COLLOQUIUM MATHEMATICUM

VOL. 104 2006 NO. 1

A BASIS OF $\mathbb{Z}_m$

BY

MIN TANG (Nanjing and Wuhu) and YONG-GAO CHEN (Nanjing)

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 order 2 of $\mathbb{N}$, $\sigma_A(n)$ is unbounded. In 1990, Imre Z. Ruzsa constructed a basis A of order 2 of $\mathbb{N}$ for which $\sigma_A(n)$ is bounded in the square mean. In this paper, we show that there exists a positive integer m_0 such that, for any integer $m \geq m_0$, we have a set $A \subset \mathbb{Z}_m$ such that $A + A = \mathbb{Z}_m$ and $\sigma_A(\overline{n}) \leq 768$ for all $\overline{n} \in \mathbb{Z}_m$.

1. Introduction. A subset A of $\mathbb{N}$ is called a *basis of order* 2 if every sufficiently large natural number can be written as a sum of two numbers of A. For $n \in \mathbb{N}$ write $\sigma(n) = \sigma_A(n) = |\{(a,a') \in A^2 : a + a' = n\}|$. In 1941, using complex function theory, Erdős and Turán [3] proved that $\sigma(n)$ cannot become constant for large enough natural number n (Dirac [1] proved it more easily by elementary methods), and they conjectured that for any basis A of $\mathbb{N}, \sigma_A(n)$ is unbounded, which is called the *Erdős–Turán conjecture*. In 1954, by use of probabilistic methods, Erdős [2] proved the existence of a basis of $\mathbb{N}$ for which $\sigma(n)$ satisfies

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

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 constructed a basis of $\mathbb{N}$ for which $\sigma(n)$ is bounded in the square mean.

In this paper, replacing $\mathbb{N}$ by $\mathbb{Z}_m$, for $A \subseteq \mathbb{Z}_m$ and $\overline{n} \in \mathbb{Z}_m$, we define $\sigma_A(\overline{n}) = |\{(\overline{a}_1, \overline{a}_2) \in A^2 : \overline{a}_1 + \overline{a}_2 = \overline{n}\}|$, and obtain the following result:

THEOREM. *There exists a positive integer m_0 such that, for any integer $m \geq m_0$, there is a set $A \subseteq \mathbb{Z}_m$ such that $A + A = \mathbb{Z}_m$ and $\sigma_A(\overline{n}) \leq 768$ for all $\overline{n} \in \mathbb{Z}_m$.*

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

2000 *Mathematics Subject Classification*: 11B13, 11B34.

Key words and phrases: Erdős–Turán conjecture, basis, congruence.

Research supported by NNSF of China, Grant No 10471064 and the SF of AnHui Province, Grant No 01046103.

be the mapping

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

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

2. Proofs

LEMMA 1 [4, Lemma 2.1]. *For $g = (a,b) \in G$, and fixed $k, l \in \mathbb{Z}_p \setminus \{0\}$, consider the equation*

$$g = x + y, \qquad x \in Q_k,\ y \in Q_l.$$

If $k + l \ne 0$, 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.

REMARK 1. For fixed $k, l \in \mathbb{Z}_p \setminus \{0\}$, if $k + l \ne 0$, then $x + y = 0$ with $x \in Q_k$, $y \in Q_l$ if and only if $x = y = (0,0)$.

LEMMA 2. *Let p be prime for which $p > 5$ and $\left(\frac{2}{p}\right) = -1$, and put $B = Q_3 \cup Q_4 \cup Q_6$. Then $B + B = G$ and $\sigma_B(g) \le 16$ for all $g \in G$.*

Proof. Lemma 2.2 of [4] shows that $G = (Q_4 + Q_4) \cup (Q_3 + Q_6)$, which is stronger than the required $B + B = G$.

Now, we prove that $\sigma_B(g) \le 16$ for all $g \in G$. For any $g = (a,b) \in G$, we have:

(a) *If $b \ne 2a^2$, then $g \notin (Q_4 + Q_4) \cap (Q_3 + Q_6)$.*

Indeed, if $g \in Q_4 + Q_4$ and $g \in Q_3 + Q_6$, then by Lemma 1, we have

$$\left(\frac{8b - 16a^2}{p}\right) = 1, \qquad \left(\frac{9b - 18a^2}{p}\right) = 1,$$

thus

$$1 = \left(\frac{(8b - 16a^2)(9b - 18a^2)}{p}\right) = \left(\frac{2}{p}\right) = -1.$$

Hence, there are at most eight sub-equations for $g = x + y,\ x, y \in B$, each of which has at most two solutions by Lemma 1; therefore $\sigma_B(g) \le 16$.

(b) *If $b = 2a^2$ and $a \ne 0$, then $g \notin Q_3 + Q_4$ and $g \notin Q_4 + Q_3$.*

Since

$$\left(\frac{7b - 12a^2}{p}\right) = \left(\frac{2a^2}{p}\right) = \left(\frac{2}{p}\right) = -1,$$

by Lemma 1, it is easy to conclude that $g \notin Q_3 + Q_4$ and $g \notin Q_4 + Q_3$.

Hence, there are at most seven sub-equations for $g = x + y,\ x, y \in B$; therefore $\sigma_B(g) \le 14$.

(c) *If* $b = 2a^2$ *and* $a = 0$, *that is,* $g = (0, 0) \in G$. *By Remark* 1, $\sigma_B(g) = 1$.

Therefore, we have $\sigma_B(g) \le 16$ for all $g \in G$.

This completes the proof of Lemma 2.

The following Lemma 3 belongs to Ruzsa [4, Lemma 3.1] (several printing mistakes have been corrected here).

Lemma 3. *Let* p *be prime for which* $p > 5$ *and* $\left(\frac{2}{p}\right) = -1$, $B = Q_3 \cup Q_4 \cup Q_6$ *and* $B' = \varphi(B)$. *Then* $\sigma_{B'}(n) \le 16$ *for all* n. *Moreover, for every integer* $0 \le n < 2p^2$, *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 $B' + B'$.

Lemma 4. *Let* p *be prime for which* $p > 5$ *and* $\left(\frac{2}{p}\right) = -1$. *There exists a set* $V \subset [0, 4p^2)$ *of integers with* $|V| \le 12p$ *such that* $[4p^2, 6p^2) \subseteq V + V$ *and* $\sigma_V(n) \le 256$ *for all* n.

Proof. Let B' be the set of Lemma 3, and put $V = B' + \{0, 2p^2 - p, 2p^2, 2p^2 + p\}$. Since $B' \subset [0, 2p^2 - p)$, we know $V \subset [0, 4p^2)$. And $|V| \le 4|B'| = 4|B| \le 12p$.

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 3, we have $[4p^2, 6p^2) \subseteq V + V$.

Now, V is the union of four translated copies of B'. Hence the equation $n = u + v,\ u, v \in V$, is composed of 16 equations for elements of B'. Thus

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

This completes the proof of Lemma 4.

Proof of Theorem. By the Prime Number Theorem in arithmetic progression, there exists a positive integer m_0 such that, for any integer $m \ge m_0$, we can choose a prime p with $\left(\frac{2}{p}\right) = -1$ such that

$$\sqrt{\frac{9}{16}m} \le p < \sqrt{\frac{5}{8}m}.$$

Let V be the set in the proof of Lemma 4 corresponding to the selected p. For a given integer m ($\ge m_0$), consider the canonical map

$$\psi : \mathbb{Z} \to \mathbb{Z}_m, \qquad n \mapsto \overline{n}.$$

Let $A = \psi(V)$. By the definition, we have $A \subseteq \mathbb{Z}_m$. Thus $A + A \subseteq \mathbb{Z}_m$. By Lemma 4, we have $[4p^2, 6p^2) \subseteq V + V$. Thus $\mathbb{Z}_m \subseteq A + A$. Hence, $A + A = \mathbb{Z}_m$.

For any $n \in [0, m-1]$, consider the equation

$$\overline{u} + \overline{v} = \overline{n}, \qquad \overline{u}, \overline{v} \in A. \tag{2}$$

Let $\overline{u} = \psi(u)$ and $\overline{v} = \psi(v)$ with $u, v \in V$. Then

$$u + v \equiv n \pmod{m}, \qquad u, v \in V. \tag{3}$$

Clearly, the number of solutions of (2) does not exceed that of (3). Since $0 \le u + v < 8p^2 < 5m$, we have

$$\{u+v \mid u, v \in V \text{ and } u+v \equiv n \pmod{m}\} \subseteq \{n, n+m, n+2m, n+3m, n+4m\}.$$

CASE 1: $u + v = n$. Since $0 \le n \le m - 1 \le 16p^2/9 - 1$ and $B' + B' \subset [0, 4p^2 - 2p)$, there is only one case, that is, $u, v \in B'$. By Lemma 3, we have

$$\max \sigma_V(n) \le \max \sigma_{B'}(n) \le 16.$$

CASE 2: $u + v = n + m$. Since $n + m \le 32p^2/9 - 1$ and $B' + B' \subset [0, 4p^2 - 2p)$, there are the following seven cases: (1) $u, v \in B'$; (2) $u \in B'$, $v \in B' + 2p^2 - p$; (3) $u \in B'$, $v \in B' + 2p^2$; (4) $u \in B'$, $v \in B' + 2p^2 + p$; (5) $u \in B' + 2p^2 - p$, $v \in B'$; (6) $u \in B' + 2p^2$, $v \in B'$; (7) $u \in B' + 2p^2 + p$, $v \in B'$. Thus

$$\max \sigma_V(n + m) \le 7 \cdot 16 = 112.$$

CASE 3: $u + v = n + 2m$. Then

$$\max \sigma_V(n + 2m) \le 16 \cdot 16 = 256.$$

CASE 4: $u + v = n + 3m$. Since $n + 3m \ge 24p^2/5 > 4p^2$ and $B' + B' \subset [0, 4p^2 - 2p)$, the case $u, v \in B'$ cannot hold. Thus

$$\max \sigma_V(n + 3m) \le 15 \cdot 16 = 240.$$

CASE 5: $u + v = n + 4m$. Since $n + 4m \ge 32p^2/5 > 6p^2$ and $B' + B' \subset [0, 4p^2 - 2p)$, the following seven cases cannot hold: (1) $u, v \in B'$; (2) $u \in B'$, $v \in B' + 2p^2 - p$; (3) $u \in B'$, $v \in B' + 2p^2$; (4) $u \in B'$, $v \in B' + 2p^2 + p$; (5) $u \in B' + 2p^2 - p$, $v \in B'$; (6) $u \in B' + 2p^2$, $v \in B'$; (7) $u \in B' + 2p^2 + p$, $v \in B'$. Thus

$$\max \sigma_V(n + 4m) \le 9 \cdot 16 = 144.$$

Hence, we have

$$\sigma_A(\overline{n}) \le \sum_{i=0}^{4} \max \sigma_V(n + im) \le 16 + 112 + 256 + 240 + 144 = 768$$

for all $\overline{n} \in \mathbb{Z}_m$ $(m \ge m_0)$.

This completes the proof of the Theorem.

REMARK 2. Let $[x]$ denote the integer part of the real number x. Comparing with the result of the Theorem, we have the following example. Put

$$V = \{0, 1, 2, \ldots, [\sqrt{m}]\} \cup \{2[\sqrt{m}], 3[\sqrt{m}], \ldots, ([\sqrt{m}] + 1)[\sqrt{m}]\}.$$

Let ψ be the canonical map as defined in the proof of the Theorem. Let $A = \psi(V)$. Then A is a basis of $\mathbb{Z}_m$, $|A| \le 2[\sqrt{m}] + 1$ and

$$\sup_{n\in\mathbb{Z}_m} \sigma_A(n) \ge \sigma_A([\sqrt{m}] + 1) \ge [\sqrt{m}].$$

Acknowledgements. The authors would like to thank the referee for his/her detailed comments and helpful suggestions.

REFERENCES

[1] G. A. Dirac, *Note on a problem in additive number theory*, J. London Math. Soc. 26 (1951), 312–313.

[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. London Math. Soc. 16 (1941), 212–215.

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

Department of Mathematics
Anhui Normal University
Wuhu 241000, China

Department of Mathematics
Nanjing Normal University
Nanjing 210097, China
E-mail: ygchen@njnu.edu.cn

Received 2 September 2004;
revised 15 June 2005 (4494)