COLLOQUIUM MATHEMATICUM

VOL. 108 2007 NO. 1

A BASIS OF $\mathbb{Z}_m$*, II*

BY

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

Abstract. Given a set $A \subset \mathbb{N}$ let $\sigma_A(n)$ denote the number of ordered pairs $(a, a') \in A \times A$ such that $a + a' = n$. Erdős and Turán conjectured that for any asymptotic basis A of $\mathbb{N}$, $\sigma_A(n)$ is unbounded. We show that the analogue of the Erdős–Turán conjecture does not hold in the abelian group $(\mathbb{Z}_m, +)$, namely, for any natural number m, there exists a set $A \subseteq \mathbb{Z}_m$ such that $A + A = \mathbb{Z}_m$ and $\sigma_A(\overline{n}) \le 5120$ for all $\overline{n} \in \mathbb{Z}_m$.

1. Introduction. Given a set $A \subset \mathbb{N}$ let $\sigma_A(n)$ denote the number of ordered pairs $(a, a') \in A \times A$ such that $a + a' = n$. The set A is called an *asymptotic basis of order two* if there is $n_0 = n_0(A)$ such that $\sigma_A(n) \ge 1$ for each positive integer $n \ge n_0$. In particular, we call A a *basis* if $\sigma_A(n) \ge 1$ for all positive integers n. The celebrated *Erdős–Turán conjecture* [3, 5] states that if A is an asymptotic basis, then the representation function $\sigma_A(n)$ must be unbounded. In 1990, Ruzsa [12] found a basis A for which the number of representations $n = a + a'$, $a, a' \in A$, is bounded in the square mean, that is, $\sum_{n \le N} \sigma_A(N)^2 = O(N)$.

While the above famous conjecture is still an unsolved problem, a natural related question which has been raised is: in which abelian groups or semigroups is the analogue of this conjecture valid? Erdős [2] proved that for the semigroup $(\mathbb{N}, \cdot)$ of positive integers under ordinary multiplication, if A is a basis, then the representation function $\sigma_A(n)$ is unbounded. Puš [11] first established that the analogue of the Erdős–Turán conjecture fails to hold in some abelian groups. Nathanson [8] constructed a family of arbitrarily sparse unique representation bases for $\mathbb{Z}$, and in [10], he proved that large classes of additive abelian semigroups fail to satisfy the Erdős–Turán property in a spectacular way. Chen [1] constructed a unique representation basis whose growth is more than $x^{1/2-\varepsilon}$ for infinitely many positive integers x. For related problems see [4], [6] and [9].

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

Key words and phrases: Erdős–Turán conjecture, additive bases, representation function.

Research supported by the National Natural Science Foundation of China, Grant No 10471064, the Doctoral Foundation and the Youth Foundation of Anhui Normal University Grant No 2006xqn52.

Let $G = \{a_1, \ldots, a_m\}$ be a finite abelian group. Using similar notations, for $A \subseteq G$ and $n \in G$, we define $\sigma_A(n) = \sharp\{(a_i, a_j) \in A \times A : a_i + a_j = n\}$, $r_A(n) = \sharp\{(a_i, a_j) \in A \times A : a_i + a_j = n,\ i \le j\}$. Then we call $A \subseteq G$ a *basis* if $\sigma_A(n) \ge 1$ for all $n \in G$, and a *unique representation basis* if $r_A(n) = 1$ for all $n \in G$. In [13], by using Ruzsa's method we proved that for every large enough integer m, there exists a basis A of $\mathbb{Z}_m$ such that $\sigma_A(\overline{n}) \le 768$ for all $\overline{n} \in \mathbb{Z}_m$. In this paper, the following result is proved.

THEOREM. *For any natural number m, there exists a set $A \subseteq \mathbb{Z}_m$ such that $A + A = \mathbb{Z}_m$ and $\sigma_A(\overline{n}) \le 5120$ for all $\overline{n} \in \mathbb{Z}_m$.*

REMARK 1. The analogue of the theorem fails for elementary 2-groups. In fact, if A is a basis of $\mathbb{Z}_2^N$ having t elements, then $t^2 \ge 2^N$, and since for every $a \in A$ one has $a + a = 0$, it follows that $\sigma_A(0) \ge t \ge 2^{N/2}$, which tends to infinity as $N \to \infty$.

REMARK 2. By a simple counting argument, we can show that there does not exist a unique representation basis for any finite abelian group G, except for $|G| = 1$ or $|G| = 3$.

REMARK 3. Let

$$\Phi(m) = \min_{A \subset \mathbb{Z}_m} \max_{\overline{n} \in \mathbb{Z}_m} \sigma_A(\overline{n}).$$

The theorem gives $\Phi(m) \le 5120$ for all positive integers m, and Remark 2 gives $\Phi(m) \ge 3$ for $m \ne 1, 3$.

REMARK 4. Let G be a countably infinite abelian group. For every positive integer h, define $h * G = \{hg : g \in G\}$. In [10], Nathanson proved that if G is a countably infinite abelian group such that $12 * G$ is infinite, and if $f : G \to \mathbb{N}_0 \cup \{\infty\}$ is a map such that the set $Z_0 = f^{-1}(0)$ is finite, then there exists an asymptotic basis A for G such that $r_A(x) = f(x)$ for all $x \in G$. By Remark 2, we find that the story of the finite abelian group is very different from that of the infinite abelian group in this respect.

2. Proofs. We start by recalling some notations used in [13]: 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

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

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

LEMMA 1 ([13, Lemma 3]). *Let $p > 5$ be a prime for which $\left(\frac{2}{p}\right) = -1$, and let $B = Q_3 \cup Q_4 \cup Q_6$ 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 2 ([13, Lemma 4]). *Let $p > 5$ be a prime for which $\left(\frac{2}{p}\right) = -1$, and let $B = Q_3 \cup Q_4 \cup Q_6$ and $B' = \varphi(B)$. Put $V = B' + \{0, 2p^2 - p, 2p^2, 2p^2 + p\}$. Then $V \subset [0, 4p^2)$, $[4p^2, 6p^2) \subseteq V + V$ and $\sigma_V(n) \le 256$ for all n.*

LEMMA 3 ([7]). *For arbitrary natural numbers m and d (≥ 2) and real $z > 1$, let $B_m(z, d) = \liminf\{c :$ for every $x \ge c$ the interval (x, zx) contains at least m primes $\equiv a \pmod d$ for every integer a satisfying $(a, d) = 1\}$. Then $B_1(3.15, 8) \le 24$.*

Proof of the Theorem. We may assume $m > 5120$, since for smaller m the assertion is trivially true.

When $m > 5120$, $\sqrt{m/2} > 24$, by Lemma 3, we can choose a prime $p > 5$ for which $\left(\frac{2}{p}\right) = -1$ such that

$$\sqrt{m/2} < p < 3.15\sqrt{m/2}.$$

Let B' and V be the sets of Lemma 2 corresponding to the selected p. For the given positive integer m (> 5120), we consider the canonical map

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

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

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

$$\overline{u} + \overline{v} = \overline{n}, \quad \overline{u}, \overline{v} \in A. \tag{1}$$

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

$$u + v \equiv n \pmod m, \quad u, v \in V. \tag{2}$$

Clearly, the number of solutions of (1) does not exceed that for (2).

Since $V \subset [0, 4p^2)$ and $0 \le u + v < 8p^2 < 39.69m$, we have

$$\{u + v : u, v \in V \text{ and } u + v \equiv n \pmod m\} \subseteq \{n, n + m, \ldots, n + 39m\}.$$

Let k_0, k_1, k_2, k_3, k_4 be five integers such that $k_0 = -1$ and

$$\begin{aligned}
n + k_1 m &< 2p^2 - p \le n + (k_1 + 1)m, \\
n + k_2 m &< 4p^2 - 2p \le n + (k_2 + 1)m, \\
n + k_3 m &< 6p^2 - p \le n + (k_3 + 1)m, \\
n + k_4 m &< 8p^2 \le n + (k_4 + 1)m.
\end{aligned}$$

Then $k_0 \le k_1 \le k_2 \le k_3 \le k_4 \le 39$.

Since $p < 3.15\sqrt{m/2}$ and $m > 5120$ we have

$$k_{i+1} - (k_i + 1) < \frac{2p^2 + p}{m} < 10, \quad i = 0, 1, 2, 3.$$

Hence $k_{i+1} - k_i \le 10$, $i = 0, 1, 2, 3$.

Case 1: $u+v=n+im$, $k_0+1\le i\le k_1$. As $n+im<2p^2-p$ and $B'+B'\subseteq[0,4p^2-2p)$, there is only one posibility: $u,v\in B'$. By Lemma 1, we have

$$\sum_{k_0+1\le i\le k_1}\sigma_V(n+im)\le 16(k_1-k_0)\le 160.$$

In case $k_1=k_0$, this inequality also holds.

Case 2: $u+v=n+im$, $k_1+1\le i\le k_2$. As $n+im<4p^2-2p$ and $B'+B'\subseteq[0,4p^2-2p)$, there are at most seven possibilities: (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

$$\sum_{k_1+1\le i\le k_2}\sigma_V(n+im)\le 7\cdot 16(k_2-k_1)\le 1120.$$

In case $k_2=k_1$, this inequality also holds.

Case 3: $u+v=n+im$, $k_2+1\le i\le k_3$. As $n+im\ge 4p^2-2p$ and $B'+B'\subseteq[0,4p^2-2p)$, the case $u,v\in B'$ cannot hold. Thus

$$\sum_{k_2+1\le i\le k_3}\sigma_V(n+im)\le 15\cdot 16(k_2-k_1)\le 2400.$$

In case $k_3=k_2$, this inequality also holds.

Case 4: $u+v=n+im$, $k_3+1\le i\le k_4$. As $n+im\ge 6p^2-p$ and $B'+B'\subseteq[0,4p^2-2p)$, 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

$$\sum_{k_3+1\le i\le k_4}\sigma_V(n+im)\le 9\cdot 16(k_2-k_1)\le 1440.$$

In case $k_4=k_3$, this inequality also holds.

Hence, for all $\overline{n}\in\mathbb{Z}_m$ $(m>5120)$, we have

$$\sigma_A(\overline{n})\le\sum_{k_0+1\le i\le k_4}\sigma_V(n+im)\le 160+1120+2400+1440=5120.$$

Therefore, for any natural number m, there exists a set $A\subseteq\mathbb{Z}_m$ such that $A+A=\mathbb{Z}_m$ and $\sigma_A(\overline{n})\le 5120$ for all $\overline{n}\in\mathbb{Z}_m$.

This completes the proof of the Theorem.

Acknowledgements. We are grateful to the referee for his/her detailed comments.

REFERENCES

[1] Y. G. Chen, *A problem on unique representation bases*, European J. Combin. 28 (2007), 33–35.
[2] P. Erdős, *On the multiplicative representation of integers*, Israel J. Math. 2 (1964), 251–261.
[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] L. Haddad and C. Helou, *Bases in some additive groups and the Erdős–Turán conjecture*, J. Combin. Theory Ser. A 108 (2004), 147–153.
[5] H. Halberstam and K. F. Roth, *Sequences*, Clarendon Press, Oxford, 1966.
[6] B. Lindström, *An inequality for B_2-sequences*, J. Combin. Theory 6 (1969), 211–212.
[7] P. Moree, *Bertrand's postulate for primes in arithmetical progressions*, Comput. Math. Appl. 26 (1993), 35–43.
[8] M. B. Nathanson, *Unique representation bases for integers*, Acta Arith. 108 (2003), 1–8.
[9] —, *The inverse problem for representation functions of additive bases*, in: Number Theory (New York, 2003), Springer, 2004, 253–262.
[10] —, *Representation functions of additive bases for abelian semigroups*, Int. J. Math. Math. Sci. 2004, no. 29-32, 1589–1597.
[11] V. Puš, *On multiplicative bases in abelian groups*, Czechoslovak Math. J. 41 (1991), 282–287.
[12] I. Z. Ruzsa, *A just basis*, Monatsh. Math. 109 (1990), 145–151.
[13] M. Tang and Y. G. Chen, *A basis of $\mathbb{Z}_m$*, Colloq. Math. 104 (2006), 99–103.

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

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

Received 26 August 2005;
revised 8 September 2006 (4655)