ON THE INTEGERS OF THE FORM \( p^2 + b^2 + 2^n \) AND \( b_1^2 + b_2^2 + 2^n \)

HAO PAN AND WEI ZHANG

Abstract. We prove that the sumset \( \{ p^2 + b^2 + 2^n : p \text{ is prime and } b, n \in \mathbb{N} \} \) has positive lower density. We also construct a residue class with an odd modulus that contains no integer of the form \( p^2 + b^2 + 2^n \). Similar results are established for the sumset \( \{ b_1^2 + b_2^2 + 2^n : b_1, b_2, n \in \mathbb{N} \} \).

1. Introduction

Let \( \mathcal{P} \) denote the set of all primes. In 1934, Romanoff [25] proved that the sumset \( \mathcal{S}_1 = \{ p + 2^n : p \in \mathcal{P}, n \in \mathbb{N} \} \) has positive lower density. Subsequently, van der Corput [13] proved that the complement of \( \mathcal{S}_1 \), i.e., \( \mathbb{N} \setminus \mathcal{S}_1 \), also has positive lower density. In fact, Erdős [14] showed that every positive integer \( n \) with \( n \equiv 7629217 \pmod{11184810} \) is not of the form \( p + 2^n \) with \( p \in \mathcal{P} \) and \( n \in \mathbb{N} \). The key ingredient of Erdős’s proof is to find a finite set of residue classes with distinct moduli, which covers all integers. Over the years, Erdős’s idea has been greatly extended [11, 10, 3, 26, 4, 5, 27, 28, 6, 30, 7, 21, 8, 9, 29].

In 1999, with the help of Brüdern and Fouvry’s estimates on sums of squares [2], Liu, Liu and Zhan [22] proved a Romanoff-type result:

The sumset
\[
\mathcal{S}_2 = \{ p_1^2 + p_2^2 + 2^{n_1} + 2^{n_2} : p_1, p_2 \in \mathcal{P}, \ n_1, n_2 \in \mathbb{N} \}
\]
has positive lower density.

The key part of their proof is the following lemma:

Lemma 1.1. For \( 1 \leq m \leq N \),
\[
|\{ p_1^2 + p_2^2 - p_3^2 - p_4^2 = m : p_i \in \mathcal{P}, \ p_i^2 \leq N \}| \ll \mathfrak{G}_-(m) \frac{N}{(\log N)^4},
\]
where \( \mathfrak{G}_- \) will be introduced in Section 2.
In the other direction, recently Crocker [12] proved that there exist infinitely many positive integers not representable as the sum of two squares and two (or fewer) powers of 2.

By the prime number theorem, clearly,

$$|\left\{ p^2 + b^2 \leq N : p \in \mathcal{P}, \ b \in \mathbb{N} \right\}| \leq |\mathcal{P} \cap [0, \sqrt{N}]] \cdot |\mathbb{N} \cap [0, \sqrt{N}]]| \ll \frac{N}{\log N}.$$ 

On the other hand, in [24], Rieger proved that

$$|\left\{ p^2 + b^2 \leq N : p \in \mathcal{P}, \ b \in \mathbb{N} \right\}| \gg \frac{N}{\log N}.$$ 

Motivated by all of these results, in the present paper, we shall study the sumset

$$S_3 = \left\{ p^2 + b^2 + 2^n : p \in \mathcal{P}, \ b, n \in \mathbb{N} \right\}.$$ 

First, we have the following Romanoff-type result.

**Theorem 1.1.** The set $S_3$ has positive lower density.

Next, we need to say something about the complement of $S_3$. It is not difficult to see that almost all integers in $S_3$ are of the form $4k + 1$ or $8k + 2$. However, we shall prove that

**Theorem 1.2.** There exists a residue class with an odd modulus that contains no integer of the form $p^2 + b^2 + 2^n$ with $p \in \mathcal{P}$ and $b, n \in \mathbb{N}$.

Since the modulus in Theorem 1.2 is odd, by the Chinese remainder theorem, clearly both the sets

$$\left\{ x \in \mathbb{N} : x \equiv 1 \pmod{4}, \ x \not\in S_3 \right\}$$

and

$$\left\{ x \in \mathbb{N} : x \equiv 2 \pmod{8}, \ x \not\in S_3 \right\}$$

have positive lower densities.

Furthermore, we also have a similar result on the integers not of the form $p^2 + b^2 - 2^n$.

**Theorem 1.3.** There exists a residue class with an odd modulus that contains no integer of the form $p^2 + b^2 - 2^n$ with $p \in \mathcal{P}$ and $b, n \in \mathbb{N}$.

In fact, as we shall see later, our proof can provide the explicit values of the residues and moduli described in Theorems 1.2 and 1.3, although these values are too large to write down here.

A well-known result due to Landau [20] asserts that

$$\left\{ b_1^2 + b_2^2 \leq N : b_1, b_2 \in \mathbb{N} \right\} = \frac{KN}{\sqrt{\log N}}(1 + o(1))$$

where

$$K = \frac{1}{\sqrt{2}} \prod_{\substack{p \in \mathcal{P} \\ p \equiv 3 \pmod{4}}} \left( 1 - \frac{1}{p^2} \right)^{-1/2} = 0.764223653 \ldots.$$ 

Obviously,

$$\left\{ n \in \mathbb{N} : 2^n \leq N \right\} \ll \sqrt{\log N}.$$ 

These facts suggest that we can obtain the following results.
ON THE INTEGERS OF THE FORM $p^2 + b^2 + 2^n$ AND $b_1^2 + b_2^2 + 2^n$

Theorem 1.4. The subset

$$S_4 = \{b_1^2 + b_2^2 + 2^n : b_1, b_2, n \in \mathbb{N}\}$$

has positive lower density. Conversely, there also exists a residue class with an odd modulus that contains no integer of the form $b_1^2 + b_2^2 + 2^n$.

As to the latter conclusion of the theorem, we actually establish a stronger result (see Theorem 4.1 below).

The proofs of Theorem 1.1 and the former conclusion of Theorem 1.4 are applications of the sieve method. We shall construct a suitable cover of $\mathbb{Z}$ with odd moduli to prove Theorem 1.2, Theorem 1.3, and the latter assertion of Theorem 1.4. Throughout this paper, the constants implied by $\ll$, $\gg$ and $O(\cdot)$ will always be absolute.

2. Proof of Theorem 1.1

For $d = (d_1, d_2, d_3, d_4)$ with $\mu(d) := \mu(d_1)\mu(d_2)\mu(d_3)\mu(d_4) \neq 0$, define

$$A(m, q, d) = q^{-4} \sum_{1 \leq a \leq q \atop (a, q) = 1} e(-am/q)S(q, ad_1)S(q, ad_2)S(q, -ad_2^*)S(q, -ad_3^*)$$

and

$$\mathcal{S}(m, d) = \sum_{q=1}^{\infty} A(m, q, d),$$

where

$$S(q, a) = \sum_{x=1}^{q} e(ax^2/q)$$

and $e(\alpha) = \exp(2\pi \sqrt{-1}\alpha)$. In particular, we set $\mathcal{S}_-(m) = \mathcal{S}(m, (1, 1, 1, 1))$ and $\omega(d, m) = \mathcal{S}(m, d)/\mathcal{S}_-(m)$.

For a prime $p$ and a positive integer $m$, if $p \nmid m$, then define

$$\omega_{1,0}(p, m) = \begin{cases} p/(p-1), & \text{if } \left(\frac{m}{p}\right) = 1, \\ p/(p+1), & \text{if } \left(\frac{m}{p}\right) = -1, \end{cases}$$

$$\omega_{0,1}(p, m) = \begin{cases} p/(p-1), & \text{if } \left(\frac{m}{p}\right) = 1, \\ p/(p+1), & \text{if } \left(\frac{m}{p}\right) = -1, \end{cases}$$

and $\omega_{1,1}(p, m) = p/(p + 1)$. Also, if $p^\beta | m$ for some $\beta \geq 1$, where $p^\beta | m$ means $p^\beta \mid m$ but $p^{\beta+1} \nmid m$, then define

$$\omega_{1,0}(p, m) = \omega_{0,1}(p, m) = \frac{1 + p^{-1} - p^{-\beta} - p^{-\beta-1}}{1 + p^{-1} - p^{-\beta-1} - p^{-\beta-2}}$$

and

$$\omega_{1,1}(p, m) = \frac{3 - p^{-1} - p^{1-\beta} - p^{-\beta}}{1 + p^{-1} - p^{-\beta-1} - p^{-\beta-2}}.$$
Lemma 2.1 (Liu, Liu and Zhan [22, eq. (8.7), Lemmas 8.1 and 8.2]). Suppose that $d_1, d_2, d_3, d_4$ are square-free and $(d_1, d_4) = (d_2, d_3) = 1$. Then for $d = (d_1, d_2, d_3, d_4)$ and positive integer $m$, we have
\[
\omega(d, m) = \prod_{p|d_1d_2d_3d_4} \omega_{u,v}(p, m),
\]

Let
\[
\mathcal{A} = \{(x_1, x_2, x_3, x_4) : x_1^2 + x_2^2 = x_3^2 + x_4^2 + m, \ 1 \leq x_i^2 \leq N\},
\]
and for $d = (d_1, d_2, d_3, d_4)$, let
\[
\mathcal{A}_d = \{(x_1, x_2, x_3, x_4) \in \mathcal{A} : x_1 \equiv 0 \pmod{d_1}\}.
\]

Lemma 2.2 (Brüdern and Fouvry [2, Theorem 3], Liu, Liu and Zhan [22, Lemma 9.1]). Let
\[
|\mathcal{A}_d| = \frac{\omega(d, m)}{d_1d_2d_3d_4} \pi 16 \mathfrak{F}_-(m) \mathfrak{J}(m/N) N + R(m, N, d),
\]
where
\[
\mathfrak{J}(\theta) = 2 \int_{\max(0,-\theta)}^{\min(1,1-\theta)} t^{-1/2}(1 - \theta - t)^{1/2} dt,
\]
and the remainder term $R(m, N, d)$ satisfies
\[
\sum_{d_1, d_2, d_3, d_4 \leq N^{1/23}} |R(m, N, d)| \ll N^{1-\epsilon}
\]
for sufficiently small $\epsilon > 0$.

Since $m$ is always fixed, below we abbreviate $\omega_{u,v}(p, m)$ to $\omega_{u,v}(p)$.

Let $D = N^{1/30}$ and $z = N^{1/300}$. Define
\[
P(z) = \prod_{p < z, p \text{ prime}} p.
\]

Let
\[
f(k) = \{\{x_1, x_2, x_3, x_4\} \in \mathcal{A} : x_1x_2 = k\}.
\]

Lemma 2.3. For any $d | P(z)$ with $d \leq \sqrt{D}$,
\[
\sum_{k \equiv 0 \pmod{d}} f(k) = \frac{\pi}{16} \mathfrak{F}_-(m) \mathfrak{J}(m/N) N \prod_{p|d} \left( \frac{\omega_{1,0}(p)}{p} + \frac{\omega_{0,1}(p)}{p} - \frac{\omega_{1,1}(p)}{p^2} \right) + O \left( \sum_{d_1, d_2 | d, \ t_1 | d_1, \ t_2 | d_2} |R(m, N, d)| \right).
\]
Proof. Applying Lemma 2.2 we have

\[
\sum_{d|k} f(k) = \sum_{d_1,d_2|d} \left( \sum_{t_1|d, t_2|d} \mu(t_1) \sum_{t_2|(x_4,d)/d_2} \mu(t_2) \right)
\]

\[
= \sum_{d_1,d_2|d} \sum_{t_1|d_1, t_2|d_2} \mu(t_1) \mu(t_2) \sum_{(x_1,x_2,x_3) \in \mathcal{A}} \mu(x_1,d_1) \mu(x_2,d_2) \mu(x_3,d_3) \mu(x_4,d_4)
\]

\[
= \sum_{d_1,d_2|d} \mu(t_1) \mu(t_2) \prod_{p|d_1} \left( \frac{\omega_1(p)}{p} \right) \prod_{p|d_2} \left( \frac{\omega_1(p)}{p} \right)
\]

\[
\prod_{p|d} \left( \frac{\omega_1(p)}{p} + \frac{\omega_0(p)}{p} - \frac{\omega_1(p)}{p^2} \right).
\]

Suppose that 0 < m \leq 2N. Clearly,

\[
|\{(x_1, x_2, x_3, x_4) : x_1^2 + x_2^2 = x_2^2 + x_3^2 + m, 1 \leq x_i^2 \leq N, (x_1x_2, P(z)) = 1\}| = \sum_{(k, P(z)) = 1} f(k) \sum_{d|(k, P(z))} \lambda_d^2
\]

\[
\sum_{d_1,d_2|P(z)} \lambda_{d_1} \lambda_{d_2} \sum_{k=0 \mod [d_1,d_2]} f(k),
\]

where \( \lambda_d \) are the weights appearing in Selberg’s sieve method with \( \lambda_d = 0 \) for \( d \not\geq z \) (cf. [19 Chapter 3]). In view of Lemma 2.3.
Also, it had been shown \[22, \text{eq. (2.9)}\] that
\[
\sum_{d_1, d_2 \mid P(z)} \lambda_{d_1} \lambda_{d_2} \sum_{k \equiv 0 \mod [d_1, d_2]} f(k)
\]
\[
= \frac{\pi}{16} \mathcal{S}_-(m) \mathfrak{I}(m/N) N \sum_{d_1, d_2 \mid P(z)} \lambda_{d_1} \lambda_{d_2} \prod_{p \mid [d_1, d_2]} \left( \frac{\omega_{1,0}(p)}{p} + \frac{\omega_{0,1}(p)}{p} - \frac{\omega_{1,1}(p)}{p^2} \right)
\]
\[
+ \sum_{d_1, d_2 \mid P(z)} \lambda_{d_1} \lambda_{d_2} \cdot O\left( \sum_{d = (d_1, d_2, 2, 1, 1)} |R(m, N, d)| \right).
\]

By Selberg’s sieve method, we have
\[
\sum_{d_1, d_2 \mid P(z)} \lambda_{d_1} \lambda_{d_2} \prod_{p \mid [d_1, d_2]} \left( \frac{\omega_{1,0}(p)}{p} + \frac{\omega_{0,1}(p)}{p} - \frac{\omega_{1,1}(p)}{p^2} \right) = \frac{1}{G_1(z)},
\]
where
\[
G_1(z) = \sum_{d \mid P(z)} \prod_{d < z} \frac{\omega_{1,0}(p)p^{-1} + \omega_{0,1}(p)p^{-1} - \omega_{1,1}(p)p^{-2}}{1 - \omega_{1,0}(p)p^{-1} - \omega_{0,1}(p)p^{-1} + \omega_{1,1}(p)p^{-2}}.
\]

Since $|\lambda_d| \leq 1$,
\[
\sum_{d_1, d_2 \mid P(z)} \lambda_{d_1} \lambda_{d_2} \cdot O\left( \sum_{d_1, d_2 \mid [d_1, d_2], \ [d_1, d_2] \mid d_1' d_2'} \tau(d_1)^2 \tau(d_2)^2 |R(m, N, d)| \right) \ll N^{1-\epsilon/2},
\]
where $\tau$ is the divisor function. Noting that $\omega_{1,0}(p), \omega_{0,1}(p) = 1 + O(1/p)$ and $\omega_{1,1}(p) = O(1)$, we have (cf. \[19\] Lemma 4.1)]
\[
G_1(z) \gg \prod_{p < z} \left( 1 + \frac{\omega_{1,0}(p)}{p} + \frac{\omega_{0,1}(p)}{p} - \frac{\omega_{1,1}(p)}{p^2} \right) \gg (\log z)^2.
\]

Also, it had been shown \[22\, \text{eq. (2.9)}\] that
\[
\mathcal{S}_-(m) \ll \prod_{p \mid m, p \geq 3} \left( 1 + \frac{1}{p - 1} - \frac{1}{p^{\beta+2}} \right).
\]
Finally,

\[
\left| \{(x_1, x_2, x_3, x_4) \in \mathcal{A} : |x_1| < z \text{ or } |x_2| < z \} \right|
\leq \sum_{|x_1| < z, \; x_2^2 \leq N \atop \text{or } |x_2| < z, \; x_2^2 \leq N} \left| \{(x_3, x_4) : x_4^2 - x_3^2 = x_2^2 - x_1^2 + m, \; x_3^2, x_4^2 \leq N \} \right|
\leq \left| \{(x_1, x_2) : (x_1 - x_2)(x_1 + x_2) = m \} \right| \cdot \left| \{(x_3, x_4) : x_4^2 = x_3^2, \; x_3^2, x_4^2 \leq N \} \right|
+ \sum_{|x_1| < z, \; x_2^2 \leq N \atop \text{or } |x_2| < z, \; x_2^2 \leq N} \left| \{(x_3, x_4) : (x_4 - x_3)(x_4 + x_3) = x_2^2 - x_1^2 + m \} \right|
\ll \tau(m)\sqrt{N} + \sum_{|x_1| < z, \; x_2^2 \leq N \atop \text{or } |x_2| < z, \; x_2^2 \leq N} \tau(x_2^2 - x_1^2 + m) \ll N^{2/3}.}

Thus we obtain that

**Theorem 2.1.** For a positive integer \( m \), we have

\[
\left| \{(p_1, p_2, b_3, b_4) : p_1^2 + b_3^2 = p_2^2 + b_4^2 + m, \; p_i \in \mathcal{P}, \; b_i \in \mathbb{N}, \; p_i^2, b_i^2 \leq N \} \right|
\ll \frac{N}{(\log N)^2} \prod_{p|m} \left( 1 + \frac{1}{p} \right).
\]

Now we are ready to prove Theorem 1.1.

**Proof of Theorem 1.1.** Define

\[
r(x) = \left| \{(p, b, n) : p^2 + b^2 + 2^n = x, \; p \in \mathcal{P}, \; b, n \in \mathbb{N} \} \right|.
\]

Recall that \( \mathcal{S}_3 = \{ x \in \mathbb{N} : r(x) \geq 1 \} \). Then, by the Cauchy-Schwarz inequality,

\[
\left| \{(p, b, n) : p^2 + b^2 + 2^n \leq N, \; p \in \mathcal{P}, \; b, n \in \mathbb{N} \} \right|
= \sum_{x \leq N} r(x) \leq \sqrt{|\mathcal{S}_3 \cap [1, N]|} \cdot \sqrt{\sum_{x \leq N} r(x)^2}.
\]

Clearly,

\[
\left| \{(p, b, n) : p^2 + b^2 + 2^n \leq N, \; p \in \mathcal{P}, \; b, n \in \mathbb{N} \} \right|
\geq |\{ p \in \mathcal{P} : p^2 \leq N/3 \}| \cdot |\{ b \in \mathbb{N} : b^2 \leq N/3 \}| \cdot |\{ n \in \mathbb{N} : 2^n \leq N/3 \}| \gg N.
\]

So it suffices to show that

\[
\sum_{x \leq N} r(x)^2 \ll N.
\]
Apparently,

\[ \left| \{(p, b) : p^2 + b^2 \leq N, p \in \mathcal{P}, b \in \mathbb{N} \} \right| \ll \frac{N}{\log N}. \]

Also, Rieger had proved \( [24, (h2)] \) that

\[ \left| \{(p_1, p_2, b_1, b_2) : p_1^2 + b_1^2 = p_2^2 + b_2^2 \leq N, p_1 \neq p_2, p_1, p_2 \in \mathcal{P}, b_1, b_2 \in \mathbb{N} \} \right| \ll \frac{N}{\log N}. \]

Thus applying Theorem 2.1, we have

\[
\sum_{x \leq N} r(x)^2 = \left| \{(p_1, p_2, b_1, b_2, n_1, n_2) : p_1^2 + b_1^2 + 2^{n_1} p_2^2 + b_2^2 \leq N, p_i \in \mathcal{P}, b_i \in \mathbb{N} \} \right|
\ll \sum_{2^{n_1} < 2^{n_2} \leq N} \left| \{(p_1, p_2, b_1, b_2) : p_1^2 + b_1^2 = p_2^2 + b_2^2 \leq N, p_i \in \mathcal{P}, b_i \in \mathbb{N} \} \right|
\ll \sum_{2^{n_1} < 2^{n_2} \leq N} \frac{N}{(\log N)^2} \prod_{p | 2^{n_2} - 2^{n_1}} \left( 1 + \frac{1}{p} \right) + \frac{N}{\log N} \frac{\log N}{\log 2}.
\]

By Romanoff’s arguments \( [25] \) (or see \( [23, p. 203] \)), we know that

\[ \sum_{2^{n_1} < 2^{n_2} \leq N} \prod_{p | 2^{n_2} - 2^{n_1} - 1} \left( 1 + \frac{1}{p} \right) \ll (\log N)^2. \]

\[ \square \]

3. Proof of Theorems 1.2 and 1.3

For an integer \( a \) and a positive integer \( n \), let \( a(n) \) denote the residue class \( \{ x \in \mathbb{Z} : x \equiv a \pmod{n} \} \). For a finite system \( \mathcal{A} = \{ a_s(n_s) \}^k_{s=1} \), we say \( \mathcal{A} \) is a cover of \( \mathbb{Z} \) provided that

\[ \bigcup_{s=1}^{k} a_s(n_s) = \mathbb{Z}. \]

Our aim is to find a cover \( \{ a_s(n_s) \}^k_{s=1} \) of \( \mathbb{Z} \) and distinct primes \( p_1, p_2, \ldots, p_k \) with \( p_s \equiv 3 \pmod{4} \) and \( 2^{n_s} \equiv 1 \pmod{p_s} \). With help from the book \( [1] \), the following lemma can be directly verified.
Lemma 3.1. Let
\[
\{(d_s',n_s',p_s)\}_{s=1}^{49} = \{(0,3,7),(1,15,11),(4,15,31),(7,15,151),(10,15,331),
(13,105,43),(28,105,71),(43,105,127),(58,105,211),
(73,105,29191),(88,105,86171),(103,315,870031),
(208,315,983431),(313,315,1765891),(2,9,19),(5,27,87211),
(14,81,71119),(41,81,97685839),(68,81,163),(23,135,271),
(50,135,631),(77,135,811),(104,135,23311),(131,135,348031),
(53,99,599479),(62,99,33057806959),(71,99,242099935645987),
(80,495,991),(179,495,2971),(278,495,3191),
(377,495,48912491),(476,495,2252127523412251),(89,693,463),
(188,693,5419),(287,693,14323),(386,693,289511839),
(485,693,35532364099),(584,693,28685147519807),
(683,693,581283643249112959),(98,297,694387),
(197,297,1497366897175265228063698945547),(296,891,1783),
(593,891,140903331387825109224688819),
(890,891,12430037668834128259094186647)\}
\]

Then \(A = \{a'_s(n'_s)\}_{s=1}^{49}\) is a cover of \(\mathbb{Z}\). Furthermore, for \(1 \leq s \leq 49\), we have \(p_s | 2^n - 1\) or \(p_s | 2^n + 1\).

Remark. In [29], Wu and Sun constructed a cover of \(\mathbb{Z}\) with 173 odd moduli and distinct primitive prime divisors.

For \(1 \leq s \leq 49\), let \(n_s = 2n'_s\) and let \(a_s\) be an integer such that \(a_s \equiv a'_s \pmod {n'_s}\) and \(a_s \equiv 1 \pmod 2\). Let \(a_{50} = 0\), \(n_{50} = 2\) and \(p_{50} = 3\). Then by the Chinese remainder theorem,
\[
(*) \quad A = \{a_s(n_s)\}_{s=1}^{50}
\]
is a cover of \(\mathbb{Z}\), and \(2^{n_s} \equiv 1 \pmod {p_s}\) for \(1 \leq s \leq 50\). Let
\[
M_1 = \prod_{s=1}^{50} p_s
\]
and let \(\alpha_1\) be an integer such that
\[
\alpha_1 \equiv 2^{n_s} \pmod {p_s}
\]
for \(1 \leq s \leq 50\).

Let \(x\) be an arbitrary positive integer with \(x \equiv \alpha_1 \pmod {M_1}\). Suppose that \(x \in S_3\), i.e., \(x = p^2 + b^2 + 2^n\) for some \(p \in \mathcal{P}\) and \(b, n \in \mathbb{N}\). Since \(A\) is a cover of \(\mathbb{Z}\), there exists \(1 \leq s \leq 50\) such that \(n \equiv a_s \pmod {n_s}\). Then
\[
p^2 + b^2 = x - 2^n \equiv \alpha_1 - 2^{n_s} \equiv 0 \pmod {p_s}.
\]
Noting that \( p_s \equiv 3 \pmod{4} \), \(-1\) is a quadratic nonresidue modulo \( p_s \). It follows that
\[
p \equiv b \equiv 0 \pmod{p_s}.
\]

Since \( p \) is prime, we must have \( p = p_s \).

Below, we require some additional congruences. Arbitrarily choose distinct primes \( q_1, q_2, \ldots, q_{50} \) such that \((q_s, M_1) = 1\) and \( q_s \equiv 7 \pmod{8} \) for \( 1 \leq s \leq 50 \). Clearly, \( 2 \) is a quadratic residue and \(-1\) is a quadratic non-residue modulo \( q_s \). So \(-2^n\) is a quadratic non-residue modulo \( q_s \) for any \( n \geq 0 \). Let
\[
M_2 = \prod_{s=1}^{50} q_s,
\]
and let \( \alpha_2 \) be an integer such that
\[
\alpha_2 \equiv p_s^2 \pmod{q_s}
\]
for every \( 1 \leq s \leq 50 \).

Let \( M = M_1 M_2 \), and let \( \alpha \) be an integer such that
\[
\alpha \equiv \alpha_i \pmod{M_i}
\]
for \( i = 1, 2 \). Then we have \( \{ x \in \mathbb{N} : x \equiv \alpha \pmod{M} \} \cap S_3 = \emptyset \). In fact, assume on the contrary, that \( x \equiv \alpha \pmod{M} \) and \( x = p^2 + b^2 + 2^n \) for some \( p \in \mathcal{P} \) and \( b, n \in \mathbb{N} \). Noting that \( x \equiv \alpha_1 \pmod{M_1} \), we know \( p = p_s \) for some \( 1 \leq s \leq 50 \). But since \( x \equiv \alpha_2 \pmod{M_2} \),
\[
x - p_s^2 - 2^n \equiv \alpha_2 - p_s^2 - 2^n \equiv -2^n \pmod{q_s}.
\]
So \( x - p_s^2 - 2^n \) is a quadratic non-residue modulo \( q_s \), which leads to an evident contradiction since \( x - p_s^2 - 2^n = b^2 \).

Now let us turn to the proof of Theorem 1.3. We still use the cover \( A \) in (4). Now suppose that \( x \equiv -\alpha_1 \pmod{M_1} \) and there exist \( p \in \mathcal{P} \) and \( b, n \in \mathbb{Z} \) such that \( x = p^2 + b^2 - 2^n \). Then \( n \equiv a_s \pmod{n_s} \) for some \( 1 \leq s \leq 50 \), and
\[
x + 2^n \equiv -\alpha_1 + 2^{a_s} \equiv 0 \pmod{p_s}.
\]
It follows that \( p = p_s \). The main difficulty is to find the additional congruences.
Lemma 3.2. Let
\[
\{(c_s, r_s)\}_{s=1}^{50} = \{(505, 47 \times 17 \times 181), (5519, 601 \times 1801), (366, 2731 \times 8191),
(1303, 73 \times 262657), (5149, 233 \times 2089), (5938, 43691 \times 131071),
(182725, 223 \times 616318177), (12153, 174763 \times 524287),
(148671, 13367 \times 164511353), (490297, 431 \times 2099863),
(115115, 2351 \times 13264529), (2370639, 6361 \times 20394401),
(37, 5 \times 17 \times 257), (5615, 13 \times 37 \times 109), (146, 89 \times 397 \times 2113),
(637, 97 \times 241 \times 673), (6393, 103 \times 2143 \times 11119),
(13847, 53 \times 157 \times 1613), (1799, 29 \times 113 \times 15790321),
(335, 59 \times 1103 \times 3033169), (451, 337 \times 92737 \times 649657),
(1479, 641 \times 65537 \times 6700417), (40655, 137 \times 953 \times 26317),
(13353, 228479 \times 48544121 \times 212885833),
(23775, 439 \times 2298041 \times 9361973132609), (10334, 229 \times 457 \times 525313),
(65971, 2687 \times 202029703 \times 1113491139767), (5893, 41 \times 61681 \times 4278255361),
(1344867, 911 \times 112901153 \times 21340471537), (560826, 277 \times 1013 \times 30269),
(406789, 283 \times 4513 \times 165768537521),
(415099, 191 \times 420778751 \times 30327152671),
(61153, 101 \times 4051 \times 8101), (1261375, 307 \times 2857 \times 6529),
(1324442, 107 \times 69431 \times 28059810762433),
(1663519, 321679 \times 26295457 \times 319020217),
(2094571, 3391 \times 23279 \times 65993), (1032375, 571 \times 32377 \times 1212847),
(6321391, 14951 \times 4036961 \times 2646507710984041),
(19031871, 937 \times 6553 \times 7830118297), (7918330, 2833 \times 37171 \times 179951),
(2286429, 61 \times 1321 \times 4562284561), (2227201, 5581 \times 8681 \times 49477),
(207773684, 131 \times 409891 \times 7623851), (2526613, 281 \times 122921 \times 7416361),
(5596695, 433 \times 577 \times 38737), (25234915, 593 \times 1777 \times 25781083),
(7950774, 251 \times 100801 \times 10567201), (10130779, 313 \times 21841 \times 121369),
(14272093, 1429 \times 3361 \times 14449)\}
\]
Then for every \(1 \leq s \leq 50\) and \(n \in \mathbb{N}\), \(c_s + 2^n\) is a quadratic non-residue modulo \(r_s\).

Lemma 3.2 can be checked via a direct computation. In fact, we only need to consider those \(c_s + 2^n\) modulo \(r_s\) for \(0 \leq n < \text{ord}_2(r_s)\), where \(\text{ord}_2(r)\) denotes the least positive integer such that \(2^{\text{ord}_2(r)} \equiv 1 \pmod{r}\).

Notice that \((r_i, M_1) = 1\) and \((r_i, r_j) = 1\) for any distinct \(i, j\). Let
\[
M_3 = \prod_{s=1}^{50} r_s
\]
and let \(\alpha_3\) be an integer such that
\[
\alpha_3 \equiv c_s + p_s^2 \pmod{r_s}.
\]
Let $M' = M_1M_3$ and let $\alpha'$ be an integer satisfying

$$\alpha' \equiv -\alpha_1 \pmod{M_1} \quad \text{and} \quad \alpha' \equiv \alpha_3 \pmod{M_3}.$$ 

For any $x \equiv \alpha' \pmod{M'}$, assume on the contrary that $x = p_s^2 + b^2 - 2^n$ for some $1 \leq s \leq 50$ and $b,n \in \mathbb{N}$. Then

$$b^2 = x + 2^n - p_s^2 \equiv \alpha_3 + 2^n - p_s^2 \equiv c_s + 2^n \pmod{r_s}.$$ 

This is impossible, since $c_s + 2^n$ is a quadratic non-residue modulo $r_s$. Hence the residue class $\{x \in \mathbb{N} : x \equiv \alpha' \pmod{M'}\}$ contains no integer of the form $p^2 + b^2 - 2^n$. \hfill \Box

Remark. Observe that the moduli appearing in Lemma 3.2 are all composite. So we have the following problem.

**Problem.** Does there exist infinitely many primes $p$ such that the set

$$\{1 \leq c \leq p : c + 2^n \text{ is a quadratic non-residue modulo } p \text{ for every } n \in \mathbb{N}\}$$

is non-empty?

In fact, we do not know of any such prime $p$. For example, let $p = 2^{19} - 1$, then $27006 + 2^n, 27006 + 2^2, \ldots, 27006 + 2^{18}$ are all quadratic non-residues modulo $p$, but $27006 + 2^{19}$ is a quadratic residue modulo $p$.

4. The integers of the form $b_1^2 + b_2^2 + 2n^2$

**Proof of the first assertion of Theorem 1.4.** Let

$$Q = \{x \in \mathbb{N} : x \text{ has no prime factor of the form } 4k + 3\}.$$ 

Clearly,

$$Q \subseteq \{b_1^2 + b_2^2 : b_1, b_2 \in \mathbb{N}\}.$$ 

We only need to prove that the set

$$\{x + 2n^2 : x \in Q, n \in \mathbb{N}\}$$

has positive lower density. As an application of the half-dimensional sieve method [16], we know that

$$|\{x \in Q : x \leq N\}| \gg \frac{N}{\sqrt{\log N}}.$$ 

With help from Selberg’s sieve method, it is not difficult to see that

$$|\{(x_1, x_2) : x_1 = x_2 + m, x_i \in Q, x_i \leq N\}| \ll \frac{N}{\log N} \prod_{p|n} \left(1 + \frac{1}{p}\right)$$

for every positive integer $m$. By the Cauchy-Schwarz inequality,

$$|\{x + 2n^2 : x + 2n^2 \leq N, x \in Q, n \in \mathbb{N}\}| \geq \frac{|\{(x,n) : x + 2n^2 \leq N, x \in Q, n \in \mathbb{N}\}|^2}{|\{(x_1, x_2, n_1, n_2) : x_1 + 2n_1^2 = x_2 + 2n_2^2 \leq N, x_i \in Q, n_i \in \mathbb{N}\}|}.$$ 

So it suffices to show that

$$|\{(x_1, x_2, n_1, n_2) : x_1 + 2n_1^2 = x_2 + 2n_2^2 \leq N, x_i \in Q, n_i \in \mathbb{N}\}| \ll N.$$
Now 

$$|\{(x_1, x_2, n_1, n_2) : x_1 + 2n_1 = x_2 + 2n_2 \leq N, \ x_i \in \mathbb{Q}, \ n_i \in \mathbb{N}\}|$$

$$\leq |\{(x_1, n_1) : x_1 + 2n_1^2 \leq N, \ x_1 \in \mathbb{Q}, \ n_1 \in \mathbb{N}\}|$$

$$+ 2 \sum_{0 \leq n_1 < n_2 \leq \sqrt{\log N/\log 2}} |\{(x_1, x_2) : x_1 - x_2 = 2n_2^2 - 2n_1^2, \ x_i \in \mathbb{Q} \cap [1, N]\}|$$

$$\leq N + \frac{N}{\log N} \sum_{0 \leq n_1 < n_2 \leq \sqrt{\log N/\log 2}} \prod_{p \equiv 3 \pmod{4}} \left(1 + \frac{1}{p}\right).$$

Obviously,

$$\sum_{0 \leq n_1 < n_2 \leq \sqrt{\log N/\log 2}} \prod_{p \equiv 3 \pmod{4}} \left(1 + \frac{1}{p}\right) \leq \sum_{0 \leq n_1 < n_2 \leq \sqrt{\log N/\log 2}} \prod_{p \equiv 3 \pmod{4}} \left(1 + \frac{1}{p}\right) \leq \sum_{d \mid n_2 - n_1} \sum_{n_1 \leq n_2 \leq \sqrt{\log N/\log 2}} \frac{1}{n_2 \equiv n_1^2 \pmod{\text{ord}_2(d)}}.$$

Suppose that $p$ is an odd prime, $\beta \geq 1$ and $1 \leq a \leq p^\beta$. Then we have

$$|\{1 \leq x \leq p^\beta : x^2 \equiv a \pmod{p^\beta}\}| \leq 2p^{\nu_p(a)/2},$$

since the multiplicative group modulo $p^\beta$ is cyclic, where $\nu_p(a)$ denotes the greatest integer such that $p^{\nu_p(a)} \mid a$. Thus

$$\sum_{0 \leq n_1 < n_2 \leq \sqrt{\log N/\log 2}} \frac{1}{n_2 \equiv n_1^2 \pmod{\text{ord}_2(d)}} \leq \sqrt{\log 2} \left(\sqrt{\log 2} + \frac{2^{\omega(\text{ord}_2(d))}}{\sqrt{\text{ord}_2(d)}} + 1\right),$$

where $\omega(r)$ denotes the number of distinct prime factors of $r$. We only need to prove that

$$\sum_d \frac{2^{\omega(\text{ord}_2(d))}}{d^{\sqrt{\text{ord}_2(d)}}}$$

converges. Define

$$E(x) = \sum_{k \leq x} \sum_{\text{ord}_2(d) = k} \frac{1}{d}.$$

Romanoff had shown that $E(x) \ll x \log x$ (cf. [23, pp. 200-201]). So

$$\sum_d \frac{2^{\omega(\text{ord}_2(d))}}{d^{\sqrt{\text{ord}_2(d)}}} = \sum_k \frac{2^{\omega(k)}}{\sqrt{k}} \sum_{\text{ord}_2(d) = k} \frac{1}{d} \ll \int_1^\infty x^{-1/3} d(E(x))$$

$$= x^{-1/3} E(x) \bigg|_1^\infty + \frac{1}{3} \int_1^\infty x^{-4/3} E(x) dx = O(1). \quad \square$$
Let \( \mathcal{A} = \{a_s(n_s)\}_{s=1}^{50} \) be the cover in (3), and let \( p_1, \ldots, p_{50} \) be the corresponding primes with \( p_s \equiv 3 \pmod{4} \) and \( p_s \mid 2^{n_s} - 1 \). Since every \( p_s \) has at least one quadratic non-residue modulo \( p_s \), the second assertion of Theorem 1.1 is an immediate consequence of the following stronger result.

**Theorem 4.1.** Let \( \mathcal{N} \) be a set of non-negative integers. Suppose that for every \( 1 \leq s \leq 50 \), there exists a residue class with an odd modulus that contains no integer of the form \( b_1^2 + b_2^2 + 2^n \) with \( n \in \mathcal{N} \).

Then there exists a residue class with an odd modulus that contains no integer of the form \( b_1^2 + b_2^2 + 2^n \) with \( n \in \mathcal{N} \).

**Proof.** Let \( n_s^* = \text{ord}_2(p_s) \). Noting that \( n_s^* \mid n_s \) and \( (n_s, p_s) = 1 \), for every \( 1 \leq s \leq 50 \), let \( a_s^* \) be an integer such that

\[
a_s^* \equiv a_s \pmod{n_s^*}
\]

and

\[
a_s^* \equiv e_s \pmod{p_s}.
\]

Clearly, \( \mathcal{A}^* = \{a_s^*(n_s^*)\}_{s=1}^{50} \) is also a cover of \( \mathbb{Z} \).

Let

\[
\mathcal{H}_s = \mathcal{N} \cap \{ x \in \mathbb{N} : x \equiv e_s \pmod{p_s} \} = \{ h_{s,1}, h_{s,2}, \ldots, h_{s,|\mathcal{H}_s|} \}
\]

for \( 1 \leq s \leq 50 \). Choose \( |\mathcal{H}_1| + |\mathcal{H}_2| + \cdots + |\mathcal{H}_{50}| \) distinct primes

\[
q_{1,1}, \ldots, q_{1,|\mathcal{H}_1|}, q_{2,1}, \ldots, q_{2,|\mathcal{H}_2|}, \ldots, q_{50,1}, \ldots, q_{50,|\mathcal{H}_{50}|}
\]

satisfying

\[
q_{s,t} \equiv 3 \pmod{4}
\]

and

\[
q_{s,t} \not\in \{p_1, p_2, \ldots, p_{50}\}
\]

for every \( 1 \leq s \leq 50 \) and \( 1 \leq t \leq |\mathcal{H}_s| \).

Let

\[
M^* = \left( \prod_{1 \leq s \leq 50} p_s \cdot \prod_{1 \leq s \leq 50} q_{s,t} \right)^2
\]

and \( \alpha^* \) be an integer such that

\[
\alpha^* \equiv 2^n \pmod{p_s^2}
\]

and

\[
\alpha^* \equiv 2^{h_{s,t}} + q_{s,t} \pmod{q_{s,t}^2}
\]

for every \( s, t \).

We claim that for any \( x \equiv \alpha^* \pmod{M^*} \), \( x \) is not of the form \( b_1^2 + b_2^2 + 2^n \) with \( n \in \mathcal{N} \). Assume on the contrary that \( x \equiv \alpha^* \pmod{M^*} \) and \( x = b_1^2 + b_2^2 + 2^n \) with \( n \in \mathcal{N} \). Since \( \mathcal{A}^* = \{a_s^*(n_s^*)\}_{s=1}^{50} \) is a cover, by arguing similarly as in the proof of Theorems 1.2 and 1.3 we know that

\[
b_1 \equiv b_2 \equiv 0 \pmod{p_s}
\]

for some \( 1 \leq s \leq 50 \). It follows that

\[
x - 2^n \equiv 2^n - 2^n \equiv 0 \pmod{p_s^2},
\]
that is, \( n \equiv a_s^* \pmod{\text{ord}_2(p_s^2)} \). It is not difficult to check that
\[
2^{n_s^*} = 2^{\text{ord}_2(p_s)} \not\equiv 1 \pmod{p_s^2}.
\]
(In fact, the only known primes \( p \) with \( 2^{p-1} \equiv 1 \pmod{p^2} \) are 1093 and 3511.)
Also,
\[
2^{n_s^*}p = \sum_{k=0}^{p} \binom{p}{k}(2^{n_s^*} - 1)^k \equiv 1 \pmod{p_s^2}.
\]
So we must have \( \text{ord}_2(p_s^2) = n_s^*p \). Consequently,
\[
n \equiv a_s^* \equiv e_s \pmod{p_s}.
\]
Since \( n \in \mathcal{N} \), we have \( n \in \mathcal{H}_s \) and there exists \( 1 \leq t \leq |\mathcal{H}_s| \) such that \( n = h_{s,t} \). It follows that
\[
(\phi) \quad b_1^2 + b_2^2 = x - 2^n \equiv \alpha^* - 2^{h_{s,t}} \equiv q_{s,t} \pmod{q_{s,t}^2}.
\]
So \( b_1^2 + b_2^2 \equiv 0 \pmod{q_{s,t}} \). However, recalling that \( q_{s,t} \equiv 3 \pmod{4} \), \( q_{s,t} \) divides \( b_1^2 + b_2^2 \) implies that
\[
b_1 \equiv b_2 \equiv 0 \pmod{q_{s,t}}.
\]
Hence,
\[
b_1^2 + b_2^2 \equiv 0 \pmod{q_{s,t}^2},
\]
which is evidently contradicted with (\( \phi \)).

\textbf{Corollary 4.1.} There exists a positive integer \( m \) such that the set
\[
\{ x \in \mathbb{N} : x \text{ is even and } x \text{ is not of the form } b_1^2 + b_2^2 + 2^{mn}\}
\]
contains an infinite arithmetic progression.

\textbf{Proof.} Let \( m = p_1p_2 \cdots p_{50} \) where \( p_1, p_2, \ldots, p_{50} \) are the primes in Lemma 3.1.
Thus substituting \( \mathcal{N} = \{ x \in \mathbb{N} : x \equiv 0 \pmod{m} \} \) and \( e_s = 1 \) in Theorem 4.1, we are done.

\textbf{Problem.} Does there exist a residue class with an odd modulus that contains no integer of the form \( b_1^2 + b_2^2 + 2^n \) with \( b_1, b_2, n \in \mathbb{N} \)?

\textbf{Acknowledgements}

We express our gratitude to the anonymous referee for his/her very useful comments on our paper. We are also grateful to Professors Hongze Li and Zhi-Wei Sun for their helpful suggestions.

\textbf{References}


[26] K.-J. Wu and Z.-W. Sun, *Covers of the integers with odd moduli and their applications to the forms $x^m - 2^n$ and $x^2 - F_{3n}/2$*, Math. Comp., 78 (2009), 1853-1866. MR2501080 (2010g:11019)


Department of Mathematics, Nanjing University, Nanjing 210093, People’s Republic of China

E-mail address: haopan79@yahoo.com.cn

E-mail address: zhangwei07@yahoo.com.cn

License or copyright restrictions may apply to redistribution; see http://www.ams.org/journal-terms-of-use