DOUBLE AND TRIPLE SUMS MODULO A PRIME

KATALIN GYARMATI, SERGEI KONYAGIN, AND IMRE Z. RUZSA

Abstract. We study the connection between the sizes of $2A$ and $3A$ (twofold and threefold sums), where A is a set of residues modulo a prime p.

1. Introduction

Lev [3] observed that for a set A of integers the quantity

$$\frac{|kA|-1}{k}$$

is increasing. The first cases of this result assert that

$$|2A| \geq 2|A|-1 \tag{1.1}$$

and

$$|3A| \geq \frac{3}{2}|2A| - \frac{1}{2}. \tag{1.2}$$

Inequality (1.1) can be extended to different summands as

$$|A+B| \geq |A|+|B|-1, \tag{1.3}$$

and this inequality can be extended to sets of residues modulo a prime p, the only obstruction being that a cardinality cannot exceed p:

$$|A+B| \geq \min(|A|+|B|-1, p); \tag{1.4}$$

this familiar result is known as the Cauchy-Davenport inequality.

In this paper we deal with the possibility of extending inequality (1.2) to residues. We also have the obstruction at p, and the third author initially hoped that this is the only one, so an inequality like

$$|3A| \geq \min\left(\frac{3}{2}|2A| - \frac{1}{2}, p\right)$$

may hold; in particular, this would imply $3A = \mathbb{Z}_p$ for $|2A| > 2p/3$. M. Garaev asked (personal communication) whether this holds at least under the stronger assumption $|2A| > cp$ with some absolute constant $c < 1$. It turned out that the answer even to this question is negative, and the relationship between the sizes of $2A$ and $3A$ is seemingly complicated.

1991 *Mathematics Subject Classification.* 11B50, 11B75, 11P70.

Supported by Hungarian National Foundation for Scientific Research (OTKA), Grants No. T 43631, T 43623, T 49693.

Supported by the Russian Foundation for Basic Research, Grant 05-01-00066, and by Grant NSh-5813.2006.1.

Supported by Hungarian National Foundation for Scientific Research (OTKA), Grants No. T 43623, T 42750, K 61908.

Theorem 1.1. *Let p be a prime.*

(a) For every $m < \sqrt{p}/3$ there is a set $A \subset \mathbb{Z}_p$ such that $|3A| \le p - m^2$ and $|2A| \ge p - m(2\sqrt{p} - m + 3) - Cp^{1/4}$. Here C is a positive absolute constant.

(b) In particular, there is a set $A \subset \mathbb{Z}_p$ such that $3A \ne \mathbb{Z}_p$ and $|2A| \ge p - 2\sqrt{p} - Cp^{1/4}$.

Our positive results are as follows. (Since the structure of sumsets is trivial when the set has 1 or 2 elements, we assume $|A| \ge 3$.)

Theorem 1.2. *Let $p \ge 29$ be a prime, $A \subset \mathbb{Z}_p$, $|A| \ge 3$ and write $|2A| = n$, $|3A| = s$.*

(a) There is a positive absolute constant c such that for $n < cp$ we have

$$s \ge \frac{3n - 1}{2}.$$

(b) For $6 \le n < p/2$ we have $s > \sqrt{2}n$.

(c) If $n = (p + 1)/2$, then

$$s \ge \frac{3n - 1}{2} = \frac{3p + 1}{4}.$$

(d) For $n \ge (p + 3)/2$ we have

$$s \ge \frac{n(2p - n)}{p}.$$

(e) If $n > p - \sqrt{2p} + 2$, then $3A = \mathbb{Z}_p$.

A drawback of this theorem is the discontinuous nature of the bounds in (a)–(b)–(c). It is possible to modify the argument in the proof of (c) to get a continuously deteriorating bound for n just below $p/2$, but it is hardly worth the trouble. It is unlikely that the actual behaviour of $\min s$ changes in this interval, so it seems safe to conjecture the following.

Conjecture 1.3. If $n \le (p + 1)/2$, then $s \ge (3n - 1)/2$.

To find the smallest value of n provided by Theorem 1.1 for which $s < (3n - 1)/2$ can happen we have to solve a quadratic inequality for m. This gives $m \approx \sqrt{p}/5$ and $n \approx 16p/25$.

Theorem 1.1 and part (d) of Theorem 1.2 describe the quadratic connection between n and s for large values of n. Indeed, (d) can be reformulated as follows: if $s \le p - m^2$, then $n \le p - m\sqrt{p}$, thus the difference is the coefficient 1 or 2 of $m\sqrt{p}$. Similarly, the theorems locate the point after which necessarily $3A = \mathbb{Z}_p$ between $p - 2\sqrt{p}$ and $p - \sqrt{2p}$. We do not have a plausible conjecture about the correct coefficient of $\sqrt{p}$ in these results.

2. Construction

We prove Theorem 1.1.

Without loss of generality we may assume that p is large enough.

We will use the integers $0, \dots, p-1$ to represent the residues modulo p. We will write $[a, b]$ to denote a discrete interval, that is, the set of integers $a \le i \le b$.

Take an integer $q \sim \sqrt{p}$, and write $p = qt + r$ with $1 \le r \le q - 1$. We will consider sets of the form $A = K \cup L$, where

$$K = [0, k - 1],\ |K| = k \le q - 1$$

and

$$L = \{0, q, 2q, \dots, (l-1)q\}, \ |L| = l \le t-1.$$

Our parameters will satisfy $k > q/2 + 3$ and $l \ge 2t/3 + 2$. We assume that $t > 6$.

All the sums $x + y$, $x \in K$, $y \in L$ are distinct and hence we have

$$|2A| \ge |K + L| = kl.$$

It would not be difficult to calculate $|2A|$ more exactly, but it would only minimally affect the final result.

The set $3A$ is the union of $3K$, $2K + L$, $K + 2L$ and $3L$. We consider $2K + L$ first. We have $2K = [0, 2k-2]$. Since $2k - 2 > q$, the sets $2K$, $2K + q$, ... overlap and we have

$$2K + L = [0, q(l-1) + 2k - 2] = [0, ql + (2k - 2 - q)].$$

So $3A$ contains $[0, ql]$ and we will study in detail the structure in $[ql, p-1]$.

We have $3K \subset [0, 3q]$, so we do not get any new element (assuming $l \ge 3$).

Now we study $K + 2L$. The set $2L$ contains $0, q, \dots, qt$ and then $q(t+1) - p = q - r, 2q - r, \dots, q(2l-2) - p = q(2l-2-t) - r$. By adding the set K to the second type of elements we get numbers in

$$[0, q(2l-1-t)] \subset [0, ql],$$

so no new elements again. By adding K to iq we stay in $[0, ql]$ as long as $i \le l-1$, and for $l \le i \le t$ we get

$$[ql, ql+k-1] \cup [(l+1)q, (l+1)q+k-1] \cup \cdots \cup [(t-1)q, (t-1)q+k-1] \cup [qt, qt+\min(k-1, r)].$$

If $r \le k-1$, the last of the above intervals covers $[qt, p]$, so we can restrict our attention to $[ql, qt-1]$. If $r > k-1$, then some elements near $p-1$ may not be in $K + 2L$, but as $r \le k-1$ will typically hold in our choice, we will not try to exploit this possible gain. Note that the final segment of $2K + L$, that is, $[ql, ql + (2k-2-q)]$ is contained in the first of the above intervals.

Finally $3L$ consists of elements of the form $iq - jp$, where $0 \le i \le 3l-3$ and $0 \le j \le 2$. Those with $j = 0$ are already listed above. Those with $j = 2$ are in $[0, ql]$, so no new element. Finally with $j = 1$ we have $iq - p = (i-t)q - r$ with $t+1 \le i \le 2t$, and also with $i = 2t+1$ if $r > q/2$. Among these elements the possible new ones are

$$(l+1)q - r, (l+2)q - r, \dots, (t+1)q - r.$$

This gives no new element if

$$r \ge q - k + 1. \tag{2.1}$$

So under this additional assumption the intervals $[iq + k, iq + q - 1]$ are disjoint to $3A$ for $l \le i \le t-1$, and this gives

$$|3A| \le p - (t-l)(q-k).$$

For a given m we will take $l = t - m$, $k = q - m$, hence the bound $|3A| \le p - m^2$. With this choice we have

$$|2A| \ge kl = (q-m)(t-m) = p - m(q + t - m) - r. \tag{2.2}$$

Now we select q, t and r. Define the integer v by

$$(v-1)^2 < p < v^2,$$

and write $p = v^2 - w$, $0 < w < 2v$. With arbitrary i we have

$$p = (v - i)(v + i) + (i^2 - w).$$

Hence $q = v - i$, $t = v + i$ and $r = i^2 - w$ may be a good choice. We have a lower bound for r given by (2.1), which now reads $r \geq m + 1$, but otherwise the smaller the value of r the better the bound on $2A$ in (2.2), so we take

$$i = 1 + \left[\sqrt{w + m + 1}\right].$$

Then $r = m + O(\sqrt{w + m + 1}) = m + O(p^{1/4})$. Since $q + t = 2v < 2\sqrt{p} + 2$, (2.2) yields the bound in part (a) of Theorem 1.1.

3. Estimates

Here we prove Theorem 1.2.

We will assume that $0 \in A$ and consequently $A \subset 2A$, since this can be achieved by a translation which does not affect the studied cardinalities.

The proof will be based on certain Plünnecke-type estimates. These will be quoted from [5]; the basic ideas go back to Plünnecke [4].

Proof of (a).

Lemma 3.1. *Let $i < h$ be integers, U, V sets in a commutative group and write $|U| = m$, $|U + iV| = \alpha m$. We have*

$$|hV| \leq \alpha^{h/i} m.$$

This is Corollary 2.4 of [5].

Take a set $A \subset \mathbb{Z}_p$ such that $|2A| = n$, $|3A| = s$ and $s < 3n/2$. We apply the above lemma with $i = 1$, $h = 4$, $U = 2A$, $V = A$. We get

$$|4V| < (3/2)^4 \, |U| .$$

Since $4V = 4A = 2U$, this means that the set $U = 2A$ has a small doubling property, namely $|2U| < (81/16)\, |U|$, and this permits us to "rectify" it. There are several ways to do this; the most comfortable is the following form, taken from [1], Theorem 1.2, with some change in the notation.

Lemma 3.2. *Let p be a prime and let $U \subseteq \mathbb{Z}/p\mathbb{Z}$ be a set with $|U| = \delta p$ and $\min(|2U|, |U - U|) = \alpha |U|$. Suppose that $\delta \leq (16\alpha)^{-12\alpha^2}$. Then the diameter of U is at most*

$$12\delta^{1/4\alpha^2}\sqrt{\log(1/\delta)}p. \tag{3.1}$$

The *diameter* in the above lemma is the length of the shortest arithmetical progression containing the set. We apply this lemma for our set $U = 2A$. We fix $\alpha = 81/16$ and select c so that for $\delta \leq c$ the bound in (3.1) be $< p/4$, and it should include the upper bound imposed on δ. (Actually the second requirement is stronger and it gives the value $c = 2^{-3^9/2^4}$.) This will be the constant c in (a) of the theorem.

The lemma yields that $A \subset 2A \subset \{-kd, -(k-1)d, \ldots, -d, 0, d, 2d, \ldots, ld\}$ with a suitable d and integers k, l such that $k + l < p/4$. Let

$$A' = \{j : -k \leq j \leq l, jd \in A\}.$$

Then $4A' \subset [-4k, 4l]$, still an interval of length $< p$, hence $|4A| = |4A'|$ and the claim follows from Lev's result (1.2) on sets of integers. $\square$

Proof of (b).

Lemma 3.3. *Let $U, V \subset \mathbb{Z}_p$, $|U| \geq 2$, $|V| \geq 2$, $|U| + |V| \leq p - 1$. Then either $|U + V| \geq |U| + |V|$, or U, V are arithmetic progressions with a common difference.*

This is the Cauchy-Davenport inequality with Vosper's description of the extremal pairs incorporated; see e. g. [2].

Lemma 3.4. *If $A \subset \mathbb{Z}_p$ and $2A$ is an arithmetic progression, then $s \geq \min(p, (3n - 1)/2)$.*

Proof. First, use a dilation to make the difference of the arithmetic progression 1, and then a translation to achieve $0 \in A$; these transformations do not change the size of our sets. In this case $A \subset 2A$, so we can write

$$2A = \{k, k+1, \ldots, -1, 0, 1, \ldots, l\}, \ k \leq 0 \leq l, \ l - k = n - 1.$$

Let the first and last elements of A (in the list above) be a and b. We have $k \leq a \leq 0 \leq b \leq l$. Furthermore $2A \subset [2a, 2b]$, that is, $n = |2A| \leq 2(b-a)+1$ and so $b-a \geq (n-1)/2$. Now $3A$ contains the residue of every integer in the set

$$[k, l] + \{a, b\} = [k + a, l + b],$$

an interval of length $l + b - k - a \geq 3(n-1)/2$ (to see that it is an interval observe that $l + a \geq k + b$), hence its cardinality is at least the cardinality of this interval or p. □

Lemma 3.4 allows us to prove slightly stronger results than we would obtain by applying the Cauchy-Davenport inequality directly, the main benefit being that the statements of the results become simpler.

Lemma 3.5. *Let $i < h$ be integers, U, V sets in a commutative group and write $|U| = m$, $|U + iV| = \alpha m$. There is an $X \subset U$, $X \neq \emptyset$ such that*

$$|X + hV| \leq \alpha^{h/i}|X|.$$

This is Theorem 2.3 of [5].

Now we prove part (b). We apply the above lemma with $i = 1$, $h = 2$ for $U = 2A$, $V = A$, so that $\alpha = s/n$. We get that there is a nonempty $X \subset 2A$ such that

$$|X + 2A| \leq \alpha^2 |X|. \tag{3.2}$$

We will now apply Lemma 3.3 to the sets X and $2A$. To check the conditions observe that $|X| + |2A| \leq 2n \leq p - 1$. The condition $|X| \geq 2$ may not hold. If it fails, then (3.2) reduces to $n \leq \alpha^2$ and hence $\alpha \geq \sqrt{2}$. If $2A$ is an arithmetic progression, then we get (b) by Lemma 3.4. If none of these happens, then by Lemma 3.3 we know that $|X + 2A| \geq |X| + n$, and then (3.2) can be rearranged as

$$n \leq (\alpha^2 - 1)\,|X| \leq (\alpha^2 - 1)n,$$

that is, $\alpha \geq \sqrt{2}$ as claimed. □

Proof of (e). If $3A \neq \mathbb{Z}_p$, then $|2A| + |A| \leq p$ (by the Cauchy-Davenport inequality, or by an appropriate application of the pigeonhole principle). Write $|A| = m$. We have $n \leq m(m+1)/2$, hence $m \geq \sqrt{2n} - 1/2$ and the previous inequality implies $n + \sqrt{2n} \leq p + 1/2$. By solving this as a quadratic inequality for $\sqrt{n}$ we obtain

$$n \leq p - \sqrt{2p + 2} + \frac{3}{2} < p - \sqrt{2p} + 2.$$

□

Proof of (c) and (d). We will prove that

$$s \geq \min\left(\frac{3n-1}{2}, \frac{n(2p-n)}{p}\right),$$

which implies both (c) and (d). Indeed, observe that the bound in (c), $(3n-1)/2$, is smaller than the bound $n(2p-n)/p$ in (d) for $n = (p+1)/2$ and it is larger otherwise.

If $s = p$, we are done. If $s = p-1$, then from part (e) we get that $n < p - \sqrt{2p} + 2 < p - \sqrt{p}$ and then $n(2p-n)/p < p-1$, and again we are done. So assume $s \leq p-2$.

Lemma 3.6. *Let $i < h$ be positive integers, U, V, W sets in a commutative group and write $|U| = m$, $|(U + iV) \setminus (W + (i-1)V)| \leq \beta m$. There is an $X \subset U$, $X \neq \emptyset$ such that*

$$|(X + hV) \setminus (W + (h-1)V)| \leq \beta^{h/i}|X|.$$

This is Theorem 2.8 of [5].

Lemma 3.7. *Let U, V be sets in a commutative group and write $|U| = m$, $|U + V| \leq \alpha m$. There is an $X \subset U$, $X \neq \emptyset$ such that*

$$|X + 2V| \leq \alpha m + (\alpha - 1)^2 |X|.$$

Proof. We apply the previous lemma with $i = 1$, $h = 2$, $W = U + v$ with an arbitrary $v \in V$; clearly $\beta = \alpha - 1$. We obtain the existence of an $X \subset U$, $X \neq \emptyset$ such that

$$|(X + 2V) \setminus (U + V + v)| \leq (\alpha - 1)^2 |X|.$$

The claim follows by observing that $|U + V + v| \leq \alpha m$. □

Consider the set $D = \mathbb{Z}_p \setminus (-3A)$. We have $m = |D| = p - s \geq 2$. The set $D + A$ is disjoint to $-2A$, hence $|D + A| \leq p - n$. We apply the previous lemma with $U = D$, $V = A$ and $\alpha = (p-n)/(p-s)$. We obtain the existence of a nonempty $X \subset D$ such that

$$|X + 2A| \leq p - n + (\alpha - 1)^2 |X|. \tag{3.3}$$

We have $|X| + |2A| \leq p - s + n \leq p - 1$. By lemma 3.3 either we have

$$|X + 2A| \geq |X| + |2A|, \tag{3.4}$$

or $|X| = 1$, or $2A$ is an arithmetic progression. In the last case the claim follows from Lemma 3.4, since $n(2n-p)/p < (3n-1)/2$ for $n > (p+1)/2$.

If (3.4) holds, then (3.3) implies

$$2n - p \leq \alpha(\alpha - 2)\,|X|\,. \tag{3.5}$$

Since the left side is positive, so is the right side, that is, necessarily $\alpha \geq 2$, and then using that $|X| \leq |D| = p - s$, (3.5) becomes

$$2n - p \leq \alpha(\alpha - 2)(p - s). \tag{3.6}$$

Substituting $\alpha = (p-n)/(p-s)$ and $\alpha - 2 = (2s - n - p)/(p - s)$ this becomes

$$(2n - p)(p - s) \leq (p - n)(2s - n - p)$$

which can be rearranged to give the bound in (d).

If (3.4) fails, then $|X| = 1$ and (3.3) becomes

$$2n - p \leq (\alpha - 1)^2. \tag{3.7}$$

If α is such that $(\alpha-1)^2 \le 2\alpha(\alpha-2)$, then, as $p-s \ge 2$, (3.6) holds again and we complete the proof as before. If this is not the case, then $\alpha < 1+\sqrt{2}$, and (3.7) yields $2n-p<2$. Since p is odd, this leaves the only possibility $n=(p+1)/2$. Now (3.7) becomes $\alpha \ge 2$, that is, $p-n \ge 2(p-s)$,

$$s \ge \frac{p+n}{2} = \frac{3p+1}{4}$$

as wanted.

□

Acknowledgement. The authors are grateful to a referee for remarks and corrections.

References

[1] B. Green and I. Z. Ruzsa, *Sets with small sumsets and rectification*, Bull. London Math. Soc. **38** (2006), 43–52.
[2] K. F Halberstam, H.; Roth, *Sequences*, Clarendon, London, 1966, 2nd ed. Springer, 1983.
[3] V. F. Lev, *Structure theorem for multiple addition and the Frobenius problem*, J. Number Theory **58** (1996), 79–88.
[4] H. Plünnecke, *Eine zahlentheoretische anwendung der graphtheorie*, J. Reine Angew. Math. **243** (1970), 171–183.
[5] I. Z. Ruzsa, *Cardinality questions about sumsets*, Montréal school on combinatorial number theory, to appear.

Alfréd Rényi Institute of Mathematics, Budapest, Pf. 127, H-1364 Hungary
E-mail address: gykati@cs.elte.hu

Department of Mechanics and Mathematics, Moscow State University, Moscow, 119992, Russia
E-mail address: konyagin@ok.ru

Alfréd Rényi Institute of Mathematics, Budapest, Pf. 127, H-1364 Hungary
E-mail address: ruzsa@renyi.hu