Counting Sumsets and Sum-Free Sets, I

Ben Green[1] and Imre Z. Ruzsa

1. Introduction. Let p be a prime number and write $\mathbf{Z}_p$ for the group of residues modulo p. Write $\mathrm{SF}(\mathbf{Z}_p)$ for the collection of all sum-free subsets of $\mathbf{Z}_p$, by which we mean sets $A \subset \mathbf{Z}_p$ for which $(A+A) \cap A = \emptyset$. Equivalently, A is sumfree if there are no solutions to $x+y=z$ with $x, y, z \in A$. The question of estimating $|\mathrm{SF}(\mathbf{Z}_p)|$ was addressed in [4] and [5]. In [5] the following result was proved:

Theorem 1 (Lev, Schoen) *Let p be a sufficiently large prime. Then we have*

$$p2^{\lfloor \frac{p-2}{3} \rfloor}(1+o(1)) \leq |\mathrm{SF}(\mathbf{Z}_p)| \leq 2^{0.498p}.$$

Another rather natural enumeration problem does not seem to have been considered in the literature. Write $\mathrm{SS}(\mathbf{Z}_p)$ for the collection of sumsets in $\mathbf{Z}_p$, that is to say sets $A \subset \mathbf{Z}_p$ which are exactly equal to $B+B$ for some $B \subset \mathbf{Z}_p$. Jacques Verstrate asked the first author to estimate $|\mathrm{SS}(\mathbf{Z}_p)|$.

The objective of this paper is to prove the following theorem, which improves on the upper bound of Lev and Schoen and goes some distance towards answering the question of Verstrate.

Theorem 2 *Let p be prime. Then we have*

(i) $|\mathrm{SF}(\mathbf{Z}_p)| \leq 2^{p/3+\kappa(p)}$;

(ii) $p^2 2^{p/3} \ll |\mathrm{SS}(\mathbf{Z}_p)| \leq 2^{p/3+\kappa(p)}$

where $\kappa(p)/p \to 0$ as $p \to \infty$ and in fact we can take

$$\kappa(p) \ll p(\log\log p)^{2/3}(\log p)^{-1/9}.$$

2. Granular structure of sets. In this section we will state and prove a proposition which is central to our argument. Before doing so we introduce some notation. If $f : \mathbf{Z}_p \to \mathbf{R}$ is a function and $n \in \mathbf{Z}_p$ then write $r(f,n)$ for the autoconvolution $\sum_m f(m)f(n-m)$. In the special case that $s = \chi_S$ is the characteristic function of a set, $r(s,n)$ is the number of ordered pairs $(s_1, s_2) \in S^2$ with $s_1 + s_2 = n$. In the proposition there will be sets A, A' and A_1; we use the letters a, a' and a_1 respectively to denote their characteristic functions.

Finally, let L be a positive integer and consider the partition of $\mathbf{Z}_p$ into intervals $J_i =$

[1]The first author is supported by a grant from the Engineering and Physical Sciences Research Council of the UK and a Fellowship of Trinity College Cambridge.

$\{iL+1,\dots,(i+1)L\}$ of length exactly L together with a leftover interval J of length less than L. We say that a set $B \subset \mathbf{Z}_p$ is *L-granular* if some dilate of B is a union of some of the intervals J_i.

Proposition 3 *Let $A \subseteq \mathbf{Z}_p$ have size αp, let $\varepsilon_1, \varepsilon_2, \varepsilon_3$ be positive real numbers and L a positive integer. Suppose that*

$$p \;>\; (4L)^{256\alpha^2\varepsilon_1^{-4}\varepsilon_2^{-2}\varepsilon_3^{-1}}.$$

Then there is a set $A' \subset \mathbf{Z}_p$ with the following properties:

(i) $|A \setminus A'| \;\leq\; \varepsilon_1 p$;

(ii) $A+A$ *contains all x for which $r(a',x) \geq \varepsilon_2 p$, with at most $\varepsilon_3 p$ exceptions;*

(iii) A' *is L-granular.*

Proof. Let f be the Fourier transform of the characteristic function of A, so that

$$f(x) \;=\; \sum_{n\in A} e(nx/p)$$

for all $x \in \mathbf{Z}_p$. Take a small positive δ (our choice will be $\delta = \frac{1}{16}\varepsilon_1^2\varepsilon_2\varepsilon_3^{1/2}\alpha^{-1/2}$). Let R, $|R| = k$, be the set of all $r \neq 0$ for which $|f(r)| \geq \delta p$. We will find a $d \in \mathbf{Z}_p^\times$ such that the function

$$g(x) = \frac{1}{2L-1}\sum_{j=-(L-1)}^{L-1} e(jdx/p)$$

satisfies

$$|f(x)||1-g(x)^2| \;\leq\; \delta p \tag{1}$$

for all x. This automatically holds for $x=0$, as $g(x)=1$, and also whenever $|f(x)| \leq \delta p$, since $g(x) \in [-1,1]$. We will now select d so that (1) holds for the remainder of $\mathbf{Z}_p$, which is to say the elements of R.

For any $x \in \mathbf{Z}_p$ we may estimate $1-g(x)$ as follows. Writing $\|t\|$ for the distance of t from the nearest integer we have the inequality $1-\cos 2\pi t \leq 2\pi^2\|t\|^2$. It follows that

$$\begin{aligned}
1-g(x) \;&=\; \frac{2}{2L-1}\sum_{j=1}^{L-1}\left(1-\cos\frac{2\pi jdx}{p}\right)\\
&\leq\; \frac{4\pi^2}{2L-1}\sum_{j=1}^{L-1}\left\|\frac{jdx}{p}\right\|^2\\
&\leq\; \frac{4\pi^2}{2L-1}\left\|\frac{dx}{p}\right\|^2\sum_{j=1}^{L-1} j^2\\
&\leq\; \frac{2\pi^2L^2}{3}\left\|\frac{dx}{p}\right\|^2. \qquad (2)
\end{aligned}$$

Hence

$$\begin{aligned} |f(x)||1-g(x)^2| &\leq 2|f(x)||1-g(x)| \\ &\leq 14L^2||dx/p||^2|f(x)| \end{aligned}$$

and so, by our earlier remarks, a sufficient condition for (1) to hold is that

$$||dr/p|| \leq \frac{1}{4L}\left(\frac{\delta p}{|f(r)|}\right)^{1/2}$$

for all $r \in R$. It follows by a standard application of the pigeonhole principle that such a d exists if

$$p > (4L)^k \left(\prod_{r\in R} \frac{|f(r)|}{\delta p}\right)^{1/2}. \tag{3}$$

We claim that this inequality is a consequence of the hypothesis on $p, L, \varepsilon_1, \varepsilon_2$ and ε_3 in the statement of the proposition. Indeed, observe that Parseval's identity implies that

$$\sum_{r\in R} |f(r)|^2 \leq \alpha p^2, \tag{4}$$

from which the arithmetic-geometric mean inequality gives

$$\prod_{r\in R} |f(r)| \leq \left(\frac{\alpha p^2}{k}\right)^{k/2}.$$

It follows that the right side of (3) is at most

$$(4L\alpha^{1/4}\delta^{-1/2}k^{-1/4})^k, \tag{5}$$

which is an increasing function of k in the range $k < \left(\frac{256L^4}{e}\right)\frac{\alpha}{\delta^2}$. However another consequence of (4) is the inequality $k < \alpha/\delta^2$, and hence (5) is itself bounded above by $(4L)^{\alpha/\delta^2}$. Recalling our choice of δ confirms the claim, and hence there is a d for which (1) holds.

By dilating A if necessary we may assume that $d = 1$. Recall that we partitioned $\mathbf{Z}_p$ into intervals $J_1, \ldots, J_m$ of length exactly L together with a leftover interval J of length less than L. Define A' to be the union of all the J_i for which $|A \cap J_i| \geq \varepsilon_1 L/2$. Property (iii) of the proposition follows immediately from this definition. The remainder of the proof consists in checking properties (i) and (ii).

We begin with property (i). If $x \in A \setminus A'$ then either $x \in J$ or else $|A \cap J_i| \leq \varepsilon_1 L/2$, where $x \in J_i$. For each i there clearly cannot be more than $\varepsilon_1 L/2$ points $x \in A$ with the latter property, and so we estimate

$$\begin{aligned} |A \setminus A'| &\leq \tfrac{1}{2}\varepsilon_1 p + L \\ &\leq \varepsilon_1 p. \end{aligned}$$

To establish property (ii) we define a function a_1 by

$$a_1(n) \;=\; \frac{1}{|P|}(a*\chi_P)(n) \;=\; \frac{1}{|P|}|A\cap(P+n)|,$$

where $P=\{-(L-1),...,L-1\}$. Observe that the Fourier transform of a_1, f_1, is equal to the product of f and g. Thus we have, by two applications of Parseval, that

$$\begin{aligned}\sum_n |r(a,n)-r(a_1,n)|^2 &= p^{-1}\sum_x \left|f(x)^2-f_1(x)^2\right|^2\\ &= p^{-1}\sum_x |f(x)|^4\left(1-g(x)^2\right)^2\\ &\le p^{-1}\left(\sup_x |f(x)||1-g(x)^2|\right)^2\sum_x |f(x)|^2\\ &= \alpha p\left(\sup_x |f(x)||1-g(x)^2|\right)^2. \qquad (6)\end{aligned}$$

(1) therefore implies that

$$\sum_n |r(a,n)-r(a_1,n)|^2 \;\le\; \alpha\delta^2p^3. \qquad (7)$$

Now if $n\in A'$ then there is an interval of length L containing n (and hence contained in $[n-(L-1),n+(L-1)]$) which contains at least $\varepsilon_1L/2$ points of A. Hence $a_1(n)$ is certainly at least $\varepsilon_1/4$, and so $a_1(n)\ge\varepsilon_1a(n)/4$ for all values of n. It follows immediately that $r(a_1,n)\ge\varepsilon_1^2r(a,n)/16$ for all n, and hence that if $r(a,n)\ge\varepsilon_2p$ then $r(a_1,n)\ge\varepsilon_1^2\varepsilon_2p/16$. We are to show that there are not many points n for which this is true whilst $r(a,n)=0$. Letting B denote the set of these "bad" points, observe that $n\in B$ implies that

$$|r(a,n)-r(a_1,n)|^2 \;\ge\; \frac{\varepsilon_1^4\varepsilon_2^2p^2}{256}.$$

Substituting into (7) gives the bound

$$|B| \;\le\; \frac{256\alpha\delta^2}{\varepsilon_1^4\varepsilon_2^2}p \;\le\; \varepsilon_3p$$

(this explains our choice of δ). This is property (ii). □

3. A corollary to a theorem of Pollard. The object of this section is to prove Proposition 5. This proposition is a simple corollary of the following theorem of Pollard [6].

Theorem 4 (Pollard) *Let $B\subset\mathbf{Z}_p$, and let N_r, $1\le r\le|B|$, denote the number of elements $n\in\mathbf{Z}_p$ for which $r(B,n)\ge r$. Then*

$$N_1+\ldots+N_r \;\ge\; r(\min(p,2|B|)-r).$$

Proposition 5 *Let $B \subset \mathbf{Z}_p$ have cardinality at most $p/2$. Let K be a positive integer, and write $S_K(B) = \{n : r(B,n) \geq K\}$ for the set of K-popular sums in $B+B$. Then $|S_K(B)| \geq \min(2|B|, p) - 2\sqrt{Kp}$.*

Proof. In the notation of Theorem4, we have $N_j \leq |S_K(B)|$ for $j \geq K$. Thus, if $r \geq K$, we have

$$r(\min(2|B|, p) - r) \ \leq \ N_1 + \ldots + N_r \ \leq \ Kp + |S_K(B)|r.$$

Taking $r = \sqrt{Kp}$ gives the bound claimed. □

4. Proof of Theorem2. Upper bounds. We are now in a position to derive the upper bounds in Theorem 2. We begin with the upper bound for $|\mathrm{SF}(\mathbf{Z}_p)|$. Observe, first of all, that the number of subsets of $\mathbf{Z}_p$ having cardinality at most $p/17$ is $O(2^{p/3})$. Let us therefore assume that $A \subset \mathbf{Z}_p$ is sumfree and that $|A| \geq p/17$. Letting $\varepsilon_1, \varepsilon_2, \varepsilon_3$ be positive reals and L a positive integer to be chosen later we may, for p sufficiently large, apply Proposition 3 to get a set A' satisfying the conclusions of that proposition. We will count sumfree sets A by counting pairs (A', A). It is not hard to see that

$$\text{number of choices for } A' \ \leq \ p2^{p/L}.$$

Supposing now that A' is given we consider seperately the two cases $|A'| \geq p/3$ and $|A'| < p/3$. In the first case we use Proposition 3(ii), which says that $A + A$ contains $S_{\varepsilon_2 p}(A')$, with the exception of at most $\varepsilon_3 p$ points. Since A is sumfree, this means that A must be a subset of $S_{\varepsilon_2 p}(A')^c$ together with at most $\varepsilon_3 p$ points. Proposition 5 tells us that

$$|S_{\varepsilon_2 p}(A')| \ \geq \ \min(2|A'|, p) - 2\varepsilon_2^{1/2} p \ \geq \ \frac{2p}{3} - 2\varepsilon_2^{1/2} p.$$

Thus, if $|A'| \geq p/3$,

$$\text{number of choices for } A \ \leq \ 2^{p/3} \exp\left(C\left(\varepsilon_2^{1/2} + \varepsilon_3 \log(1/\varepsilon_3)\right) p\right).$$

If $|A'| < p/3$ things are easier. Proposition 3(i) tells us that A is a subset of A' together with at most $\varepsilon_1 p$ extra points. Thus in this case

$$\text{number of choices for} A \ \leq \ 2^{p/3} \exp\left(C\varepsilon_1 \log(1/\varepsilon_1) p\right).$$

Hence if Proposition 3 applies with $\varepsilon_1 = \varepsilon_3 = \epsilon/\log(1/\epsilon)$, $\varepsilon_2 = \varepsilon^2$ and $L = 1 + [1/\varepsilon]$, then we have the bound

$$|\mathrm{SF}(\mathbf{Z}_p)| \ \leq \ 2^{p/3 + C\varepsilon p}.$$

A short calculation confirms that we can take $\varepsilon = O\left((\log\log p)^{2/3} (\log p)^{-1/9}\right)$.

Slightly suprisingly the proof of the upper bound for $|\mathrm{SS}(\mathbf{Z}_p)|$ is almost identical. The only

difference is that in the case $|A'| \geq p/3$ we use the fact that $(A+A)^c$ must be a subset of $S_{\varepsilon_2 p}(A')^c$ together with at most $\varepsilon_3 p$ points, and observe that sumsets $X+X$ and their complements $(X+X)^c$ are in 1-1 correspondence. This completes the proof of the upper bound part of Theorem 2. $\Box$

5. A lower bound for $|\mathrm{SS}(\mathbf{Z}_p)|$. In this section we prove the lower bound in Theorem2. We do not give a lower bound for $|\mathrm{SF}(\mathbf{Z}_p)|$ as this has already been done in [5] and we do not see how to improve on it.

Lemma 6 *Let p be large. Let P_1, P_2 be two arithmetic progressions in $\mathbf{Z}_p$ with length $L = \lfloor \frac{p}{3} \rfloor$ and common differences d_1, d_2. Suppose that $d_1 \neq \pm d_2$. Then $|P_1 \cap P_2| \leq p/4 + 4$.*

Proof. Without loss of generality we may take $P_1 = \{0, 1, \ldots, L-1\}$ and $P_2 = \{a, a+d, \ldots, a+(L-1)d\}$, where $2 \leq d \leq p/2$. Colour each $\lambda \in \{0, \ldots, L-1\}$ red or blue according to whether $a + \lambda d \in P_1$ or not. This divides $\{0, \ldots, L-1\}$ into monochromatic strings. The length of each red string is at most $N_1 = \lceil L/d \rceil$, and that of each blue string is at least $N_2 = \lfloor (p-L)/d \rfloor$. $|P_1 \cap P_2|$ is the number of red elements, and we can bound this above by partitioning into consecutive red/blue blocks. Allowing for the possibility that both end blocks may be red we have

$$|P_1 \cap P_2| \;\leq\; \frac{N_1 L}{N_1 + N_2} + N_1. \tag{8}$$

Observe that $N_1 \leq N_2$. Indeed if this is not the case then $(p-L)/d < L/d + 1$. If $L < p/4$ this is impossible, so we must have $L \in [p/4, p/3]$ and $d \geq p - 2L \geq p/3$. Thus $N_1 = 1$, and we must have $N_2 = 0$. This, however, is also impossible.

It follows that $N_1/(N_1+N_2) \leq 1/2$, and so if $N_1 \leq p/12 + 1$ the result is immediate from(8). If $N_1 \geq p/12 + 1$ then we must have $d = 2, 3$ or 4. These cases are easy to check by hand. $\Box$

Remark. A much more precise result than this could be obtained, but some quite tedious calculations would almost certainly be required.

Let $L = \lfloor p/3 \rfloor - 1$, and let $P = \{a+d, a+2d, \ldots, a+2Ld\}$ be an arithmetic progression of length $2L$. We say that a set $X \subset \mathbf{Z}_p$ *exactly contains* P if $P \subset X$ but neither of the points a or $a + (2L+1)d$ lie in X.

Lemma 7 *Let P be any progression of length $2L$. Then there are at least $c2^{p/3}$ sets of the form $A + A$ which exactly contain P.*

Proof. By dilating and translating we may assume that $P = \{1, \ldots, 2L\}$. All of our sets A will be of the form $B \cup \{2L+1\}$, where $B \subset [L] = \{1, \ldots, L\}$. Observe that distinct sets B give rise to distinct sumsets $A + A$, and that $A + A$ never contains either 0 or $2L+1$. We will show that there are many choices of B for which $A + A$ contains P.

Choose a set B by including the elements $1, 2, \ldots, 14$ and $L-13, \ldots, L-1, L$ automatically and picking every element in $\{15, \ldots, L-14\}$ independently at random with probability $1/2$. The elements $2, 3, \ldots, 28$ and $2L-26, \ldots, 2L$ all lie in $B+B$. Let $x \in \{29, \ldots, L\}$. Then, with an obvious abuse of notation, there are at least $\lfloor x/2 \rfloor$ disjoint pairs $(u, v) \in [L]^2$ with $u+v=x$. Thus we see that

$$\mathbf{P}(x \notin B+B) \ \leq \ \left(\frac{3}{4}\right)^{-\lfloor x/2 \rfloor}.$$

Similar statements hold for $x \in \{L+1, \ldots, 2L-27\}$ and hence the probability that $B+B$ does not contain all of P is at most

$$2 \sum_{x \geq 29} \left(\frac{3}{4}\right)^{-\lfloor x/2 \rfloor},$$

which is less than $1/2$. It follows that there are at least 2^{L-29} sets $B \subset [L]$ for which $B+B$ contains P, and the lemma follows immediately from the remarks at the start of the proof.□

There are very few sets which exactly contain two different progressions Q_1 and Q_2 of length $2L$. Such progressions must have distinct common differences, and so Lemma 6 applies to give that $|Q_1^c \cap Q_2^c| \leq \frac{p}{4} + 10$. It follows that $|Q_1 \cup Q_2| \geq \frac{3p}{4} - 10$, and so the number of $X \subset \mathbf{Z}_p$ which exactly contain two different progressions is certainly $o\left(2^{p/3}\right)$.

The lower bound in Theorem 2 follows at once by applying Lemma 7 for each of the $p(p-1)/2$ choices for P. □

Concluding remarks. We think it quite likely that $|\mathrm{SF}(\mathbf{Z}_p)| = O(p2^{p/3})$ and $|\mathrm{SS}(\mathbf{Z}_p)| = O(p^2 2^{p/3})$, but do not see how to prove this. It may be that establishing this is similar in difficulty to proving the well-known conjecture of Cameron and Erdős concerning sum-free subsets of $[n] = \{1, \ldots, n\}$:

Conjecture 8 (Cameron – Erdős) *The number of sum-free subsets of* $[n]$ *is* $O(2^{n/2})$.

The bound $O(2^{n/2+o(n)})$ for this problem was proved independently by Alon [1], Calkin [2] and Erdős and Granville (unpublished).

It is natural to ask whether the methods of our paper extend to abelian groups in general. The answer is that they do, but not in a straightforward way, and our second paper will focus on the difficulties that arise. A particular problem is that $\mu(G)$, the maximal density of a sumfree subset of G, is not known for all groups. The survey article [3] may be consulted for more details, but we remark that problems arise when all prime factors of n are of the form $3k+1$. For example it is clear that $\mu\left(\mathbf{Z}_{91}^n\right) \geq 30/91$, but it does not seem to be known whether or not equality holds for all n.

References

[1] Alon, N., *Independent sets in regular graphs and sum-free subsets of abelian groups*, Israel Jour. Math. **73** (1991) 247 – 256.

[2] Calkin, N.J.,*On the number of sum-free sets,* Bull. London Math. Soc. **22** (1990), no. 2, 141–144.

[3] Kedlaya, K.S., *Product-free subsets of groups,* Amer. Math. Monthly **105** (1998), no. 10, 900–906.

[4] Lev, V.F., Łuczak, T. and Schoen, T. *Sum-free sets in abelian groups,* Israel Jour. Math. **125**(2001) 347 – 367.

[5] Lev, V.F. and Schoen, T. *Cameron-Erdős modulo a prime,* preprint.

[6] Pollard, J.M. *A generalisation of the theorem of Cauchy and Davenport,* J. Lond. Math. Soc. **8**(1974) 460–462

Ben Green
Trinity College, Cambridge, England.
email: bjg23@hermes.cam.ac.uk

Imre Z. Ruzsa
Mathematical Institute of the Hungarian Academy of Sciences, Budapest, Pf. 127, H-1364 Hungary.
email: ruzsa@renyi.hu