ACTA ARITHMETICA
180.2 (2017)

A lower bound of Ruzsa's number related to the Erdős–Turán conjecture

by

Csaba Sándor (Budapest) and Quan-Hui Yang (Nanjing)

1. Introduction. Let $\mathbb{N}$ be all nonnegative integers. For any subsets A, B of $\mathbb{N}$ and $n \in \mathbb{N}$, let

$$R_{A,B}(n) = \sharp\{(a,b) : a \in A,\ b \in B,\ a+b=n\}.$$

Let $R_A(n) = R_{A,A}(n)$. The definitions of $R_{A,B}$ and R_A can be repeated verbatim with $\mathbb{N}$ replaced by any additive semigroup.

In the case of $\mathbb{N}$, if $R_A(n) \geq 1$ for all sufficiently large integers n, then we say that A is a *basis* of $\mathbb{N}$. The celebrated Erdős–Turán conjecture [ET] states that if A is a basis of $\mathbb{N}$, then $R_A(n)$ cannot be bounded. Erdős [E] proved that there exists a basis A and two constants $c_1, c_2 > 0$ such that $c_1 \log n \leq R_A(n) \leq c_2 \log n$ for all sufficiently large integers n. Recently, Dubickas [D] gave the explicit values of c_1 and c_2.

In 2003, Nathanson [N] proved that the Erdős–Turán conjecture does not hold on $\mathbb{Z}$. In fact, he proved that there exists a set $A \subseteq \mathbb{Z}$ such that $1 \leq R_A(n) \leq 2$ for all integers n. In the same year, Grekos et al. [GHHP] proved that if $R_A(n) \geq 1$ for all n, then $\limsup_{n\to\infty} R_A(n) \geq 6$. Later, Borwein et al. [BCC] improved 6 to 8. In 2013, Konstantoulas [K] proved that if the upper density $\overline{d}(\mathbb{N}\setminus(A+A))$ of the set of numbers not representable as sums of two numbers of A is less than $1/10$, then $R_A(n) > 5$ for infinitely many natural numbers n. Chen [C12] proved that there exists a basis A of $\mathbb{N}$ such that the set of n with $R_A(n) = 2$ has density 1. Later, the second author [Y] and Tang [T] generalized that result. For the analogue of the Erdős–Turán conjecture in groups, one can refer to [CS], [HH04], [HH08] and [KL].

For a positive integer m, let $\mathbb{Z}_m$ be the set of residue classes mod m. If $R_A(n) \geq 1$ for all $n \in \mathbb{Z}_m$, then A is called an *additive basis* of $\mathbb{Z}_m$.

2010 *Mathematics Subject Classification*: Primary 11B34; Secondary 11B13.
Key words and phrases: representation function, Ruzsa's number, Erdős–Turán conjecture.
Received 27 December 2016; revised 21 February 2017.
Published online 30 August 2017.

In 1990, Ruzsa [R] found a basis A of $\mathbb{N}$ for which $R_A(n)$ is bounded in the square mean. Ruzsa's method implies that there exists a constant C such that for any positive integer m, there exists an additive basis A of $\mathbb{Z}_m$ with $R_A(n) \le C$ for all $n \in \mathbb{Z}_m$. For each positive integer m, Chen [C08] defined Ruzsa's number R_m to be the least positive integer r such that there exists an additive basis A of $\mathbb{Z}_m$ with $R_A(n) \le r$ for all $n \in \mathbb{Z}_m$. In that paper, Chen also proved that $R_m \le 288$ for all positive integers m and $R_{2p^2} \le 48$ for all prime numbers p. Until now, this is the best upper bound for Ruzsa's number and there is no nontrivial lower bound. In fact, in the same paper, Chen says "We have $R_m \ge 3$ for $m \ne 1, 2, 3$. Now we cannot improve this trivial lower bound".

In this paper, we give a nontrivial lower bound of Ruzsa's number.

Theorem 1.1. *$R_m = 2$ if and only if $m = 2, 3$; and $R_m = 3$ if and only if $m = 4, 5, 7$.*

Remark 1.1. If $m > 1$ and $A \subseteq \mathbb{Z}_m$ is an additive basis, then $|A| \ge 2$. It follows that there exist distinct $a, a' \in A$, and so $R_A(a + a') \ge 2$. Hence $R_m = 1$ if and only if $m = 1$.

Theorem 1.2. *$R_m = 4$ if and only if $m = 6, 8, 9, 10, 11, 12, 13, 14, 15, 19$; and $R_m = 5$ if and only if $m = 16, 17, 18, 20, 21, 22, 23, 24, 25, 27, 28, 35$.*

From Theorems 1.1 and 1.2, we have the following corollary.

Corollary 1.1. *If $m \ge 36$, then $R_m \ge 6$.*

Remark 1.2. Furthermore, if $m \le 35$, then $R_m \le 6$. We list all the values of R_m ($2 \le m \le 35$) and a set $A \subseteq \mathbb{Z}_m$ such that $1 \le R_A(n) \le R_m$ for all $n \in \mathbb{Z}_m$ in the Appendix.

2. Proofs. In order to prove Theorems 1 and 2, we need some lemmas. The first one, due to Lev and Sárközy [LS], is the main tool of our proofs.

Lemma 2.1 (Lev and Sárközy's lower bound). *If A is a subset of a finite nontrivial abelian group G, then for any real number c we have*

$$\sum_{g \in G} (R_A(g) - c)^2 \ge \frac{1}{|G| - 1}\left(\frac{|A|^4}{|G|} - 2|A|^3 + |A|^2|G|\right).$$

Lemma 2.2. *Let $A \subseteq \mathbb{Z}_m$. If $R_A(n) \ge 1$ for all $n \in \mathbb{Z}_m$, then $|A| > \sqrt{2m} - 1/2$.*

Proof. Since $R_A(n) \ge 1$ for all $n \in \mathbb{Z}_m$, we have

$$\begin{aligned}|A|^2 &= \sum_{n=0}^{m-1} R_A(n)\\ &\ge |\{n : n \in \mathbb{Z}_m,\ R_A(n) = 1\}| + 2|\{n : n \in \mathbb{Z}_m,\ R_A(n) \ge 2\}|\\ &= 2|\{n : n \in \mathbb{Z}_m\}| - |\{n : n \in \mathbb{Z}_m,\ R_A(n) = 1\}|\\ &= 2m - |\{n : n \in \mathbb{Z}_m,\ R_A(n) = 1\}| \ge 2m - |A|.\end{aligned}$$

Hence $(|A| + 1/2)^2 > 2m$, that is, $|A| > \sqrt{2m} - 1/2$. ∎

LEMMA 2.3. *Let $A \subseteq \mathbb{Z}_m$ and c be a positive integer. If $R_A(n) \le c$ for all $n \in \mathbb{Z}_m$, then $|A| \le \sqrt{cm}$.*

This lemma follows from $|A|^2 = \sum_{n=0}^{m-1} R_A(n) \le cm$ immediately.

LEMMA 2.4 (see [B, p. 827, Test C]). *Suppose that v, λ, k $(v \ge k \ge \lambda)$ are positive integers. Let p be a prime divisor of $k - \lambda$ and let $w \ge 1$ with $(w, p) = 1$ be a divisor of v for which there exists an integer $f > 0$ such that $p^f \equiv -1 \pmod{w}$. If p^e exactly divides $k - \lambda$ and p^l $(l \ge 0)$ exactly divides v, then there exists a set $A \subseteq \mathbb{Z}_v$ with $|A| = k$ such that the congruence $a - a' \equiv b \pmod{v}$ with $a, a' \in A$ has exactly λ distinct solutions (a, a') for all $b \not\equiv 0 \pmod{v}$ if and only if*

$$p^{\lfloor e/2 \rfloor} < (v/w)p^{-l},$$

where $\lfloor x \rfloor$ denotes the largest integer $\le x$.

LEMMA 2.5. *Let A be an additive basis of $\mathbb{Z}_m$ and k, l be positive integers with $(l, m) = 1$. Then $A + k$ and lA are also additive bases and*

$$\max_{n \in \mathbb{Z}_m} R_A(n) = \max_{n \in \mathbb{Z}_m} R_{A+k}(n) = \max_{n \in \mathbb{Z}_m} R_{lA}(n).$$

This follows from $R_A(n) = R_{A+k}(n + 2k) = R_{lA}(ln)$ for all $n \in \mathbb{Z}_m$ immediately.

Proof of Theorem 1.1. If $m \le 11$, by a computer check we can find that $R_m = 2$ if and only if $m = 2, 3$, and $R_m = 3$ if and only if $m = 4, 5, 7$. Now it suffices to prove that $R_m \le 3$ implies $m \le 11$. Suppose that $m \ge 12$ and there exists a subset $A \subseteq \mathbb{Z}_m$ such that $1 \le R_A(n) \le 3$ for all $n \in \mathbb{Z}_m$.

Setting $G = \mathbb{Z}_m$ and $c = 2$ in Lemma 2.1, we infer that for any subset $A \subseteq \mathbb{Z}_m$,

$$\sum_{n=0}^{m-1} (R_A(n) - 2)^2 \ge \frac{|A|^2(m - |A|)^2}{m(m - 1)}. \tag{2.1}$$

Since $1 \le R_A(n) \le 3$, it follows that

$$(R_A(n)-2)^2 = \begin{cases} 1 & \text{if } R_A(n) \text{ is odd,} \\ 0 & \text{if } R_A(n) \text{ is even.} \end{cases}$$

Furthermore, if $R_A(n)$ is odd, then there exists $a \in A$ such that $n = 2a$, and so

$$\sum_{n=0}^{m-1} (R_A(n)-2)^2 = \sum_{\substack{n=0 \\ 2\nmid R_A(n)}}^{m-1} 1 \le \sum_{a\in A} 1 = |A|. \tag{2.2}$$

By (2.1) and (2.2),

$$|A|(m-|A|)^2 \le m(m-1) < m^2.$$

On the other hand, Lemmas 2.2 and 2.3 yield $\sqrt{2m} - 1/2 < |A| \le \sqrt{3m}$. Hence

$$|A|(m-|A|)^2 > (\sqrt{2m}-1/2)(m-\sqrt{3m})^2 > m^2,$$

because $\sqrt{2m} - 1/2 > 4$ and $\sqrt{3m} \le m/2$ for $m \ge 12$. This is a contradiction. ∎

Proof of Theorem 1.2. We first prove that $R_m \le 5$ implies that $m \le 500$. Suppose that $m > 500$ and there exists $A \subseteq \mathbb{Z}_m$ such that $1 \le R_A(n) \le 5$ for all $n \in \mathbb{Z}_m$. By Lemma 2.1, taking $G = \mathbb{Z}_m$ and $c = 3$, we get

$$\sum_{n=0}^{m-1} (R_A(n)-3)^2 \ge \frac{|A|^2(m-|A|)^2}{m(m-1)}. \tag{2.3}$$

If $R_A(n)$ is odd, then $(R_A(n)-3)^2 \le 4$. If $R_A(n)$ is even, then $(R_A(n)-3)^2 = 1$. Hence

$$\begin{aligned} \sum_{n=0}^{m-1} & (R_A(n)-3)^2 \\ & \le 4|\{n : n \in \mathbb{Z}_m,\ R_A(n) \text{ is odd}\}| + |\{n : n \in \mathbb{Z}_m,\ R_A(n) \text{ is even}\}| \\ & = m + 3|\{n : n \in \mathbb{Z}_m,\ R_A(n) \text{ is odd}\}| \le m + 3|A|. \end{aligned} \tag{2.4}$$

By (2.3) and (2.4),

$$|A|^2(m-|A|)^2 \le (m+3|A|)m(m-1). \tag{2.5}$$

On the other hand, Lemmas 2.2 and 2.3 yield $\sqrt{2m} - 1/2 < |A| \le \sqrt{5m}$. Hence

$$\begin{aligned} |A|^2(m-|A|)^2 &> (\sqrt{2m}-1/2)^2(m-\sqrt{5m})^2 > (1.9\cdot 0.9^2)m^3 \\ &> 1.3m^3 > (m+3\sqrt{5m})m^2 > (m+3|A|)m(m-1), \end{aligned}$$

because $\sqrt{2m} - 1/2 > \sqrt{1.9m}$, $m - \sqrt{5m} > 0.9m$ and $m + 3\sqrt{5m} < 1.3m$ for $m > 500$. This contradicts (2.5). Thus, if $m > 500$, then $R_m \ge 6$.

Now we only need to consider the cases $m \le 500$.

If $m \le 20$, then we can run a computer check over all the sets $A \subseteq \mathbb{Z}_m$ with $\sqrt{2m} - 1/2 \le |A| \le \sqrt{5m}$ and determine the values of R_m. We find that $R_m = 4$ for $m \in \{6, 8, 9, 10, 11, 12, 13, 14, 15, 19\}$ and $R_{16} = R_{17} = R_{18} = R_{20} = 5$.

Next we assume that $21 \le m \le 500$. A routine computer-based calculation shows that the maximal pair of (m, k) satisfying

$$21 \le m \le 500, \qquad \sqrt{2m} - 1/2 \le |A| = k \le \sqrt{5m} \tag{2.6}$$

and (2.5) is $(m, k) = (91, 13)$. This value of (m, k) is too large for a computer check of all sets $A \subseteq \mathbb{Z}_{91}$ with $|A| = 13$.

In the following, we need three steps to reduce these values.

Our task is to find all exact pairs of (m, k) with the following property: There exists $A \subseteq \mathbb{Z}_m$ with $|A| = k$ such that $1 \le R_A(n) \le 5$ for all $n \in \mathbb{Z}_m$. In the first step, for $i \in \{1, 2, 3, 4, 5\}$, let

$$k_i = |\{n : n \in \mathbb{Z}_m,\ R_A(n) = i\}|.$$

Then

$$k_1 + k_2 + k_3 + k_4 + k_5 = k, \qquad k_i \in \mathbb{N}\ (1 \le i \le 5), \tag{2.7}$$

$$k^2 = |A|^2 = \sum_{n=0}^{m-1} R_A(n) = k_1 + 2k_2 + 3k_3 + 4k_4 + 5k_5, \tag{2.8}$$

$$k_1 + k_3 + k_5 \le |A| = k, \qquad \text{with equality when } m \text{ is odd.} \tag{2.9}$$

By Lemma 2.1, taking $c = k^2/m$, we have

$$\begin{aligned} \sum_{n=0}^{m-1} \left(R_A(n) - \frac{k^2}{m} \right)^2 &= \sum_{i=1}^{5} \left(i - \frac{k^2}{m} \right)^2 k_i \\ &\ge \frac{|A|^2 (m - |A|)^2}{m(m-1)} = \frac{k^2 (m-k)^2}{m(m-1)}. \end{aligned} \tag{2.10}$$

By a computer check, the maximal value of (m, k) such that there exist nonnegative integers k_1, k_2, k_3, k_4, k_5 satisfying (2.6)–(2.10) is $(50, 12)$. This value is also too large for a computer check of all subsets $A \subseteq \mathbb{Z}_{50}$ with $|A| = 12$.

In the second reduction step, we shall delete all pairs (m, k) for which $42 \le m \le 50$. Here we need to improve the Lev–Sárközy bound. Clearly,

$$\begin{aligned} \sum_{n=0}^{m-1} \left(R_A(n) - \frac{k^2}{m} \right)^2 &= \sum_{n=0}^{m-1} R_A^2(n) - \frac{2k^2}{m} \sum_{n=0}^{m-1} R_A(n) + \frac{k^4}{m} \\ &= \sum_{n=0}^{m-1} R_A^2(n) - \frac{2k^2}{m} \cdot k^2 + \frac{k^4}{m} = \sum_{n=0}^{m-1} R_A^2(n) - \frac{k^4}{m}. \end{aligned} \tag{2.11}$$

Next we use Lev–Sárközy's arguments to obtain a better lower bound for $\sum_{n=0}^{m-1}(R_A(n)-k^2/m)^2$. Clearly, $\sum_{n=0}^{m-1} R_A^2(n)$ counts the number of solutions of the equation

$$a_1+a_2=a_3+a_4, \qquad a_1,a_2,a_3,a_4\in A.$$

One can rewrite this equation as $a_1-a_3=a_4-a_2$. Hence

$$\sum_{n=0}^{m-1} R_A^2(n)=\sum_{n=0}^{m-1} R_{A,-A}^2(n)=k^2+\sum_{n=1}^{m-1} R_{A,-A}^2(n).$$

Clearly, $\sum_{n=1}^{m-1} R_{A,-A}^2(n)=k^2-k$. Let $k^2-k=q(m-1)+r$, where q,r are nonnegative integers and $0\le r<m-1$. Then

$$q=\left\lfloor\frac{k^2-k}{m-1}\right\rfloor \quad\text{and}\quad r=k^2-k-\left\lfloor\frac{k^2-k}{m-1}\right\rfloor(m-1).$$

Hence

$$\begin{aligned}(2.12)\qquad \sum_{n=0}^{m-1} R_A^2(n)&=k^2+\sum_{n=1}^{m-1} R_{A,-A}^2(n)\\ &\ge k^2+(q+1)^2r+q^2(m-1-r)=k^2+(2q+1)r+q^2(m-1)\\ &=k^2+\left(2\left\lfloor\frac{k^2-k}{m-1}\right\rfloor+1\right)\left(k^2-k-\left\lfloor\frac{k^2-k}{m-1}\right\rfloor(m-1)\right)+\left\lfloor\frac{k^2-k}{m-1}\right\rfloor^2(m-1).\end{aligned}$$

By (2.10)–(2.12), we get the following improvement of (2.10):

$$\begin{aligned}(2.13)\qquad \sum_{i=1}^{5}\left(i-\frac{k^2}{m}\right)^2 k_i\ge k^2+\left\lfloor\frac{k^2-k}{m-1}\right\rfloor^2(m-1)-\frac{k^4}{m}\\ +\left(2\left\lfloor\frac{k^2-k}{m-1}\right\rfloor+1\right)\left(k^2-k-\left\lfloor\frac{k^2-k}{m-1}\right\rfloor(m-1)\right).\end{aligned}$$

A computer check yields all pairs (m,k) such that there exist nonnegative integers k_1,k_2,k_3,k_4,k_5 satisfying (2.6)–(2.9) and (2.13):

$(m,k)\in$
$\{(21,7),\ (21,8),\ (21,9),\ (22,7),\ (22,8),\ (22,9),\ (23,7),\ (23,8),\ (23,9),\ (24,8),\ (24,9),$
$(25,8),\ (25,9),\ (26,8),\ (26,9),\ (27,8),\ (27,9),\ (28,8),\ (28,9),\ (28,10),\ (29,8),\ (29,9),$
$(29,10),(30,9),(30,10),(31,9),(31,10),(32,9),(32,10),(33,9),(33,10),(34,10),(35,10),$
$(36,10),\ (36,11),\ (37,11),\ (38,11),\ (39,11),\ (40,11),\ (41,11),\ (45,12)\}.$

In the last step, we deal with the cases $(m,k)=(40,11),(41,11),(45,12)$, since such values are also too large for computer checks.

We first deal with the largest case $(m,k)=(45,12)$. Take $v=45$, $\lambda=3$, $k=12$, $p=3$, $w=5$, $f=2$, $e=2$, $l=2$. By Lemma 2.4, there is no subset $A\subseteq\mathbb{Z}_{45}$ with $|A|=12$ such that $R_{A,-A}(n)=3$ for all $n\not\equiv 0 \pmod{45}$. In other words, for any set $A \subseteq \mathbb{Z}_{45}$, there exists $n \not\equiv 0 \pmod{45}$ such that $R_{A,-A}(n) \neq 3$. Noting that $\sum_{n=1}^{44} R_{A,-A}(n) = k^2 - k = 132$, we have

$$\sum_{n=1}^{44} R_{A,-A}^2(n) \geq 3^2 \times 42 + 2^2 + 4^2 = 398.$$

Hence, by (2.11) and (2.12),

$$\sum_{n=0}^{44} \left(R_A(n) - \frac{12^2}{45} \right)^2 = 12^2 + \sum_{n=1}^{44} R_{A,-A}^2(n) - \frac{12^4}{45} \geq 81.2.$$

On the other hand, we list all values of $(k_1, k_2, k_3, k_4, k_5)$ when $(m, k) = (45, 12)$:

k_1	k_2	k_3	k_4	k_5	k_1	k_2	k_3	k_4	k_5	k_1	k_2	k_3	k_4	k_5
0	24	0	9	12	5	14	0	19	7	9	6	0	27	3
1	22	0	11	11	6	12	0	21	6	10	4	0	29	2
2	20	0	13	10	7	10	0	23	5	11	2	0	31	1
4	16	0	17	8	8	8	0	25	4	12	0	0	33	0

For all the values listed above, we have

$$\sum_{n=0}^{44} \left(R_A(n) - \frac{12^2}{45} \right)^2 = \sum_{i=1}^{5} \left(i - \frac{12^2}{45} \right)^2 k_i = 79.2.$$

This is a contradiction.

Finally, we deal with the cases $(m, k) = (41, 11)$ and $(40, 11)$, since the number of sets A for which a computer check is possible is about $\binom{39}{9}$. If $m = 41$, then by Lemma 2.5 we can assume that $0, 40 \in A$. Hence the number of such A is $\binom{39}{9}$, and a computer check is possible. Now we consider the case $m = 40$. If there is an element in A coprime to 40, then by Lemma 2.5 we can assume that $0, 39 \in A$, and so a computer check is also possible. If there is no element in A coprime to 40, then we can assume that $0 \in A$ and A is contained in

$$\{0, 2, 4, 5, 6, 8, 10, 12, 14, 15, 16, 18, 20, 22, 24, 25, 26, 28, 30, 32, 34, 35, 36, 38\}.$$

In this case, there are only $\binom{23}{10}$ sets A and we can run a computer check.

Using these ideas, and performing computer checks, we obtain

$$R_m = 4 \quad \text{if and only if} \quad m = 6, 8, 9, 10, 11, 12, 13, 14, 15, 19,$$
$$R_m = 5 \quad \text{if and only if} \quad m = 16, 17, 18, 20, 21, 22, 23, 24, 25, 27, 28, 35. \blacksquare$$

Appendix

m	R_m	A	m	R_m	A
2	2	$\{0,1\}$	19	4	$\{0,1,5,7,8,15,18\}$
3	2	$\{0,1\}$	20	5	$\{0,1,2,5,6,13,16\}$
4	3	$\{0,1,2\}$	21	5	$\{0,1,2,3,4,6,13,16\}$
5	3	$\{0,1,2\}$	22	5	$\{0,1,2,4,5,9,15,17\}$
6	4	$\{0,3,4,5\}$	23	5	$\{0,1,2,3,5,11,14,18\}$
7	3	$\{0,1,2,4\}$	24	5	$\{0,1,2,6,9,10,12,17\}$
8	4	$\{0,3,5,6,7\}$	25	5	$\{0,1,2,4,9,12,20,22\}$
9	4	$\{0,4,6,7,8\}$	26	6	$\{0,1,2,5,15,19,20,22\}$
10	4	$\{0,1,2,3,6\}$	27	5	$\{0,1,2,3,5,11,15,18,23\}$
11	4	$\{0,4,6,8,9\}$	28	5	$\{0,1,2,4,5,8,10,17,22\}$
12	4	$\{0,1,6,8,9,11\}$	29	6	$\{0,1,2,3,4,6,10,17,22\}$
13	4	$\{0,5,7,8,11,12\}$	30	6	$\{0,1,2,3,4,5,7,11,17,22\}$
14	4	$\{0,4,8,9,11,12\}$	31	6	$\{0,1,2,3,4,5,9,13,20,25\}$
15	4	$\{0,6,8,11,12,14\}$	32	6	$\{0,1,2,3,4,5,8,15,20,26\}$
16	5	$\{0,1,2,3,4,7,11\}$	33	6	$\{0,1,2,3,4,6,10,14,21,26\}$
17	5	$\{0,1,2,3,4,7,12\}$	34	6	$\{0,1,2,3,4,6,13,19,26,29\}$
18	5	$\{0,1,2,3,5,8,12\}$	35	5	$\{0,1,4,5,10,12,16,19,26,34\}$

Acknowledgements. The first author was supported by the OTKA Grant No. K109789 and the János Bolyai Research Scholarship of the Hungarian Academy of Sciences. The second author was supported by the National Natural Science Foundation for Youth of China, Grant No. 11501299, the Natural Science Foundation of Jiangsu Province, Grant Nos. BK20150889, 15KJB110014, and the Startup Foundation for Introducing Talent of NUIST, Grant No. 2014r029. We would like to thank the anonymous referee for his/her useful comments.

References

[B] L. D. Baumert, *Difference sets*, SIAM J. Appl. Math. 17 (1969), 826–833.

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

[C08] Y.-G. Chen, *The analogue of Erdős–Turán conjecture in* $\mathbb{Z}_m$, J. Number Theory 128 (2008), 2573–2581.

[C12] Y.-G. Chen, *On the Erdős–Turán conjecture*, C. R. Math. Acad. Sci. Paris 350 (2012), 933–935.

[CS] Y.-G. Chen and T. Sun, *The difference basis and bi-basis of* $\mathbb{Z}_m$, J. Number Theory 130 (2010), 716–726.

[D] A. Dubickas, *A basis of finite and infinite sets with small representation function*, Electron. J. Combin. 19 (2012), no. 1, paper 6, 16 pp.

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

[ET] P. Erdős 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.

[GHHP] G. Grekos, L. Haddad, C. Helou and J. Pihko, *On the Erdős–Turán conjecture*, J. Number Theory 102 (2003), 339–352.

[HH04] L. Haddad and C. Helou, *Bases in some additive groups and the Erdős–Turán conjecture*, J. Combin. Theory Ser. A 108 (2004), 147–153.

[HH08] L. Haddad and C. Helou, *Additive bases representations in groups*, Integers 8 (2008), no. 2, A5, 9 pp.

[K] I. Konstantoulas, *Lower bounds for a conjecture of Erdős and Turán*, Acta Arith. 159 (2013), 301–313.

[KL] S. V. Konyagin and V. F. Lev, *The Erdős–Turán problem in infinite groups*, in: Additive Number Theory, Springer, New York, 2010, 195–202.

[LS] V. F. Lev and A. Sárközy, *An Erdős–Fuchs type theorem for finite groups*, Integers 11 (2011), 487–494.

[N] M. B. Nathanson, *Unique representation bases for integers*, Acta Arith. 108 (2003), 1–8.

[R] I. Z. Ruzsa, *A just basis*, Monatsh. Math. 109 (1990), 145–151.

[T] M. Tang, *On the Erdős–Turán conjecture*, J. Number Theory 150 (2015), 74–80.

[Y] Q.-H. Yang, *A generalization of Chen's theorem on the Erdős–Turán conjecture*, Int. J. Number Theory 9 (2013), 1683–1686.

Csaba Sándor
Department of Stochastics
Budapest University of
Technology and Economics
H-1529 B.O. Box
Budapest, Hungary
E-mail: csandor@math.bme.hu

Quan-Hui Yang
School of Mathematics and Statistics
Nanjing University of
Information Science and Technology
Nanjing 210044, China
E-mail: yangquanhui01@163.com