A NOTE ON SUMSETS OF SUBGROUPS IN $\mathbb{Z}_p$.

DERRICK HART

Abstract. Let $A$ be a multiplicative subgroup of $\mathbb{Z}_p^*$. Define the $k$-fold sumset of $A$ to be $kA = \{x_1 + \cdots + x_k : x_i \in A, 1 \leq i \leq k\}$. We show that $6A \supseteq \mathbb{Z}_p^*$ for $|A| > p^{\frac{23}{29} + \frac{1}{27}}$. In addition, we extend a result of Shkredov to show that $|2A| \gg |A|^\frac{9}{7} - \epsilon$ for $|A| \ll p^\frac{9}{7}$.

1. Introduction

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

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 1. Let $|A| > p^{\frac{3}{2} + \epsilon}$, $\epsilon > 0$ then $2A$ contains $\mathbb{Z}_p^*$.

It is relatively simple, using exponential sum bounds, to show that if $|A| > p^\frac{3}{2}$ 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 $|A| > p^{\frac{3}{2} + \epsilon}$; 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 $|A| > p^{\frac{3}{2} + \frac{1}{27}}$ 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 $|A| \geq 2p^7$. Using an improved exponential sum bound, Schoen and Shkredov [5, Theorem 2.6] showed that $7A \supseteq \mathbb{Z}_p^*$ for $|A| > p^\frac{3}{2}$. There was subsequent improvement to this result by Shkredov and Vyugin [7] followed by Schoen and Shkredov [6]. Recently, Shkredov [4] has shown that $6A \supseteq \mathbb{Z}_p^*$ if $|A| > p^{\frac{25}{112} + \epsilon} = p^{491\ldots + \epsilon}$.

In this paper we elaborate on the methods in the above mentioned papers to show that $6A \supseteq \mathbb{Z}_p^*$ if $|A| > p^{\frac{23}{29} + \epsilon} = p^{478\ldots + \epsilon}$. In addition, we extend a result of Shkredov ([4]) to show that $|2A| \gg |A|^\frac{9}{7} - \epsilon$ for $|A| \ll p^\frac{9}{7}$.

2. 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 $(A * B)(z) = \sum_{x+y=z} A(x)B(y) = |A \cap (B + z)|$. 

1
The additive energy between $A$ and $B$ be given by,

$$E(A, B) = \left| \{ (x, y, z, w) \in A \times B \times A \times B : x + y = z + w \} \right|$$

$$= \sum_z (A * B)^2(z) = \sum_z |A \cap (z - B)|^2$$

$$= \sum_z (A * -A)(z)(B * -B)(z) = \sum_z |A_z||B_z|,$$

where here and throughout the paper we will 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 rth 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,

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

where $e_p(x) = e^{2\pi ix/p}$. For a subset $A$ of $\mathbb{Z}_p$ we define $\Phi_A = \max_{\lambda \neq 0} \left| \sum_{x \in A} e_p(\lambda) \right|$.

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

**Theorem 2** ([2]). Let $A$ be a multiplicative subgroup of $\mathbb{Z}_p^\times$ with $|A| \ll p^{\frac{5}{2}}$. Then

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

In [4] Shkredov gave the following combinatorial lemma.

**Lemma 3** ([4], 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 ([5]) gave an estimate for $E_3(A)$.

**Lemma 4** ([5], Lemma 3.3). Let $A$ be a multiplicative subgroup $A$ of $\mathbb{Z}_p^\times$ with $|A| \ll p^{\frac{5}{2}}$. Then we have,

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

Combining Lemma [4] and Lemma [5] and noting that $|A + A_s| \leq |(2A)_s|$ gives the following lemma.

**Lemma 5.** Let $A$ be a multiplicative subgroup $A$ of $\mathbb{Z}_p^\times$ with $|A| \ll p^{\frac{5}{2}}$. Then we have,

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

Shkredov used this inequality in [4] to give the following estimate on the additive energy.

**Theorem 6** ([4], Theorem 30). Let $A$ be a multiplicative subgroup of $\mathbb{Z}_p^\times$ such that $|A| \ll p^{\frac{5}{2}}$. If $E(A) \ll |A|^{\frac{5}{2}} \sqrt{p} \log(|A|)$ then

$$E(A) \ll |A|^{\frac{3}{2}} |2A|^{\frac{5}{2}} \log(|A|).$$

In addition, using different methods he proved an energy estimate independent of the size of the sumset.
**Theorem 7** ([4], Theorem 34). Let $A$ be a multiplicative subgroup of $\mathbb{Z}_p^*$ such that $|A| \ll p^{\frac{2}{3}}$. Then

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

Combining Theorem 6 and Theorem 7 and applying the trivial estimate $|2A| \geq |A|^4 E^{-1}(A)$ gives the following sumset estimate.

**Theorem 8.** Let $A$ be a multiplicative subgroup of $\mathbb{Z}_p^*$ such that $|A| \ll p^{\frac{2}{3}}$. Then

$$|2A| \gg \begin{cases} |A|^\frac{2}{3} \log^{-\frac{1}{3}}(|A|), & |A| \ll p^{\frac{2}{3}}; \\ |A|^{\frac{14}{3}} \log^{-\frac{1}{3}}(|A|), & |A| \ll p^3 \log^{\frac{3}{2}}(|A|); \\ |A| p^{\frac{1}{3}} \log^{-\frac{1}{3}}(|A|), & |A| \gg p^3 \log^{\frac{3}{2}}(|A|). \end{cases}$$

Here we give the following energy estimate.

**Theorem 9.** Let $A$ be a multiplicative subgroup of $\mathbb{Z}_p^*$ such that $|A| \ll p^{\frac{2}{3}}$. Then

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

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

**Theorem 10.** Let $A$ be a multiplicative subgroup of $\mathbb{Z}_p^*$ such that $|A| \ll p^{\frac{2}{3}}$. Then

$$|2A| \gg \begin{cases} |A|^\frac{2}{3} \log^{-\frac{1}{3}}(|A|), & |A| \ll p^{\frac{2}{3}} \log^{-\frac{1}{3}}(|A|); \\ |A| p^{\frac{1}{3}} \log^{-\frac{1}{3}}(|A|), & |A| \gg p^{\frac{2}{3}} \log^{-\frac{1}{3}}(|A|). \end{cases}$$

Using, Plancherel or orthogonality one can very quickly prove that for a multiplicative subgroups $A$, $\Phi_A \ll \sqrt{p}$ for $|A| \gg p^{\frac{1}{2}}$. This is only non-trivial when $|A| > p^{\frac{1}{2}}$. Shparlinski ([3]) improved this result in some ranges with the bound $\Phi_A \ll |A|^\frac{1}{17} p^{\frac{2}{3}}$ for $p^{\frac{2}{3}} \ll |A| \ll p^{\frac{2}{3}}$. Heath-Brown and Konyagin used the energy estimate of Theorem 2 to obtain the following improvement.

**Theorem 11.** Let $A$ be a multiplicative subgroup. Then,

$$\Phi_A \ll \begin{cases} \sqrt{p}, & p^{\frac{2}{3}} \ll |A| \leq p; \\ p^{\frac{4}{3}} |A|^{-\frac{1}{3}} E^{\frac{1}{3}}(A) \ll p^\frac{4}{3} |A|^\frac{2}{3}, & p^\frac{2}{3} \ll |A| \ll p^{\frac{2}{3}}; \\ p^\frac{4}{3} E^{\frac{1}{3}}(A) \ll p^\frac{4}{3} |A|^\frac{2}{3}, & p^{\frac{2}{3}} \ll |A| \ll p^{\frac{2}{3}}. \end{cases}$$

Using Shkredov’s energy estimate, then one may improve this result in some ranges in the case that the sumset is small. Let $|A| \ll p^{\frac{2}{3}}$ then,

$$\Phi_A \ll p^\frac{4}{3} |A|^\frac{2}{3} |2A|^\frac{1}{3} \log^{\frac{1}{3}}.$$  

Using the same methods used to prove Lemma 4 one may obtain $E_{3/2}(A) \ll |A|^\frac{2}{3}$. In the case that the sumset is small we are able to significantly improve this bound.

**Lemma 12.** Let $A$ be a multiplicative subgroup with $|A| \ll p^{\frac{1}{3}}$. Then

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

This Lemma allows us to obtain the following exponential sum bound which is an improvement of the result of Shkredov as long as $|2A| \ll |A|^\frac{2}{3}$. 

Lemma 13. Let $A$ be a multiplicative subgroup with $|A| \ll p^{\frac{3}{8}}$. Then
\[ \Phi_A \ll p^{\frac{3}{8}}|A|^{-\frac{1}{8}} |2A|^{\frac{3}{8}} E^{\frac{1}{2}} (|A|) \log^{\frac{7}{8}} (|A|). \]

In particular, applying Theorem 9 we have
\[ \Phi_A \ll p^{\frac{3}{8}}|A|^{\frac{3}{8}} |2A|^{\frac{1}{8}} \log^{\frac{3}{8}} (|A|). \]

With Lemma 13 in tow, we may now prove our main result.

Theorem 14. Let $A$ be a multiplicative subgroup of $\mathbb{Z}_p^*$ with $|A| \gg p^\frac{11}{23} \log^\frac{15}{23} (|A|)$. Then $6A \supseteq \mathbb{Z}_p^*$.

Proof. Fix $a$ in $\mathbb{Z}_p^*$. We may assume that $|A| \ll p^\frac{3}{8}$ as the result is already known in the range $|A| \gg p^\frac{3}{8}$.

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,
\[ N = \frac{|2A|^2 |A|^3}{p} + \frac{1}{p} \sum_{x \in 2A} \left( \sum_{\lambda \neq 0} e_p (\lambda x) \right)^2 \left( \sum_{y \in A} e_p (\lambda y) \right)^2 \left( \sum_{z \in A} e_p (-\lambda za) \right), \]
which by Plancherel implies that we have that $N > 0$ as long as, $|2A||A|^3 > p\Phi^3_A$.

Applying Theorem gives the condition,
\[ |2A||A|^3 \gg p^{\frac{11}{23}} |2A|^{\frac{3}{8}} \log^{\frac{15}{8}} (|A|), \]
which in turn gives the condition,
\[ |A| \gg p^{\frac{11}{23}} \log^{\frac{15}{23}} (|A|). \]

□

3. 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 15. (Shkredov and Vyugin [7, Corollary 5.1]) Let $A$ be a multiplicative subgroup of $\mathbb{Z}_p$ and $S_1, S_2, S_3$ 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 3.1. The above lemma has been modified slightly from its original form in order to allow $S_1, S_2, S_3$ contain the zero element. One may check that the additional terms in $\sum_{z \in S_3} (S_1 * S_2)(z)$ allowing $S_1, S_2$, and to contain the zero element only affect the implied constant.
We can now give slight generalizations of several results of Schoen and Shkredov ([5], [6]).

Lemma 16. Let $k \gg 1$ and $S_1, S_2$ be $A$-invariant sets and let $M$ be any $A$-invariant subset of the set $\{z : (S_1 \ast S_2)(z) \geq k\}$. If $|S_1| |S_2| |M| |A| \ll \min\{|A|^{\delta}, p^3\}$ then for $r \geq 1, r \neq 3$,

$$\sum_{z \in M} (S_1 \ast S_2)^r(z) \ll |S_1|^2 |S_2|^2 |A|^{-1} k^{r-3},$$

and

$$\sum_{z \in M} (S_1 \ast S_2)^3(z) \ll |S_1|^2 |S_2|^2 |A|^{-1} \log(|S_1|^2 |S_2|^2 |A|^{-2} k^{-3}).$$

Proof. Let $l_i = (S_1 \ast S_2)(z_i), z_i \neq 0$ where $l_1 \geq l_2 \geq \ldots$ are arranged in decreasing order. For each $z$ in the coset $aA = \{aa' : a' \in A\}, a \in \mathbb{Z}_p$ note that $(S_1 \ast S_2)(z) = (S_1 \ast S_2)(a)$. By the coset $a_iA$ we will mean the coset on which $l_i = (S_1 \ast S_2)(a_i)$. Let $M$ be any $A$-invariant subset of the set $\{z : (S_1 \ast S_2)(z) \geq k\}$ and $M_i = \bigcup_{j=1}^i a_j A \subseteq M$. From Lemma 15 we have that

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

as long as $i |A| |S_1| |S_2| \ll |M| |S_1| |S_2| \ll \min\{|A|^{\frac{5}{4}}, p^3 |A|^{-1}\}$. Now,

$$\sum_{z \in M} (S_1 \ast S_2)^r(z) \ll \sum_{i \ll |S_1|^3 |S_2|^3 |A|^{-2} k^{-3}} l_i^r \ll |A| \sum_{i \ll |S_1|^2 |S_2|^2 |A|^{-2} k^{-3}} \left(i^{-\frac{1}{2}} |A|^{-\frac{3}{2}} |S_1|^\frac{1}{2} |S_2|^\frac{1}{2}\right)^r.$$

\qed

4. Additive Energy Bound: Proof of Theorem 9

We may assume that $E(A) \gg \max\{|A|^{\frac{7}{8}} 2A |2A|^{\frac{3}{4}} \log^{\frac{3}{4}}(|A|), |A|^2 p^{-1} \log(|A|)\}$. Combining this with the energy estimate from Theorem 2 we may also assume that

$$|2A| \ll \max\{|A|^\frac{7}{8} \log^{-\frac{3}{4}}(|A|), |A|^\frac{3}{4} p^\frac{1}{2} \log^{-\frac{1}{2}}(|A|)\}.$$ 

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 $|M_1| \ll |A|^{2k_1^{-1}} = |A|^4 E^{-1}(|A|)$. Now by Lemma 5 we have,

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

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

By Lemma 15 we have that $k_2 |M_2| \ll |A|^{-\frac{1}{3}} 2A |2A|^{\frac{4}{3}} |M_2|^{\frac{1}{3}}$ yielding $|M_2| \ll |2A|^4 |A|^{-1} k_2^{-3}$ as long as $|2A|^2 |M_2| \ll \min\{|A|^{\delta}, p^3 |A|^{-1}\}$. In order to see that first condition is satisfied, 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,

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

followed by applying the bound \( \max_{m \neq 0} \left| \sum_{x \in M_2} e_p(xm) \right| \ll p^{\frac{3}{2}} |M_2|^{\frac{3}{2}} |A|^{-\frac{3}{2}} \) to give,

\[ |M_2| k_2 \ll \max \{ p^{-1} |2A|^2 |M_2|, p^{\frac{3}{2}} |2A||M_2|^{\frac{3}{2}} |A|^{-\frac{3}{2}} \}. \]

If the first of these two bounds hold then we have \( E(A) \ll |A|^4 |2A|^{2} p^{-1} \log(|A|) \). 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 \( |A| \ll p^{\frac{3}{2}} \), we have that \( |M_2| \ll |2A|^4 |A|^{-1} k_2^{-3} \). 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 \( M_3 = \{ s : s \in M_2, |A_s| \gg k_3 \} \).

Finally, applying Lemma 16 we have,

\[ E(A) \ll |A|^4 |2A|^{2} \log^2(|A|) E^{-2}(|A|), \]

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

---

5. \( E_{3/2}(A) \): Proof of Lemma 12

Let \( l_i = |A_{z_i}|, z_i \neq 0 \) where \( l_1 \geq l_2 \geq \ldots \) 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 \( M_i = \cup_{j=1}^{i} a_j A \subseteq M \). Set \( k = |2A|^2 |A|^{-3} \).

We have that

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

Now

\[ \sum_{z \in M_i} |A_z| = \sum_{z \in M_i} \frac{|A_z|}{|2A|} \left( |2A| z \right)^{\frac{1}{2}} \leq \left( \sum_{z} \frac{|A_z|^2}{|2A_z|} \right)^{\frac{1}{2}} \left( \sum_{z \in M_i} |2A_z| \right)^{\frac{1}{2}}. \]

Therefore, by Lemma 5 we have that

\[ l_i^2 |A|^2 l^2 \ll |A| \log(|A|) \sum_{z \in M_i} |2A_z|, \]

Noting that \( |M_i| \ll |A|^2 k^{-1} \) we have \( |M_i| |2A|^2 \ll |A|^5 \). Therefore we can apply Lemma 15 to give,

\[ l_i^2 |A|^2 l^2 \ll |2A|^{\frac{4}{3}} |A|^{\frac{4}{3}} \log |A|. \]

Therefore

\[ l_i \ll |2A|^{\frac{5}{6}} i^{-\frac{2}{3}} |A|^{-\frac{1}{3}} \log^{\frac{1}{2}} |A|, \]
for $i \ll |A - A||A|^{-1} \leq |A|$. 

Now,

$$
\sum_{z} |A_z|^{\frac{7}{3}} \ll k^{\frac{1}{7}} |A|^2 + |A| \sum_{i \ll |A|} |l_i|^{\frac{7}{3}} \\
\ll k^{\frac{1}{7}} |A|^2 + |A|^{\frac{3}{7}} 2A |\log^7(|A|),
$$
giving the desired result.

6. Exponential Sum Bound: Proof of Lemma 13

We begin by expanding the sum below and performing a basic substitution,

$$
|A| \left| \sum_{x \in A} e_p(\lambda x) \right|^2 = \left| \sum_{y \in A} \sum_{x \in A} e_p(\lambda yx) \right|^2 \\
= \sum_{x_1, x_2 \in A} \sum_{y \in A} e_p(\lambda y(x_1 - x_2)) = \sum_{s} |A_s| \sum_{y \in A} e_p(\lambda ys).
$$

Now we may take absolute values and estimate from above,

$$
|A| \Phi^2_A \leq \sum_{s} |A_s| \sum_{y \in A} e_p(\lambda ys).
$$

Applying Holder we have,

$$
|A| \Phi^2_A \ll \left( \sum_{s} |A_s|^\frac{4}{7} \right)^\frac{7}{4} \left( \sum_{s} \left| \sum_{y \in A} e_p(\lambda ys) \right|^4 \right)^\frac{1}{4},
$$

which by Plancherel gives,

(1) $$
|A| \Phi^2_A \ll \left( \sum_{s} |A_s|^\frac{4}{7} \right)^\frac{3}{7} p^{\frac{1}{7}} E^\frac{1}{7}(A).
$$

Now again applying Holder,

$$
\sum_{s} |A_s|^\frac{4}{7} = \sum_{s} |A_s||A_s|^\frac{1}{3} \ll \left( \sum_{s} |A_s|^\frac{3}{7} \right)^\frac{4}{7} |A|^\frac{3}{7},
$$

and applying Lemma 12,

$$
\sum_{s} |A_s|^\frac{4}{7} \ll |A|^\frac{2}{7} \left( |A|^{\frac{1}{7}} 2A |\log^\frac{7}{6}(|A|) \right)^\frac{1}{7} \ll |A||2A|^{\frac{5}{7}} \log^\frac{7}{6}(|A|).
$$

Putting this estimate into (1) gives the stated result.
REFERENCES

[1] A. A. Glibichuk, *Combinational properties of sets of residues modulo a prime and the Erdős-Graham problem*, Mat. Zametki 79, no. 3, (2006), 384-395. Translated in Math. Notes 79, no. 3, (2006), 356-365.

[2] D. R. Heath-Brown and S. V. Konyagin, *New bounds for Gauss sums derived from kth powers, and for Heilbronn’s exponential sum*, Q. J. Math. 51 (2000), no. 2, 221-235.

[3] I. E. Shparlinski, *On Bounds of Gaussian Sums*, Mat. Zametki, 50 (1991), 122-130.

[4] I. D. Shkredov, *Some new inequalities in additive combinatorics*, preprint.

[5] T. Schoen and I. D. Shkredov, *On a question of Cochrane and Pinner concerning multiplicative subgroups*, arXiv:1008.0723v2, May 27, 2011, 1-10.

[6] I. D. Shkredov, *Higher moments of convolutions*, arXiv:1110.2986v1, Oct. 13, 2011, 1-35.

[7] I. D. Shkredov and I. V. Vyugin, *On additive shifts of multiplicative subgroups*, arXiv:1102.1172v1, Feb. 6, 2011, 1-18.

Department of Mathematics, Kansas State University, Manhattan, KS 66506

E-mail address: dnhart@math.ksu.edu

8