

A NOTE ON A RESULT OF RUZSA, II

MIN TANG

(Received 21 February 2010)

Abstract

Let $\sigma_A(n) = |\{(a, a') \in A^2 : a + a' = n\}|$, where $n \in \mathbb{N}$ and A is a subset of \mathbb{N} . Erdős and Turán conjectured that for any basis A of \mathbb{N} , $\sigma_A(n)$ is unbounded. In 1990, Ruzsa constructed a basis $A \subset \mathbb{N}$ for which $\sigma_A(n)$ is bounded in square mean. Based on Ruzsa's method, we proved that there exists a basis A of \mathbb{N} satisfying $\sum_{n \leq N} \sigma_A^2(n) \leq 1\,449\,757\,928N$ for large enough N . In this paper, we give a quantitative result for the existence of N , that is, we show that there exists a basis A of \mathbb{N} satisfying $\sum_{n \leq N} \sigma_A^2(n) \leq 1\,069\,693\,154N$ for $N \geq 7.628\,517\,798 \times 10^{27}$, which improves earlier results of the author ['A note on a result of Ruzsa', *Bull. Aust. Math. Soc.* **77** (2008), 91–98].

2000 *Mathematics subject classification*: primary 11B13.

Keywords and phrases: Erdős–Turán conjecture, basis.

1. Introduction

For $A, B \subseteq \mathbb{Z}$ and $n \in \mathbb{Z}$, let

$$\begin{aligned}\sigma_{A,B}(n) &= |\{(a, b) \in A \times B : a + b = n\}|, \\ \delta_{A,B}(n) &= |\{(a, b) \in A \times B : a - b = n\}|.\end{aligned}$$

Let $\sigma_A(n) = \sigma_{A,A}(n)$ and $\delta_A(n) = \delta_{A,A}(n)$. A subset A of \mathbb{N} is called a basis of \mathbb{N} if $\sigma_A(n) \geq 1$ for $n \geq n_0$. In 1941, Erdős and Turán [3] formulated the following attractive conjecture.

CONJECTURE (Erdős–Turán). If $A \subset \mathbb{N}$ is a basis of \mathbb{N} , then $\sigma_A(n)$ cannot be bounded:

$$\limsup_{n \rightarrow +\infty} \sigma_A(n) = +\infty.$$

This harmless-looking conjecture seems to be extremely difficult. In 1954, using probabilistic methods, Erdős [2] proved the existence of a basis of \mathbb{N} for which $\sigma(n)$ satisfies $c_1 \log n < \sigma(n) < c_2 \log n$ for all n with certain positive constants c_1, c_2 . In 1990, Ruzsa [5] constructed a basis A of \mathbb{N} for which $\sigma_A(n)$ is bounded in mean

The author was supported by the National Natural Science Foundation of China, Grant No. 10901002.

© 2010 Australian Mathematical Publishing Association Inc. 0004-9727/2010 \$16.00

square, that is, he constructed a basis A satisfying $\sum_{n \leq N} \sigma_A^2(n) = O(N)$. Based on Ruzsa's method, Tang [6] proved that there exists a basis A of \mathbb{N} satisfying $\sum_{n \leq N} \sigma_A^2(n) \leq 1\,449\,757\,928N$ for large enough N .

In this paper, improving Ruzsa's method and employing a result concerning the function $\pi(x)$ of Panaitopol, we give a quantitative result for the existence of N and obtain a stronger version of the above result.

THEOREM 1.1. *There exists a set A of nonnegative integers that forms a basis of \mathbb{N} , and satisfies $\sum_{n \leq N} \sigma_A^2(n) \leq 1\,069\,693\,154N$ for $N \geq 7.628\,517\,798 \times 10^{27}$.*

Throughout this paper, let p be an odd prime, \mathbb{Z}_p be the set of residue classes mod p and $G = \mathbb{Z}_p^2$. For $A, B \subseteq G$, let $A - B = \{a - b : a \in A, b \in B\}$. Denote $Q_k = \{(u, ku^2) : u \in \mathbb{Z}_p\} \subset G$ and for a finite set A , let

$$D(A) = \sum_{-\infty}^{+\infty} \sigma_A^2(n) = |\{(a, b, c, d) \in A^4 : a + b = c + d\}|.$$

φ is a mapping

$$\varphi : G \rightarrow \mathbb{Z}, \quad \varphi(a, b) = a + 2pb,$$

where we identify the residues mod p with the integers $0 \leq j \leq p - 1$.

2. Proofs

LEMMA 2.1. *For any real number $x \geq 1342$, there exists at least one prime in the interval $(x, 1.0147x]$.*

PROOF. By direct calculation we know that Lemma 2.1 is true for $1342 \leq x \leq 1\,341\,755\,571\,000$.

We now assume that $x > 1\,341\,755\,571\,000$. We employ a result concerning the function $\pi(x)$ of Panaitopol [4]. That is,

$$\pi(x) < \frac{x}{\log x - 1 - (\log x)^{-0.5}} \quad \forall x \geq 6.$$

and

$$\pi(x) > \frac{x}{\log x - 1 + (\log x)^{-0.5}} \quad \forall x \geq 59.$$

Thus it suffices to prove that for $x > 1\,341\,755\,571\,000$,

$$\begin{aligned} & \pi(1.0147x) - \pi(x) \\ & > \frac{1.0147x}{\log(1.0147x) - 1 + (\log(1.0147x))^{-0.5}} - \frac{x}{\log x - 1 - (\log x)^{-0.5}} \\ & \geq 0. \end{aligned}$$

This is equivalent to showing that

$$147 \log x \geq 147 + 10^4 \log 1.0147 + 10147(\log x)^{-0.5} + 10^4(\log x + \log 1.0147)^{-0.5}.$$

It is easy to verify that the inequality is true for $x = 1\,341\,755\,571\,000$. Hence the inequality is true for $x > 1\,341\,755\,571\,000$.

This completes the proof of Lemma 2.1. □

LEMMA 2.2 [6, Lemma 2]. *For $g = (a, b) \in G$, and fixed $k, l \in \mathbb{Z}_p \setminus \{0\}$, consider the equation*

$$g = x - y, \quad x \in Q_k, y \in Q_l.$$

If $k - l \neq 0$, this equation is solvable unless

$$\left(\frac{(k - l)b + kla^2}{p} \right) = -1,$$

and it has at most two solutions. If $k - l = 0$, it has at most one solution except for $g = 0$, when it has p solutions.

LEMMA 2.3. *Let $p (\geq 11)$ be prime and m be a quadratic nonresidue of p with $m + 1 \not\equiv 0 \pmod p$, $3m + 1 \not\equiv 0 \pmod p$ and $m + 3 \not\equiv 0 \pmod p$. Put $B = Q_{m+1} \cup Q_{m(m+1)} \cup Q_{2m}$. Then $1 \leq \sigma_B(g) \leq 16$ for all $g \in G$ and $1 \leq \delta_B(g) \leq 11$ for all $g \neq 0$.*

PROOF. The statement that $1 \leq \sigma_B(g) \leq 16$ for all $g \in G$ is obtained by Yong-Gao Chen in [1, Lemma 2]. We now show that $1 \leq \delta_B(g) \leq 11$ for all $g \neq 0$.

Suppose that there is a $g = (a, b) \in G$, $g \notin Q_{2m} - Q_{m+1}$, $g \notin Q_{m(m+1)} - Q_{2m}$. Note that m is a quadratic nonresidue of p , hence $m - 1 \not\equiv 0 \pmod p$ and, by Lemma 2.2,

$$\left(\frac{(m - 1)b + 2m(m + 1)a^2}{p} \right) = -1, \quad \left(\frac{m(m - 1)b + 2m^2(m + 1)a^2}{p} \right) = -1.$$

Thus

$$1 = \left(\frac{(m - 1)b + 2m(m + 1)a^2}{p} \right)^2 \left(\frac{m}{p} \right) = \left(\frac{m}{p} \right) = -1.$$

This contradiction shows that

$$G = (Q_{2m} - Q_{m+1}) \cup (Q_{m(m+1)} - Q_{2m}),$$

which is stronger than the required $B - B = G$.

Let

$$T = \{m + 1, m(m + 1), 2m\}.$$

If $g = (a, b) \in G$ ($g \neq 0$), then $(m - 1)b$ cannot equal both $2m(m + 1)a^2$ and $-2m(m + 1)a^2$. Now we consider the following three cases.

Case 1. $(m - 1)b \neq 2m(m + 1)a^2$ and $(m - 1)b \neq -2m(m + 1)a^2$. Then we have $g \notin (Q_{m+1} - Q_{2m}) \cap (Q_{2m} - Q_{m(m+1)})$ and $g \notin (Q_{2m} - Q_{m+1}) \cap (Q_{m(m+1)} - Q_{2m})$.

Indeed, if $g \in (Q_{m+1} - Q_{2m}) \cap (Q_{2m} - Q_{m(m+1)})$, by $(m - 1)b \neq 2m(m + 1)a^2$ we have

$$\left(\frac{(-m + 1)b + 2m(m + 1)a^2}{p}\right) = 1, \quad \left(\frac{(-m^2 + m)b + 2m^2(m + 1)a^2}{p}\right) = 1.$$

Thus

$$1 = \left(\frac{(-m + 1)b + 2m(m + 1)a^2}{p}\right)^2 \left(\frac{m}{p}\right) = \left(\frac{m}{p}\right) = -1.$$

Similarly, by $(m - 1)b \neq -2m(m + 1)a^2$, we can show that

$$g \notin (Q_{2m} - Q_{m+1}) \cap (Q_{m(m+1)} - Q_{2m}).$$

Hence, for $g \neq 0$, by Lemma 2.2,

$$\delta_B(g) \leq \sum_{r,s \in T} \delta_{Q_r, Q_s}(g) = \sum_{\substack{r,s \in T \\ r \neq s}} \delta_{Q_r, Q_s}(g) + \sum_{r \in T} \delta_{Q_r}(g) \leq 2 \times 4 + 1 \times 3 = 11.$$

Case 2. $(m - 1)b = 2m(m + 1)a^2$ and $(m - 1)b \neq -2m(m + 1)a^2$. Then

$$g \notin (Q_{2m} - Q_{m+1}) \cap (Q_{m(m+1)} - Q_{2m}).$$

Moreover, if $g \in Q_{m+1} - Q_{2m}$, then there exists $(u, v) \in \mathbb{Z}_p^2$ such that

$$a = u - v, \quad b = (m + 1)u^2 - 2mv^2. \tag{2.1}$$

Thus

$$b = (-m + 1)v^2 + 2(m + 1)av + (m + 1)a^2.$$

We have $m - 1 \not\equiv 0 \pmod p$ and $(m - 1)b = 2m(m + 1)a^2$, thus

$$((-m + 1)v + (m + 1)a)^2 = 2m(m + 1)a^2 + (-m + 1)b = 0. \tag{2.2}$$

Thus, there is a unique v satisfying (2.2), hence $\delta_{Q_{m+1}, Q_{2m}}(g) = 1$. Similarly, we can show that if $g \in Q_{2m} - Q_{m(m+1)}$, then $\delta_{Q_{2m}, Q_{m(m+1)}}(g) = 1$. Hence, for $g \neq 0$, by Lemma 2.2,

$$\delta_B(g) \leq \sum_{r,s \in T} \delta_{Q_r, Q_s}(g) = \sum_{\substack{r,s \in T \\ r \neq s}} \delta_{Q_r, Q_s}(g) + \sum_{r \in T} \delta_{Q_r}(g) \leq 2 \times 3 + 1 \times 5 = 11.$$

Case 3. $(m - 1)b = -2m(m + 1)a^2$ and $(m - 1)b \neq 2m(m + 1)a^2$. Then

$$g \notin (Q_{m+1} - Q_{2m}) \cap (Q_{2m} - Q_{m(m+1)}).$$

Moreover, if $g \in Q_{2m} - Q_{m+1}$, then $\delta_{Q_{2m}, Q_{m+1}}(g) = 1$; if $g \in Q_{m(m+1)} - Q_{2m}$, then $\delta_{Q_{m(m+1)}, Q_{2m}}(g) = 1$. Hence, for $g \neq 0$, by Lemma 2.2,

$$\delta_B(g) \leq \sum_{r,s \in T} \delta_{Q_r, Q_s}(g) = \sum_{\substack{r,s \in T \\ r \neq s}} \delta_{Q_r, Q_s}(g) + \sum_{r \in T} \delta_{Q_r}(g) \leq 2 \times 3 + 1 \times 5 = 11.$$

This completes the proof of Lemma 2.3. □

REMARK 2.4. Since the number of quadratic nonresidues mod p is $(p - 1)/2 \geq 5$ for $p \geq 11$, there exists a quadratic nonresidue m such that $m + 1 \not\equiv 0 \pmod p$, $3m + 1 \not\equiv 0 \pmod p$ and $m + 3 \not\equiv 0 \pmod p$.

LEMMA 2.5. Let $p (\geq 11)$ be prime and m be a quadratic nonresidue of p with $m + 1 \not\equiv 0 \pmod p$, $3m + 1 \not\equiv 0 \pmod p$ and $m + 3 \not\equiv 0 \pmod p$. Put $B = Q_{m+1} \cup Q_{m(m+1)} \cup Q_{2m}$ and $B' = \varphi(B)$. Then $\sigma_{B'}(n) \leq 16$ for all n and $\delta_{B'}(n) \leq 11$ for all $n \neq 0$. Moreover, for every integer $0 \leq n < 2p^2$, at least one of the six numbers $n - p, n, n + p, n + 2p^2 - p, n + 2p^2, n + 2p^2 + p$ is in $B' + B'$.

PROOF. Let $g, g', h, h' \in B$. It is easy to verify that $\varphi(g) + \varphi(g') = \varphi(h) + \varphi(h')$ is possible only if $g + g' = h + h'$ and that $\varphi(g) - \varphi(g') = \varphi(h) - \varphi(h')$ is possible only if $g - g' = h - h'$. That is, φ cannot increase the values of σ and δ . By Lemma 2.3, we have $\sigma_{B'}(n) \leq 16$ for all n and $\delta_{B'}(n) \leq 11$ for all $n \neq 0$.

Now take an arbitrary $n \in [0, 2p^2)$ and write it in the form

$$n = a + 2pb, \quad 0 \leq a \leq 2p - 1, \quad 0 \leq b \leq p - 1.$$

We can find $(x, y) \in B$ and $(x', y') \in B$ such that

$$a \equiv x + x' \pmod p, \quad b \equiv y + y' \pmod p.$$

We have

$$\begin{aligned} -(2p - 1) &\leq x + x' - a \leq 2(p - 1), \\ -(p - 1) &\leq y + y' - b \leq 2(p - 1), \end{aligned}$$

thus $x + x' - a = -p, 0, p$ and $y + y' - b = 0, p$.

Case 1. $x + x' - a = -p$ and $y + y' - b = 0$. Then

$$n - p = a + 2pb - p = x + 2py + x' + 2py' \in B' + B'.$$

Case 2. $x + x' - a = 0$ and $y + y' - b = 0$. Then

$$n = a + 2pb = x + 2py + x' + 2py' \in B' + B'.$$

Case 3. $x + x' - a = p$ and $y + y' - b = 0$. Then

$$n + p = a + 2pb + p = x + 2py + x' + 2py' \in B' + B'.$$

Case 4. $x + x' - a = -p$ and $y + y' - b = p$. Then

$$n + 2p^2 - p = a + 2pb + 2p^2 - p = x + 2py + x' + 2py' \in B' + B'.$$

Case 5. $x + x' - a = 0$ and $y + y' - b = p$. Then

$$n + 2p^2 = a + 2pb + 2p^2 = x + 2py + x' + 2py' \in B' + B'.$$

Case 6. $x + x' - a = p$ and $y + y' - b = p$. Then

$$n + 2p^2 + p = a + 2pb + 2p^2 + p = x + 2py + x' + 2py' \in B' + B'.$$

This completes the proof of Lemma 2.5. □

LEMMA 2.6. *Let $p(\geq 11)$ be prime and m be a quadratic nonresidue of p with $m + 1 \not\equiv 0 \pmod p$, $3m + 1 \not\equiv 0 \pmod p$ and $m + 3 \not\equiv 0 \pmod p$. Put $B = Q_{m+1} \cup Q_{m(m+1)} \cup Q_{2m}$, $B' = \varphi(B)$ and $V = B' + \{0, 2p^2 - p, 2p^2, 2p^2 + p\}$. Then $V \subset [0, 4p^2)$ is a set with $|V| \leq 12p$ and satisfies $[4p^2, 6p^2) \subseteq V + V$, $\sigma_V(n) \leq 256$ for all n and $\delta_V(n) \leq 176$ for all n with at most 11 exceptions.*

PROOF. Note that $B' \subset [0, 2p^2 - p)$, thus $V \subset [0, 4p^2)$. In addition $|V| \leq 4|B'| = 4|B| \leq 12p$.

Since

$$V + V = B' + B' + \{0, 2p^2 - p, 2p^2, 2p^2 + p, 4p^2 - 2p, 4p^2 - p, 4p^2, 4p^2 + p, 4p^2 + 2p\},$$

by Lemma 2.5, we have $[4p^2, 6p^2) \subseteq V + V$, and V is the union of four translated copies of B' , hence

$$\max \sigma_V(n) \leq 16 \max \sigma_{B'}(n) \leq 16 \times 16 = 256.$$

Since

$$V - V = B' - B' + \{0, \pm(2p^2 - p), \pm 2p^2, \pm(2p^2 + p), \pm p, \pm 2p\},$$

by Lemma 2.5,

$$\delta_V(n) \leq 16 \times \max \delta_{B'}(n) \leq 16 \times 11 = 176,$$

unless $n = 0, \pm(2p^2 - p), \pm 2p^2, \pm(2p^2 + p), \pm p, \pm 2p$.

This completes the proof of Lemma 2.6. □

LEMMA 2.7. *Let X be a finite set of integers and $p(\geq 11)$ be a prime. There is a set Y such that*

$$Y \subset \left(\frac{7p^2}{8}, 5p^2\right), \quad |Y| \leq 12p, \quad \left[6p^2, \frac{31}{4}p^2\right) \subset Y + Y, \quad (2.3)$$

and

$$D(X \cup Y) < D(X) + \frac{96}{p}|X|^3 + 864|X|^2 + 6672p|X| + 73728p^2. \quad (2.4)$$

PROOF. Let V be the set of Lemma 2.6 and put $Y = V + t$ where t is an integer in $(7p^2/8, p^2]$. Equation (2.3) holds for any choice of t ; we show that (2.4) holds for a suitable choice of t .

Let $Z = X \cup Y$. $D(Z)$ is the number of quadruples (z_1, z_2, z_3, z_4) of elements of Z satisfying

$$z_1 + z_2 = z_3 + z_4. \quad (2.5)$$

We split Equation (2.5) into the following five classes.

- (a) All four unknowns are from X . This gives the term $D(X)$.
- (b) One comes from Y , three from X . Equation (2.5) can be written as

$$t = x_1 + x_2 - x_3 - v, \quad v \in V.$$

Let S_t be the number of solutions,

$$\sum_{7p^2/8 < t \leq p^2} S_t \leq 12p|X|^3.$$

Hence

$$(p^2/8) \cdot \min S_t < \min S_t \cdot \sum_{7p^2/8 < t \leq p^2} 1 \leq 12p|X|^3,$$

thus

$$\min S_t \leq \frac{96|X|^3}{p}.$$

(c) Two come from Y , two come from X .

Case 1. The unknowns y_1 and y_2 are on the same side. Equation (2.5) can be written as

$$y_1 + y_2 = x_1 + x_2, \quad y_i \in Y, x_i \in X.$$

By Lemma 2.6, for every pair x_1, x_2 , there are at most 256 solutions which give a total of $256|X|^2$. According to the position of the y s in (2.5), the contribution of this term is at most $2 \times 256|X|^2 = 512|X|^2$.

Case 2. The unknowns y_1 and y_2 are on different sides, that is,

$$y_1 - y_2 = x_1 - x_2, \quad y_i \in Y, x_i \in X.$$

By Lemma 2.6, if $x_1 - x_2$ is none of the 11 exceptional numbers, then the contribution of this term is at most $2 \times 176|X|^2 = 352|X|^2$; if $x_1 - x_2$ is one of the 11 exceptional numbers, then after fixing the value of $x_1 - x_2$, the numbers x_1 and y_1 determine x_2 and y_2 uniquely, thus the contribution of this term is at most $4 \times 11 \times |X| \times |Y| \leq 528p|X|$.

(d) Three come from Y , one comes from X . Equation (2.5) can be written as

$$y_1 + y_2 = y_3 + x, \quad y_i \in Y, x \in X.$$

In this case, the contribution of this term is at most $2 \times 256 \times |X| \times 12p = 6144p|X|$.

(e) Four unknowns are from Y . The contribution of this term is at most $2 \times 256 \times (12p)^2 = 73728p^2$.

Hence

$$D(X \cup Y) < D(X) + \frac{96}{p}|X|^3 + 864|X|^2 + 6672p|X| + 73728p^2.$$

This completes the proof of Lemma 2.7. □

PROOF OF THEOREM 1.1. By Lemma 2.1, for $x \geq 1342$, there is a prime p for which $x < p < 1.0147x$. Thus we can take a sequence p_1, p_2, \dots of primes such that $p_1 = 1361$ and $1.12p_i < p_{i+1} \leq 1.0147 \times 1.12p_i < \sqrt{\frac{31}{24}}p_i$ for all i , that is, $1.12 < p_{i+1}/p_i < \sqrt{\frac{31}{24}}$ for all i . This ensures that the intervals $[6p_i^2, \frac{31}{4}p_i^2)$ overlap and

together cover $[6p_1^2, +\infty)$. Applying Lemma 2.7 to $p = p_i$, we get the set Y_i . Let $X_0 = [0, 6p_1^2]$ and $X_i = X_{i-1} \cup Y_i$. Then $A = \bigcup_{i=0}^{\infty} X_i$ will be a basis of \mathbb{N} .

For $N \geq 7.628\,517\,798 \times 10^{27} > \frac{1}{2}(6p_1^2 + 1)^4$, there exists an $i > 1$ such that $p_i^2 < 2N < p_{i+1}^2$, so

$$\begin{aligned} |X_{i-1}| &\leq |X_0| + 12(p_1 + p_2 + \cdots + p_{i-1}) \\ &= |X_0| + 12p_i \left(\frac{25}{28} + \cdots + \left(\frac{25}{28} \right)^{i-1} \right) \\ &< 101p_i. \end{aligned}$$

By Lemma 2.7,

$$\begin{aligned} D(X_i) &= D(X_{i-1} \cup Y_i) \\ &< D(X_{i-1}) + \frac{96}{p_i} |X_{i-1}|^3 + 864 |X_{i-1}|^2 + 6672 p_i |X_{i-1}| + 73\,728 p_i^2 \\ &< D(X_{i-1}) + 108\,470\,160 p_i^2. \end{aligned}$$

By induction,

$$\begin{aligned} D(X_i) &< D(X_0) + 108\,470\,160(p_1^2 + \cdots + p_i^2) \\ &= D(X_0) + 108\,470\,160 p_i^2 \left(1 + \left(\frac{25}{28} \right)^2 + \cdots + \left(\frac{25}{28} \right)^{2i-2} \right) \\ &< (6p_1^2 + 1)^4 + 534\,846\,576 p_i^2 \\ &< 534\,846\,577 p_i^2. \end{aligned}$$

Therefore,

$$\sum_{n \leq N} \sigma_A^2(n) \leq D(X_i) < 534\,846\,577 p_i^2 \leq 1\,069\,693\,154 N.$$

This concludes the proof. \square

References

- [1] Y. G. Chen, 'The analogue of Erdős–Turán conjecture in \mathbb{Z}_m ', *J. Number Theory* **128** (2008), 2573–2581.
- [2] P. Erdős, 'On a problem of Sidon in additive number theory', *Acta Sci. Math. (Szeged)* **15** (1954), 255–259.
- [3] P. Erdős and P. Turán, 'On a problem of Sidon in additive number theory, and on some related problems', *J. Lond. Math. Soc.* **16** (1941), 212–215.
- [4] L. Panaitopol, 'Inequalities concerning the function $\pi(x)$: applications', *Acta Arith.* **94**(4) (2000), 373–381.
- [5] I. Z. Ruzsa, 'A just basis', *Monatsh. Math.* **109** (1990), 145–151.
- [6] M. Tang, 'A note on a result of Ruzsa', *Bull. Aust. Math. Soc.* **77** (2008), 91–98.

MIN TANG, Department of Mathematics, Anhui Normal University,
Wuhu 241000, PR China
e-mail: tmzzz2000@163.com