1. Introduction

Recently, Khalfalah and Szemerédi [7] proved the following theorem, which was conjectured by Erdős, Roth, Sárközy and Sós [3]:

**Theorem 1.1.** Let \( \psi \) be a polynomial with integral coefficients and positive leading coefficient. Suppose that \( \psi(1) \psi(0) \) is even. Then for any \( m \)-coloring of all positive integers (i.e., partitioning \( \mathbb{Z}^+ \) into \( m \) disjoint non-empty subsets), there exist monochromatic distinct \( x, y \) such that \( x + y = \psi(z) \) for an integer \( z \).

In particular, if all positive integers are colored with \( m \)-colors, then there exists a monochromatic pair \( x, y \) with \( x \neq y \) such that \( x + y \) is a perfect square.

On the other hand, suppose that \( \psi \) is a polynomial with rational coefficients and zero constant term, in [9] Li and Pan proved that for any subset \( A \) of positive integers with

\[
\limsup_{x \to \infty} \frac{|A \cap [1, x]|}{x} > 0,
\]

there exist \( x, y \in A \) and a prime \( p \) such that \( x - y = \psi(p - 1) \). This commonly generalizes two well-known results of Furstenberg [4] and Sárközy [10, 11].

Define

\[
\lambda_{b,W}(x) = \begin{cases} 
\phi(W) \log(Wx + b) & \text{if } Wx + b \text{ is prime}, \\
0 & \text{otherwise},
\end{cases}
\]

where \( \phi \) is the Euler totient function and

\[
\Lambda_{b,W} = \{x : Wx + b \text{ is prime}\}
\]

for \( 1 \leq b \leq W \) with \( (b,W) = 1 \). In the present paper, our main result is the following theorem:

**Theorem 1.2.** Let \( m, b_0, W_0 \) be positive integers satisfying \( b_0 \leq W_0 \) and \( (b_0, W_0) = 1 \). Let \( \psi(x) \) be a polynomial with integral coefficients and positive leading coefficient satisfying that

\[
\begin{cases} 
\psi(1) \text{ or } \psi(0) \text{ is even} & \text{if } 2 \mid W_0, \\
\psi(b_0 - 1) \text{ is even} & \text{if } 2 \nmid W_0.
\end{cases}
\]

2000 Mathematics Subject Classification. Primary 11P32; Secondary 05D99, 11P55.

This work was supported by the National Natural Science Foundation of China (Grant No. 10471090).
Suppose that all positive integers are colored with \( m \) colors. Then there exist distinct monochromatic \( x, y \) such that \( x + y = \psi(z) \) where \( z \in \Lambda_{b_0,W_0} \).

We shall use one of Green's ingredients in his proof of Roth's theorem in primes. The key of Green’s proof is a transference principle (which was greatly developed in [6]), i.e., transferring a subset of primes with positive relative density to a subset of \( \mathbb{Z}_N = \mathbb{Z}/NZ \) with positive density, where \( N \) is a large prime. In the proof of Theorem 1.2 we shall transfer one subset of \( \{ \psi(z) : z \in \Lambda_{b,W} \} \) to a subset of \( \mathbb{Z}_N = \mathbb{Z}/NZ \) with the density very close to 1.

**Theorem 1.3.** Let \( m, b_0, W_0 \) be positive integers satisfying \( b_0 \leq W_0 \) and \( (b_0, W_0) = 1 \). Let \( \psi(x) \) be a polynomial with integral coefficients and positive leading coefficient satisfying that

\[
\begin{cases}
\psi(1) \text{ or } \psi(0) \text{ is even} & \text{if } 2 \mid W_0, \\
\psi(b_0 - 1) \text{ is even} & \text{if } 2 \nmid W_0.
\end{cases}
\]

Also, suppose that for each prime \( p \), there exists \( 1 \leq c_p \leq p \) such that both \( W_0c_p + b_0 \) and \( \frac{1}{2}\psi(c_p) \) are not divisible by \( p \). Then for any \( m \)-coloring of all primes, there exist distinct monochromatic primes \( x, y \) such that \( x + y = \psi(z) \) where \( z \in \Lambda_{b_0,W_0} \).

Let us explain why the existence of \( c_p \) is necessary. Assume that there exists a prime \( p \) such that \( c_p \) doesn’t exist. That is, for each \( 1 \leq c \leq p \), either \( W_0c + b_0 \) or \( \frac{1}{2}\psi(c) \) is divisible by \( p \). Then we may partition the set of all primes into \( 3p \) disjoint sets \( X_1, \ldots, X_{3p} \) with

\[
X_j = \{ x \text{ is prime } : x \leq \psi((p - b_0)/W_0)/2, x \equiv j \pmod{p} \},
\]

and

\[
X_{p+j} = \{ x \text{ is prime } : x > \psi((p - b_0)/W_0), x \equiv j \pmod{p} \}
\]

and

\[
X_{2p+j} = \{ x \text{ is prime } : \psi((p - b_0)/W_0)/2 < x \leq \psi((p - b_0)/W_0), x \equiv j \pmod{p} \}
\]

for \( j = 1, 2, \ldots, p \). We claim that for each \( 1 \leq j \leq 3p \), the set

\[
\{ (x, y, z) : x, y \in X_j, z \in \Lambda_{b_0,W_0}, x \neq y, x + y = \psi(z) \}
\]

is empty.

In fact, notice that now \( p \) divides one of \( W_0z + b_0 \) and \( \frac{1}{2}\psi(z) \) since \( c_p \) doesn’t exist. If \( p \) divides \( W_0z + b_0 \), we must have \( W_0z + b_0 = p \) since \( z \in \Lambda_{b_0,W_0} \). But it is easy to see that for \( 1 \leq j \leq p \)

\[
\max\{ x + y : x, y \in X_j, x \neq y \} < 2 \cdot \psi((p - b_0)/W_0)/2 = \psi(z),
\]

and for \( p + 1 \leq j \leq 3p \)

\[
\min\{ x + y : x, y \in X_j, x \neq y \} > 2 \cdot \psi((p - b_0)/W_0)/2 = \psi(z).
\]

So it is impossible that

\[
\psi(z) \in X_j + X_j := \{ x + y : x, y \in X_j, x \neq y \}
\]

for any \( 1 \leq j \leq 3p \).

On the other hand, suppose that \( p \) divides \( \frac{1}{2}\psi(z) \). Note that for any \( 1 \leq j \leq 3p \) and \( x, y \in X_j, x \equiv y \equiv j \pmod{p} \). So if \( x + y = \psi(z) \), then we must have
\(x \equiv y \equiv 0 \pmod{p}\). Thus we have \(x = y = p\) since \(x, y\) are both primes. This also concludes that \(\psi(z) \not\equiv X_j + X_j\) for each \(j\).

2. Proof of Theorem 1.2

Assume that \(n\) is a sufficiently large integer, and
\[
\{1, 2, \ldots, n\} = X_1 \cup \cdots \cup X_m
\]
where \(X_i \cap X_j = \emptyset\) if \(i \neq j\).

Lemma 2.1. Let \(p\) be a prime. Let \(h(x)\) be a non-zero polynomial over \(\mathbb{Z}_p\). Suppose that \(S \subseteq \mathbb{Z}_p\) and \(|S| \geq \deg h + 1\). Then there exists \(b \in S\) such that \(h(b) \not\equiv 0 \pmod{p}\).

Proof. This lemma easily follows from the fact that
\[
|h(x) - h(y)| \leq \deg h \cdot |x - y|
\]
since \(h(x)\) doesn’t vanish over \(\mathbb{Z}_p\). \(\square\)

Suppose \(\psi(x) = a_1 x^k + \cdots + a_k x + a_0\) be a polynomial with integral coefficients. Let \(\Psi = \max\{(k+1)W_0, |a_1|, \ldots, |a_k|\}\). Let \(\psi'\) denote the derivative of \(\psi\). Then for any prime \(p > \Psi\), by Lemma 2.1, there exists \(1 \leq b_p \leq p-1\) with \(b_p \equiv b_0 \pmod{W_0}\) such that \(\psi'((b_p - b_0)/W_0), p) = 1\). And for each prime \(p \leq \Psi\), we may choose \(b_p \geq 1\) with \(p \mid b_p\) such that \(b_p \equiv b_0 \pmod{W_0}\) and \(\psi'((b_p - b_0)/W_0) > 0\). In particular, we may assume that \(\psi((b_2 - b_0)/W_0)\) is even if \(2 \mid W_0\). Let
\[
K = \prod_{p \text{ prime}} p^{
u_p(\psi'((b_p - b_0)/W_0))},
\]
where \(\nu_p(x) = \max\{v \in \mathbb{Z} : p^v \mid x\}\).

Let \(\kappa = 10^{-4}K^{-1}m^{-1}\). Let \(w = \lceil \log \log \log n \rceil\) and
\[
W = \prod_{p \text{ prime}} p^w.
\]

Without loss of generality, we may assume that \(w \geq \Psi\). Suppose that \(N\) is a prime in the interval \((2n/W, (2 + \kappa)n/W)\). Thanks to the prime number theorem, such prime \(N\) always exists whenever \(n\) is sufficiently large. By the Chinese remainder theorem, there exists \(0 \leq b \leq W - 1\) such that for each prime \(p \leq w\)
\[
W_0 b + b_0 \equiv b_p \pmod{W_0}.
\]
since \(b_p \equiv b_0 \pmod{W_0}\). Clearly \((W_0 b + b_0, WW_0) = 1\). We claim that \(\psi(b)\) is even. In fact, when \(W_0\) is odd, \(b \equiv b_2 - b_0 \equiv b_0 - 1 \pmod{2}\). And if \(W_0\) is even, we also have \(2 \mid \psi(b)\) since \(b \equiv (b_2 - b_0)/W_0 \pmod{2}\).

Define
\[
\psi_{b,W}(x) = \psi(Wx + b) - \psi(b).
\]
Let \(M = \max\{x \in \mathbb{N} : \psi_{b,W}(x) < KN\}\). Let \(B\) be a sufficiently large positive constant (only depending on \(k\)). Let
\[
\mathfrak{M}_{a,q} = \{\alpha \in \mathbb{T} : |\alpha q - a| \leq (\log M)^B/\psi_{b,W}(M)\},
\]
\[ M = \bigcup_{1 \leq a \leq q \leq (\log M)^B} M_{a,q} \]

and \( m = \mathbb{T} \setminus M \), where \( \mathbb{T} = \mathbb{R}/\mathbb{Z} \).

**Lemma 2.2.** For \( \alpha \in M_{a,q} \),
\[
\sum_{x=1}^{M} \psi_{a,W}^\Delta(x - 1)\lambda_{W_{b} + b_0,WW_0}(x)e(\alpha\psi_{b,W}(x))
= \frac{\phi(WW_0)}{\phi(WW_0q)} \sum_{1 \leq r \leq q} e(a\psi_{b,W}(r)/q) \sum_{x=1}^{\psi_{b,W}(M)} e((\alpha - a/q)\psi_{b,W}(x))
+ O(\psi_{b,W}(M)(\log M)^{-B}),
\]
where \( \psi_{b,W}(x) = \psi_{b,W}(x + 1) - \psi_{b,W}(x) \).

**Lemma 2.3.** Suppose that \( U \geq e^aW^k \). For any \( A > 0 \), there is a \( B = B(A,k) > 0 \) such that,
\[
\sum_{x=1}^{N} \lambda_{b,W}(x)e(\alpha\psi(x)) \ll_B N(\log N)^{-A}
\]
provided that \( |\alpha - a/q| \leq q^{-2} \) with \( 1 \leq a \leq q \), \( (a,q) = 1 \) and \( (\log N)^B \leq q \leq \psi(N)(\log N)^{-B} \).

Lemma 2.2 is the immediate consequence of Lemmas 2.3 and 2.4 of [9]. The proof of Lemma 2.3 is standard but too long, so we omit the details here. And the readers may refer to [9] for the proof.

Clearly \( \psi_{b,W} \) is positive and strictly increasing on \([1,M]\) provided that \( W \) is sufficiently large. Define
\[
a(x) = \begin{cases} 
\psi_{a,W}^\Delta(z - 1)\lambda_{W_{b} + b_0,WW_0}(z)/\psi_{b,W}(M) & \text{if } x = \psi_{b,W}(z) \text{ for a } 1 \leq z \leq M, \\
0 & \text{otherwise}.
\end{cases}
\]

For any \( f : \mathbb{Z}_N \to \mathbb{C} \), define
\[
\hat{f}(r) = \sum_{x=1}^{N} f(x)e(-xr/N).
\]

**Lemma 2.4.** For any \( 0 \neq r \in \mathbb{Z}_N \),
\[
|\hat{a}(r)| \leq C_1 Kw^{-\frac{1}{\kappa(k+1)}}, \quad (2.1)
\]
where \( C_1 \) is a constant (only depending on \( k \)).

**Proof.** If \( r/N \in m \), then by Lemma 2.3 and partial summation,
\[
\hat{a}(r) = \frac{1}{\psi_{b,W}(M)} \sum_{z=1}^{M} \psi_{a,W}^\Delta(z - 1)\lambda_{W_{b} + b_0,WW_0}(z)e(-\psi_{b,W}(z)r/N) \ll (\log M)^{-1}.
\]
Suppose that $r/N \in \mathfrak{m}_{a,q}$. Then by Lemma 2.2

$$\frac{1}{\psi_{b,W}(M)} \sum_{z=1}^{M} \psi_{b,W}^\Delta(z-1) \lambda_{W_0b+b_0} \psi_{W_0}(z)e(-\psi_{b,W}(z)r/N)$$

$$= \frac{\phi(WW_0)}{\phi(WW_0q)\psi_{b,W}(M)} \sum_{1 \leq s \leq q} e(-\psi_{b,W}(s)a/q) \sum_{x=1}^{\psi_{b,W}(M)} e(x(r/N - a/q))$$

$$+ O((\log M)^{-B})$$

Notice that the leading coefficient of $\psi_{b,W}(x)$ is $a_1W^{k-1}$, and the coefficient of $x^1$ in $\psi_{b,W}(x)$ coincides with

$$\psi_{b,W}'(0) = \lim_{x \to 0} \left( \frac{d}{dx} \left( \frac{\psi(Wx + b) - \psi(b)}{W} \right) \right) = \lim_{x \to b} \left( \frac{d\psi(x)}{dx} \right) = \psi'(b).$$

Also, clearly for each prime $p \leq w$, $\psi'(b) \equiv \psi'((b_p - b_0)/W_0) \pmod{p^w}$ since $W_0b + b_0 \equiv b_p \pmod{p^{w+\nu_p(W_0)}}$. Therefore when $w$ is sufficiently large, we have

$$(\psi'(b), a_1W^{k-1}) = (\psi'(b), W) = \prod_{p \leq \Psi} p^{\nu_p(\psi'((b_p - b_0)/W_0))} = K.$$

Thus by Lemma 2.7 of [9],

$$\sum_{1 \leq s \leq q} e(\psi_{b,W}(s)a/q) \ll K q^{1 - \frac{1}{\pi(1) + 2}}.$$

Let $q_2$ be the largest divisor of $q$ prime to $W$ and $q_1 = q/q_2$. If $q \nmid W$, then either $q_2 > w$ or $q \geq 2^w$. Hence

$$\frac{\phi(WW_0)}{\phi(WW_0q)\psi_{b,W}(M)} \sum_{1 \leq s \leq q} e(\psi_{b,W}(s)a/q) \sum_{x=1}^{\psi_{b,W}(M)} e(x(r/N - a/q))$$

$$\ll K q^{1 - \frac{1}{\pi(1) + 2}} q_1 q_2 q_2 \psi_{b,W}(M) \sum_{x=1}^{\psi_{b,W}(M)} e(x(r/N - a/q))$$

$$\ll Kw^{-\frac{1}{\pi(1) + 2}}.$$

Below assume that $q \mid W$. Since $W$ divides the coefficients of $x^i$ in $\psi_{b,W}(x)$ for $2 \leq i \leq k$, we have

$$\sum_{1 \leq s \leq q} e(\psi_{b,W}(s)a/q) = \sum_{1 \leq s \leq q} e(\psi'(b)sa/q) = \begin{cases} q & \text{if } q \mid (\psi'(b), W) = K, \\ 0 & \text{otherwise}. \end{cases}$$
Now suppose that \( q \mid K \). Since \( KN - \psi_{b,W}(M) \leq \psi_{b,W}(M) \), then
\[
\sum_{x=1}^{\psi_{b,W}(M)} e(x(r/N - a/q)) = \sum_{x=1}^{KN} e(x(r/N - a/q)) + O(\psi_{b,W}(M))
= O(\psi_{b,W}(M)).
\]
This concludes that if \( q \mid W \) then
\[
\frac{\phi(WW_0)}{\phi(WW_0q)\psi_{b,W}(M)} \sum_{1 \leq s \leq q} e(\psi_{b,W}(s)a/q) \sum_{x=1}^{\psi_{b,W}(M)} e(x(r/N - a/q))
= O((\log M)^{-B}).
\]
\[\square\]

By the pigeonhole principle, there exists \( 1 \leq i \leq m \) such that
\[
|\{x \in X_i \cap [\psi(W), n] : x \equiv \psi(b)/2 \pmod{KW}\}| \geq \frac{n}{mKW} - \psi(W) \geq \frac{N}{4mK}.
\]
Without loss of generality, we may assume that \( X_1 \) is such a set. Let
\[
A = \{(x - \psi(b)/2)/W : x \in X_1 \cap [\psi(W), n] : x \equiv \psi(b)/2 \pmod{KW}\}.
\]
Suppose that there exist \( x', y' \in A \) and \( z' \in A_{W_0+b_0,WW_0} \) such that \( x' + y' = \psi_{b,W}(z') \). Then letting \( x = Wx' + \psi(b)/2, y' = Wy' + \psi(b)/2 \in X_1 \) and \( z = Wz' + b \in A_{b_0,W_0} \), we have \( x + y = \psi(z) \).

Below we consider \( A \) as a subset of \( \mathbb{Z}_N \). We claim that if \( x, y \in A \) and \( z \in A_{W_0+b_0,WW_0} \cap [1, M] \) satisfy \( x + y = \psi_{b,W}(z) \) in \( \mathbb{Z}_N \), then the equality also holds in \( \mathbb{Z} \). Suppose that \( x + y = \psi_{b,W}(z) - lN \) for an integer \( l \). Then \( 0 \leq l < K \) since \( n/W < N/2 \) and \( \psi_{b,W}(z) < KN \). Notice that \( K \) divides \( x + y \) and all coefficients of \( \psi_{b,W} \). We must have \( K \mid l \), whence \( l = 0 \). Furthermore, we may consider \( a \) as a function over \( \mathbb{Z}_N \), i.e.,
\[
a(x) = \begin{cases} 
\psi_{b,W}(z-1)/\psi_{b,W}(M) & \text{if } x = \psi_{b,W}(z) \text{ in } \mathbb{Z}_N \text{ for a } 1 \leq z \leq M, \\
0 & \text{otherwise}.
\end{cases}
\]
This function is well-defined. In fact, assume that \( 1 \leq z_1, z_2 \leq M \) and \( \psi_{b,W}(z_1) = \psi_{b,W}(z_2) \) in \( \mathbb{Z}_N \). Then \( \psi_{b,W}(z_1) = \psi_{b,W}(z_2) + lN \) in \( \mathbb{Z} \) where \( |l| < K \). But \( \psi_{b,W}(z_1) \equiv \psi_{b,W}(z_2) \pmod{K} \), so \( l = 0 \) and \( z_1 = z_2 \).

Let \( \eta \) and \( \epsilon \) be two positive real numbers to be chosen later. Let
\[
\mathcal{R} = \{r \in \mathbb{Z}_N : |\bar{a}(r)| \geq \eta\}
\]
and
\[
\mathcal{B} = \{x \in \mathbb{Z}_N : \|xr/N\| \leq \epsilon \text{ for all } r \in \mathcal{R}\},
\]
where \( \|x\| = \min\{|x-z| : z \in \mathbb{Z}\} \). Define \( b = 1_B/|B| \) and \( a' = a \ast b \ast b \), where \( 1_B(x) = 1 \) or \( 0 \) according to whether \( x \in B \) or not and
\[
f \ast g(x) = \sum_{y \in \mathbb{Z}_N} f(y)g(x-y).
\]
Lemma 2.5. If \( e^{|R|} \geq \kappa^{-1} C_1 K w^{-\kappa(k+3)} \), then for any \( x \in \mathbb{Z}_N \)

\[
|a'(x)| \leq \frac{1 + 2\kappa}{N}.
\]

Proof. It is easy to see that \( \tilde{\tilde{f}} \star \tilde{g} = \tilde{f} \cdot \tilde{g} \). By Lemma 2.2 for \( \alpha = 0 \) and Lemma 2.4,

\[
|a'(x)| = \left| \frac{1}{N} \sum_r \tilde{\tilde{a}}(r) \tilde{\tilde{b}}(r)^2 e\left( \frac{xy}{N} \right) \right|
\]

\[
\leq \frac{1}{N} \left( \tilde{\tilde{b}}(0) \right)^2 \left( \psi_{b,W}^A(z-1) \lambda_{W_{b+b_0,W_{b_0}}(z)} + \frac{1}{N} \sup_{r \neq 0} |\tilde{a}(r)| \sum_{r \neq 0} |\tilde{b}(r)|^2 \right)
\]

\[
\leq \frac{1 + \kappa}{N} + \frac{C_1 K w^{-\kappa(k+3)}}{|B|}.
\]

By the pigeonhole principle (cf. [12, Lemma 1.4]), we have \(|B| \geq \frac{\epsilon^{|R|}}{|R|} N\). All are done.

Lemma 2.6.

\[
\sum_{r \in \mathbb{Z}_N} |\tilde{a}(r)|^\rho \leq C(\rho) K.
\]

provided that \( \rho \geq k 2^{k+3} \), where \( C(\rho) \) is a constant only depending on \( \rho \).

Proof. Note that

\[
\sum_{r \in \mathbb{Z}_N} |\tilde{a}(r)|^\rho = \frac{1}{\psi_{b,W}(M)^\rho} \sum_{r \in \mathbb{Z}_N} \left( \sum_{z=1}^M \psi_{b,W}^A(z-1) \lambda_{W_{b+b_0,W_{b_0}}(z)} e\left( -\psi_{b,W}(z)r/N \right) \right)^\rho.
\]

Thus Lemma 2.6 easily follows from Lemma 2.10 of [9].

Lemma 2.7.

\[
\left| \sum_{1 \leq x,y,z \leq N} 1_A(x) 1_A(y) a(z) - \sum_{1 \leq x,y,z \leq N} 1_A(x) 1_A(y) a'(z) \right|
\]

\[
\leq C_2 K \left( e^2 \eta^{-k 2^{k+3}} + \eta^{k 2^{k+3}+1} \right) N,
\]

where \( C_2 \) is a positive constant (only depending on \( k \)).

Proof. It is easy to see that

\[
\sum_{1 \leq x,y,z \leq N} 1_A(x) 1_A(y) a(z) = \frac{1}{N} \sum_{r \in \mathbb{Z}_N} \tilde{1}_A(r) \tilde{1}_A(-r) \tilde{a}(r)
\]

and

\[
\sum_{1 \leq x,y,z \leq N} 1_A(x) 1_A(y) a'(z) = \frac{1}{N} \sum_{r \in \mathbb{Z}_N} \tilde{1}_A(r) \tilde{1}_A(-r) \tilde{a}(r) \tilde{b}(r)^2.
\]
Hence
\[
\sum_{1 \leq x, y, z \leq N \atop x+y=z} 1_A(x)1_A(y)a(z) - \sum_{1 \leq x, y, z \leq N \atop x+y=z} 1_A(x)1_A(y)a'(z) = \frac{1}{N} \sum_{r \in \mathbb{Z}_N} \tilde{1}_A(r)\tilde{1}_A(-r)\tilde{a}(r)(1 - \tilde{b}(r)^2).
\]

Let \( \rho = k2^{k+3} \). If \( r \in \mathbb{R} \), then by the proof of Lemma 6.7 of [5]
\[|1 - \tilde{b}(r)^2| \leq 32\epsilon^2.\]

So
\[
\left| \sum_{r \in \mathbb{R}} \tilde{1}_A(r)\tilde{1}_A(-r)\tilde{a}(r)(1 - \tilde{b}(r)^2) \right| \leq |1 - \tilde{b}(r)^2| \sum_{r \in \mathbb{R}} |\tilde{1}_A(r)||\tilde{a}(r)| \leq 64\epsilon^2 N^2 |\mathcal{R}|.
\]

By Lemma 2.6 we have,
\[
|R| \leq \eta^{-\rho} \sum_{r \in \mathbb{R}} |\tilde{a}(r)|^\rho \leq C(\rho) \eta^{-\rho}.
\]

Applying the Hölder inequality,
\[
\left| \sum_{r \notin \mathbb{R}} \tilde{1}_A(r)\tilde{1}_A(-r)\tilde{a}(r)(1 - \tilde{b}(r)^2) \right|
\leq 2N^{\frac{\rho}{\rho+1}} \sup_{r \notin \mathbb{R}} |\tilde{a}(r)|^{\frac{\rho}{\rho+1}} \left( \sum_{r \notin \mathbb{R}} |\tilde{1}_A(r)|^2 \right)^{\frac{1}{\rho+1}} \left( \sum_{r \notin \mathbb{R}} |\tilde{a}(r)|^\rho \right)^{\frac{1}{\rho+1}}
\leq 2C(\rho)K^{\frac{\rho}{\rho+1}} \eta^{\frac{\rho}{\rho+1}} N^2,
\]
where we again use Lemma 2.6 in the last step. \(\square\)

**Lemma 2.8.**
\[
\sum_{x, y, z \in \mathbb{Z}_N \atop x+y=z} 1_A(x)1_A(y)a'(z) \geq \kappa^4 N.
\]

**Proof.** Let
\[\mathcal{A} = \{x \in \mathbb{Z}_N : a'(x) \geq \kappa/N \}.\]

Then by Lemma 2.5
\[
\frac{1 + 2\kappa}{N} |\mathcal{A}| + \frac{\kappa}{N} (N - |\mathcal{A}|) \geq \sum_{x \in \mathbb{Z}_N} a'(x) = \sum_{x \in \mathbb{Z}_N} a(x) \geq 1 - \kappa,
\]
whence \( |\mathcal{A}| \geq (1 - 3\kappa)N \). Define
\[
\nu_{A, A', \mathcal{A}}(x) = |\{(x_1, x_2, x_3) : x_1, x_2 \in A, x_3 \in \mathcal{A}, x_1 + x_2 - x_3 = x\}|.
\]
By Lemma 3.3 of [8], we know
\[ \nu_{A,A,-a}(x) \geq (\min\{|A|, |A|, \frac{2|A| + |A| - N}{4}\})^3 N^{-1}. \]
for any \( x \in \mathbb{Z}_N \). It follows that
\[ \sum_{x,y,z \in \mathbb{Z}_N} 1_A(x)1_A(y)a'(z) \geq \sum_{x,y \in A, z \in A} \kappa = \frac{\kappa}{N} \nu_{A,A,-a}(0) \geq \kappa^4 N. \]
\[ \square \]

Combining Lemmas 2.7 and 2.8, we obtain that
\[ \sum_{1 \leq x,y,z \leq N} 1_A(x)1_A(y)a(z) \geq \sum_{1 \leq x,y,z \leq N} 1_A(x)1_A(y)a'(z) - C_2 K \left( \epsilon^2 \eta^{-k2^{k+3}} + \eta \frac{1}{k2^{k+3+1}} \right) N \]
\[ \geq \kappa^4 N - C_2 K \left( \epsilon^2 \eta^{-k2^{k+3}} + \eta \frac{1}{k2^{k+3+1}} \right) N. \]

We may choose sufficiently small \( \eta \) and \( \epsilon \) such that
\[ \epsilon^{C(k2^{k+3})K \eta^{-k2^{k+3}}} \geq \kappa^{-1} C_1 K w^{-\frac{1}{k(k+1)}} \]
and \( C_2 K \left( \epsilon^2 \eta^{-k2^{k+3}} + \eta \frac{1}{k2^{k+3+1}} \right) \leq \kappa^4 / 2 \), provided that \( w \) is sufficiently large. Thus
\[ \sum_{x,y \in A, 1 \leq z \leq N} a(z) \geq \sum_{x,y \in A, 1 \leq z \leq N} a(z) - \sum_{1 \leq z \leq N} a(z) \geq \frac{\kappa^4}{3} N. \]
All are done. \[ \square \]

3. Proof of Theorem 1.3

Let \( \mathcal{P} \) denote the set of all primes. Assume that \( \mathcal{P} = X_1 \cup \cdots \cup X_m \) where \( X_i \cap X_j = \emptyset \) if \( i \neq j \). Also, let \( \kappa = 10^{-4} K^{-1} m^{-1} \).

Let \( \Psi = \max\{(2k + 1)W_0, |a_1|, \ldots, |a_k|\} \). Then for a prime \( p > \Psi \), by Lemma 2.1 we know that there exists \( 1 \leq b_p \leq p - 1 \) with \( b_p \equiv b_0 \pmod{W_0} \) such that
\[ \psi'(b_p - b_0)/W_0 \psi((b_p - b_0)/W_0) \not\equiv 0 \pmod{p}. \]
For a prime \( p \leq \Psi \), we may choose \( b_p \geq 1 \) such that
\[ b_p \equiv W_0 c_p + b_0 \pmod{pW_0} \]
and \( \psi'((b_p - b_0)/W_0) > 0 \). Let
\[ K = \prod_{p \text{ prime \hspace{1em} } p \leq \Psi} p^{\nu_p(\psi'((b_p - b_0)/W_0))}, \]
where \( \nu_p(x) = \max\{v \in \mathbb{Z} : p^v \mid x\} \).
Suppose that $n$ is a sufficiently large integer. Let $w = \lfloor \log \log \log \log n \rfloor$ and

$$W = \prod_{\text{prime } p \leq w} p^w.$$ 

Same as previous section, there exists $1 \leq b \leq W - 1$ such that

$$W_0b + b_0 \equiv b_p \pmod{p^{w + \nu_p(W_0)}}$$

for each prime $p \leq w$. And also we know that $\psi(b)$ is even.

By the prime number theorem, we know

$$\sum_{1 \leq x \leq n, \ x\text{ prime}} x \equiv \frac{\psi(b)}{2} (\mod KW)$$

$$\log x = \frac{1 + o(1)}{\phi(KW)} n.$$ 

Hence in view of the pigeonhole principle, without loss of generality, we may assume that

$$\sum_{x \in X_1 \cap [\psi(W), n]} \log x \geq \frac{(1 - \kappa)n}{m\phi(KW)}.$$ 

Let $N$ be a prime in $(2n/W, (2 + \kappa)n/W]$ and

$$A = \{(x - \psi(b)/2)/W : x \in X_1 \cap [\psi(W), n], x \equiv \psi(b)/2 \pmod{KW}\}.$$ 

Below we consider $A$ as a subset of $\mathbb{Z}_N$. Similarly, if $x' + y' = \psi_{b,W}(z')$ holds in $\mathbb{Z}_N$ for $x', y' \in A$ and $z' \in \Lambda_{W_0b+b_0,WW_0}$, then we also have $x + y = \psi(z)$ holds in $\mathbb{Z}$ where $x = Wx' + \psi(b)/2$, $y = Wy' + \psi(b)/2 \in X_1$ and $z = Wz' + b \in \Lambda_{b_0,W_0}$.

Define $a = 1_A\lambda_{\psi(b)/2,KW}/N$. Clearly we have

$$\sum_{x=1}^{N} a(x) \geq \frac{1}{3mK}.$$ 

**Lemma 3.1** (Bourgain [1, 2] and Green [5]).

$$\sum_{r=1}^{N} |\tilde{a}(r)|^{\rho} \leq C'(\rho)$$

for any $\rho > 2$.

**Proof.** See [5, Lemma 6.6]. \qed

Let

$$R = \{r \in \mathbb{Z}_N : |\tilde{a}(r)| \geq \eta\}$$

and

$$B = \{x \in \mathbb{Z}_N : \|xr/N\| \leq \epsilon \text{ for all } r \in R\}.$$ 

Define $\beta = 1_B/|B|$ and $a' = a * \beta * \beta$. 

Lemma 3.2. 

\[ \left| \sum_{1 \leq x, y, z \leq N \atop x + y = z} a(x)a(y)a(z) - \sum_{1 \leq x, y, z \leq N \atop x + y = z} a'(x)a'(y)a'(z) \right| \]

\[ \leq C_3 K^{\frac{1}{p+1}} (\epsilon^2 \eta^{-k^{2k+3}} + \eta^{\frac{1}{2k+3+1}}) N^{-1}, \]

where \( C_3 \) is a positive constant (only depending on \( k \)).

Proof. We have

\[ \sum_{1 \leq x, y, z \leq N \atop x + y = z} a(x)a(y)a(z) - \sum_{1 \leq x, y, z \leq N \atop x + y = z} a'(x)a'(y)a'(z) \]

\[ = \frac{1}{N} \sum_{r \in \mathbb{Z}_N} \tilde{a}(r) \tilde{a}(-r) \tilde{a}(r) \left( 1 - \tilde{\beta}(r)^2 \tilde{\beta}(-r)^2 \tilde{b}(r)^2 \right). \]

Let \( \rho = k^{2k+3} \). If \( r \in R \cap \mathcal{R} \), then by Lemma 6.7 of [5],

\[ |1 - \tilde{\beta}(r)^2 \tilde{\beta}(-r)^2 \tilde{b}(r)^2| \leq 2^{15} \epsilon^2. \]

It follows that

\[ \left| \sum_{r \in R \cap \mathcal{R}} \tilde{a}(r) \tilde{a}(-r) \tilde{a}(r) \left( 1 - \tilde{\beta}(r)^2 \tilde{\beta}(-r)^2 \tilde{b}(r)^2 \right) \right| \]

\[ \leq 2^{15} \epsilon^2 \sum_{r \in R \cap \mathcal{R}} |\tilde{a}(r)|^2 |\tilde{a}(r)| \]

\[ \leq 2^{16} \epsilon^2 \min\{|R|, |\mathcal{R}|\}. \]

And by Lemma 2.6 we have \(|R| \leq C'(\rho) \eta^{-\rho}\). Also, by the Hölder inequality, Lemmas 2.6 and 3.1

\[ \left| \sum_{r \in R \cap \mathcal{R}} \tilde{a}(r) \tilde{a}(-r) \tilde{a}(r) \left( 1 - \tilde{\beta}(r)^2 \tilde{\beta}(-r)^2 \tilde{b}(r)^2 \right) \right| \]

\[ \leq 2 \sup_{r \in R \cap \mathcal{R}} |\tilde{a}(r)| \tilde{a}(r) \left( \sum_{r \in R \cap \mathcal{R}} |\tilde{a}(r)|^2 \right)^{\frac{\rho}{p+1}} \left( \sum_{r \in R \cap \mathcal{R}} |\tilde{a}(r)|^\rho \right)^{\frac{1}{p+1}} \]

\[ \leq 2C'(2 + 1/\rho)^{p+1} C(\rho)^{\frac{1}{p+1}} K^{\frac{1}{p+1}} \eta^{\frac{1}{p+1}}. \]

\( \Box \)

Lemma 3.3. If \(|R| \geq 2 \log \log w/w\), then \(|a'(x)| \leq 2/N\) for any \( x \in \mathbb{Z}_N \).

Proof. See [5] Lemma 6.3. \( \Box \)

Let

\( A' = \{ x \in \mathbb{Z}_N : a'(x) \geq \kappa/N \}, \quad \mathfrak{A} = \{ x \in \mathbb{Z}_N : a'(x) \geq \kappa/N \}. \)

Then by the proof of Lemma 2.8 we have \(|\mathfrak{A}| \geq (1 - 3\kappa)N\). By Lemma 3.3 we have

\[ \frac{2}{N}|A'| + \frac{\kappa}{N}(N - |A'|) \geq \sum_{x \in \mathbb{Z}_N} a'(x) = \sum_{x \in \mathbb{Z}_N} a(x) \geq \frac{1}{3mK}. \]
\[ |A'| \geq \frac{N}{2} \left( \sum_{x \in \mathbb{Z}_N} a'(x) - \frac{\kappa}{N} \cdot N \right) = \frac{N}{2} \left( \sum_{x \in \mathbb{Z}_N} a(x) - \frac{\kappa}{N} \cdot N \right) \geq 2\kappa N. \]

Hence by Lemma 3.3 of [8],

\[ \sum_{1 \leq x, y, z \leq N} a'(x)a'(y)a'(z) \geq \sum_{x, y \in A', z \in A} a'(x)a'(y)a'(z) \geq \frac{\kappa^3}{N^3} \nu_{A', A', -A}(0) \geq \frac{\kappa^6}{N}. \]

We may choose sufficiently small \( \eta \) and \( \epsilon \) such that

\[ \epsilon C(k \eta^{-k^{2k+3}}) \geq \frac{1}{\kappa} C(T) K \eta^{-k^{2k+3}}, \]

\[ \epsilon C' \left( k \eta^{-k^{2k+3}} \right) \geq 2 \log \log w / w \]

and

\[ C_3 K \frac{1}{\rho+1} \left( \epsilon^2 \eta^{-k^{2k+3}} + \frac{1}{\eta^{k^{2k+3}+1}} \right) \leq \frac{\kappa^6}{2}. \]

So by Lemma 3.2, we have

\[ \phi(KW)^2 \left( \log(KWN + \psi(b)) \right)^2 \sum_{x, y \in A, 1 \leq z \leq N} a(z) \]

\[ \geq \sum_{x, y \in \mathbb{Z}_N, x \neq y, x + y = z} a'(x)a'(y)a'(z) - C_3 K \frac{1}{\rho+1} \left( \epsilon^2 \eta^{-k^{2k+3}} + \frac{1}{\eta^{k^{2k+3}+1}} \right) N^{-1} \]

\[ - \frac{\phi(KW)^2 \left( \log(KWN + \psi(b)) \right)^2}{K^2 W^2 N^2} \sum_{1 \leq z \leq N} a(z) \]

\[ \geq \frac{\kappa^6 N^{-1}}{3} - C_3 K \frac{1}{\rho+1} \left( \epsilon^2 \eta^{-k^{2k+3}} + \frac{1}{\eta^{k^{2k+3}+1}} \right) N^{-1} - N^{-\frac{3}{2}} \]

\[ \geq \frac{\kappa^6}{3N}. \]

\[ \square \]

**Acknowledgment.** The second author thanks Professor Zhi-Wei Sun for informing the result of Khalfalah and Szemerédi.

**References**

[1] J. Bourgain, On \( \Lambda(p) \)-subsets of squares, Israel J. Math., 67(1989), 291-311.

[2] J. Bourgain, Fourier transform restriction phenomena for certain lattice subsets and applications to nonlinear evolution equations. I. Schrödinger equations, Geom. Funct. Anal., 3(1993), 107-156.

[3] P. Erdős and A. Sárközy, On differences and sums of integers II, Bull. Greek Math. Society, 18(1977), 204-223.

[4] H. Furstenberg, Ergodic behavior of diagonal measures and a theorem of Szemerédi on arithmetical progressions, J. d’Analyse Math., 31(1977), 204-256.

[5] B. Green, Roth’s theorem in the primes, Ann. Math. (2), 161(2005), 1609-1636.

[6] B. Green and T. Tao, The primes contain arbitrarily long arithmetic progressions, Ann. Math., to appear.

[7] A. Khalfalah and E. Szemerédi, On the Number of Monochromatic Solutions of \( x + y = z^2 \), Combinatorics, Probability and Computing, 15(2006), 213-227.
[8] H.-Z. Li and H. Pan, *Ternary Goldbach problem for the subsets of primes with positive relative densities*, preprint.

[9] H.-Z. Li and H. Pan, *Difference sets and polynomials of prime variables*, preprint.

[10] A. Sárközy, *On difference sets of sequences on integers I*, Acta Math. Acad. Sci. Hungar., 31 (1978), 125-149.

[11] A. Sárközy, *On difference sets of sequences on integers III*, Acta Math. Acad. Sci. Hungar., 31 (1978), 355-386.

[12] T. Tao, *The Roth-Bourgain Theorem*, preprint, unpublished.

E-mail address: lihz@sjtu.edu.cn

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

Department of Mathematics, Shanghai Jiaotong University, Shanghai 200240, People’s Republic of China