \\
R(16n+9) &= R(4n) + \frac{1}{2}, \\
R(16n+2) &= R(4n+2), \\
R(16n+10) &= R(4n) + \frac{1}{3}, \\
R(16n+3) &= R(4n+3), \\
R(16n+11) &= R(4n) + \frac{1}{6}, \\
R(8n+4) &= R(2n+1) + T_n - \frac{1}{2}, \\
R(64n+4) &= R(16n+4), \\
R(64n+20) &= R(16n+2) + 1 - T_n, \\
R(64n+36) &= R(16n) + 1 - T_n, \\
R(64n+52) &= R(16n+4), \\
R(16n+12) &= R(4n), \\
R(8n+5) &= R(2n+1) + \frac{1}{3}, \\
R(8n+6) &= R(2n+1) + \frac{1}{6}, \\
R(8n+7) &= R(2n+1).
\end{aligned}
$$

Plugging $m = \lfloor x \rfloor$ into (8), after some manipulation we get the main part of the result.

Now, define $m_0 = 0$ and $m_{l+1} = 16m_l + 36$ for $l \in \mathbb{N}$. Using the recurrence relations above and the fact that $4 \mid m_l$, we get

$$R(m_{l+1}) = R(16m_l + 36) = R(4m_l) + 1 - T_{m_l} = R(m_l) + 1 - T_{m_l}.$$

By induction one can quickly prove that $T_{m_l} = 0$ for all $l \in \mathbb{N}$, and thus we get $R(m_l) = l$ and consequently $S_1(m_l) - m_l/12 = 2(l-1)$. The last part of the statement follows.

Now, define $m_0 = 0$ and $m_{l+1} = 16m_l + 36$ for $l \in \mathbb{N}$. Using the recurrence relations above and the fact that $4 \mid m_l$, we get

$$R(m_{l+1}) = R(16m_l + 36) = R(4m_l) + 1 - T_{m_l} = R(m_l) + 1 - T_{m_l}.$$

By induction one can quickly prove that $T_{m_l} = 0$ for all $l \in \mathbb{N}$, and thus we get $R(m_l) = l$ and consequently $S_1(m_l) - m_l/12 = 2(l-1)$. The last part of the statement follows.

Theorem 16

For all $x \geq 1$ we have

$$\left| S_3(x) - \frac{x}{12} \right| \leq \frac{1}{6}\log_2 x + \frac{3}{2}.$$

In particular, the natural density of the set S_3 in $\mathbb{N}$ exists and is equal to

$$\lim_{x\to+\infty} \frac{S_3(x)}{x} = \frac{1}{12}.$$

Moreover, there exist increasing sequences $(m_l)_{l\in\mathbb{N}}, (n_l)_{l\in\mathbb{N}} \subset \mathbb{N}$ such that

$$S_3(m_l) - \frac{m_l}{12} \sim \frac{1}{6}\log_2 m_l,$$
$$S_3(n_l) - \frac{n_l}{12} \sim -\frac{1}{6}\log_2 n_l.$$

Theorem 17

If $k \geq 3$, then for all $x \geq 2^k$ we have

$$\left| S_{2^k-1}(x) - \frac{x}{6} + 2^{k-2} \right| \leq \frac{2^{k-2}}{3} (\log_2 x - k + 17).$$

In particular, the natural density of the set S_{2^k-1} in $\mathbb{N}$ exists and is equal to

$$\lim_{x \to +\infty} \frac{S_{2^k-1}(x)}{x} = \frac{1}{6}.$$

Moreover, there exist increasing sequences $(m_l)_{l\in\mathbb{N}}, (n_l)_{l\in\mathbb{N}} \subset \mathbb{N}$ such that

$$S_{2^k-1}(m_l) - \frac{m_l}{6} \sim \frac{2^{k-2}}{3} \log_2 m_l,$$
$$S_{2^k-1}(n_l) - \frac{n_l}{6} \sim -\frac{2^{k-2}}{3} \log_2 n_l.$$

It is natural to ask whether it is possible to obtain results concerning the representation of $b_m(n)$ as a sum of three squares for any $m \in \mathbb{N}_+$.

Problem 1

Describe the set S_m for $m \in \mathbb{N}_+$.

It is natural to ask whether it is possible to obtain results concerning the representation of $b_m(n)$ as a sum of three squares for any $m \in \mathbb{N}_+$.

Problem 1

Describe the set S_m for $m \in \mathbb{N}_+$.

The direct approach we, namely reduction modulo a power of 2, is most likely not applicable in the general case, as it seems that for all $m \neq 2^k - 1$ the valuations $\nu_2(b_m(n))$ are unbounded. In such a case one would need to compute $b_m(n) \bmod 2^{\nu_2(b_m(n))+3}$ and we do not see how this can be done without prior knowledge of $\nu_2(b_m(n))$. Therefore, we expect that obtaining an exact description of S_m for even a single value $m \neq 2^k - 1$ is hard.

We obtained precise characterization of those $n \in \mathbb{N}$ such that $b(n)$ is a sum of three squares. In particular the set of such numbers has asymptotic density equal to $11/12$. A more difficult question is whether the set

$$\mathcal{T}_1 = \{n \in \mathbb{N} : \ b(2n) = \square + \square\}$$

is infinite or not.

We obtained precise characterization of those $n \in \mathbb{N}$ such that $b(n)$ is a sum of three squares. In particular the set of such numbers has asymptotic density equal to $11/12$. A more difficult question is whether the set

$$\mathcal{T}_1 = \{n \in \mathbb{N} : \ b(2n) = \Box + \Box\}$$

is infinite or not.

To get a clue what can be expected, we computed the values of $b(2n)$ for $n \leq 2^{20}$ and check whether $b(2n)$ is a sum of two squares. We put

$$\mathcal{T}_1(x) = \#(\mathcal{T}_1 \cap [0, x]).$$

In the table below we present the values of $\mathcal{T}(2^n)$ for $n \leq 20$.

n	1	2	3	4	5	6	7	8	9	10
$\mathcal{T}(2^n)$	2	3	6	8	14	21	37	64	106	174

n	11	12	13	14	15	16	17	18	19	20
$\mathcal{T}(2^n)$	325	617	1089	2018	3699	6804	12551	23624	44606	84176

In the table below we present the values of $\mathcal{T}(2^n)$ for $n \leq 20$.

n	1	2	3	4	5	6	7	8	9	10
$\mathcal{T}(2^n)$	2	3	6	8	14	21	37	64	106	174

n	11	12	13	14	15	16	17	18	19	20
$\mathcal{T}(2^n)$	325	617	1089	2018	3699	6804	12551	23624	44606	84176

Our numerical computations suggest the following

Conjecture 1

The set $\mathcal{T}$ is infinite.

In the table below we present the values of $\mathcal{T}(2^n)$ for $n \leq 20$.

n	1	2	3	4	5	6	7	8	9	10
$\mathcal{T}(2^n)$	2	3	6	8	14	21	37	64	106	174
n	11	12	13	14	15	16	17	18	19	20
$\mathcal{T}(2^n)$	325	617	1089	2018	3699	6804	12551	23624	44606	84176

Our numerical computations suggest the following

Conjecture 1

The set $\mathcal{T}$ is infinite.

Question 1

What is the asymptotic behaviour of $\mathcal{T}(x)$ as $x \to +\infty$? Is the equality $\mathcal{T}(x) = \mathcal{O}(x/\log x)$ true?

We obtained precise characterization of those $n \in \mathbb{N}$ such that $b(2n)$ is a sum of three squares. In particular the set of such numbers has natural density equal to $5/6$. Analyzing, for a given n not of the form $2^{2k+1}(8s+2t_s+3)$, the solution set (x, y, z) of the equation $b(2n) = x^2 + y^2 + z^2$, we found that in many cases one of the values x, y, z is a square, i.e., the Diophantine equation

$$b(2n) = X^2 + Y^2 + Z^4$$

has a solution in non-negative integers.

We obtained precise characterization of those $n \in \mathbb{N}$ such that $b(2n)$ is a sum of three squares. In particular the set of such numbers has natural density equal to $5/6$. Analyzing, for a given n not of the form $2^{2k+1}(8s + 2t_s + 3)$, the solution set (x, y, z) of the equation $b(2n) = x^2 + y^2 + z^2$, we found that in many cases one of the values x, y, z is a square, i.e., the Diophantine equation

$$b(2n) = X^2 + Y^2 + Z^4$$

has a solution in non-negative integers.

More precisely, for $n \leq 10^3$ we know that there are exactly 916 values of n such that $b(2n)$ is a sum of three squares. Among them, there are exactly 831 values of n such that $b(2n)$ is a sum of two squares and a fourth power. This large number of solutions suggest the following

Conjecture 2

Let $Q_1 := \{n \in \mathbb{N} : \; b(2n) = x^2 + y^2 + z^4$ for some $x, y, z \in \mathbb{N}\}$. The set Q_1 is infinite. Moreover, the set Q_1 has positive natural density in $\mathbb{N}$.

Thank you for your attention;-)