Journal of Integer Sequences, Vol. 14 (2011),
Article 11.1.8

Unique Difference Bases of $\mathbb{Z}$

Chi-Wu Tang, Min Tang,[1] and Lei Wu
Department of Mathematics
Anhui Normal University
Wuhu 241000
P. R. China
tmzzz2000@163.com

Abstract

For $n \in \mathbb{Z}, A \subset \mathbb{Z}$, let $\delta_A(n)$ denote the number of representations of n in the form $n = a - a'$, where $a, a' \in A$. A set $A \subset \mathbb{Z}$ is called a unique difference basis of $\mathbb{Z}$ if $\delta_A(n) = 1$ for all $n \neq 0$ in $\mathbb{Z}$. In this paper, we prove that there exists a unique difference basis of $\mathbb{Z}$ whose growth is logarithmic. These results show that the analogue of the Erdős-Turán conjecture fails to hold in $(\mathbb{Z}, -)$.

1 Introduction

For sets A and B of integers and for any integer c, we define the set

$$A - B = \{a - b : a \in A, b \in B\},$$

and the translations

$$A - c = \{a - c : a \in A\},$$
$$c - A = \{c - a : a \in A\}.$$

The counting function for the set A is

$$A(y, x) = \text{card}\{a \in A : y \leq a \leq x\}.$$

For $n \in \mathbb{Z}$, we write

$$\delta_A(n) = \text{card}\{(a, a') \in A \times A : a - a' = n\},$$

[1] Corresponding author. The second author was supported by the National Natural Science Foundation of China, Grant No. 10901002 and the SF of the Education Department of Anhui Province, Grant No. KJ2010A126.

$$\sigma_A(n) = \mathrm{card}\{(a, a') \in A \times A : a + a' = n\}.$$

We call $A \subset \mathbb{Z}$ a difference basis of $\mathbb{Z}$ if $\delta_A(n) \geq 1$ for all $n \in \mathbb{Z}$, and a unique difference basis of $\mathbb{Z}$ if $\delta_A(n) = 1$ for all $n \neq 0$ in $\mathbb{Z}$. We call A a subset of $\mathbb{N}$ an additive asymptotic basis of $\mathbb{N}$ if there is $n_0 = n_0(A)$ such that $\sigma_A(n) \geq 1$ for all $n \geq n_0$. The celebrated Erdős-Turán conjecture [1] states that if $A \subset \mathbb{N}$ is an additive asymptotic basis of $\mathbb{N}$, then the representation function $\sigma_A(n)$ must be unbounded. In 1990, Ruzsa [5] constructed a basis of $A \subset \mathbb{N}$ for which $\sigma_A(n)$ is bounded in the square mean. Pŭs [4] first established that the analogue of the Erdős-Turán conjecture fails to hold in some abelian groups. Nathanson [3] constructed a family of arbitrarily sparse unique additive representation bases for $\mathbb{Z}$. In 2004, Haddad and Helou [2] showed that the analogue of the Erdős-Turán conjecture does not hold in a variety of additive groups derived from those of certain fields. Let K be a finite field of characteristic $\neq 2$ and G the additive group of $K \times K$. Recently, Chi-Wu Tang and Min Tang [6] proved there exists a set $B \subset G$ such that $1 \leq \delta_B(g) \leq 14$ for all $g \neq 0$.

It is natural to consider the analogue of the Erdős-Turán conjecture in $(\mathbb{Z}, -)$. In this paper, we obtain the following results.

Theorem 1. *There exists a family of unique difference bases of $\mathbb{Z}$.*

Theorem 2. *There exists a unique difference basis A of $\mathbb{Z}$ such that*

$$\frac{2\log(3x+3)}{\log 3} - \frac{2\log 5}{\log 3} < A(0, x) \leq \frac{2\log(x+3)}{\log 2} - 2 \text{ for all } x \geq 1.$$

2 Proof of Theorem 1.

We shall construct an ascending sequence $A_1 \subseteq A_2 \subseteq \cdots$ of finite sets of nonnegative integers such that

$$|A_k| = 2k, \text{ for all } k \geq 1,$$

$$\delta_{A_k}(n) \leq 1, \text{ for all } n \neq 0.$$

We shall prove that the infinite set

$$A = \bigcup_{k=1}^{\infty} A_k$$

is a unique difference basis of $\mathbb{Z}$.

We construct the sets A_k by induction. Let $A_1 = \{0, 1\}$. We assume that for some $k \geq 1$ we have constructed sets $A_1 \subseteq \cdots \subseteq A_k$ such that $|A_i| = 2i$ and $\delta_{A_i}(n) \leq 1$ for all $1 \leqslant i \leqslant k$ and all integers $n \neq 0$. We define the integers

$$d_k = \max\{a : a \in A_k\},$$

$$b_k = \min\{|b| : b \notin A_k - A_k\}.$$

To construct the set A_{k+1}, we choose an integer c_k such that $c_k > d_k$. Let

$$A_{k+1} = A_k \cup \{2c_k, b_k + 2c_k\}.$$

Then $|A_{k+1}| = 2k+2 = 2(k+1)$ for all $k \ge 1$, and $A_k \subseteq [0, d_k],\ A_k - A_k \subseteq [-d_k, d_k]$.

Note that

$$A_{k+1} - A_{k+1} = (A_k - A_k) \cup (A_k - (b_k + 2c_k))$$
$$\cup((b_k + 2c_k) - A_k) \cup (A_k - 2c_k) \cup (2c_k - A_k) \cup \{b_k, -b_k\}. \tag{1}$$

We shall show that $A_{k+1} - A_{k+1}$ is the disjoint union of the above six sets.
If $u \in A_k - A_k$, then

$$-d_k \le u \le d_k. \tag{2}$$

If $v_1 \in A_k - (b_k + 2c_k)$ and $v_2 \in (b_k + 2c_k) - A_k$, then there exist $a, a' \in A_k$ such that $v_1 = a - (b_k + 2c_k)$ and $v_2 = (b_k + 2c_k) - a'$. Since $0 \le a, a' \le d_k$, we have

$$-b_k - 2c_k \le v_1 \le -b_k - 2c_k + d_k, \tag{3}$$

$$b_k + 2c_k - d_k \le v_2 \le b_k + 2c_k. \tag{4}$$

If $w_1 \in A_k - 2c_k$ and $w_2 \in 2c_k - A_k$, similarly, we have

$$-2c_k \le w_1 \le -2c_k + d_k, \tag{5}$$

$$2c_k - d_k \le w_2 \le 2c_k. \tag{6}$$

For any $n \in \mathbb{Z}$, if $n \in A_k - A_k$, then $-n \in A_k - A_k$, thus by the definition of b_k, we have

$$b_k \notin A_k - A_k \text{ and } -b_k \notin A_k - A_k. \tag{7}$$

Assume $(2c_k - A_k) \cap ((b_k + 2c_k) - A_k) \neq \emptyset$, then there exist $a, a' \in A_k$ such that $b_k + 2c_k - a = 2c_k - a'$, $b_k = a - a' \in A_k - A_k$ which contradicts with the fact $b_k \notin A_k - A_k$. Similarly, we have $(A_k - (b_k + 2c_k)) \cap (A_k - 2c_k) = \emptyset$.

Moreover, we have $d_k \in A_k - A_k$, hence $b_k \neq d_k$. If $b_k < d_k$, it is easy to see that the set $\{-b_k, b_k\}$ is disjoint with the other five sets. If $b_k > d_k$, since $d_k \in A_k - A_k$ and by the definition of b_k, we have $b_k = d_k + 1$. Then $2c_k - d_k \geqslant 2(d_k + 1) - d_k = d_k + 2 > b_k$ and $-2c_k + d_k \leqslant -2(d_k + 1) + d_k = -d_k - 2 < -b_k$, thus the set $\{-b_k, b_k\}$ is disjoint with the other five sets.

By Eq. (1)–(6) and the above discussion, we know that the sets $A_k - A_k,\ A_k - (b_k + 2c_k),\ (b_k + 2c_k) - A_k,\ A_k - 2c_k,\ 2c_k - A_k,\ \{b_k, -b_k\}$ are pairwise disjoint. That is, $\delta_{A_{k+1}}(n) \le 1$ for all integers $n \neq 0$.

Let $A = \bigcup\limits_{k=1}^{\infty} A_k$. Then for all $k \ge 1$, by (7) and the definition of b_k, we have

$$\{-b_k + 1, -b_k + 2, \cdots, -1, 1, \cdots, b_k - 2, b_k - 1\} \subset A_k - A_k \subset A - A,$$

and the sequence $\{b_k\}_{k \geqslant 1}$ is strictly increasing, since $A_k - A_k \subset A_{k+1} - A_{k+1}$ and $\pm b_k \in A_{k+1} - A_{k+1}$ but $\pm b_k \notin A_k - A_k$. Thus A is a difference basis of $\mathbb{Z}$. If $\delta_A(n) \ge 2$ for some n, then by construction, $\delta_{A_k}(n) \ge 2$ for some k, which is impossible. Therefore, A is a unique difference basis of $\mathbb{Z}$.

It completes the proof of Theorem 1.

3 Proof of Theorem 2.

We apply the method of Theorem 1 with

$$c_k = d_k + 1 \text{ for all } k \geq 1.$$

This is essentially a greedy algorithm construction, since at each iteration we choose the smallest possible value of c_k. It is instructive to compute the first few sets A_k. Since

$$A_1 = \{0, 1\}, \quad A_1 - A_1 = \{-1, 0, 1\},$$

we have $b_1 = 2, d_1 = 1$, and $c_1 = d_1 + 1 = 2$. Then

$$A_2 = \{0, 1, 4, 6\}, \quad A_2 - A_2 = \{-6, -5, -4, -3, -2, -1, 0, 1, 2, 3, 4, 5, 6\},$$

hence $b_2 = 7, d_2 = 6$, $c_2 = d_2 + 1 = 7$. The next iteration of the algorithm produces the sets

$$A_3 = \{0, 1, 4, 6, 14, 21\},$$

$$\begin{aligned} A_3 - A_3 = \{&-21, -20, -17, -15, -14, -13, -10, -8, \\ &-7, 7, 8, 10, 13, 14, 15, 17, 20, 21\} \cup (A_2 - A_2), \end{aligned}$$

so we obtain $b_3 = 9, d_3 = 21, c_3 = 22$, and

$$A_4 = \{0, 1, 4, 6, 14, 21, 44, 53\}.$$

We shall compute upper and lower bounds for the counting function $A(0, x)$. We observe that if $x \geq d_1$ and k is the unique integer such that $d_k \leq x < d_{k+1}$, by the construction of A, we know $A_k = |2k|$ and $A_{k+1} = A_k \cup \{2c_k, 2c_k + b_k\}$, then

$$A(0, x) = A_{k+1}(0, x) = \begin{cases} 2k, & \text{if } d_k \leq x < 2c_k, \\ 2k + 1, & \text{if } 2c_k \leq x < 2c_k + b_k = d_{k+1}. \end{cases}$$

For $k \geq 1$, we have $1 < b_k \leq d_k + 1 = c_k$ and $c_{k+1} = d_{k+1} + 1 = 2c_k + b_k + 1$, hence

$$2c_k + 2 < c_{k+1} \leq 3c_k + 1.$$

Since $c_1 = d_1 + 1 = 2$, it follows by induction on k that

$$2^{k+1} - 2 \leq c_k \leq \frac{5}{2} \cdot 3^{k-1} - \frac{1}{2},$$

and so

$$\frac{\log \frac{6}{5}\left(c_k + \frac{1}{2}\right)}{\log 3} \leq k \leq \frac{\log \frac{c_k + 2}{2}}{\log 2} \text{ for all } k \geq 1.$$

We obtain an upper bound for $A(0, x)$ as follows. If $d_k \leq x < 2c_k$, then $c_k \leq x + 1$, and

$$A(0, x) = A_{k+1}(0, x) = 2k \leq 2\frac{\log \frac{c_k + 2}{2}}{\log 2} = \frac{2\log(c_k + 2)}{\log 2} - 2 \leq \frac{2\log(x + 3)}{\log 2} - 2.$$

If $2c_k \le x < d_{k+1}$, then $c_k \le \frac{x}{2}$, and

$$A(0,x) = A_{k+1}(0,x) = 2k+1 \le \frac{2\log\frac{c_k+2}{2}}{\log 2} + 1 \le \frac{2\log\left(\frac{x}{4}+1\right)}{\log 2} + 1 = \frac{2\log(x+4)}{\log 2} - 3.$$

Therefore,

$$A(0,x) \le \frac{2\log(x+3)}{\log 2} - 2 \text{ for all } x \ge 1.$$

Similarly, we obtain a lower bound for $A(0,x)$. If $d_k \le x < 2c_k$, then

$$A(0,x) = 2k \ge \frac{2\log\frac{6}{5}\left(c_k+\frac{1}{2}\right)}{\log 3} > \frac{2\log\frac{3}{5}(x+1)}{\log 3} = \frac{2\log(3x+3)}{\log 3} - \frac{2\log 5}{\log 3}.$$

If $2c_k \le x < d_{k+1}$, then $d_{k+1} = b_k + 2c_k \le 3c_k$. So $c_k \ge \frac{1}{3}d_{k+1} > \frac{1}{3}x$ and

$$A(0,x) = 2k+1 \ge \frac{2\log\frac{6}{5}\left(c_k+\frac{1}{2}\right)}{\log 3} + 1 > \frac{2\log\frac{6}{5}\left(\frac{x}{3}+\frac{1}{2}\right)}{\log 3} + 1 = \frac{2\log(2x+3)}{\log 3} + 1 - \frac{2\log 5}{\log 3}.$$

Therefore,

$$A(0,x) > \frac{2\log(3x+3)}{\log 3} - \frac{2\log 5}{\log 3} \text{ for all } x \ge 1.$$

This completes the proof of Theorem 2.

4 Acknowledgements

We would like to thank the referee for his/her many helpful suggestions.

References

[1] 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.

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

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

[4] V. Pŭs, On multiplicative bases in abelian groups, *Czech. Math. J.* **41** (1991), 282–287.

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

[6] Chi-Wu Tang and Min Tang, Note on a result of Haddad and Helou, *Integers* **10** (2010), 229–232. Available electronically at http://integers-ejcnt.org/vol10.html.

2000 *Mathematics Subject Classification*: Primary 11B13; Secondary 11B34.
Keywords: Erdős-Turán conjecture; difference bases; counting function.

Received October 12 2010; revised version received January 26 2011. Published in *Journal of Integer Sequences*, February 9 2011.

Return to Journal of Integer Sequences home page.