Journal of Mathematical Research & Exposition
May, 2010, Vol. 30, No. 3, pp. 557–561
DOI:10.3770/j.issn:1000-341X.2010.03.021
Http://jmre.dlut.edu.cn

The New Upper Bounds of Some Ruzsa Numbers R_m

Min TANG[1,*], Yong Gao CHEN[2]
1. *Department of Mathematics, Anhui Normal University, Anhui* 241000*, P. R. China;*
2. *Department of Mathematics, Nanjing Normal University, Jiangsu* 210097*, P. R. China*

Abstract For $A \subseteq \mathbf{Z}_m$ and $n \in \mathbf{Z}_m$, let $\sigma_A(n)$ be the number of solutions of equation $n = x+y, x, y \in A$. Given a positive integer m, let R_m be the least positive integer r such that there exists a set $A \subseteq \mathbf{Z}_m$ with $A + A = \mathbf{Z}_m$ and $\sigma_A(n) \leq r$. Recently, Chen Yonggao proved that all $R_m \leq 288$. In this paper, we obtain new upper bounds of some special type R_{kp^2}.

Keywords Erdős-Turán conjecture; additive bases; Ruzsa numbers.

Document code A
MR(2000) Subject Classification 11B13; 11B34
Chinese Library Classification O156.1

1. Introduction

Given a set $A \subset \mathbf{N}$, let $\sigma_A(n)$ be the number of ordered pairs $(a, a') \in A \times A$ such that $a + a' = n$. Erdős and Turán [4] conjectured that if $\sigma_A(n) \geq 1$ for all $n \geq n_0$, then $\sigma_A(n)$ must be unbounded. This conjecture has attracted much attention since 1941. To our regret, no serious advance has been made. Erdős-Turán conjecture seems to be extremely difficult. While this 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? Pŭs [6] first established that the analogue of Erdős-Turán conjecture fails to hold in some abelian groups. For related problems, see [2, 3, 5].

For $A, B \subseteq \mathbf{Z}_m$ and $n \in \mathbf{Z}_m$, let $\sigma_{A,B}(n)$ be the number of solutions of equation $n = x + y$, $x \in A$, $y \in B$. Let $\sigma_A(n) = \sigma_{A,A}(n)$. For each positive integer m, let Ruzsa number R_m be the least positive integer r such that there exists a set $A \subseteq \mathbf{Z}_m$ with $A + A = \mathbf{Z}_m$ and $\sigma_A(n) \leq r$. Based on Ruzsa's method [7], Tang and Chen [8] showed that the analogue of Erdős-Turán conjecture fails to hold in $(\mathbf{Z}_m, +)$, namely, for any sufficiently large integer m, $R_m \leq 768$. In [9], Tang and Chen showed that $R_m \leq 5120$ for any natural number m. Recently, Chen [1] improved the previous upper bounds to $R_m \leq 288$ for any positive integer m and $R_{2p^2} \leq 48$ for any prime p.

In this paper, the following results are proved.

Received November 5, 2008; Accepted May 16, 2009
Supported by the National Natural Science Foundation of China (Grant Nos. 10901002; 10771103).
* Corresponding author
E-mail address: tmzzz2000@163.com (M. TANG); ygchen@njnu.edu.cn (Y. G. CHEN)

Theorem *Let k be a positive integer, $p \geq 7$ be a prime, and let $T \subseteq \mathbf{Z}$ such that $T+T$ contains at least $k+1$ consecutive integers. Then*

$$R_{kp^2} \leq 16 \cdot \max_{0 \leq m \leq k-1} \sum_{w=-\infty}^{+\infty} \max\{\sigma_T(kw+m-1), \sigma_T(kw+m)\}.$$

Corollary 1 *Let $k \geq 2$ be a positive integer, $p \geq 7$ be a prime, and let $T \subseteq \{0, 1, 2, \ldots, k-1\}$ such that $T+T$ contains at least $k+1$ consecutive integers. Then*

$$R_{kp^2} \leq 16 \cdot \max_{0 \leq m \leq k-1} (\max\{\sigma_T(m-1), \sigma_T(m)\} + \max\{\sigma_T(k+m-1), \sigma_T(k+m)\}).$$

Corollary 2 *Let p be a prime. Then $R_{p^2} \leq 96$, $R_{4p^2} \leq 48$ and $R_{kp^2} \leq 64$ for $k = 3, 5, 6, 7, 8, 9, 10$.*

Remark 1 The method used here is based on Chen's method as in the proof of Theorem 1 [1]. By employing Corollary 1, we can find the new upper bounds of R_{kp^2} for some $k \geq 11$.

2. Proofs

For an integer k, let

$$Q_k = \{(u, ku^2) : u \in \mathbf{Z}_p\} \subseteq \mathbf{Z}_p^2.$$

Lemma ([1]) *Let p be an odd prime and m be a quadratic nonresidue of p with $m+1 \not\equiv 0 \pmod p$, $3m+1 \not\equiv 0 \pmod p$, $m+3 \not\equiv 0 \pmod p$. Put $B = Q_{m+1} \cup Q_{m(m+1)} \cup Q_{2m}$. Then for any $(c, d) \in \mathbf{Z}_p^2$ we have $1 \leq \sigma_B(c, d) \leq 16$, where $\sigma_B(c, d)$ is the number of solutions of the equation $(c, d) = x + y$, $x, y \in B$.*

Remark 2 By simple observation, we see that if $p = 3, 5$, there does not exist the corresponding m satisfying the above conditions. If $p = 7$, we can choose $m = 3$ or $m = 5$. Since the number of quadratic nonresidue of modulo p is $(p-1)/2 \geq 5$ for $p \geq 11$, there exists a quadratic nonresidue m such that $m+1 \not\equiv 0 \pmod p$, $3m+1 \not\equiv 0 \pmod p$, $m+3 \not\equiv 0 \pmod p$.

Proof of Theorem Assume that

$$\{l, l+1, \ldots, l+k\} \subseteq T+T.$$

In the following proofs, for $(u, v) \in B$ we always assume that $0 \leq u \leq p-1, 0 \leq v \leq p-1$.

For $n \in \mathbf{Z}_{kp^2}$, $0 \leq n \leq kp^2 - 1$, write $n = c + kpd$, $(l+1)p \leq c \leq (l+1+k)p - 1$, $c, d \in \mathbf{Z}$. By the lemma there exist $(u_1, v_1), (u_2, v_2) \in B$ such that

$$c \equiv u_1 + u_2 \pmod p, \quad d \equiv v_1 + v_2 \pmod p.$$

Put

$$c = u_1 + u_2 + sp, \ d = v_1 + v_2 + tp, \quad s, t \in \mathbf{Z}.$$

By $(l+1)p \leq c \leq (l+1+k)p - 1$ and $0 \leq u_1 + u_2 \leq 2p - 2$, we have

$$(l-1)p + 2 \leq sp \leq (l+1+k)p - 1.$$

So $l \leq s \leq l+k$. Since

$$\{l, l+1, \ldots, l+k\} \subseteq T+T,$$

there exist $t_1, t_2 \in T$ such that $s = t_1 + t_2$. Thus

$$\begin{aligned} n = c + kpd &\equiv u_1 + u_2 + sp + kpv_1 + kpv_2 \\ &\equiv (u_1 + kpv_1 + t_1p) + (u_2 + kpv_2 + t_2p) \pmod{kp^2}. \end{aligned}$$

Let

$$A_1 = \{u + kpv \,|\, (u, v) \in B\}, \quad A = \bigcup_{t \in T} (A_1 + tp),$$

where

$$A_1 + tp = \{a + tp \,|\, a \in A_1\}.$$

Then $\sigma_A(n) \geq 1$.

For $n \in \mathbf{Z}_{kp^2}$, by the definition of A, we have

$$\begin{aligned} \sigma_A(n) &\leq \sum_{t_1, t_2 \in T} \sigma_{A_1 + t_1p, A_1 + t_2p}(n) = \sum_{t_1, t_2 \in T} \sigma_{A_1}(n - (t_1 + t_2)p) \\ &= \sum_{t=-\infty}^{+\infty} \sigma_T(t) \sigma_{A_1}(n - tp). \end{aligned}$$

Write $n = c' + kpd'$, $0 \leq c' \leq kp - 1$, $0 \leq d' \leq p - 1$, $c', d' \in \mathbf{Z}$. Let $c' = mp + r$, $0 \leq r \leq p - 1$, $m, r \in \mathbf{Z}$. Then $0 \leq m \leq k - 1$.

Assume that $\sigma_{A_1}(n - tp) \geq 1$. Then there exist $(u_1, v_1), (u_2, v_2) \in B$ such that

$$n - tp \equiv u_1 + kpv_1 + u_2 + kpv_2 \pmod{kp^2}.$$

That is,

$$mp + r + kpd' - tp \equiv u_1 + kpv_1 + u_2 + kpv_2 \pmod{kp^2}. \tag{1}$$

Thus

$$r \equiv u_1 + u_2 \pmod{p}.$$

Since $0 \leq r$, u_1, $u_2 \leq p - 1$, we have $r = u_1 + u_2$ or $r = u_1 + u_2 - p$. If $r = u_1 + u_2$, then by (1) we have

$$m + kd' - t \equiv kv_1 + kv_2 \pmod{kp}. \tag{2}$$

Then $k | m - t$. Let $m - t = kw$. By (2) we have

$$d' + w \equiv v_1 + v_2 \pmod{p}.$$

If $r = u_1 + u_2 - p$, then by (1) we have

$$m - 1 + kd' - t \equiv kv_1 + kv_2 \pmod{kp}. \tag{3}$$

Then $k | m - 1 - t$. Let $m - 1 - t = kw'$. By (3) we have

$$d' + w' \equiv v_1 + v_2 \pmod{p}.$$

Hence, by the lemma we have

$$\sigma_A(n) \leq \sum_{w=-\infty}^{+\infty} \sigma_T(m - kw) \cdot \#\{r = u_1 + u_2, d' + w \equiv v_1 + v_2 \,(\mathrm{mod}\ p)\} +$$

$$\sum_{w'=-\infty}^{+\infty}\sigma_T(m-1-kw')\cdot\#\{r=u_1+u_2-p,d'+w'\equiv v_1+v_2\,(\mathrm{mod}\ p)\}$$
$$=\sum_{w=-\infty}^{+\infty}\sigma_T(m-kw)\cdot\#\{r=u_1+u_2,d'+w\equiv v_1+v_2\,(\mathrm{mod}\ p)\}+$$
$$\sum_{w=-\infty}^{+\infty}\sigma_T(m-1-kw)\cdot\#\{r=u_1+u_2-p,d'+w\equiv v_1+v_2\,(\mathrm{mod}\ p)\}$$
$$\leq\sum_{w=-\infty}^{+\infty}\max\{\sigma_T(m-kw),\sigma_T(m-1-kw)\}\sigma_B(r,d'+w)$$
$$\leq 16\sum_{w=-\infty}^{+\infty}\max\{\sigma_T(m-kw),\sigma_T(m-1-kw)\}$$
$$\leq 16\cdot\max_{0\leq m\leq k-1}\sum_{w=-\infty}^{+\infty}\max\{\sigma_T(kw+m-1),\sigma_T(kw+m)\}.$$

This completes the proof of the Theorem. □

Proof of Corollary 1 For any t_1, $t_2\in T$ we have $0\leq t_1+t_2\leq 2k-2$. So $\sigma_T(t)=0$ for $t<0$ or $t>2k-2$. Now Corollary 1 follows from Theorem immediately.

Proof of Corollary 2 If $k=1$, it is easy to verify $R_{p^2}\leq 96$ holds for $p=2,3,5$. As for $3\leq k\leq 10$, if $p=2,3,5$, let

$$A=\{0,1,2,\dots,p,2p,3p,\dots,(kp-1)p\}.$$

We have $1\leq\sigma_A(n)\leq(k+1)p-1$ for all $n\in\mathbf{Z}_{kp^2}$. Then $\sigma_A(n)\leq 48$ for $k\leq 8$ and $p=2,3,5$, and $\sigma_A(n)\leq 64$ for $k=9,10$ and $p=2,3,5$.

Now we assume that $p\geq 7$.

$k=1$.

Let $T=\{0,1\}$. Then $T+T=\{0,1,2\}$ and $\sigma_T(0)=1$, $\sigma_T(1)=2$, $\sigma_T(2)=1$. By Theorem we have $R_{p^2}\leq 96$.

$k=3,4$.

Let $T=\{0,1,2\}$. Then $T+T=\{0,1,2,3,4\}$ and $\sigma_T(0)=1$, $\sigma_T(1)=2$, $\sigma_T(2)=3$, $\sigma_T(3)=2$, $\sigma_T(4)=1$. By Corollary 1 we have $R_{3p^2}\leq 64$ and $R_{4p^2}\leq 48$.

$k=5,6$.

Let $T=\{0,1,2,3\}$. Then $T+T=\{0,1,2,3,4,5,6\}$ and $\sigma_T(0)=1$, $\sigma_T(1)=2$, $\sigma_T(2)=3$, $\sigma_T(3)=4$, $\sigma_T(4)=3$, $\sigma_T(5)=2$, $\sigma_T(6)=1$. By Corollary 1 we have $R_{kp^2}\leq 64$ $(k=5,6)$.

$k=7,8$.

Let $T=\{0,1,3,4\}$. Then $T+T=\{0,1,2,3,4,5,6,7,8\}$ and $\sigma_T(0)=1$, $\sigma_T(1)=2$, $\sigma_T(2)=1$, $\sigma_T(3)=2$, $\sigma_T(4)=4$, $\sigma_T(5)=2$, $\sigma_T(6)=1$, $\sigma_T(7)=2$, $\sigma_T(8)=1$. By Corollary 1 we have $R_{kp^2}\leq 64$ $(k=7,8)$.

$k=9,10$.

Let $T=\{0,1,3,4,5\}$. Then $T+T=\{0,1,2,3,4,5,6,7,8,9,10\}$ and $\sigma_T(0)=1$, $\sigma_T(1)=2$,

$\sigma_T(2) = 1$, $\sigma_T(3) = 2$, $\sigma_T(4) = 4$, $\sigma_T(5) = 4$, $\sigma_T(6) = 3$, $\sigma_T(7) = 2$, $\sigma_T(8) = 3$, $\sigma_T(9) = 2$, $\sigma_T(10) = 1$. By Corollary 1 we have $R_{kp^2} \leq 64$ $(k = 9, 10)$.

This completes the proof of Corollary 2. □

References

[1] CHEN Yonggao. *The analogue of Erdös-Turán conjecture in Z_m* [J]. J. Number Theory, 2008, **128**(9): 2573–2581.

[2] CHEN Yonggao. *A problem on unique representation bases* [J]. European J. Combin., 2007, **28**(1): 33–35.

[3] ERDÖS P. *On the multiplicative representation of integers* [J]. Israel J. Math., 1964, **2**: 251–261.

[4] ERDÖS P, TURÁN P. *On a problem of Sidon in additive number theory, and on some related problems* [J]. J. London Math. Soc., 1941, **16**: 212–215.

[5] NATHANSON M B. *Unique representation bases for the integers* [J]. Acta Arith., 2003, **108**(1): 1–8.

[6] PUŠ V. *On multiplicative bases in abelian groups* [J]. Czechoslovak Math. J., 1991, **41**(2): 282–287.

[7] RUZSA I Z. *A just basis* [J]. Monatsh. Math., 1990, **109**(2): 145–151.

[8] TANG Min, CHEN Yonggao. *A basis of $\mathbf{Z}_m$* [J]. Colloq. Math., 2006, **104**(1): 99–103.

[9] TANG Min, CHEN Yonggao. *A basis of $\mathbf{Z}_m$ (II)* [J]. Colloq. Math., 2007, **108**(1): 141–145.