#A18 INTEGERS 10 (2010), 229-232

NOTE ON A RESULT OF HADDAD AND HELOU

Chi-Wu Tang
Department of Mathematics, Anhui Normal University, Wuhu 241000, China
tangchiwu@126.com

Min Tang[1]
Department of Mathematics, Anhui Normal University, Wuhu 241000, China
tmzzz2000@163.com

Received: 7/31/09, Revised: 1/18/10, Accepted: 1/23/10, Published: 5/12/10

Abstract

Let K be a field of characteristic $\neq 2$ and G the additive group of $K \times K$. In 2004, Haddad and Helou constructed an additive basis B of G for which the number of representations of $g \in G$ as a sum $b_1 + b_2 (b_1, b_2 \in B)$ is bounded by 18. In this paper, we proceed to investigate the parallel problem for differences.

1. Introduction

Let G be a semi-group. For $A, B \subseteq G$ and $g \in G$, we define

$$\sigma_{A,B}(g) = |\{(a, b) \in A \times B : a + b = g\}|,$$

$$\delta_{A,B}(g) = |\{(a, b) \in A \times B : a - b = g\}|.$$

Let $\sigma_A(g) = \sigma_{A,A}(g)$, $\delta_A(g) = \delta_{A,A}(g)$, and $A - B = \{a - b : a \in A, b \in B\}$.

The celebrated Erdős-Turán conjecture [3] 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. This conjecture has had an important impact in additive number theory. In 1954, Erdős [2] proved the function $\sigma_A(n)$ can have logarithmic growth. In 1990, Ruzsa [7] constructed a basis of $A \subset \mathbf{N}$ for which $\sigma_A(n)$ is bounded in the square mean. These results indicate the difficulty involved in the conjecture and leads to the consideration of the problem in other semigroups. Pŭs [6] first established that the analogue of the Erdős-Turán conjecture fails to hold in some abelian groups. Nathanson [4] constructed a family of arbitrarily sparse unique representation bases for $\mathbb{Z}$. In 2004, Haddad and Helou [5] showed that the analogue of the Erdős-Turán conjecture does not hold in a variety of additive groups derived from those of certain fields. In [8], Tang and Chen showed that the analogue of the Erdős-Turán conjecture fails to hold in $(\mathbb{Z}_m, +)$. For the related problems see [1,9].

[1]Supported by the National Natural Science Foundation of China, Grant No 10901002.

It is natural to consider the parallel problems for differences. In this paper, based on the methods of Haddad and Helou, we obtain the following result.

Theorem 1. *Let K be a finite field of characteristic $\neq 2$ and G the additive group of $K \times K$. Then there exists a set $B \subset G$ such that $B - B = G$, and $\delta_B(g) \leq 14$ for all $g \neq 0$.*

Remark 2. This result is a generalization of the result obtained by Tang [10, Lemma 3]. For example, let p be prime with $p \geq 3$. By the theorem, there exists a set $B \subset \mathbb{Z}_p \times \mathbb{Z}_p$ such that $B - B = G$ and $\delta_B(g) \leq 14$ for all $g \neq 0$.

Throughout this paper, let K be a field of characteristic $\neq 2$ and G the additive group of $K \times K$. We denote by $K^* = K \setminus \{0\}$ the multiplicative group of K and by $S(K^*) = \{x^2 : x \in K^*\}$ the subgroup of the square elements of K^*. For $k \in K^*$, let $Q_k = \{(u, ku^2) : u \in K\} \subset G$.

2. Proofs

Lemma 3. *For $g = (a, b) \in G$ and fixed $k, l \in K^*$, consider the equation*

$$g = x - y,\ x \in Q_k,\ y \in Q_l.$$

If $k - l \neq 0$, then the set $Q_k - Q_l$ consists of all the elements $(a, b) \in G$ such that $b(k - l) + a^2 kl$ is a square in K, and for any $g \in G$, $\delta_{Q_k,Q_l}(g) \leq 2$. If $k - l = 0$, it has at most one solution except if $g = 0$, when it has $|K|$ solutions.

Proof. Let $g = (a, b) \in G$. Consider the system of equations

$$a = u - v, \tag{1}$$

$$b = ku^2 - lv^2. \tag{2}$$

Substituting the value of u from (1) into (2), we get the equation

$$b = (k - l)v^2 + 2kav + ka^2. \tag{3}$$

`Case 1.` $k - l \neq 0$. This is a quadratic equation in v, and it has exactly one or two solutions in the field K if and only if its discriminant $4a^2k^2 - 4(k - l)(a^2k - b) = 4\big((k-l)b + kla^2\big)$ is a square in K. Since the characteristic of K is $\neq 2$, the non-zero square factor 4 can be discarded in the latter condition. Thus for any $g = (a, b) \in G$, we have $\delta_{Q_k,Q_l}(g) \leq 2$.

`Case 2.` Case 2. $k - l = 0$. Then (3) is an equation of degree 1. If $a \neq 0$, (3) has one solution. If $a = b = 0$, (3) has $|K|$ solutions. If $a = 0, b \neq 0$, (3) has no solution.

This completes the proof of Lemma 3. □

Lemma 4 [5, Lemma 3.7]. *If K is a finite field of characteristic $\neq 2$, then the index of the subgroup $S(K^*)$ in the multiplicative group of K^* is 2. Thus the product of two non-square elements of K^* is a square element of K^*.*

Lemma 5. *If K is a finite field of characteristic $\neq 2$ and $|K| \geq 5$, then there exist elements $j, k \in K^*$ such that $j \in S(K^*)$, $k \notin S(K^*)$, and $k \neq -j$.*

Proof. By Lemma 4, $S(K^*) \neq K^*$ and $|S(K^*)| = |K^*|/2 \geq 2$, thus we can choose $j \in S(K^*)$, $k \in K^* \setminus S(K^*)$, and $k \neq -j$. □

Proof of Theorem 1. If $K = \mathbb{F}_3 = \{0, 1, 2\}$, put $B = \{(0,0),\ (0,1),\ (0,2),\ (1,1),\ (2,0)\} \subset \mathbb{F}_3 \times \mathbb{F}_3$. Then we have $B - B = G$ and $\delta_B(g) \leq 3$ for all $g \neq 0$.

Now we consider K to be a finite field of characteristic $\neq 2$ and $|K| \geq 5$.

Let $j, k \in K^*$ such that $j \in S(K^*)$, $k \notin S(K^*)$, and $k \neq -j$. Put $n = 2jk/(j+k)$, $B = Q_j \cup Q_k \cup Q_n$. By the fact that $k \neq j$, we have $j \neq n, k \neq n$.

By Lemma 3, $Q_j - Q_n = \{(a,b) \in G : b(j-n) + a^2jn \in S(K^*) \cup \{0\}\}$; similarly, $Q_n - Q_k = \{(a,b) \in G : b(n-k) + a^2nk \in S(K^*) \cup \{0\}\}$.

Let

$$e = b(j-n) + a^2jn, \quad f = b(n-k) + a^2nk.$$

Thus an element $(a,b) \neq (0,0)$ of G lies in $Q_j - Q_n$ (respectively, in $Q_n - Q_k$) if and only if e (respectively, f) is a square in K.

By simple calculation, we have $f = kj^{-1}e$. Since $j \in S(K^*)$, $j^{-1} \in S(K^*)$, by Lemma 4, we have $kj^{-1} \notin S(K^*)$, and thus $f \in S(K^*)$ if and only if $e \notin S(K^*)$. Hence, if an element $(a,b) \neq (0,0)$ of G does not lie in $Q_j - Q_n$ then it lies in $Q_n - Q_k$. Therefore, $G = (Q_j - Q_n) \cup (Q_n - Q_k)$, which is stronger than the required $B - B = G$.

By the above discussion, for $g(\neq 0) \in G$, we have the following two cases.

`Case 1.` $e \notin S(K^*)$ and $f \in S(K^*)$. If $g \in Q_j - Q_n$, then $e = 0$, and by the proof of Lemma 3 we have $\delta_{Q_j,Q_n}(g) = 1$.

`Case 2.` $e \in S(K^*)$ and $f \notin S(K^*)$. If $g \in Q_n - Q_k$, then $f = 0$, and by the proof of Lemma 3 we have $\delta_{Q_n,Q_k}(g) = 1$.

Hence,

$$\delta_B(g) \leq \sum_{r,s \in \{j,k,n\}} \delta_{Q_r,Q_s}(g) = \sum_{\substack{r,s \in \{j,k,n\} \\ r \neq s}} \delta_{Q_r,Q_s}(g) + \sum_{r \in \{j,k,n\}} \delta_{Q_r}(g) \leq 14.$$

This completes the proof of the theorem. □

References

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

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

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

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

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

[8] M. Tang and Y. G. Chen, *A basis of* $\mathbb{Z}_m$, Colloq. Math. **104** (2006), 99-103.

[9] M. Tang and Y. G. Chen, *A basis of* $\mathbb{Z}_m$*,II*, Colloq. Math. **108** (2007), 141-145.

[10] M. Tang, *A note on a result of Ruzsa*, Bull. Austral. Math. Soc. **77** (2008), 91-98.