Bull. Austral. Math. Soc. **77** (2008), 91–98
doi: 10.1017/S0004972708000075

A NOTE ON A RESULT OF RUZSA

MIN TANG

(Received 3 May 2007)

Abstract

Let $\sigma_A(n) = |\{(a, a') \in A^2 : a + a' = n\}|$, where $n \in \mathbb{N}$ and A is a subset of $\mathbb{N}$. Erdös 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 the square mean. In this paper, based on Ruzsa's method, we show that there exists a basis A of $\mathbb{N}$ satisfying $\sum_{n\le N} \sigma_A(n)^2 \le 1\,449\,757\,928N$ for large enough N.

2000 *Mathematics subject classification*: 11B13.
Keywords and phrases: Erdös–Turán conjecture, basis.

1. Introduction

For a set A of integers and $n \in \mathbb{Z}$ write

$$\sigma(n) = \sigma_A(n) = |\{(a, a') \in A^2 : a + a' = n\}|,$$
$$\delta(n) = \delta_A(n) = |\{(a, a') \in A^2 : a - a' = n\}|.$$

A subset A of $\mathbb{N}$ is called a basis of $\mathbb{N}$ if $\sigma_A(n) \ge 1$ for $n \ge n_0$. In 1941, Erdös and Turán [2] formulated the following attractive conjecture.

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

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

This harmless looking conjecture proved to be extremely difficult. In 1954, using probabilistic methods, Erdös [1] proved the existence of a basis of $\mathbb{N}$ for which $\sigma(n)$ satisfies

$$c_1 \log n < \sigma(n) < c_2 \log n, \tag{1}$$

The author was supported by the Youth Foundation of Mathematical Tianyuan, Grant No. 10726074, the SF of the Education Department of Anhui Province, Grant No. KJ2007B029 and the Youth Foundation of the Education Department of Anhui Province, Grant No. 2007jq1056zd.

for all n with certain positive constants c_1, c_2. It is still a challenging problem to give a constructive proof of (1). In 1990, Ruzsa [6] constructed a basis of $\mathbb{N}$ for which $\sigma(n)$ is bounded in the square mean. In 2003, Grekos *et al.* [3] proved that if A is a basis of $\mathbb{N}$, then $\max_{n\in\mathbb{N}} \sigma_A(n) \geq 6$. In 2005, Borwein *et al.* [5] improved this result. They showed that the maximum number of representations of any basis is at least eight. For other related problems, see [4, 7, 8].

Based on Ruzsa's method, we obtain the following result.

THEOREM. *There exists a set A of non-negative integers that forms a basis of $\mathbb{N}$, and satisfies $\sum_{n\leq N} \sigma_A(n)^2 \leq 1\,449\,757\,928N$ for large enough N.*

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

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

φ is a mapping

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

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

2. Proofs

LEMMA 1 (Tang and Chen [7, Lemma 4]). *Let p be prime for which $p > 5$ and $p \equiv 5 \bmod 8$. Put $B = Q_3 \cup Q_4 \cup Q_6$ and $V = \varphi(B) + \{0, 2p^2 - p, 2p^2, 2p^2 + p\}$. Then $V \subset [0, 4p^2)$ is a set with $|V| \leq 12p$ and $[4p^2, 6p^2) \subseteq V + V$, $\sigma_V(n) \leq 256$ for all n.*

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.

PROOF. Let $g = (a, b)$. Consider the system of equations

$$a = u - v, \tag{2}$$
$$b = ku^2 - lv^2. \tag{3}$$

https://doi.org/10.1017/S0004972708000075 Published online by Cambridge University Press

Substituting the value of u from (2) into (3), we obtain the equation

$$b = (k-l)v^2 + 2kav + ka^2. \tag{4}$$

CASE 1. $k - l \neq 0$. Then we have

$$((k-l)v + ka)^2 = kla^2 + (k-l)b.$$

This is an equation of degree two; it is solvable unless the right-hand side is a quadratic non-residue mod p, that is,

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

and it has at most two solutions.

CASE 2. $k - l = 0$. Then (4) is an equation of degree one. If $a \neq 0$, (4) has one solution. If $a = b = 0$, (4) has p solutions. If $a = 0$, $b \neq 0$, (4) has no solution.

This completes the proof of Lemma 2. □

LEMMA 3. *Let p be prime for which $p > 5$ and $p \equiv 5 \bmod 8$. Put $B = Q_3 \cup Q_4 \cup Q_6$ and let $B - B = \{b_1 - b_2 : b_1, b_2 \in B\}$. Then $B - B = G$, $\delta_B(g) \leq 11$ for all $g \neq 0$.*

PROOF. Suppose that there exists a $g = (a, b) \in G$, $g \notin Q_4 - Q_3$, $g \notin Q_6 - Q_4$. By Lemma 2, we have

$$\left(\frac{b + 12a^2}{p}\right) = -1, \quad \left(\frac{2b + 24a^2}{p}\right) = -1.$$

Thus

$$1 = \left(\frac{(b + 12a^2)(2b + 24a^2)}{p}\right) = \left(\frac{2}{p}\right) = -1.$$

Hence, $G = (Q_4 - Q_3) \cup (Q_6 - Q_4)$, which is stronger than the required $B - B = G$.

For any $g = (a, b) \in G$ $(g \neq 0)$, by $p > 5$ we know that $b = 12a^2$ and $b = -12a^2$ cannot hold at the same time. Now we consider the following three cases.

CASE 1. $b \neq 12a^2$ and $b \neq -12a^2$. Then we have $g \notin (Q_3 - Q_4) \cap (Q_4 - Q_6)$ and $g \notin (Q_4 - Q_3) \cap (Q_6 - Q_4)$.

Indeed, if $g \in Q_3 - Q_4$ and $g \in Q_4 - Q_6$, by $b \neq 12a^2$, we have

$$\left(\frac{-b + 12a^2}{p}\right) = 1, \quad \left(\frac{-2b + 24a^2}{p}\right) = 1.$$

Thus

$$1 = \left(\frac{(-b + 12a^2)(-2b + 24a^2)}{p}\right) = \left(\frac{2}{p}\right) = -1.$$

Similarly, by $b \neq -12a^2$, we can show that $g \notin (Q_4 - Q_3) \cap (Q_6 - Q_4)$.

https://doi.org/10.1017/S0004972708000075 Published online by Cambridge University Press

CASE 2. $b = 12a^2$ and $b \neq -12a^2$. Then $g \notin (Q_4 - Q_3) \cap (Q_6 - Q_4)$ and $g \notin Q_3 - Q_6$.

Indeed, if $g \in Q_4 - Q_3$ and $g \in Q_6 - Q_4$, then

$$\left(\frac{24a^2}{p}\right) = \left(\frac{b + 12a^2}{p}\right) = 1, \quad \left(\frac{48a^2}{p}\right) = \left(\frac{2b + 24a^2}{p}\right) = 1.$$

By $p \equiv 5 \bmod 8$,

$$1 = \left(\frac{24a^2 \times 48a^2}{p}\right) = \left(\frac{2}{p}\right) = -1.$$

Thus, $g \notin (Q_4 - Q_3) \cap (Q_6 - Q_4)$.

Further, since

$$\left(\frac{-3b + 18a^2}{p}\right) = \left(\frac{-18a^2}{p}\right) = \left(\frac{-2}{p}\right) = -1,$$

by Lemma 2, we have $g \notin Q_3 - Q_6$.

CASE 3. $b = -12a^2$ and $b \neq 12a^2$. Then $g \notin (Q_3 - Q_4) \cap (Q_4 - Q_6)$ and $g \notin Q_6 - Q_3$.

Hence, there are at most four sub-equations for the equation

$$g = x - y, \quad x \in Q_i,\ y \in Q_j\,(i, j \in \{3, 4, 6\}, i \neq j)$$

and three sub-equations for the equation

$$g = x - y, \quad x, y \in Q_i\ (i = 3, 4, 6).$$

By Lemma 2, we have $\delta_B(g) \leq 11$ for all $g \neq 0$.

This completes the proof of Lemma 3. □

LEMMA 4. *Let p be prime for which $p > 5$ and $p \equiv 5 \bmod 8$, $B = Q_3 \cup Q_4 \cup Q_6$ and $B' = \varphi(B)$. Then $\delta_{B'}(n) \leq 11$ for all $n \neq 0$.*

PROOF. Let $g = (a, b)$, $g' = (a', b')$, $h = (c, d)$, $h' = (c', d') \in B$.

If $\varphi(g) - \varphi(g') = \varphi(h) - \varphi(h')$, then

$$2p|(b + d' - b' - d)| = |c + a' - c' - a|;$$

thus, $b - b' = d - d'$, $a - a' = c - c'$.

Hence, $\varphi(g) - \varphi(g') = \varphi(h) - \varphi(h')$ is possible only if $g - g' = h - h'$. This shows that φ cannot increase the value of δ. By Lemma 3, we have $\delta_{B'}(n) \leq 11$ for all $n \neq 0$.

This completes the proof of Lemma 4. □

LEMMA 5. *Let p be prime for which $p > 5$ and $p \equiv 5 \bmod 8$. Put $B = Q_3 \cup Q_4 \cup Q_6$ and $V = \varphi(B) + \{0, 2p^2 - p, 2p^2, 2p^2 + p\}$. Then $V \subset [0, 4p^2)$ is a set with $|V| \le 12p$ and $\delta_V(n) \le 176$ for all n with at most 11 exceptions.*

PROOF. By the Proof of [7, Lemma 4], we have $V \subset [0, 4p^2)$ and $|V| \le 12p$. Note that

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

By Lemma 4,

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

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

This completes the proof of Lemma 5. □

The following Lemma 6 belongs to Ruzsa [6, Lemma 4.1]; here we give a stronger version by explicit computation.

LEMMA 6. *Let X be a finite set of integers and p be a prime for which $p > 5$ and $p \equiv 5 \bmod 8$. There is a set Y such that*

$$Y \subset \left(\frac{p^2}{2}, 5p^2\right), \quad |Y| \le 12p, \quad [6p^2, 7p^2) \subset Y + Y, \tag{5}$$

and

$$D(X \cup Y) < D(X) + \frac{24}{p}|X|^3 + 928|X|^2 + 6672p|X| + 73\,728p^2. \tag{6}$$

PROOF. Let V be the set of Lemma 5, and put $Y = V + t$ with an integer $t \in ((p^2/2), p^2]$. Equation (5) holds for any choice of t; we show that (6) holds for a suitable choice.

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

$$z_1 + z_2 = z_3 + z_4. \tag{7}$$

We split equation (7) 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 (7) can be written as

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

Let S_t be the number of solutions; so we have

$$\sum S_t \le 12p|X|^3,$$

https://doi.org/10.1017/S0004972708000075 Published online by Cambridge University Press

thus

$$\left(\left[\frac{p^2}{2}\right]+1\right)\min S_t \le 12p|X|^3,$$

and hence

$$\min S_t \le \frac{24|X|^3}{p}.$$

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

CASE 1. The two y are on the same side. Equation (7) can be written as

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

By Lemma 1, 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 (7), the contribution of this term is at most $2 \times 256|X|^2 = 512|X|^2$.

CASE 2. The y 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 5, 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 $4 \times 11 \times |X| \times |Y| \le 528p|X|$.

(d) Three come from Y, one comes from X. Equation (7) 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 $2 \times 256 \times (12p)^2 = 73\,728p^2$.

Hence

$$D(X \cup Y) < D(X) + \frac{24}{p}|X|^3 + 864|X|^2 + 6672p|X| + 73\,728p^2.$$

This completes the proof of Lemma 6. □

PROOF OF THEOREM. By the Prime number theorem in arithmetic progression, there exists an M such that if $x > M$, there is a prime p for which $1.08x < p < \sqrt{7/6}x$. Thus we can take a sequence $p_1, p_2, \ldots$ of primes such that $p \equiv 5 \bmod 8$

and $1.08 < p_{i+1}/p_i < \sqrt{7/6}$ for all i. This ensures that the intervals $[6p_i^2, 7p_i^2)$ overlap and together cover $[6p_1^2, +\infty)$. Apply Lemma 6 to $p = p_i$, we obtain the set Y_i. Let $X_0 = [0, 6p_1^2]$ and $X_i = X_{i-1} \cup Y_i$. Then the set $A = \bigcup_{i=0}^{\infty} X_i$ will be a basis of $\mathbb{N}$.

For large enough N $(> (7/12)(6{p_1}^2 + 1)^4)$, there exists $i > 1$ such that $p_i^2 < 2N < p_{i+1}^2$, so

$$\begin{aligned} |X_{i-1}| &\le |X_0| + 12(p_1 + p_2 + \cdots + p_{i-1}) \\ &= |X_0| + 12p_i\left(\frac{25}{27} + \cdots + \left(\frac{25}{27}\right)^{i-1}\right) \\ &< 151p_i. \end{aligned}$$

By Lemma 6,

$$\begin{aligned} D(X_i) &= D(X_{i-1} \cup Y_i) \\ &< D(X_{i-1}) + \frac{24}{p_i}|X_{i-1}|^3 + 864|X_{i-1}|^2 + 6672p_i|X_{i-1}| + 73\,728p_i^2 \\ &< D(X_{i-1}) + 103\,412\,088{p_i}^2. \end{aligned}$$

By induction,

$$\begin{aligned} D(X_i) &< D(X_0) + 103\,412\,088(p_i^2 + \cdots + p_1^2) \\ &= D(X_0) + 103\,412\,088p_i^2\left(1 + \left(\frac{25}{27}\right)^2 + \cdots + \left(\frac{25}{27}\right)^{2i-2}\right) \\ &< (6p_1^2 + 1)^4 + 724\,878\,963p_i^2 \\ &< 724\,878\,964p_i^2. \end{aligned}$$

Therefore,

$$\sum_{n \le N} \sigma(n)^2 \le D(X_i) < 724\,878\,964p_i^2 \le 1\,449\,757\,928N. \qquad \square$$

References

[1] P. Erdös, 'On a problem of Sidon in additive number theory', *Acta Sci. Math. (Szeged)* **15** (1954), 255–259.

[2] P. Erdös and P. Turán, 'On a problem of Sidon in additive number theory, and on some related problems', *J. London Math. Soc.* **16** (1941), 212–215.

[3] G. Grekos, L. Haddad, C. Helou and J. Pihko, 'On the Erdös–Turán Conjecture', *J. Number Theory* **102** (2003), 339–352.

[4] J. Nešetřil and O. Serra, 'The Erdös–Turán property for a class of bases', *Acta Arith.* **115** (2004), 245–254.

[5] P. Borwein, S. Choi and F. Chu, 'An old conjecture of Erdös–Turán on additive bases', *Math. Comp.* **75** (2005), 475–484.

https://doi.org/10.1017/S0004972708000075 Published online by Cambridge University Press

[6] I. Z. Ruzsa, 'A just basis', *Monatsh. Math.* **109** (1990), 145–151.
[7] M. Tang and Y. G. Chen, 'A basis of $\mathbb{Z}_m$', *Colloq. Math.* **104** (2006), 99–103.
[8] ———, 'A basis of $\mathbb{Z}_m$. II', *Colloq. Math.* **108** (2007), 141–145.

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