MATHEMATICS OF COMPUTATION
Volume 80, Number 275, July 2011, Pages 1849–1864
S 0025-5718(2011)02445-2
Article electronically published on February 25, 2011

ON THE INTEGERS OF THE FORM $p^2 + b^2 + 2^n$ AND $b_1^2 + b_2^2 + 2^{n^2}$

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

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 $1 \leqslant m \leqslant N$,*

$$|\{p_1^2 + p_2^2 - p_3^2 - p_4^2 = m : p_i \in \mathcal{P},\ p_i^2 \leqslant N\} \ll \mathfrak{S}_-(m)\frac{N}{(\log N)^4},$$

where $\mathfrak{S}_-$ will be introduced in Section 2.

Received by the editor May 23, 2009 and, in revised form, April 25, 2010.
2010 *Mathematics Subject Classification.* Primary 11P32; Secondary 11A07, 11B05, 11B25, 11N36.
Key words and phrases. Positive lower density, arithmetical progression, prime, square, power of 2.
The first author is supported by the National Natural Science Foundation of China (Grant No. 10771135 and 10901078).

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,

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

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

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

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

$$\mathcal{S}_3=\{p^2+b^2+2^n:\ p\in\mathcal{P},\ b,n\in\mathbb{N}\}.$$

First, we have the following Romanoff-type result.

Theorem 1.1. *The set $\mathcal{S}_3$ has positive lower density.*

Next, we need to say something about the complement of $\mathcal{S}_3$. It is not difficult to see that almost all integers in $\mathcal{S}_3$ 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

$$\{x\in\mathbb{N}:x\equiv 1\ (\mathrm{mod}\ 4),\ x\notin\mathcal{S}_3\}$$

and

$$\{x\in\mathbb{N}:x\equiv 2\ (\mathrm{mod}\ 8),\ x\notin\mathcal{S}_3\}$$

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

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

where

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

Obviously,

$$\{n\in\mathbb{N}:\ 2^{n^2}\leqslant N\}\ll\sqrt{\log N}.$$

These facts suggest that we can obtain the following results.

Theorem 1.4. *The sumset*

$$\mathcal{S}_4 = \{b_1^2 + b_2^2 + 2^{n^2} : b_1, b_2, n \in \mathbb{N}\}$$

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

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

$$A(m, q, \mathbf{d}) = q^{-4} \sum_{\substack{1 \leqslant a \leqslant q \\ (a,q)=1}} e(-am/q) S(q, ad_1^2) S(q, ad_4^2) S(q, -ad_2^2) S(q, -ad_3^2)$$

and

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

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 $\mathfrak{S}_-(m) = \mathfrak{S}(m, (1, 1, 1, 1))$ and $\omega(\mathbf{d}, m) = \mathfrak{S}(m, \mathbf{d})/\mathfrak{S}_-(m)$.

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 $\beta \geqslant 1$, 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 $\mathbf{d} = (d_1, d_2, d_3, d_4)$ and positive integer m, we have*

$$\omega(\mathbf{d}, m) = \prod_{\substack{p \mid d_1 d_2 d_3 d_4 \\ p^u \| d_1 d_4,\ p^v \| d_2 d_3}} \omega_{u,v}(p, m),$$

Let

$$\mathscr{A} = \{(x_1, x_2, x_3, x_4) : x_1^2 + x_4^2 = x_2^2 + x_3^2 + m,\ 1 \leqslant x_i^2 \leqslant N\},$$

and for $\mathbf{d} = (d_1, d_2, d_3, d_4)$, let

$$\mathscr{A}_{\mathbf{d}} = \{(x_1, x_2, x_3, x_4) \in \mathscr{A} : x_i \equiv 0 \pmod{d_i}\}.$$

Lemma 2.2 (Brüdern and Fouvry [2, Theorem 3], Liu, Liu and Zhan [22, Lemma 9.1])**.** *Let*

$$|\mathscr{A}_{\mathbf{d}}| = \frac{\omega(\mathbf{d}, m)}{d_1 d_2 d_3 d_4} \frac{\pi}{16} \mathfrak{S}_-(m) \mathfrak{I}(m/N) N + R(m, N, \mathbf{d}),$$

where

$$\mathfrak{I}(\theta) = 2 \int_{\max\{0, -\theta\}}^{\min\{1, 1-\theta\}} t^{-1/2} (1 - \theta - t)^{1/2} dt,$$

and the remainder term $R(m, N, \mathbf{d})$ satisfies

$$\sum_{\substack{d_1, d_2, d_3, d_4 \leqslant N^{1/23} \\ \mathbf{d} = (d_1, d_2, d_3, d_4) \\ |\mu(d)| = 1}} |R(m, N, \mathbf{d})| \ll_\epsilon N^{1-\epsilon}$$

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

$$P(z) = \prod_{\substack{p < z \\ p \text{ prime}}} p.$$

Let

$$f(k) = |\{(x_1, x_2, x_3, x_4) \in \mathscr{A} : x_1 x_2 = k\}|.$$

Lemma 2.3. *For any $d \mid P(z)$ with $d \leqslant \sqrt{D}$,*

$$\sum_{k \equiv 0 \pmod{d}} f(k) = \frac{\pi}{16} \mathfrak{S}_-(m) \mathfrak{I}(m/N) N \prod_{p \mid d} \left(\frac{\omega_{1,0}(p)}{p} + \frac{\omega_{0,1}(p)}{p} - \frac{\omega_{1,1}(p)}{p^2} \right)$$
$$+ O\Bigg(\sum_{\substack{d_1, d_2 \mid d,\ d \mid d_1 d_2 \\ t_1 \mid d/d_1,\ t_2 \mid d/d_2 \\ \mathbf{d} = (d_1 t_1, d_2 t_2, 1, 1)}} |R(m, N, \mathbf{d})| \Bigg).$$

Proof. Applying Lemma 2.2, we have

$$\begin{aligned}
\sum_{d|k} f(k) &= \sum_{\substack{d_1,d_2|d\\ d|d_1d_2}} |\{(x_1,x_2,x_3,x_4)\in\mathscr{A} : (x_1,d)=d_1,\ (x_2,d)=d_2\}| \\
&= \sum_{\substack{d_1,d_2|d\\ d|d_1d_2}} \sum_{\substack{(x_1,x_2,x_3,x_4)\in\mathscr{A}\\ d_1|x_1,\ d_2|x_2}} \Bigg(\sum_{t_1|(x_1,d)/d_1}\mu(t_1)\Bigg)\Bigg(\sum_{t_2|(x_2,d)/d_2}\mu(t_2)\Bigg) \\
&= \sum_{\substack{d_1,d_2|d\\ d|d_1d_2}} \sum_{\substack{t_1|d/d_1\\ t_2|d/d_2}} \mu(t_1)\mu(t_2) \sum_{\substack{(x_1,x_2,x_3,x_4)\in\mathscr{A}\\ d_1t_1|x_1,\ d_2t_2|x_2}} 1 \\
&= \sum_{\substack{d_1,d_2|d,\ d|d_1d_2\\ t_1|d/d_1,\ t_2|d/d_2\\ \mathbf{d}=(d_1t_1,d_2t_2,1,1)}} \mu(t_1)\mu(t_2)\Bigg(\frac{\omega(\mathbf{d},m)}{d_1t_1d_2t_2}\frac{\pi}{16}\mathfrak{S}_-(m)\mathfrak{I}(m/N)N + R(m,N,\mathbf{d})\Bigg).
\end{aligned}$$

In view of Lemma 2.1,

$$\begin{aligned}
&\sum_{\substack{d_1,d_2|d,\ d|d_1d_2\\ t_1|d/d_1,\ t_2|d/d_2\\ \mathbf{d}=(d_1t_1,d_2t_2,1,1)}} \mu(t_1)\mu(t_2)\frac{\omega(\mathbf{d},m)}{d_1t_1d_2t_2} \\
&= \sum_{\substack{[d_1,d_2]=d\\ t_1|d_2/(d_1,d_2)\\ t_2|d_1/(d_1,d_2)}} \mu(t_1)\mu(t_2) \prod_{p|t_1t_2(d_1,d_2)} \frac{\omega_{1,1}(p)}{p^2} \prod_{p|d_1/(d_1,d_2t_2)} \frac{\omega_{1,0}(p)}{p} \prod_{p|d_2/(d_1t_1,d_2)} \frac{\omega_{0,1}(p)}{p} \\
&= \sum_{t_1t_2t_3t_4t_5=d} \mu(t_1)\mu(t_2) \prod_{p|t_1t_2t_3} \frac{\omega_{1,1}(p)}{p^2} \prod_{p|t_4} \frac{\omega_{1,0}(p)}{p} \prod_{p|t_5} \frac{\omega_{0,1}(p)}{p} \\
&= \prod_{p|d}\Bigg(\frac{\omega_{1,0}(p)}{p}+\frac{\omega_{0,1}(p)}{p}-\frac{\omega_{1,1}(p)}{p^2}\Bigg). \qquad \square
\end{aligned}$$

Suppose that $0<m\leqslant 2N$. Clearly,

$$\begin{aligned}
&|\{(x_1,x_2,x_3,x_4) : x_1^2+x_4^2=x_2^2+x_3^2+m,\ 1\leqslant x_i^2\leqslant N,\ (x_1x_2,P(z))=1\}| \\
&\quad = \sum_{(k,P(z))=1} f(k) \leqslant \sum_k f(k)\Bigg(\sum_{d|(k,P(z))}\lambda_d\Bigg)^2 \\
&\quad = \sum_{d_1,d_2|P(z)} \lambda_{d_1}\lambda_{d_2} \sum_{k\equiv 0 \bmod [d_1,d_2]} f(k),
\end{aligned}$$

where λ_d are the weights appearing in Selberg's sieve method with $\lambda_d=0$ for $d\geqslant z$ (cf. [19, Chapter 3]). In view of Lemma 2.3,

$$\begin{aligned}&\sum_{d_1,d_2|P(z)}\lambda_{d_1}\lambda_{d_2}\sum_{k\equiv 0 \bmod [d_1,d_2]} f(k)\\ =&\frac{\pi}{16}\mathfrak{S}_-(m)\mathfrak{I}(m/N)N\sum_{d_1,d_2|P(z)}\lambda_{d_1}\lambda_{d_2}\prod_{p|[d_1,d_2]}\left(\frac{\omega_{1,0}(p)}{p}+\frac{\omega_{0,1}(p)}{p}-\frac{\omega_{1,1}(p)}{p^2}\right)\\ &+\sum_{d_1,d_2|P(z)}\lambda_{d_1}\lambda_{d_2}\cdot O\Bigg(\sum_{\substack{d_1',d_2'|[d_1,d_2],\ [d_1,d_2]|d_1'd_2'\\ t_1|[d_1,d_2]/d_1',\ t_2|[d_1,d_2]/d_2'\\ \mathbf{d}=(d_1t_1,d_2t_2,1,1)}}|R(m,N,\mathbf{d})|\Bigg).\end{aligned}$$

By Selberg's sieve method, we have

$$\sum_{d_1,d_2|P(z)}\lambda_{d_1}\lambda_{d_2}\prod_{p|[d_1,d_2]}\left(\frac{\omega_{1,0}(p)}{p}+\frac{\omega_{0,1}(p)}{p}-\frac{\omega_{1,1}(p)}{p^2}\right)=\frac{1}{G_1(z)},$$

where

$$G_1(z)=\sum_{\substack{d|P(z)\\ d<z}}\prod_{p|d}\frac{\omega_{1,0}(p)p^{-1}+\omega_{0,1}(p)p^{-1}-\omega_{1,1}(p)p^{-2}}{1-\omega_{1,0}(p)p^{-1}-\omega_{0,1}(p)p^{-1}+\omega_{1,1}(p)p^{-2}}.$$

Since $|\lambda_d|\leqslant 1$,

$$\begin{aligned}&\sum_{d_1,d_2|P(z)}\lambda_{d_1}\lambda_{d_2}\cdot O\Bigg(\sum_{\substack{d_1',d_2'|[d_1,d_2],\ [d_1,d_2]|d_1'd_2'\\ t_1|[d_1,d_2]/d_1',\ t_2|[d_1,d_2]/d_2'\\ \mathbf{d}=(d_1t_1,d_2t_2,1,1)}}|R(m,N,\mathbf{d})|\Bigg)\\ \ll&\sum_{\substack{d_1,d_2|P(z)\\ d_1,d_2<z^2\\ \mathbf{d}=(d_1,d_2,1,1)}}\tau(d_1)^2\tau(d_2)^2\tau(d_1d_2)^2|R(m,N,\mathbf{d})|\ll N^{1-\epsilon/2},\end{aligned}$$

where τ 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, eq. (2.9)] that

$$\mathfrak{S}_-(m)\ll\prod_{\substack{p^\beta\|m\\ p\geqslant 3\\ \beta\geqslant 0}}\left(1+\frac{1}{p}-\frac{1}{p^{\beta+1}}-\frac{1}{p^{\beta+2}}\right).$$

Finally,

$$\begin{aligned}
&|\{(x_1,x_2,x_3,x_4)\in\mathscr{A}:\ |x_1|<z \text{ or } |x_2|<z\}|\\
\leqslant&\sum_{\substack{|x_1|<z,\ x_2^2\leqslant N\\ \text{or } |x_2|<z,\ x_1^2\leqslant N}}|\{(x_3,x_4):\ x_4^2-x_3^2=x_2^2-x_1^2+m,\ x_3^2,x_4^2\leqslant N\}|\\
\leqslant&|\{(x_1,x_2):\ (x_1-x_2)(x_1+x_2)=m\}|\cdot|\{(x_3,x_4):\ x_4^2=x_3^2,\ x_3^2,x_4^2\leqslant N\}|\\
&+\sum_{\substack{|x_1|<z,\ x_2^2\leqslant N\\ \text{or } |x_2|<z,\ x_1^2\leqslant N\\ x_2^2-x_1^2+m\neq 0}}|\{(x_3,x_4):\ (x_4-x_3)(x_4+x_3)=x_2^2-x_1^2+m\}|\\
\ll&\tau(m)\sqrt{N}+\sum_{\substack{|x_1|<z,\ x_2^2\leqslant N\\ \text{or } |x_2|<z,\ x_1^2\leqslant N\\ x_2^2-x_1^2+m\neq 0}}\tau(x_2^2-x_1^2+m)\ll N^{2/3}z.
\end{aligned}$$

Thus we obtain that

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

$$\begin{aligned}
&|\{(p_1,p_2,b_3,b_4):\ p_1^2+b_4^2=p_2^2+b_3^2+m,\ p_i\in\mathcal{P},\ b_i\in\mathbb{N},\ p_i^2,b_i^2\leqslant N\}|\\
&\quad\ll\frac{N}{(\log N)^2}\prod_{p\mid m}\left(1+\frac{1}{p}\right).
\end{aligned}$$

Now we are ready to prove Theorem 1.1.

Proof of Theorem 1.1. Define

$$r(x)=|\{(p,b,n):\ p^2+b^2+2^n=x,\ p\in\mathcal{P},\ b,n\in\mathbb{N}\}|.$$

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

$$\begin{aligned}
&|\{(p,b,n):\ p^2+b^2+2^n\leqslant N,\ p\in\mathcal{P},\ b,n\in\mathbb{N}\}|\\
&\quad=\sum_{x\leqslant N}r(x)\leqslant\sqrt{|\mathcal{S}_3\cap[1,N]|}\cdot\sqrt{\sum_{x\leqslant N}r(x)^2}.
\end{aligned}$$

Clearly,

$$\begin{aligned}
&|\{(p,b,n):\ p^2+b^2+2^n\leqslant N,\ p\in\mathcal{P},\ b,n\in\mathbb{N}\}|\\
&\quad\geqslant|\{p\in\mathcal{P}:\ p^2\leqslant N/3\}|\cdot|\{b\in\mathbb{N}:\ b^2\leqslant N/3\}|\cdot|\{n\in\mathbb{N}:\ 2^n\leqslant N/3\}|\gg N.
\end{aligned}$$

So it suffices to show that

$$\sum_{x\leqslant N}r(x)^2\ll N.$$

Apparently,

$$|\{(p,b) : p^2+b^2 \leqslant N, p\in\mathcal{P}, b\in\mathbb{N}\}| \ll \frac{N}{\log N}.$$

Also, Rieger had proved [24, (h 2)] that

$$|\{(p_1,p_2,b_1,b_2) : p_1^2+b_1^2=p_2^2+b_2^2 \leqslant N, p_1\neq p_2, p_1,p_2\in\mathcal{P}, b_1,b_2\in\mathbb{N}\}| \ll \frac{N}{\log N}.$$

Thus applying Theorem 2.1, we have

$$\begin{aligned}
\sum_{x\leqslant N} r(x)^2 &= |\{(p_1,p_2,b_1,b_2,n_1,n_2) : p_1^2+b_1^2+2^{n_1} \\
&= p_2^2+b_2^2+2^{n_2} \leqslant N, p_i\in\mathcal{P}, b_i,n_i\in\mathbb{N}\}| \\
&\ll \sum_{2^{n_1}<2^{n_2}\leqslant N} |\{(p_1,p_2,b_1,b_2) : p_1^2+b_1^2-p_2^2-b_2^2 \\
&= 2^{n_2}-2^{n_1}, p_i^2, b_i^2 \leqslant N, p_i\in\mathcal{P}, b_i\in\mathbb{N}\}| \\
&\quad + \sum_{2^n\leqslant N} |\{(p_1,p_2,b_1,b_2) : p_1^2+b_1^2=p_2^2+b_2^2\leqslant N-2^n, p_i\in\mathcal{P}, b_i\in\mathbb{N}\}| \\
&\ll \sum_{2^{n_1}<2^{n_2}\leqslant N} \frac{N}{(\log N)^2} \prod_{p\mid 2^{n_2}-2^{n_1}} \left(1+\frac{1}{p}\right) + \frac{N}{\log N}\cdot\frac{\log N}{\log 2}.
\end{aligned}$$

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

$$\sum_{2^{n_1}<2^{n_2}\leqslant N} \prod_{p\mid 2^{n_2-n_1}-1} \left(1+\frac{1}{p}\right) \ll (\log N)^2. \qquad \square$$

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 $\mathcal{A}=\{a_s(n_s)\}_{s=1}^k$, 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 $\{a_s(n_s)\}_{s=1}^k$ 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*

$$\begin{aligned}
&\{(a'_s, n'_s, p_s)\}_{s=1}^{49} \\
&\quad = \{(0,3,7),(1,15,11),(4,15,31),(7,15,151),(10,15,331), \\
&\quad (13,105,43),(28,105,71),(43,105,127),(58,105,211), \\
&\quad (73,105,29191),(88,105,86171),(103,315,870031), \\
&\quad (208,315,983431),(313,315,1765891),(2,9,19),(5,27,87211), \\
&\quad (14,81,71119),(41,81,97685839),(68,81,163),(23,135,271), \\
&\quad (50,135,631),(77,135,811),(104,135,23311),(131,135,348031), \\
&\quad (8,99,23),(17,99,67),(26,99,199),(35,99,683),(44,99,5347), \\
&\quad (53,99,599479),(62,99,33057806959),(71,99,242099935645987), \\
&\quad (80,495,991),(179,495,2971),(278,495,3191), \\
&\quad (377,495,48912491),(476,495,2252127523412251),(89,693,463), \\
&\quad (188,693,5419),(287,693,14323),(386,693,289511839), \\
&\quad (485,693,35532364099),(584,693,2868251407519807), \\
&\quad (683,693,581283643249112959),(98,297,694387), \\
&\quad (197,297,14973866897175265228063698945547),(296,891,1783), \\
&\quad (593,891,1409033313878253109224688819), \\
&\quad (890,891,12430037668834128259094186647)\}
\end{aligned}$$

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

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

For $1 \leqslant s \leqslant 49$, 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,

$$\mathcal{A} = \{a_s(n_s)\}_{s=1}^{50} \tag{$*$}$$

is a cover of $\mathbb{Z}$, and $2^{n_s} \equiv 1 \pmod{p_s}$ for $1 \leqslant s \leqslant 50$. Let

$$M_1 = \prod_{s=1}^{50} p_s$$

and let α_1 be an integer such that

$$\alpha_1 \equiv 2^{a_s} \pmod{p_s}$$

for $1 \leqslant s \leqslant 50$.

Let x be an arbitrary positive integer with $x \equiv \alpha_1 \pmod{M_1}$. Suppose that $x \in \mathcal{S}_3$, i.e., $x = p^2+b^2+2^n$ for some $p \in \mathcal{P}$ and $b, n \in \mathbb{N}$. Since $\mathcal{A}$ is a cover of $\mathbb{Z}$, there exists $1 \leqslant s \leqslant 50$ such that $n \equiv a_s \pmod{n_s}$. Then

$$p^2+b^2 = x-2^n \equiv \alpha_1 - 2^{a_s} \equiv 0 \pmod{p_s}.$$

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 $1 \leqslant s \leqslant 50$. 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 $n \geqslant 0$. Let

$$M_2 = \prod_{s=1}^{50} q_s,$$

and let α_2 be an integer such that

$$\alpha_2 \equiv p_s^2 \pmod{q_s}$$

for every $1 \leqslant s \leqslant 50$.

Let $M = M_1 M_2$, and let α be an integer such that

$$\alpha \equiv \alpha_i \pmod{M_i}$$

for $i = 1, 2$. Then we have $\{x \in \mathbb{N} : x \equiv \alpha \pmod M\} \cap \mathcal{S}_3 = \emptyset$. 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 $1 \leqslant s \leqslant 50$. 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 $x - p_s^2 - 2^n = b^2$. $\square$

Now let us turn to the proof of Theorem 1.3. We still use the cover $\mathcal{A}$ in $(*)$. 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 $1 \leqslant s \leqslant 50$, 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*

$$
\begin{aligned}
&\{(c_s, r_s)\}_{s=1}^{50}\\
&\quad = \{(505, 47 \times 178481), (5519, 601 \times 1801), (366, 2731 \times 8191),\\
&\quad (1303, 73 \times 262657), (5149, 233 \times 2089), (5938, 43691 \times 131071),\\
&\quad (182725, 223 \times 616318177), (12153, 174763 \times 524287),\\
&\quad (148671, 13367 \times 164511353), (490297, 431 \times 2099863),\\
&\quad (115115, 2351 \times 13264529), (2370639, 6361 \times 20394401),\\
&\quad (37, 5 \times 17 \times 257), (5615, 13 \times 37 \times 109), (146, 89 \times 397 \times 2113),\\
&\quad (637, 97 \times 241 \times 673), (6393, 103 \times 2143 \times 11119),\\
&\quad (13847, 53 \times 157 \times 1613), (1799, 29 \times 113 \times 15790321),\\
&\quad (335, 59 \times 1103 \times 3033169), (451, 337 \times 92737 \times 649657),\\
&\quad (1479, 641 \times 65537 \times 6700417), (40655, 137 \times 953 \times 26317),\\
&\quad (13353, 228479 \times 48544121 \times 212885833),\\
&\quad (23775, 439 \times 2298041 \times 9361973132609), (10334, 229 \times 457 \times 525313),\\
&\quad (65971, 2687 \times 202029703 \times 1113491139767), (5893, 41 \times 61681 \times 4278255361),\\
&\quad (1344867, 911 \times 112901153 \times 23140471537), (560826, 277 \times 1013 \times 30269),\\
&\quad (406789, 283 \times 4513 \times 165768537521),\\
&\quad (415099, 191 \times 420778751 \times 30327152671),\\
&\quad (61153, 101 \times 4051 \times 8101), (1261375, 307 \times 2857 \times 6529),\\
&\quad (1324442, 107 \times 69431 \times 28059810762433),\\
&\quad (1663519, 321679 \times 26295457 \times 319020217),\\
&\quad (2094571, 3391 \times 23279 \times 65993), (1032375, 571 \times 32377 \times 1212847),\\
&\quad (6321391, 14951 \times 4036961 \times 2646507710984041),\\
&\quad (19031871, 937 \times 6553 \times 7830118297), (7918330, 2833 \times 37171 \times 179951),\\
&\quad (2286429, 61 \times 1321 \times 4562284561), (2227201, 5581 \times 8681 \times 49477),\\
&\quad (207773684, 131 \times 409891 \times 7623851), (2526613, 281 \times 122921 \times 7416361),\\
&\quad (5596695, 433 \times 577 \times 38737), (25234915, 593 \times 1777 \times 25781083),\\
&\quad (7950774, 251 \times 100801 \times 10567201), (10130779, 313 \times 21841 \times 121369),\\
&\quad (14272093, 1429 \times 3361 \times 14449)\}.
\end{aligned}
$$

Then for every $1 \leqslant s \leqslant 50$ *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 $0 \leqslant n < \mathrm{ord}_2(r_s)$, where $\mathrm{ord}_2(r)$ denotes the least positive integer such that $2^{\mathrm{ord}_2(r)} \equiv 1 \pmod{r}$.

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 α_3 be an integer such that

$$\alpha_3 \equiv c_s + p_s^2 \pmod{r_s}.$$

Let $M' = M_1M_3$ and let α' be an integer satisfying

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

For any $x \equiv \alpha' \pmod{M'}$, assume on the contrary that $x = p_s^2 + b^2 - 2^n$ for some $1 \leqslant s \leqslant 50$ 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 $p^2 + b^2 - 2^n$. $\square$

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

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

is non-empty?

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

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

Proof of the first assertion of Theorem 1.4. Let

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

Clearly,

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

We only need to prove that the set

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

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

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

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

$$|\{(x_1, x_2) : \ x_1 = x_2 + m, \ x_i \in \mathcal{Q}, \ x_i \leqslant N\}| \ll \frac{N}{\log N} \prod_{\substack{p \mid m \\ p \equiv 3 \pmod 4}} \left(1 + \frac{1}{p}\right)$$

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

$$\begin{aligned} &|\{x + 2^{n^2} : \ x + 2^{n^2} \leqslant N, \ x \in \mathcal{Q}, \ n \in \mathbb{N}\}| \\ &\qquad \geqslant \frac{|(x, n) : \ x + 2^{n^2} \leqslant N, \ x \in \mathcal{Q}, \ n \in \mathbb{N}\}|^2}{|\{(x_1, x_2, n_1, n_2) : \ x_1 + 2^{n_1^2} = x_2 + 2^{n_2^2} \leqslant N, \ x_i \in \mathcal{Q}, \ n_i \in \mathbb{N}\}|}. \end{aligned}$$

So it suffices to show that

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

Now

$$\begin{aligned}
&|\{(x_1,x_2,n_1,n_2):\ x_1+2^{n_1^2}=x_2+2^{n_2^2}\leqslant N,\ x_i\in\mathcal{Q},\ n_i\in\mathbb{N}\}|\\
\leqslant&|\{(x_1,n_1):\ x_1+2^{n_1^2}\leqslant N,\ x_1\in\mathcal{Q},\ n_1\in\mathbb{N}\}|\\
&+2\sum_{0\leqslant n_1<n_2\leqslant\sqrt{\log N/\log 2}}|\{(x_1,x_2):\ x_1-x_2=2^{n_2^2}-2^{n_1^2},\ x_i\in\mathcal{Q}\cap[1,N]\}|\\
\ll&N+\frac{N}{\log N}\sum_{0\leqslant n_1<n_2\leqslant\sqrt{\log N/\log 2}}\prod_{\substack{p\mid 2^{n_2^2}-2^{n_1^2}\\ p\equiv 3\ (\mathrm{mod}\ 4)}}\left(1+\frac{1}{p}\right).
\end{aligned}$$

Obviously,

$$\begin{aligned}
\sum_{0\leqslant n_1<n_2\leqslant\sqrt{\log N/\log 2}}\prod_{\substack{p\mid 2^{n_2^2}-2^{n_1^2}\\ p\equiv 3\ (\mathrm{mod}\ 4)}}\left(1+\frac{1}{p}\right)\leqslant&\sum_{0\leqslant n_1<n_2\leqslant\sqrt{\log N/\log 2}}\prod_{p\mid 2^{n_2^2}-2^{n_1^2}}\left(1+\frac{1}{p}\right)\\
\leqslant&\sum_{d}\frac{1}{d}\sum_{\substack{0\leqslant n_1<n_2\leqslant\sqrt{\log N/\log 2}\\ n_2^2\equiv n_1^2\ (\mathrm{mod}\ \mathrm{ord}_2(d))}}1.
\end{aligned}$$

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

$$|\{1\leqslant x\leqslant p^\beta:\ x^2\equiv a\ (\mathrm{mod}\ p^\beta)\}|\leqslant 2p^{\nu_p(a)/2},$$

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

$$\sum_{\substack{0\leqslant n_1<n_2\leqslant\sqrt{\log N/\log 2}\\ n_2^2\equiv n_1^2\ (\mathrm{mod}\ \mathrm{ord}_2(d))}}1\ll\sqrt{\frac{\log N}{\log 2}}\left(\sqrt{\frac{\log N}{\log 2}}\cdot\frac{2^{\omega(\mathrm{ord}_2(d))}\sqrt{\mathrm{ord}_2(d)}}{\mathrm{ord}_2(d)}+1\right),$$

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

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

converges. Define

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

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

$$\begin{aligned}
\sum_d\frac{2^{\omega(\mathrm{ord}_2(d))}}{d\sqrt{\mathrm{ord}_2(d)}}=&\sum_k\frac{2^{\omega(k)}}{\sqrt{k}}\sum_{\mathrm{ord}_2(d)=k}\frac{1}{d}\\
\ll&\int_1^\infty x^{-1/3}d(E(x))\\
=&x^{-1/3}E(x)\Big|_1^\infty+\frac{1}{3}\int_1^\infty x^{-4/3}E(x)dx=O(1).
\end{aligned}$$

□

Let $\mathcal{A} = \{a_s(n_s)\}_{s=1}^{50}$ be the cover in $(*)$, and let $p_1, \dots, p_{50}$ 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 1.4 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 $1 \leqslant s \leqslant 50$, there exists $1 \leqslant e_s \leqslant p_s$ such that*

$$|\mathcal{N} \cap \{x \in \mathbb{N} :\ x \equiv e_s \pmod{p_s}\}| < \infty.$$

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 $n_s^* = \mathrm{ord}_2(p_s)$. Noting that $n_s^* \mid n_s$ and $(n_s, p_s) = 1$, for every $1 \leqslant s \leqslant 50$, 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

$$\mathscr{H}_s = \mathcal{N} \cap \{x \in \mathbb{N} :\ x \equiv e_s \pmod{p_s}\} = \{h_{s,1}, h_{s,2}, \dots, h_{s,|\mathscr{H}_s|}\}$$

for $1 \leqslant s \leqslant 50$. Choose $|\mathscr{H}_1| + |\mathscr{H}_2| + \cdots + |\mathscr{H}_{50}|$ distinct primes

$$q_{1,1},\ \dots,\ q_{1,|\mathscr{H}_1|},\ q_{2,1},\ \dots,\ q_{2,|\mathscr{H}_2|},\ \dots,\ q_{50,1},\ \dots,\ q_{50,|\mathscr{H}_{50}|}$$

satisfying

$$q_{s,t} \equiv 3 \pmod 4$$

and

$$q_{s,t} \notin \{p_1, p_2, \dots, p_{50}\}$$

for every $1 \leqslant s \leqslant 50$ and $1 \leqslant t \leqslant |\mathscr{H}_s|$.

Let

$$M^* = \Bigg(\prod_{1 \leqslant s \leqslant 50} p_s \cdot \prod_{\substack{1 \leqslant s \leqslant 50 \\ 1 \leqslant t \leqslant |\mathscr{H}_s|}} q_{s,t} \Bigg)^2$$

and α^* be an integer such that

$$\alpha^* \equiv 2^{a_s^*} \pmod{p_s^2}$$

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 $1 \leqslant s \leqslant 50$. It follows that

$$x - 2^n \equiv 2^{a_s^*} - 2^n \equiv 0 \pmod{p_s^2},$$

that is, $n \equiv a_s^* \pmod{\mathrm{ord}_2(p_s^2))}$. It is not difficult to check that

$$2^{n_s^*} = 2^{\mathrm{ord}_2(p_s)} \not\equiv 1 \pmod{p_s^2}.$$

(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 $\mathrm{ord}_2(p_s^2) = n_s^* p$. Consequently,

$$n \equiv a_s^* \equiv e_s \pmod{p_s}.$$

Since $n \in \mathcal{N}$, we have $n \in \mathscr{H}_s$ and there exists $1 \leqslant t \leqslant |\mathscr{H}_s|$ such that $n = h_{s,t}$. It follows that

$$(\diamond) \qquad b_1^2+b_2^2 = x-2^n \equiv \alpha^* - 2^{h_{s,t}} \equiv q_{s,t} \pmod{q_{s,t}^2}.$$

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 $(\diamond)$. □

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.

Proof. Let $m = p_1p_2\dots p_{50}$ where $p_1,p_2,\dots,p_{50}$ 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. □

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 $b_1,b_2,n \in \mathbb{N}$?

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.

References

[1] J. Brillhart, D. H. Lehmer, J. L. Selfridge, B. Tuckerman, and S. S. Wagstaff, Jr., *Factorizations of $b^n \pm 1, b = 2,3,5,6,7,10,11,12$ up to High Powers*, 3rd ed., Contemporary Mathematics 22, Amer. Math, Soc., Providence, RI, 2002.

[2] J. Brüdern and E. Fouvry, *Lagrange's four squares theorem with almost prime variables*, J. Reine Angew Math., **454**(1994), 59-96. MR1288679 (96e:11125)

[3] Y.-G. Chen, *On integers of the form $2^n \pm p_1^{\alpha_1}\cdots p_r^{\alpha_r}$*, Proc. Amer. Math. Soc., **128**(2000), 1613-1616. MR1695159 (2000j:11006)

[4] Y.-G. Chen, *On integers of the form $k2^n+1$*, Proc. Amer. Math. Soc., **129**(2001), 355-361. MR1800230 (2003a:11004)

[5] Y.-G. Chen, *On integers of the form $k-2^n$ and $k2^n+1$*, J. Number Theory, **89**(2001), 121-125. MR1838707 (2002b:11020)

[6] Y.-G. Chen, *On integers of the forms k^r+2^n and k^r2^n+1*, J. Number Theory, **98**(2003), 310-319. MR1955419 (2003m:11004)

[7] Y.-G. Chen, *Five consecutive positive odd numbers, none of which can be expressed as a sum of two prime powers*, Math. Comp., **74**(2005), 1025-1031. MR2114663 (2006a:11010)
[8] Y.-G. Chen, *On integers of the forms* $k \pm 2^n$ *and* $k2^n \pm 1$, J. Number Theory, **125**(2007), 14-25. MR2333115 (2008e:11015)
[9] Y.-G. Chen, R. Feng and N. Templier, *Fermat numbers and integers of the form* $a^k + a^l + p^\alpha$, Acta Arith., **135**(2008), 51-61. MR2453523 (2009h:11023)
[10] F. Cohen and J. L. Selfridge, *Not every number is the sum or difference of two prime powers*, Math. Comp., **29**(1975), 79-81. MR0376583 (51:12758)
[11] R. Crocker, *On the sum of a prime and two powers of two*, Pacific J. Math., **36**(1971), 103-107. MR0277467 (43:3200)
[12] R. Crocker, *On the sum of two squares and two powers of* k, Colloq. Math., **112**(2008), 235-267. MR2383332 (2009a:11210)
[13] J. G. van der Corput, *On de Polignac's conjecture*, Simon Stevin, **27**(1950), 99-105. MR0035298 (11:714e)
[14] P. Erdős, *On integers of the form* $2^k + p$ *and some related problems*, Summa Brasil. Math. 2(1950), 113-123. MR0044558 (13:437i)
[15] H. Iwaniec, *Primes of the type* $\phi(x, y)+A$ *where* ϕ *is a quadratic form*, Acta Arith., **21**(1972), 203-234. MR0304331 (46:3466)
[16] H. Iwaniec, *The half dimensional sieve*, Acta Arith., **29**(1976), 69-95. MR0412134 (54:261)
[17] H. Iwaniec, *Rosser's sieve*, Acta Arith., **36** (1980), 171-202. MR581917 (81m:10086)
[18] H. Iwaniec, *A new form of the error term in the linear sieve*, Acta Arith., **37** (1980), 307-320. MR598883 (82d:10069)
[19] H. Halberstam and H.-E. Richert, *Sieve methods*, London Mathematical Society Monographs, **4**, Academic Press, London–New York, 1974. MR0424730 (54:12689)
[20] E. Landau, *Über die Einteilung der positiven ganzen Zahlen in vier Klassen nach der Mindeszahl der zu ihrer additiven Zusammensetzung erforderlichen Quadrate*, Arch. Math. Phys., **13**(1908), 305-312.
[21] F. Luca and P. Stănică, *Fibonacci numbers that are not sums of two prime powers*, Proc. Amer. Math. Soc., **133**(2005), 1887-1890. MR2099413 (2005k:11023)
[22] J.-Y. Liu, M.-C. Liu and T. Zhan, *Squares of primes and powers of 2*, Monatsh. Math., **128**(1999), 283-313. MR1726765 (2000k:11110)
[23] M. B. Nathanson, *Additive Number Theory: The Classical Bases*, *Grad. Texts Math.* **164**, Springer-Verlag, New York, 1996. MR1395371 (97e:11004)
[24] G. J. Rieger, *Über die Summe aus einem Quadrat und einem Primzahlquadrat*, J. Reine Angew Math., **231**(1968), 89-100. MR0229603 (37:5177)
[25] N. Romanoff, *Über einige Sätze der additiven Zahlentheorie*, Math. Ann., **109**(1934), 668-678. MR1512916
[26] Z. W. Sun, *On integers not of the form* $\pm p^a \pm q^b$, Proc. Amer. Math. Soc., **128**(2000), 997-1002. MR1695111 (2000i:11157)
[27] Z.-W. Sun and M.-H. Le, *Integers not of the form* $c(2^a + 2^b) + p^\alpha$, Acta Arith., **99**(2001), 183-190. MR1847620 (2002e:11043)
[28] Z.-W. Sun and S.-M. Yang, *A note on integers of the form* $2^n + cp$, Proc. Edinburgh Math. Soc., **45**(2002), 155-160. MR1884609 (2002j:11117)
[29] 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)
[30] P. Z. Yuan, *Integers not of the form* $c(2^a + 2^b) + p^\alpha$, Acta Arith., **115**(2004), 23-28. MR2102803 (2005f:11035)

Department of Mathematics, Nanjing University, Nanjing 210093, People's Republic of China
E-mail address: haopan79@yahoo.com.cn

Department of Mathematics, Nanjing University, Nanjing 210093, People's Republic of China
E-mail address: zhangwei_07@yahoo.com.cn