

A note on sumsets of subgroups in \mathbb{Z}_p^*

by

DERRICK HART (Kansas City, MO)

For subsets A_1, \dots, A_k of a group define $A_1 + \dots + A_k = \{a_1 + \dots + a_k : a_i \in A_i, 1 \leq i \leq k\}$. In the case that all the subsets are equal we will denote the k -fold sumset of A by $kA = \{x_1 + \dots + x_k : x_i \in A, 1 \leq i \leq k\}$.

Let A be a multiplicative subgroup of \mathbb{Z}_p^* . What is the smallest $\alpha > 0$ such that $|A| \gg p^\alpha$ implies that $2A$ contains \mathbb{Z}_p^* ?

CONJECTURE 0.1. *Let $|A| > p^{1/2+\epsilon}$, $\epsilon > 0$. Then $2A$ contains \mathbb{Z}_p^* .*

It is relatively simple, using exponential sum bounds, to show that if $|A| > p^{3/4}$ then $2A \supseteq \mathbb{Z}_p^*$. Surprisingly, no improvement in the exponent has been made. An alternative approach would be to consider this conjecture from an inverse perspective. Let $|A| > p^{1/2+\epsilon}$; what is the smallest k_0 such that k_0A contains \mathbb{Z}_p^* ? A direct application of classical counting methods using standard exponential sum bounds does not seem to yield any answer to this question. For example, using the fact that $\max_{\lambda \neq 0} |\sum_{x \in A} e_p(x\lambda)| \leq \sqrt{p}$ one may show that if $|A| > p^{1/2+1/(2k)}$ then kA contains \mathbb{Z}_p^* .

Using combinatorial methods Glibichuk [1] gave the first answer to this question showing that $8A \supseteq \mathbb{Z}_p^*$ for $|A| \geq 2p^{1/2}$. Using an improved exponential sum bound, Schoen and Shkredov [3, Theorem 2.6] showed that $7A \supseteq \mathbb{Z}_p^*$ for $|A| > p^{1/2}$. There was subsequent improvement to this result by Shkredov and Vyugin [7] followed by Schoen and Shkredov [4]. Recently, Shkredov [5] has shown that $6A \supseteq \mathbb{Z}_p^*$ if $|A| > p^{55/112+\epsilon} = p^{491\dots+\epsilon}$.

In this paper we elaborate on the methods in the above-mentioned papers to show that $6A \supseteq \mathbb{Z}_p^*$ if $|A| > p^{11/23+\epsilon} = p^{478\dots+\epsilon}$. In addition, we extend a result of Shkredov [5] to show that $|2A| \gg |A|^{8/5-\epsilon}$ for $|A| \ll p^{5/9}$.

1. Statement of main results. Let A and B be subsets of \mathbb{Z}_p . Given a set A we will denote the indicator function of A by $A(\cdot)$. Define the convolution of A and B by $(A * B)(z) = \sum_{x+y=z} A(x)B(y) = |A \cap (z - B)|$.

2010 *Mathematics Subject Classification*: Primary 11B30; Secondary 11B13.

Key words and phrases: multiplicative subgroups, sumsets, sum-product.

The *additive energy* between A and B is given by

$$\begin{aligned} E(A, B) &= |\{(x, y, z, w) \in A \times B \times A \times B : x + y = z + w\}| \\ &= \sum_z (A * B)^2(z) = \sum_z |A \cap (z - B)|^2 \\ &= \sum_z (A * -A)(z)(B * -B)(z) = \sum_z |A_z| |B_z|; \end{aligned}$$

here and throughout, we let $C_z = C \cap (C + z)$ for any subset C of \mathbb{Z}_p . In the case that $A = B$ we will write $E(A) = E(A, A)$. Similarly, we will denote the r th *additive energy* of a subset A by $E_r(A) = \sum_s |A_s|^r$.

One may also consider the additive energy in the frequency domain. Taking an exponential sum expansion, we obtain

$$E(A, B) = p^{-1} \sum_s \left| \sum_{x \in A} e_p(sx) \right|^2 \left| \sum_{y \in B} e_p(sy) \right|^2,$$

where $e_p(x) = e^{2\pi ix/p}$. For a subset A of \mathbb{Z}_p we define

$$\Phi_A = \max_{\lambda \neq 0} \left| \sum_{x \in A} e_p(\lambda x) \right|.$$

Heath-Brown and Konyagin employed Stepanov’s method in order to give a bound on the additive energy of multiplicative subgroups of \mathbb{Z}_p^* .

THEOREM 1.1 ([2]). *Let A be a multiplicative subgroup of \mathbb{Z}_p^* with $|A| \ll p^{2/3}$. Then*

$$E(A) \ll |A|^{5/2}.$$

In [5] Shkredov gave the following combinatorial lemma.

LEMMA 1.2 ([5, equation (1)]). *Let A be a finite subset of an abelian group. Then*

$$\sum_s \frac{|A_s|^2}{|A + A_s|} \ll |A|^{-2} E_3(A).$$

Schoen and Shkredov ([3]) gave an estimate for $E_3(A)$.

LEMMA 1.3 ([3, Lemma 3.3]). *Let A be a multiplicative subgroup A of \mathbb{Z}_p^* with $|A| \ll p^{2/3}$. Then*

$$E_3(A) \ll |A|^3 \log(|A|).$$

Combining Lemmas 1.2 and 1.3 and noting that $|A + A_s| \leq |(2A)_s|$ gives the following lemma.

LEMMA 1.4. *Let A be a multiplicative subgroup A of \mathbb{Z}_p^* with $|A| \ll p^{2/3}$. Then*

$$\sum_s \frac{|A_s|^2}{|(2A)_s|} \ll |A| \log(|A|).$$

Shkredov used this inequality in [5] to give the following estimate on the additive energy.

THEOREM 1.5 ([5, Theorem 30]). *Let A be a multiplicative subgroup of \mathbb{Z}_p^* such that $|A| \ll p^{2/3}$. If $E(A) \ll |A|^{3/2} \sqrt{p} \log(|A|)$ then*

$$E(A) \ll |A|^{4/3} |2A|^{2/3} \log(|A|).$$

In addition, using different methods he proved an energy estimate independent of the size of the sumset.

THEOREM 1.6 ([5, Theorem 34]). *Let A be a multiplicative subgroup of \mathbb{Z}_p^* such that $|A| \ll p^{2/3}$. Then*

$$E(A) \ll \max\{|A|^{22/9} \log(|A|), |A|^3 p^{-1/3} \log^{4/3}(|A|)\}.$$

Combining Theorems 1.5 and 1.6 and applying the trivial estimate $|2A| \geq |A|^4 E^{-1}(A)$ gives the following sumset estimate.

THEOREM 1.7. *Let A be a multiplicative subgroup of \mathbb{Z}_p^* with $|A| \ll p^{2/3}$. Then*

$$|2A| \gg \begin{cases} |A|^{8/5} \log^{-3/5}(|A|) & \text{if } |A| \ll p^{9/17}, \\ |A|^{14/9} \log^{-1}(|A|) & \text{if } |A| \ll p^{3/5} \log^{3/5}(|A|), \\ |A| p^{1/3} \log^{-4/3}(|A|) & \text{if } |A| \gg p^{3/5} \log^{3/5}(|A|). \end{cases}$$

Here we give the following energy estimate.

THEOREM 1.8. *Let A be a multiplicative subgroup of \mathbb{Z}_p^* with $|A| \ll p^{2/3}$. Then*

$$E(A) \ll \max\{|A|^{4/3} |2A|^{2/3} \log^{1/2}(|A|), |A| |2A|^2 p^{-1} \log(|A|)\}.$$

This allows us to improve Shkredov’s sumset result in some ranges.

THEOREM 1.9. *Let A be a multiplicative subgroup of \mathbb{Z}_p^* with $|A| \ll p^{2/3}$. Then*

$$|2A| \gg \begin{cases} |A|^{8/5} \log^{-3/10}(|A|) & \text{if } |A| \ll p^{5/9} \log^{-1/18}(|A|), \\ |A| p^{1/3} \log^{-1/3}(|A|) & \text{if } |A| \gg p^{5/9} \log^{-1/18}(|A|). \end{cases}$$

Using the Plancherel identity or orthogonality one can very quickly prove that $\Phi_A \ll \sqrt{p}$ for a multiplicative subgroup A with $|A| \gg p^{1/2}$. This is only non-trivial when $|A| > p^{1/2}$. Shparlinski [6] improved this result in some ranges with the bound $\Phi_A \ll |A|^{7/12} p^{1/6}$ for $p^{2/5} \ll |A| \ll p^{4/7}$. Heath-Brown and Konyagin [2] used the energy estimate of Theorem 1.1 to obtain the following improvement.

THEOREM 1.10. *Let A be a multiplicative subgroup. Then*

$$\Phi_A \ll \begin{cases} \sqrt{p} & \text{if } p^{2/3} \ll |A| \leq p, \\ p^{1/4}|A|^{-1/4}E^{1/4}(A) \ll p^{1/4}|A|^{3/8} & \text{if } p^{1/2} \ll |A| \ll p^{2/3}, \\ p^{1/8}E^{1/4}(A) \ll p^{1/8}|A|^{5/8} & \text{if } p^{1/3} \ll |A| \ll p^{1/2}. \end{cases}$$

Using Shkredov’s energy estimate, one may improve this result in some ranges when the sunset is small. Let $|A| \ll p^{1/2}$; then

$$\Phi_A \ll p^{1/8}|A|^{1/3}|2A|^{1/6} \log^{1/4}(|A|).$$

Using the same methods employed to prove Lemma 1.3 one may obtain $E_{3/2}(A) \ll |A|^{9/4}$. If the sunset is small we are able to significantly improve this bound.

LEMMA 1.11. *Let A be a multiplicative subgroup with $|A| \ll p^{1/2}$. Then*

$$E_{3/2}(A) \ll |A|^{1/2}|2A| \log^{7/4} |A|.$$

This lemma allows us to obtain the following exponential sum bound which is an improvement of the result of Shkredov as long as $|2A| \ll |A|^{7/4-\epsilon}$.

LEMMA 1.12. *Let A be a multiplicative subgroup with $|A| \ll p^{1/2}$. Then*

$$\Phi_A \ll p^{1/8}|A|^{-1/8}|2A|^{1/4}E^{1/8}(|A|) \log^{7/16}(|A|).$$

In particular, applying Theorem 1.8 we have

$$\Phi_A \ll p^{1/8}|A|^{1/24}|2A|^{1/3} \log^{1/2}(|A|).$$

With Lemma 1.12 in tow, we may now prove our main result.

THEOREM 1.13. *Let A be a multiplicative subgroup of \mathbb{Z}_p^* with $|A| \gg p^{11/23} \log^{12/23}(|A|)$. Then*

$$6A \supseteq \mathbb{Z}_p^*.$$

Proof. Fix a in \mathbb{Z}_p^* . We may assume that $|A| \ll p^{1/2}$ as the result is already known in the range $|A| \gg p^{1/2}$.

Let N be the number of solutions to the equation

$$x_1 + x_2 + y_1 + y_2 = ay_3$$

with $x_1, x_2 \in 2A$ and $y_1, y_2, y_3 \in A$. Taking an exponential sum expansion, we obtain

$$N = \frac{|2A|^2|A|^3}{p} + \frac{1}{p} \sum_{\lambda \neq 0} \left(\sum_{x \in 2A} e_p(\lambda x) \right)^2 \left(\sum_{y \in A} e_p(\lambda y) \right)^2 \left(\sum_{z \in A} e_p(-\lambda z a) \right),$$

which by the Plancherel identity implies $N > 0$ as long as $|2A||A|^3 > p\Phi_A^3$. Applying Lemma 1.12 gives the condition

$$|2A||A|^3 \gg p^{11/8}|2A||A|^{1/8} \log^{3/2}(|A|),$$

which in turn leads to

$$|A| \gg p^{11/23} \log^{12/23}(|A|). \blacksquare$$

2. A few preliminary lemmas. We begin with a lemma of Shkredov and Vyugin [7, Corollary 5.1] which is a generalization of a result of Heath-Brown and Konyagin [2]. We say that a subset $S \neq \{0\}$ is *A-invariant* if $SA = \{sa : s \in S, a \in A\} = S$, that is, S is a union of cosets of A and possibly $\{0\}$.

LEMMA 2.1 (Shkredov and Vyugin [7, Corollary 5.1]). *Let A be a multiplicative subgroup of \mathbb{Z}_p and let S_1, S_2, S_3 be A -invariant sets such that $|S_1 \setminus \{0\}| |S_2 \setminus \{0\}| |S_3 \setminus \{0\}| \ll \min\{|A|^5, p^3|A|^{-1}\}$. Then*

$$\sum_{z \in S_3} (S_1 * S_2)(z) \ll |A|^{-1/3} (|S_1| |S_2| |S_3|)^{2/3}.$$

REMARK. The above lemma has been modified slightly from its original form in order to allow S_1, S_2, S_3 to contain the zero element. One may check that the additional terms in $\sum_{z \in S_3} (S_1 * S_2)(z)$ allowing S_1, S_2 to contain the zero element only affect the implied constant.

We can now give a variant of a result of Shkredov [5].

LEMMA 2.2 ([5, Corollary 18]). *Let $k \gg 1$ and S_1, S_2 be A -invariant sets and let M be any A -invariant subset of the set $\{z : (S_1 * S_2)(z) \geq k\}$. If $|S_1| |S_2| |M| |A| \ll \min\{|A|^6, p^3\}$ then*

$$\begin{aligned} \sum_{z \in M} (S_1 * S_2)^r(z) &\ll |S_1|^2 |S_2|^2 |A|^{-1} k^{r-3} \quad \text{for } 1 \leq r < 3, \\ \sum_{z \in M} (S_1 * S_2)^3(z) &\ll |S_1|^2 |S_2|^2 |A|^{-1} \log(|S_1|^2 |S_2|^2 |A|^{-2} k^{-3}). \end{aligned}$$

Proof. Let $l_i = (S_1 * S_2)(z_i)$, $z_i \neq 0$, where $l_1 \geq l_2 \geq \dots$ are arranged in decreasing order. For each z in the coset $aA = \{aa' : a' \in A\}$, $a \in \mathbb{Z}_p$, note that $(S_1 * S_2)(z) = (S_1 * S_2)(a)$. By the coset a_iA we will mean the coset on which $l_i = (S_1 * S_2)(a_i)$. Let M be any A -invariant subset of the set $\{z : (S_1 * S_2)(z) \geq k\}$ and $M_i = \bigcup_{j=1}^i a_jA \subseteq M$. From Lemma 2.1 we have

$$l_i |A| i \leq \sum_{j=1}^i |A| l_j \leq \sum_{z \in M_i} (S_1 * S_2)(z) \ll i^{2/3} |A|^{1/3} |S_1|^{2/3} |S_2|^{2/3},$$

as long as $i|A| |S_1| |S_2| \ll |M| |S_1| |S_2| \ll \min\{|A|^5, p^3|A|^{-1}\}$. Now,

$$\begin{aligned} \sum_{z \in M} (S_1 * S_2)^r(z) &\leq |A| \sum_{i \ll |S_1|^2 |S_2|^2 |A|^{-2} k^{-3}} l_i^r \\ &\ll |A| \sum_{i \ll |S_1|^2 |S_2|^2 |A|^{-2} k^{-3}} (i^{-1/3} |A|^{-2/3} |S_1|^{2/3} |S_2|^{2/3})^r. \blacksquare \end{aligned}$$

3. Additive energy bound: Proof of Theorem 1.8. We may assume that

$$E(A) \gg \max\{|A|^{4/3} |2A|^{2/3} \log^{1/2}(|A|), |A| |2A|^2 p^{-1} \log(|A|)\}.$$

Combining this with the energy estimate from Theorem 1.1 we may also assume that

$$|2A| \ll \max\{|A|^{7/4} \log^{-3/4}(|A|), |A|^{3/4} p^{1/2} \log^{-1/2}(|A|)\}.$$

Write

$$E(A) = \sum_s |A_s|^2 \ll \sum_{s \in M_1} |A_s|^2,$$

where $M_1 = \{s : |A_s| \gg k_1 := |A|^{-2} E(A)\}$. Note that we have the trivial estimate $|M_1| \ll |A|^2 k_1^{-1} = |A|^4 E^{-1}(|A|)$. Now Lemma 1.4 gives

$$E(A) = \sum_s |A_s|^2 \ll \frac{E(A)}{|A| \log(A)} \sum_{s \in M_2^c} \frac{|A_s|^2}{|(2A)_s|} + \sum_{s \in M_2} |A_s|^2 \ll \sum_{s \in M_2} |A_s|^2,$$

where $M_2 = \{s : s \in M_1, |(2A)_s| \gg k_2 := |A|^{-1} \log^{-1}(|A|) E(A)\}$.

By Lemma 2.1 we have $k_2 |M_2| \ll |A|^{-1/3} |2A|^{4/3} |M_2|^{2/3}$, yielding $|M_2| \ll |2A|^4 |A|^{-1} k_2^{-3}$ as long as $|2A|^2 |M_2| \ll \min\{|A|^5, p^3 |A|^{-1}\}$. In order to see that the first bound holds, one may note that $|M_2| \ll |M_1|$ combined with our assumptions on the size of energy and sumset. To show that $|2A|^2 |M_2| \ll p^3 |A|^{-1}$ we use an exponential sum expansion,

$$|M_2| k_2 \ll \sum_{s \in M} |(2A)_s| \ll \frac{1}{p} \sum_m \left| \sum_{x \in 2A} e_p(xm) \right|^2 \left(\sum_{x \in M_2} e_p(xm) \right),$$

together with the bound $\max_{m \neq 0} |\sum_{x \in M_2} e_p(xm)| \ll p^{1/2} |M_2|^{1/2} |A|^{-1/2}$, to deduce

$$|M_2| k_2 \ll \max\{p^{-1} |2A|^2 |M_2|, p^{1/2} |2A| |M_2|^{1/2} |A|^{-1/2}\}.$$

If the first of these two bounds holds then $E(A) \ll |A| |2A|^2 p^{-1} \log(|A|)$. We may then assume that $|M_2| \ll p |2A|^2 |A|^{-1} k_2^{-2}$, which implies that $|2A|^2 |M_2| \ll p |2A|^4 |A| \log^2(|A|) E^{-2}(A) \ll p^3 |A|^{-1}$.

Therefore, for $|A| \ll p^{2/3}$, we have $|M_2| \ll |2A|^4 |A|^{-1} k_2^{-3}$. Using this fact we may again reduce the number of terms:

$$E(A) = \sum_s |A_s|^2 \ll k_3^2 |M_2| + \sum_{s \in M_3} |A_s|^2 \ll \sum_{s \in M_3} |A_s|^2,$$

where $M_3 = \{s : s \in M_2, |A_s| \gg k_3 := |2A|^{-2}|A|^{-1} \log^{-3/2}(|A|)E^2(A)\}$.

Finally, applying Lemma 2.2 we have

$$E(A) \ll |A|^4 |2A|^2 \log^{3/2}(|A|) E^{-2}(|A|),$$

as long as $|A|^2 |M_3| \ll |2A|^2 |M_2| \ll \min\{|A|^5, p^3 |A|^{-1}\}$.

4. $E_{3/2}(A)$: Proof of Lemma 1.11. Let $l_i = |A_{z_i}|$, $z_i \neq 0$, where $l_1 \geq l_2 \geq \dots$ are arranged in decreasing order. For each z in the coset $aA = \{aa' : a' \in A\}$, $a \in \mathbb{Z}_p$, note that $|A_z| = |A_a|$. By the coset $a_i A$ we will mean the coset on which $l_i = |A_{a_i}|$. Let M be any A -invariant subset of the set $\{z : |A_z| \geq k\}$, and $M_i = \bigcup_{j=1}^i a_j A \subseteq M$. Set $k = |2A|^2 |A|^{-3}$.

We have

$$l_i |A| i \leq \sum_{j=1}^i |A| l_j \leq \sum_{z \in M_i} |A_z|.$$

Now

$$\sum_{z \in M_i} |A_z| = \sum_{z \in M_i} \frac{|A_z|}{|(2A)_z|^{1/2}} |(2A)_z|^{1/2} \leq \left(\sum_z \frac{|A_z|^2}{|2A_z|} \right)^{1/2} \left(\sum_{z \in M_i} |2A_z| \right)^{1/2}.$$

Therefore, by Lemma 1.4,

$$l_i^2 |A|^2 i^2 \ll |A| \log(|A|) \sum_{z \in M_i} |2A_z|.$$

Noting that $|M_i| \ll |A|^2 k^{-1}$ we have $|M_i| |2A|^2 \ll |A|^5$. Hence we can apply Lemma 2.1 to get

$$l_i^2 |A|^2 i^2 \ll |2A|^{4/3} i^{2/3} |A|^{4/3} \log |A|.$$

This implies

$$l_i \ll |2A|^{2/3} i^{-2/3} |A|^{-1/3} \log^{1/2} |A|$$

for $i \ll |A - A| |A|^{-1} \leq |A|$. Finally

$$\begin{aligned} \sum_z |A_z|^{3/2} &\ll k^{1/2} |A|^2 + |A| \sum_{i \ll |A|} |l_i|^{3/2} \\ &\ll k^{1/2} |A|^2 + |A|^{1/2} |2A| \log^{7/4}(|A|), \end{aligned}$$

giving the desired result.

5. Exponential sum bound: Proof of Lemma 1.12. We begin by expanding the sum below and performing a basic substitution:

$$\begin{aligned} |A| \left| \sum_{x \in A} e_p(\lambda x) \right|^2 &= \sum_{y \in A} \left| \sum_{x \in A} e_p(\lambda y x) \right|^2 \\ &= \sum_{x_1, x_2 \in A} \sum_{y \in A} e_p(\lambda y(x_1 - x_2)) = \sum_s |A_s| \sum_{y \in A} e_p(\lambda y s). \end{aligned}$$

Now we may take absolute values and estimate from above:

$$|A| \Phi_A^2 \leq \sum_s |A_s| \left| \sum_{y \in A} e_p(\lambda y s) \right|.$$

Applying Hölder’s inequality we have

$$|A| \Phi_A^2 \ll \left(\sum_s |A_s|^{4/3} \right)^{3/4} \left(\sum_s \left| \sum_{y \in A} e_p(\lambda y s) \right|^4 \right)^{1/4},$$

which by the Plancherel identity gives

$$(5.1) \quad |A| \Phi_A^2 \ll \left(\sum_s |A_s|^{4/3} \right)^{3/4} p^{1/4} E^{1/4}(A).$$

Another application of Hölder’s inequality shows that

$$\sum_s |A_s|^{4/3} = \sum_s |A_s| |A_s|^{1/3} \ll \left(\sum_s |A_s|^{3/2} \right)^{2/3} |A|^{2/3},$$

and by Lemma 1.11,

$$\sum_s |A_s|^{4/3} \ll |A|^{2/3} (|A|^{1/2} |2A| \log^{7/4}(|A|))^{2/3} \ll |A| |2A|^{2/3} \log^{7/6}(|A|).$$

Putting this estimate into (5.1) gives the stated result.

Acknowledgements. This research was partly supported by NSF (grant no. 1242660).

References

[1] A. A. Glibichuk, *Combinational properties of sets of residues modulo a prime and the Erdős–Graham problem*, Mat. Zametki 79 (2006), 384–395 (in Russian); English transl.: Math. Notes 79 (2006), 356–365.
 [2] D. R. Heath-Brown and S. V. Konyagin, *New bounds for Gauss sums derived from k th powers, and for Heilbronn’s exponential sum*, Quart. J. Math. 51 (2000), 221–235.
 [3] T. Schoen and I. D. Shkredov, *Additive properties of multiplicative subgroups of \mathbb{F}_p* , Quart. J. Math. 63 (2012), 713–722.
 [4] T. Schoen and I. D. Shkredov, *Higher moments of convolutions*, J. Number Theory 133 (2013), 1693–1737.
 [5] I. D. Shkredov, *Some new inequalities in additive combinatorics*, arXiv:1208.2344v3 (2012).

- [6] I. E. Shparlinskii, *Estimates of Gaussian sums*, Mat. Zametki 50 (1991), no. 1, 122–130 (in Russian); English transl.: Math. Notes 50 (1991), 740–746.
- [7] I. V. Vyugin and I. D. Shkredov, *On additive shifts of multiplicative subgroups*, Mat. Sb. 203 (2012), no. 6, 81–100 (in Russian); English transl.: Sb. Math. 203 (2012), 844–863.

Derrick Hart
Department of Mathematics
Rockhurst University
Kansas City, MO 64110, U.S.A.
E-mail: derrick.hart@rockhurst.edu

*Received on 19.3.2013
and in revised form on 4.9.2013*

(7379)

