

This is the author's manuscript for publication. The publisher-formatted version may be available through the publisher's web site or your institution's library.

Waring's number for large subgroups of double-struck \mathbb{Z}_p

Todd Cochrane, Derrick Hart, Christopher Pinner, and Craig Spencer

How to cite this manuscript

If you make reference to this version of the manuscript, use the following information:

Cochrane, T., Hart, D., Pinner, C., & Spencer, C. (2014). Waring's number for large subgroups of double-struck \mathbb{Z}_p .

Published Version Information

Citation:

Cochrane, T., Hart, D., Pinner, C., & Spencer, C. (2014). Waring's number for large subgroups of double-struck \mathbb{Z}_p . *Acta Arithmetica*, 163(4), 309-325.

Digital Object Identifier (DOI): 10.4064/aa163-4-2

Publisher's Link: <http://journals.impan.gov.pl/cgi-bin/aa/pdf?aa163-4-02>

This item was retrieved from the K-State Research Exchange (K-REx), the institutional repository of Kansas State University. K-REx is available at <http://krex.ksu.edu>

WARING'S NUMBER FOR LARGE SUBGROUPS OF \mathbb{Z}_p^*

TODD COCHRANE, DERRICK HART, CHRISTOPHER PINNER, AND CRAIG SPENCER

ABSTRACT. Let p be a prime, \mathbb{Z}_p be the finite field in p elements, k be a positive integer, and A be the multiplicative subgroup of nonzero k -th powers in \mathbb{Z}_p . The goal of this paper is to determine, for a given positive integer s , a value t_s such that if $|A| \gg t_s$ then every element of \mathbb{Z}_p is a sum of s k -th powers. We obtain $t_4 = p^{\frac{22}{39} + \epsilon}$, $t_5 = p^{\frac{15}{29} + \epsilon}$ and for $s \geq 6$, $t_s = p^{\frac{9s+45}{29s+33} + \epsilon}$. For $s \geq 24$ further improvements are made, such as $t_{32} = p^{\frac{5}{16} + \epsilon}$ and $t_{128} = p^{\frac{1}{4}}$.

1. INTRODUCTION

Let p be a prime, \mathbb{Z}_p be the finite field in p elements, $\mathbb{Z}_p^* = \mathbb{Z}_p - \{0\}$, and k be a positive integer. The smallest s such that the congruence

$$(1) \quad x_1^k + x_2^k + \cdots + x_s^k \equiv a \pmod{p}$$

is solvable for all integers a is called Waring's number (mod p), denoted $\gamma(k, p)$. If $d = (k, p - 1)$ then clearly $\gamma(d, p) = \gamma(k, p)$ and so we assume henceforth that $k|(p - 1)$.

An alternate way of defining Waring's number is in terms of sum sets. For any subsets A, B of \mathbb{Z}_p and positive integer s we let

$$A + B = \{a + b : a \in A, b \in B\}, \quad sA = A + A + \cdots + A, \quad (s\text{-times}),$$

$$AB = \{ab : a \in A, b \in B\}, \quad nAB = n(AB).$$

If A is the multiplicative subgroup of k -th powers in \mathbb{Z}_p and $A_0 = A \cup \{0\}$ then $\gamma(k, p)$ is the minimal s such that $sA_0 = \mathbb{Z}_p$. Put $t = |A| = (p - 1)/k$.

From the classical estimate of Hua and Vandiver [10], and Weil [22] for counting the number $N(a)$ of solutions of (1) over \mathbb{Z}_p ,

$$(2) \quad |N(a) - p^{s-1}| \leq (k - 1)^s p^{\frac{s-1}{2}}, \quad \text{for } a \neq 0,$$

one immediately obtains

$$(3) \quad \gamma(k, p) \leq s \quad \text{if} \quad |A| \geq p^{\frac{1}{2} + \frac{1}{2s}},$$

where A is the group of k -th powers. In particular, $\gamma(k, p) \leq 2$ if $|A| \geq p^{3/4}$ and $\gamma(k, p) \leq 3$ for $|A| \geq p^{2/3}$. It is reasonable to conjecture that $\gamma(k, p) \leq 2$ if $|A| \gg p^{\frac{1}{2} + \epsilon}$ and that $\gamma(k, p) \leq 3$ if $|A| \gg p^{\frac{1}{3} + \epsilon}$, but no further progress has been made in this direction. However, for $s \geq 4$, improvements in the lower bound on $|A|$ in (3) are available. The goal of this paper is to obtain the best available estimates of this type. Our results are summarized in Table 1 below. For a given positive

Date: October 13, 2014.

2010 Mathematics Subject Classification. 11L07, 11B30, 11P05.

Key words and phrases. Waring's problem, Exponential sums, Sum-Product sets.

The second author was partially supported by NSF grant #1242660, and the fourth author by NSA Young Investigator Grant #H98230-12-1-0220.

TABLE 1. Record breaking values for Waring numbers

s	t_s	Exponent	Proof
2	$p^{\frac{3}{4}}$.75000	(3)
3	$p^{\frac{2}{3}}$.66667	(3)
4	$p^{\frac{22}{39}+\epsilon}$.56411	Section 6.1
5	$p^{\frac{15}{29}+\epsilon}$.51725	Section 6.2
6	$p^{\frac{11}{23}+\epsilon}$.47827	Theorem 6.1
7	$p^{\frac{27}{59}+\epsilon}$.45763	Theorem 6.1
8	$p^{\frac{117}{265}+\epsilon}$.44151	Theorem 6.1
16	$p^{\frac{27}{71}+\epsilon}$.38029	Theorem 6.1
24	$p^{\frac{5}{14}+\epsilon}$.35715	Section 8
32	$p^{\frac{5}{16}+\epsilon}$.31250	Section 8
48	$p^{\frac{5}{17}+\epsilon}$.29412	Section 8
64	$p^{\frac{5}{18}+\epsilon}$.27778	Section 8
96	$p^{\frac{5}{19}+\epsilon}$.26316	Section 8
128	$p^{\frac{1}{4}}$.25000	Section 8
392	$p^{\frac{5}{21}+\epsilon}$.23810	Section 8
2888	$p^{\frac{10}{53}+\epsilon}$.18868	Section 8

integer s , we let t_s denote the smallest known value such that for any k, p with $|A| \geq t_s$ we have $\gamma(k, p) \leq s$. The values given in the table are Big-O estimates, where the constant depends on ϵ whenever ϵ is present. For $s > 8$ we have chosen a sampling of special values to serve as benchmarks. Multiples of 8 are used because of the convenience of applying the Glibichuk-Konyagin $8AB$ theorem; see Lemma 8.1. For $6 \leq s \leq 12$ the best admissible value we have found for t_s is $p^{\frac{9s+45}{29s+33}+\epsilon}$ (see Theorem 6.1), sharpening the result of Schoen and Shkredov [16, Theorem 2.6], who obtained $t_s = \min \left\{ p^{\frac{2s+2}{5s-3}}, p^{\frac{s+5}{3s+3}} \right\}$. For $s > 12$ some further improvements are available by appealing to estimates of $T_3(A)$ (see (17)), but we have not carried out these computations here.

The estimate in (3) yields no information for groups of size \sqrt{p} and so one of the targets in recent years has been the determination of $\gamma(k, p)$ for subgroups A of size $|A| > p^{1/2}$. Glibichuk [5] obtained $\gamma(k, p) \leq 8$ for such groups. This was improved by Schoen and Shkredov [16, Theorem 4.1] to $\gamma(k, p) \leq 6$ for $|A| > p^{\frac{11}{33}+\epsilon}$. Further improvements were made by Shkredov and Vyugin [19, Corollary 5.6], $\gamma(k, p) \leq 6$ for $|A| > p^{\frac{33}{67}+\epsilon}$, and Schoen and Shkredov [17, Corollary 49], $\gamma(k, p) \leq 6$ for $|A| > p^{\frac{99}{203}+\epsilon} = p^{.48768\dots+\epsilon}$, both under the assumption that $-1 \in A$. Hart [8] obtained $\gamma(k, p) \leq 6$ for any A with $|A| > p^{\frac{11}{23}+\epsilon} = p^{.47826\dots+\epsilon}$. Here we extend his method to values of $s \geq 6$. In order to obtain $\gamma(k, p) \leq 5$, the best we have been able to do is to take $|A| > p^{\frac{15}{29}+\epsilon}$. The next milestone will be to obtain $\gamma(k, p) \leq 5$ for $|A| \gg p^{1/2}$.

Bounds on Gauss sums immediately yield estimates for Waring's number. Let $e_p(\cdot) = e^{\frac{2\pi i \cdot}{p}}$ and put

$$\Phi_k = \max_{\lambda, p \nmid \lambda} \left| \sum_{x=1}^p e_p(\lambda x^k) \right|.$$

It is elementary that $|N(a) - p^{s-1}| < \Phi_k^s$, and so

$$\gamma(k, p) \leq \left\lceil \frac{\log p}{\log(p/\Phi_k)} \right\rceil.$$

In particular,

$$(4) \quad \Phi_k \leq (1 - \epsilon)p \quad \Rightarrow \quad \gamma(k, p) \ll_{\epsilon} \log p,$$

and

$$(5) \quad \Phi_k \leq p^{1-\epsilon} \quad \Rightarrow \quad \gamma(k, p) \leq \left\lceil \frac{1}{\epsilon} \right\rceil.$$

Bounds of the first type, (4), are discussed in [11] and [2]. Bounds of the latter type, (5), follow from the ϵ - δ exponential sum bound of Bourgain and Konyagin [1]: For any $\delta > 0$ there exists a constant $\epsilon = \epsilon(\delta)$ such that if $|A| \gg p^{\delta}$ then $\Phi_k \ll p^{1-\epsilon}$. Consequently, there exists a constant $c(\delta)$ such that if $|A| > p^{\delta}$ then $\gamma(k, p) \ll c(\delta)$. Glibichuk and Konyagin [6] showed, using a completely different method, that one can take $c(\delta) = 4^{1/\delta}$. We employ the methods of Glibichuk and Konyagin in this paper to deal with the cases where $s > 8$ in Table 1, and so the values we obtain reflect this order of magnitude. For small s we use the machinery developed by Schoen and Shkredov [16], [17] and Shkredov and Vyugin [19], which in turn makes use of exponential sum estimates and additive energy estimates of Heath-Brown and Konyagin [9], and Konyagin [12].

Montgomery, Vaughan and Wooley [13] have conjectured that

$$\Phi_k \ll \sqrt{kp \log(kp)}.$$

This would imply that if $|A| > p^{\delta}$, then $\gamma(k, p) \leq \frac{c}{\delta}$, for some constant c , and consequently $t_s \leq p^{c/s}$, which is best possible, up to the determination of the constant c .

Remark 1.1. With the aid of a computer, one can determine explicit upper bounds for $\gamma(k, p)$ for small k . Small [20],[21] and Moreno and Castro [14] have provided tables of such values. For instance, $\gamma(2, p) \leq 2$ for all p , $\gamma(3, p) \leq 2$ for $p > 7$, $\gamma(4, p) \leq 2$ for $p > 29$, $\gamma(4, p) \leq 3$ for $p > 5$, $\gamma(5, p) \leq 2$ for $p > 61$, etc.

One can also obtain an explicit determination of $\gamma(k, p)$ when k is very close to p in size. For instance $\gamma(p-1, p) = p-1$, $\gamma(\frac{p-1}{2}, p) = \frac{p-1}{2}$ and for $p \equiv 1 \pmod{4}$, $\gamma(\frac{p-1}{4}, p) = a-1$ where a is the positive integer satisfying $a^2 + b^2 = p$, $a > b$, $b \in \mathbb{Z}$; see [2]. See [2] and [3] for further discussion of estimates when $|A|$ is small.

2. ESTIMATING THE NUMBER OF SOLUTIONS OF (1)

In this section we outline the standard method of estimating the number of solutions of a Waring-type congruence such as (1). For any subset B of \mathbb{Z}_p and positive integer ℓ , let

$$(6) \quad T_{\ell}(B) = |\{(x_1, \dots, x_{\ell}, y_1, \dots, y_{\ell}) : x_i, y_i \in B, x_1 + \dots + x_{\ell} = y_1 + \dots + y_{\ell}\}|,$$

and $E(B) := T_2(B)$, the additive energy of B . Set

$$(7) \quad \Phi_B = \max_{p \nmid \lambda} \left| \sum_{x \in B} e_p(\lambda x) \right|,$$

where $e_p(\cdot)$ denotes the additive character $e^{\frac{2\pi i}{p} \cdot}$ on \mathbb{Z}_p . We call a subset B of \mathbb{Z}_p an A -invariant set if $AB \subseteq B$, that is, $AB = B$.

For any $a \in \mathbb{F}_p$ let $N_s(B, a)$ denote the number of s -tuples (x_1, \dots, x_s) with

$$(8) \quad x_1 + x_2 + \dots + x_s = a, \quad x_i \in B, \quad 1 \leq i \leq s.$$

Theorem 2.1. *Let A be a multiplicative subgroup of \mathbb{Z}_p , B be an A -invariant subset of \mathbb{Z}_p and a be a nonzero element of \mathbb{Z}_p . Then for any positive integers s, r with $r \leq s/2$, we have*

$$\left| N_s(B, a) - \frac{|B|^s}{p} \right| < \Phi_B^{s-2r} T_r(B) \Phi_A / |A|.$$

Special cases of this theorem have appeared throughout the literature. Letting $B = A$, we have that (8) is solvable, and consequently $\gamma(k, p) \leq s$, provided that

$$(9) \quad |A|^{s+1} > p \Phi_A^{s+1-2r} T_r(A).$$

Note that with $N_s^*(a)$ denoting the number of solutions of (1) with the x_i nonzero, we have $N_s^*(a) = k^s N_s(A, a)$ and so we obtain the estimate

$$\left| N_s^*(a) - \frac{(p-1)^s}{p} \right| < \Phi_A^{s+1-2r} k^s T_r(A) / |A|.$$

The estimate in (2) is (essentially) recovered on setting $r = 1$ and using the elementary estimate $\Phi_A \leq \frac{k-1}{k} \sqrt{p} + \frac{1}{k}$, coming from $|\sum_{x=1}^p e_p(\lambda x^k)| \leq (k-1) \sqrt{p}$.

Proof. We have for any $a \in \mathbb{Z}_p^*$,

$$p N_s(B, a) = \sum_{\lambda=1}^p \sum_{x_1 \in B} \dots \sum_{x_s \in B} e_p(\lambda(x_1 + \dots + x_s - a)).$$

Since B is A -invariant, we have $N_s(B, ax) = N_s(B, a)$ for any $x \in A$, and so

$$\begin{aligned} p|A|N_s(B, a) &= \sum_{\lambda=1}^p \sum_{x \in A} \sum_{x_1 \in B} \dots \sum_{x_s \in B} e_p(\lambda(x_1 + \dots + x_s - ax)) \\ &= |B|^s |A| + \sum_{\lambda \neq 0} \sum_{x \in A} \sum_{x_1 \in B} \dots \sum_{x_s \in B} e_p(\lambda(x_1 + \dots + x_s - ax)) \\ &= |B|^s |A| + \sum_{\lambda \neq 0} \left(\sum_{x \in A} e_p(-\lambda ax) \right) \left(\sum_{x \in B} e_p(\lambda x) \right)^s. \end{aligned}$$

Thus for any positive integer $r \leq s/2$ and $a \in \mathbb{Z}_p^*$, we have

$$(10) \quad \left| N_s(B, a) - \frac{|B|^s}{p} \right| < \frac{\Phi_B^{s-2r} \Phi_A}{p|A|} \sum_{\lambda \in \mathbb{F}_p} \left| \sum_{x \in B} e_p(\lambda x) \right|^{2r} = \frac{\Phi_B^{s-2r} \Phi_A}{|A|} T_r(B).$$

□

3. ENERGY ESTIMATES

The first estimate we give is valid for any subset A of \mathbb{Z}_p .

$$\begin{aligned} E(A) &= p^{-1} \sum_{\lambda=0}^{p-1} \left| \sum_{x \in A} e_p(\lambda x) \right|^4 \\ &= \frac{|A|^4}{p} + p^{-1} \theta \Phi_A^2 \sum_{\lambda=1}^{p-1} \left| \sum_{x \in A} e_p(\lambda x) \right|^2 \\ &= \frac{|A|^4}{p} + p^{-1} \theta' \Phi_A^2 p |A| = \frac{|A|^4}{p} + \theta' |A| \Phi_A^2, \end{aligned}$$

for some real numbers θ, θ' with $|\theta| \leq 1, |\theta'| \leq 1$. In particular, for any subset A ,

$$(11) \quad E(A) \leq \frac{|A|^4}{p} + |A| \Phi_A^2.$$

For multiplicative subgroups A , we have the elementary bound $\Phi_A \leq \sqrt{p}$, and consequently $|E(A) - \frac{|A|^4}{p}| \leq |A|p$. Thus, for multiplicative groups with $|A| > p^{2/3}$, we have $E(A) \sim |A|^4/p$ (in the appropriate sense).

For subgroups of smaller size, improvements are available. Heath-Brown and Konyagin, using the method of Stepanov established that for any multiplicative subgroup A of \mathbb{Z}_p , with $|A| < p^{2/3}$, we have $E(A) \ll |A|^{5/2}$. The constant was made explicit in the work of Cochrane and Pinner [4, Theorem 2.2]: For $|A| < p^{2/3}$,

$$(12) \quad E(A) \leq \frac{16}{3} |A|^{5/2}.$$

For subgroups of size $|A| \ll p^{6/11}$, Shkredov [18, Theorem 34] obtained the improvement

$$(13) \quad E(A) \ll |A|^{\frac{22}{9}} \log^{\frac{2}{3}} |A|.$$

Schoen and Shkredov [17, Corollary 48] obtained a new kind of upper bound on $E(A)$, expressing it in terms of $|A|$ and $|2A|$: For any multiplicative subgroup A with $|A| \ll p^{1/2}$, $E(A) \ll |A|^{\frac{31}{18}} |2A|^{\frac{4}{9}} \log^{\frac{1}{2}} |A|$. This was improved by Shkredov [18, Theorems 30, 34] to

$$(14) \quad E(A) \ll |A|^{\frac{4}{3}} |2A|^{\frac{2}{3}} \log |A|,$$

for any multiplicative subgroup A with $|A| \ll p^{\frac{9}{17}}$, improving on (13) if $|2A| \ll |A|^{\frac{5}{3}} \log^{-\frac{1}{2}} |A|$. Hart [8] made a slight improvement, replacing the $\log |A|$ in (14) with $\log^{\frac{1}{2}} |A|$, for $|A| \ll p^{\frac{9}{17}}$. Indeed, he showed that for $|A| \ll p^{\frac{2}{3}}$,

$$(15) \quad E(A) \ll \max\{|A|^{\frac{4}{3}} |2A|^{\frac{2}{3}} \log^{\frac{1}{2}} |A|, |A| |2A|^2 p^{-1} \log |A|\}.$$

We note that in the inequalities of this paragraph the set $2A$ may be replaced by $A - A$.

For higher order $T_\ell(A)$ we have the following estimate of Konyagin [12, Lemma 5] for any multiplicative group A : For any positive integer $\ell \geq 3$ there exists a constant c_ℓ such that if $|A| < p^{\frac{1}{2}}$ then

$$(16) \quad T_\ell(A) \leq c_\ell |A|^{2\ell-2+1/2^{\ell-1}}.$$

This was improved by Shkredov [18, Theorem 34] in the case $\ell = 3$ to

$$(17) \quad T_3(A) \ll |A|^{\frac{151}{36}} \log^{\frac{2}{3}} |A| \ll |A|^{4.1945},$$

for $|A| < p^{\frac{1}{2}}$.

4. BOUNDS FOR Φ_A AND Φ_{2A}

The following lemma, a generalization of [12, Lemma 3], is a key tool for bounding exponential sums in terms of energy estimates.

Lemma 4.1. *Let A, B be subsets of \mathbb{F}_p^* such that B is A -invariant. Then, for any positive integers j, ℓ we have*

$$\Phi_B \leq p^{\frac{1}{2j\ell}} T_\ell(A)^{\frac{1}{2j\ell}} T_j(B)^{\frac{1}{2j\ell}} |A|^{-\frac{1}{j}} |B|^{1-\frac{1}{\ell}}.$$

The proof of the lemma is provided in the Appendix for the convenience of the reader.

For the case of a multiplicative subgroup A of \mathbb{Z}_p^* , we deduce from Lemma 4.1 that

$$(18) \quad \Phi_A \leq \begin{cases} p^{\frac{1}{2}}, & j = 1, \ell = 1; \\ p^{\frac{1}{4}} |A|^{-\frac{1}{4}} E(A)^{\frac{1}{4}}, & j = 2, \ell = 1; \\ p^{\frac{1}{8}} E(A)^{\frac{1}{4}}, & j = 2, \ell = 2; \\ p^{\frac{1}{12}} |A|^{\frac{1}{6}} E(A)^{\frac{1}{12}} T_3(A)^{\frac{1}{12}}, & j = 2, \ell = 3. \end{cases}$$

The second and third bounds above were obtained by Heath-Brown and Konyagin [9], and the fourth bound by Konyagin [12]. Inserting the energy estimates (12), (13), (14) and (17), yields estimates for Φ_A , as given in (20). Hart [8] obtained a new estimate for $|A| \ll p^{\frac{1}{2}}$:

$$(19) \quad \Phi_A \ll p^{\frac{1}{8}} |A|^{-\frac{1}{8}} |2A|^{\frac{1}{4}} E^{\frac{1}{8}}(A) \log^{\frac{7}{16}} |A|.$$

Inserting the energy estimates (13) and (14) (with the improved $\log^{\frac{1}{2}} |A|$) yields yet two more estimates for Φ_A . The various estimates are summarized below.

$$(20) \quad \Phi_A \ll \begin{cases} p^{\frac{1}{8}} |A|^{\frac{11}{18}} \log^{\frac{1}{6}} |A|, & \text{for } |A| \ll p^{\frac{6}{11}}, & \text{by (13), (18)c;} \\ p^{\frac{1}{8}} |A|^{\frac{1}{24}} |2A|^{\frac{1}{3}} \log^{\frac{1}{2}} |A|, & \text{for } |A| \ll p^{\frac{1}{2}}, & \text{by (14),(19);} \\ p^{\frac{1}{8}} |A|^{\frac{13}{72}} |2A|^{\frac{1}{4}} \log^{\frac{25}{48}} |A|, & \text{for } |A| \ll p^{\frac{1}{2}}, & \text{by (13), (19);} \\ p^{\frac{1}{4}} |A|^{\frac{13}{36}} \log^{\frac{1}{6}} |A|, & \text{for } |A| \ll p^{\frac{6}{11}}, & \text{by (13), (18)b;} \\ p^{\frac{1}{4}} |A|^{\frac{1}{12}} |2A|^{\frac{1}{6}} \log^{\frac{1}{4}} |A|, & \text{for } |A| \ll p^{\frac{9}{17}}, & \text{by (14),(18)b;} \\ |A|^{\frac{3}{8}} p^{\frac{1}{4}}, & \text{for } |A| < p^{2/3}, & \text{by (12), (18)b;} \\ \sqrt{p}, & \text{any } A, & \text{by Gauss.} \end{cases}$$

The labels (18)a,b,c,d refer to the four different inequalities in (18). The first estimate is due to Shkredov [18, Corollary 3.7], and the sixth to Heath-Brown and Konyagin [9]. For $|A| < p^{383}$, further improvements are available using (18)d together with (17). Further applications of Lemma 4.1 with higher j, ℓ yield nontrivial estimates for Φ_A for $|A|$ as small as $p^{\frac{1}{4}+\epsilon}$, as shown by Konyagin [12]. We shall have no occasion to use these here. For $|A| < p^{\frac{1}{2}}$ the first three inequalities in (20) should be used, while for $|A| > p^{\frac{1}{2}}$ the latter four are preferable. For $|A| < p^{\frac{1}{2}}$, inequality (20)b is the optimal choice for $|2A| < |A|^{5/3}$, and (20)c is the optimal

choice for $|A|^{\frac{5}{3}} < |2A| < |A|^{\frac{31}{18}}$ (ignoring log factors). For $|A| > p^{\frac{1}{2}}$, (20)e is the optimal choice for $|2A| < |A|^{\frac{5}{3}}$ (and $|A| \ll p^{\frac{9}{17}}$.)

Setting $B = 2A$ in Lemma 4.1, we obtain analogous bounds for Φ_{2A} , namely,

$$(21) \quad \Phi_{2A} \leq \begin{cases} p^{\frac{1}{2}} |2A|^{\frac{1}{2}} |A|^{-\frac{1}{2}}, & j = 1, \ell = 1; \\ p^{\frac{1}{4}} |2A|^{\frac{3}{4}} |A|^{-1} E(A)^{\frac{1}{4}}, & j = 1, \ell = 2; \\ p^{\frac{1}{6}} |2A|^{\frac{5}{6}} |A|^{-1} T_3(A)^{\frac{1}{6}}, & j = 1, \ell = 3. \end{cases}$$

Inserting the energy estimates (13), (14), with the $\sqrt{\log |A|}$ improvement, and (17), yields,

$$(22) \quad \Phi_{2A} \ll \begin{cases} p^{\frac{1}{2}} |2A|^{\frac{1}{2}} |A|^{-\frac{1}{2}}, & \text{for any } A; \\ p^{\frac{1}{4}} |2A|^{\frac{3}{4}} |A|^{-\frac{3}{8}}, & \text{for } |A| < p^{\frac{2}{3}}, \text{ by (12), (21)b;} \\ p^{\frac{1}{4}} |2A|^{\frac{3}{4}} |A|^{-\frac{7}{18}} \log^{\frac{1}{6}} |A|, & \text{for } |A| < p^{\frac{6}{11}}, \text{ by (13), (21)b;} \\ p^{\frac{1}{4}} |2A|^{\frac{11}{12}} |A|^{-\frac{2}{3}} \log^{\frac{1}{8}} |A|, & \text{for } |A| < p^{\frac{9}{17}}, \text{ by (14), (21)b.} \end{cases}$$

The first and second bounds were obtained by Schoen and Shkredov [16, Lemma 2.1, Lemma 2.4].

5. LOWER BOUNDS FOR $|2A|$

From the Cauchy-Schwarz inequality,

$$|A|^2 = \sum_x 1_A * 1_A(x) \leq |2A|^{\frac{1}{2}} E(A)^{\frac{1}{2}},$$

and so

$$(23) \quad |2A| \geq |A|^4 / E(A).$$

Inserting the energy estimate in (12) one obtains $|2A| \gg |A|^{\frac{3}{2}}$, a result first obtained by Heath-Brown and Konyagin [9]. Their result was made numeric by Cochrane and Pinner [3]: $|2A| \geq \frac{1}{4} |A|^{\frac{3}{2}}$, for $|A| < p^{\frac{2}{3}}$. For $|A| > p^{\frac{2}{3}}$ it is elementary (see [3]) that $|2A| \geq \frac{p}{2}$.

Inserting the energy estimate of Hart (15), one obtains [8, Theorem 10],

$$(24) \quad |2A| \gg \begin{cases} |A|^{\frac{8}{5}} \log^{-\frac{3}{10}} |A|, & \text{if } |A| \ll p^{\frac{5}{9}} \log^{-\frac{1}{18}} |A|; \\ |A| p^{\frac{1}{3}} \log^{-\frac{1}{3}} |A|, & \text{if } p^{\frac{5}{9}} \log^{-\frac{1}{18}} |A| \ll |A| \ll p^{\frac{2}{3}}. \end{cases}$$

The lower bound of order $|A|^{\frac{8}{5}}$ for $|2A|$ was first obtained by Shkredov [18, Corollary 31], but for the shorter interval $|A| \ll p^{\frac{1}{2}}$. Using [18, Theorems 30,34], the interval can be improved to $|A| \ll p^{9/17}$, still short of what we obtain in (24).

Stronger lower bounds on $|A - A|$ are available in the works of Schoen and Shkredov [16, Theorem 1.1] and Shkredov and Vyugin [19, Theorem 5.5], the latter being $|A - A| \gg |A|^{\frac{5}{3}} \log^{-\frac{1}{2}} |A|$ for $|A| \ll p^{\frac{1}{2}}$. (Note: Although [19, Theorem 5.5] was stated for sum or difference sets, the proof only holds for difference sets $A - A$.)

6. HYBRID COUNTS

Let A be the group of k -th powers in \mathbb{Z}_p^* and $a \in \mathbb{Z}_p^*$. In this section we estimate the number $N_{j,l}(2A, A, a)$ of solutions to the equation

$$(25) \quad x_1 + x_2 + \cdots + x_j + y_1 + y_2 + \cdots + y_l = a,$$

with $x_i \in 2A$, $1 \leq i \leq j$, and $y_j \in A$, $1 \leq j \leq l$. If one can show that $N_{j,l}(2A, A, a)$ is positive for any $a \in \mathbb{Z}_p^*$, then it follows that $\gamma(k, p) \leq 2j + l$. Now, since $2A$ is A -invariant, we have $N_{j,l}(2A, A, ay) = N_{j,l}(2A, A, a)$ for any $y \in A$, and so, following the proof of Theorem 2.1, we have

$$p|A|N_{j,l}(2A, A, a) = |2A|^j|A|^{l+1} + \sum_{\lambda=1}^{p-1} \left(\sum_{x \in 2A} e_p(\lambda x) \right)^j \left(\sum_{y \in A} e_p(\lambda y) \right)^\ell \sum_{y \in A} e_p(-\lambda ay).$$

One then has many options for bounding the error term (the second term on the right-hand side) in terms of Φ_A , Φ_{2A} , $T_j(A)$ and $T_j(2A)$. The method we employ in the following cases (assuming $j \geq 2$) is to simply say

$$(26) \quad |\text{Error}| \leq \Phi_{2A}^{j-2} \Phi_A^{\ell+1} \sum_{\lambda=1}^{p-1} \left| \sum_{x \in 2A} e_p(\lambda x) \right|^2 < \Phi_{2A}^{j-2} \Phi_A^{\ell+1} |2A|p,$$

and thus $N_{j,l}(2A, A, a)$ is positive provided that

$$(27) \quad |2A|^{j-1} |A|^{\ell+1} > \Phi_{2A}^{j-2} \Phi_A^{\ell+1} p.$$

6.1. The case $s = 4$. It is already known that $4A \supset \mathbb{Z}_p^*$ for $|A| > p^{\frac{2}{3}}$ and so we may assume $p^{\frac{5}{9}} \ll |A| \ll p^{\frac{2}{3}}$. By (27), $N_{2,0}(2A, A, a)$ is positive provided that

$$|2A||A| > p \Phi_A.$$

Using $\Phi_A \ll |A|^{\frac{3}{8}} p^{\frac{1}{4}}$, we see that it suffices to have

$$|2A||A|^{\frac{5}{8}} \gg p^{\frac{5}{4}}$$

Using $|2A| \gg |A|p^{\frac{1}{3}-\epsilon}$ we see that it suffices to have $|A| \gg p^{\frac{22}{39}+\epsilon}$.

6.2. The case $s = 5$. By (27), we see that $N_{2,1}(2A, A, a)$ is positive provided that

$$|2A||A|^2 > \Phi_A^2 p.$$

Using $\Phi_A < |A|^{\frac{3}{8}} p^{\frac{1}{4}}$ (valid for $|A| \ll p^{\frac{2}{3}}$), and the two lower bounds on $|2A|$ in (24) we see that it suffices to have $|A| \gg p^{\frac{10}{19}+\epsilon} = p^{.52631\dots+\epsilon}$. We assume now that $|A| \ll p^{.5264}$. In particular $|A| \ll p^{\frac{9}{17}}$, and so using the stronger bound $\Phi_A \ll p^{\frac{1}{4}+\epsilon} |A|^{\frac{1}{12}} |2A|^{\frac{1}{6}}$ we see that it suffices to have $|2A|^{\frac{2}{3}} |A|^{\frac{11}{6}} \gg p^{\frac{3}{2}+\epsilon}$. Then, using $|2A| \gg |A|^{\frac{5}{8}-\epsilon}$, we see that it suffices to have $|A| \gg p^{\frac{15}{29}+\epsilon}$.

6.3. The case $s \geq 6$. .

Theorem 6.1. *For $s \geq 6$ we have that if $|A| \gg p^{\frac{9s+45}{29s+33}+\epsilon}$ then $sA \supseteq \mathbb{Z}_p^*$.*

We note that this inequality recovers the estimate of Hart [8, Theorem 13] for the case $s = 6$, $|A| \gg p^{\frac{11}{23}}$, but note the correction to the statement of his theorem, where the exponent was given to be $p^{\frac{33}{71}}$ due to an arithmetic error.

Proof. If $|A| > p^{1/2}$ it is already known by the work of Shkredov [18, Corollary 32] and Hart [8, Theorem 13 or 14] that $6A \supseteq \mathbb{Z}_p^*$, so we may assume that $|A| \ll p^{1/2}$. If $|2A| < |A|^{5/3}$, we estimate $N_{2,s-4}(2A, A, a)$, noting that it will be positive (by (27)) provided that

$$|2A||A|^{s-3} > p\Phi_A^{s-3}.$$

Using $\Phi_A \ll p^{\frac{1}{8}+\epsilon}|A|^{\frac{1}{24}}|2A|^{\frac{1}{3}}$, we see that it suffices to have

$$|A|^{\frac{23}{24}(s-3)} \gg p^{\frac{5+s}{8}}|2A|^{\frac{s}{3}-2}.$$

Since $|2A| < |A|^{5/3}$, the latter holds provided that $|A| \gg p^{\frac{9s+45}{29s+33}+\epsilon}$.

If $|2A| \geq |A|^{5/3}$, and s is even, say $s = 2n$, we estimate $N_{n,0}(2A, A, a)$, noting that it will be positive (by (27)) provided that

$$|2A|^{n-1}|A| > p\Phi_{2A}^{n-2}\Phi_A.$$

Using $\Phi_{2A} \ll p^{\frac{1}{4}+\epsilon}|2A|^{\frac{3}{4}}|A|^{-\frac{7}{18}}$, $\Phi_A \ll p^{\frac{1}{8}+\epsilon}|A|^{\frac{13}{72}}|2A|^{\frac{1}{4}}$, we see that it suffices to have

$$|2A|^{\frac{n+1}{4}}|A|^{\frac{7}{18}n+\frac{1}{24}} \gg p^{\frac{n}{4}+\frac{5}{8}+\epsilon}.$$

Since $|2A| > |A|^{5/3}$, the latter holds provided that $|A| \gg p^{\frac{18n+45}{58n+33}+\epsilon} = p^{\frac{9s+45}{29s+33}+\epsilon}$.

If $|2A| \geq |A|^{5/3}$, and s is odd, say $s = 2n + 1$, we estimate $N_{n,1}(2A, A, a)$, noting that it will be positive provided that

$$|2A|^{n-1}|A|^2 > p\Phi_{2A}^{n-2}\Phi_A^2.$$

Using $\Phi_{2A} \ll p^{\frac{1}{4}+\epsilon}|2A|^{\frac{3}{4}}|A|^{-\frac{7}{18}}$, $\Phi_A \ll p^{\frac{1}{8}+\epsilon}|A|^{\frac{13}{72}}|2A|^{\frac{1}{4}}$, we see that it suffices to have

$$|2A|^{\frac{n}{4}}|A|^{\frac{7}{18}n+\frac{31}{36}} \gg p^{\frac{n}{4}+\frac{3}{4}+\epsilon}.$$

Since $|2A| > |A|^{5/3}$, the latter holds provided that $|A| \gg p^{\frac{9n+27}{29n+31}+\epsilon} = p^{\frac{9s+45}{29s+33}+\epsilon}$. \square

7. LOWER BOUNDS FOR $|nA|$ FOR $n > 2$

From the higher order energy estimate of Konyagin, (16), one easily obtains the following lemma.

Lemma 7.1. *For any positive integer ℓ and multiplicative subgroup A of \mathbb{Z}_p^* with $|A| < p^{2/3}$ if $\ell = 2$, and $|A| < \sqrt{p}$ if $\ell \geq 3$, we have $|\ell A| \gg |A|^{2-\frac{1}{2\ell-1}}$.*

Proof. By the Cauchy-Schwarz inequality,

$$|A|^{2\ell} = \left(\sum_{a \in \mathbb{Z}_p} N_\ell(A, a) \right)^2 \leq |\ell A| \cdot \sum_{a \in \mathbb{Z}_p} N_\ell(A, a)^2 = |\ell A| \cdot T_\ell(A),$$

and the result follows from (16). \square

In particular, we have that for $|A| < p^{1/2}$,

$$|3A| \gg |A|^{\frac{7}{4}}, \quad |4A| \gg |A|^{\frac{15}{8}}.$$

These results can be superseded by using the following result of Shkredov and Vyugin [19, Corollary 5.1, part 3].

Lemma 7.2 (Shkredov-Vyugin). *Let A be a multiplicative subgroup of \mathbb{Z}_p^* and B_1, B_2, B_3 be A -invariant sets such that $|B_1||B_2||B_3| \ll \min\{|A|^5, p^3|A|^{-1}\}$. Then*

$$\sum_{x,y} B_1(x)B_2(y)B_3(x+y) \ll |A|^{-1/3}(|B_1||B_2||B_3|)^{2/3}.$$

Letting $B_3 = B_1 + B_2$, the lemma implies that for

$$(28) \quad |B_1||B_2||B_1 + B_2| \ll \min\{|A|^5, p^3|A|^{-1}\},$$

we have

$$|B_1||B_2| = \sum_{x,y} B_1(x)B_2(y)B_3(x+y) \ll |A|^{-1/3}(|B_1||B_2||B_1 + B_2|)^{2/3},$$

and consequently

$$(29) \quad |B_1 + B_2| \gg \sqrt{|B_1||B_2||A|}.$$

Lemma 7.3. *For any multiplicative subgroup A of \mathbb{Z}_p^* we have the following.*

- a) *If $\sqrt{|2A|} |A| < p$ then $|3A| \gg \sqrt{|2A|} |A|$.*
- b) *If $|A| \ll p^{1/2}$ then $|3A| \gg |A|^{\frac{9}{5}-\epsilon}$.*

Proof. Suppose that $\sqrt{|2A|} |A| < p$. Let $B_1 = A$, $B_2 = 2A$. If $|A||2A||3A| \gg |A|^5$, then $|3A| \gg |A|^4/|2A| > \sqrt{|2A|} |A|$, since $|2A| < |A|^2$. If $|A||2A||3A| \ll p^3/|A|$ then $|3A| \gg p^3/(|A|^2|2A|) > \sqrt{|2A|} |A|$, by the hypothesis that $\sqrt{|2A|} |A| < p$. Otherwise, hypothesis (28) holds and we obtain the result of the lemma from (29).

To prove part (b), first note that if $|A| \ll p^{1/2}$, then the hypothesis in part (a) holds trivially, and so $|3A| \gg \sqrt{|2A|}|A|$. The result then follows upon inserting the lower bound $|2A| \gg |A|^{\frac{9}{5}-\epsilon}$. \square

Lemma 7.4. *For any multiplicative subgroup A of \mathbb{Z}_p^* with $|A| \ll p^{1/2}$, we have*

$$|4A| \gg |A|^2.$$

Proof. Let $B_1 = B_2 = Q$, where Q is a subset of $2A$ such that Q is a union of cosets of A and $|Q| \approx |A|^{\frac{3}{2}}$. We know that such a Q exists since $|2A| \gg |A|^{3/2}$ for $|A| < p^{2/3}$. If $|Q|^2|2Q| \gg |A|^5$ then

$$|4A| \geq |2Q| \gg \frac{|A|^5}{|Q|^2} \approx |A|^2.$$

If $|Q|^2|2Q| \ll p^3/|A|$ then

$$|4A| \geq |2Q| \gg \frac{p^3}{|Q|^2|A|} \approx \frac{p^3}{|A|^4} \gg |A|^2, \quad \text{for } |A| \ll p^{1/2}.$$

Otherwise, hypothesis (28) holds and, by (29), we obtain $|4A| \geq |2Q| \gg \sqrt{|Q|^2|A|} = |A|^2$. \square

In order to beat $|nA| > |A|^2$ for some n , a different approach is taken. For any subsets X, Y of \mathbb{Z}_p let

$$\frac{X-X}{Y-Y} = \left\{ \frac{x_1 - x_2}{y_1 - y_2} : x_1, x_2 \in X, y_1, y_2 \in Y, y_1 \neq y_2 \right\}.$$

The first ingredient we need is the lemma of Glibichuk and Konyagin, [6, Lemma 3.2].

Lemma 7.5. *Let $X, Y \subseteq \mathbb{Z}_p$ such that $\frac{X-X}{Y-Y} \neq \mathbb{Z}_p$. Then,*

$$|2XY - 2XY + Y^2 - Y^2| \geq |X||Y|.$$

If A is a multiplicative subgroup and X, Y are A -invariant sets then

$$\left| \frac{X - X}{Y - Y} \right| < |X - X| |Y - Y| / |A|,$$

and so the hypothesis of Lemma 7.5 holds if $|X - X| |Y - Y| \leq p|A|$. Taking (X, Y) to be (A, A) , $(2A, A)$, $(2A, 2A)$ respectively, one obtains the following lemma.

Lemma 7.6. *For any multiplicative subgroup A of \mathbb{Z}_p^* we have the following.*

- (i) *If $|A - A|^2 \leq p|A|$, then $|3A - 3A| \geq |A|^2$.*
- (ii) *If $|2A - 2A| |A - A| \leq p|A|$, then $|5A - 5A| \geq |2A| |A|$.*
- (iii) *If $|2A - 2A|^2 \leq p|A|$, then $|12A - 12A| \geq |2A|^2$.*

In order to pass from difference sets to sum sets, we use Ruzsa's triangle inequality (see eg. Nathanson [15, Lemma 7.4]),

$$(30) \quad |S + T| \geq |S|^{1/2} |T - T|^{1/2},$$

for any $S, T \subseteq \mathbb{Z}_p$, and its corollary, for any positive integer n ,

$$(31) \quad |nS| \geq |S|^{\frac{1}{2n-1}} |S - S|^{1 - \frac{1}{2n-1}} \geq |S - S|^{1 - \frac{1}{2n}}.$$

Lemma 7.7. *For any multiplicative subgroup A of \mathbb{Z}_p^* , we have*

- (i) $|7A| \geq \min\{|2A| |A|^{\frac{1}{2}}, p^{\frac{1}{2}} |A|^{\frac{1}{4}}\}$.
- (ii) $|19A| \geq \min\{|2A|^{\frac{3}{2}} |A|^{\frac{1}{4}}, p^{\frac{1}{2}} |A|^{\frac{1}{2} - \frac{1}{27}}\}$.

Proof. By (30),

$$(32) \quad |7A| \geq |2A|^{1/2} |5A - 5A|^{1/2}.$$

If $|2A - 2A| |A - A| < p|A|$ then by Lemma 7.6 (ii),

$$(33) \quad |7A| \geq |2A|^{1/2} |2A|^{1/2} |A|^{1/2} = |2A| |A|^{1/2}.$$

Otherwise, $|5A - 5A| \geq |2A - 2A| \geq p|A| / |A - A|$. By (31), $|2A| \geq |A - A|^{3/4}$. Thus,

$$|7A| \geq |2A|^{1/2} p^{1/2} |A|^{1/2} / |A - A|^{1/2} \geq p^{1/2} |A|^{1/2} / |A - A|^{1/8} \geq p^{1/2} |A|^{1/4}.$$

For part (ii) we again start with the triangle inequality,

$$|19A| \geq |7A|^{1/2} |12A - 12A|^{1/2}.$$

If $|2A - 2A|^2 < p|A|$, then by Lemma 7.6 (iii) and (33),

$$(34) \quad |19A| \geq |7A|^{1/2} |2A| \geq |2A|^{3/2} |A|^{1/4}.$$

Otherwise $|2A - 2A| \geq p^{1/2} |A|^{1/2}$. In particular, $|A|^4 \geq p^{1/2} |A|^{1/2}$, that is, $|A| \geq p^{1/7}$. Then, by (31),

$$|19A| \geq |9 \cdot 2A| \geq |2A - 2A|^{1 - \frac{1}{29}} \geq p^{\frac{1}{2} - \frac{1}{2 \cdot 10}} |A|^{\frac{1}{2} - \frac{1}{2 \cdot 10}} \geq p^{\frac{1}{2}} |A|^{\frac{1}{2} - \frac{8}{2 \cdot 10}}. \quad \square$$

Inserting the lower bound $|2A| \gg |A|^{\frac{8}{5} - \epsilon}$ from (24), we obtain

Lemma 7.8. *For any multiplicative subgroup A with $|A| \ll p^{5/9} \log^{-\frac{1}{18}} |A|$, we have*

- (i) $|7A| \gg \min\{|A|^{\frac{21}{10} - \epsilon}, p^{\frac{1}{2}} |A|^{\frac{1}{4}}\}$.
- (ii) $|19A| \gg \min\{|A|^{\frac{53}{20} - \epsilon}, p^{\frac{1}{2}} |A|^{\frac{1}{2} - \frac{1}{27}}\}$.

Thus,

$$\begin{aligned} |7A| &\gg |A|^{\frac{21}{10}-\epsilon}, & \text{for } |A| &\ll p^{\frac{10}{37}} = p^{27027\dots}; \\ |19A| &\gg |A|^{\frac{53}{20}-\epsilon}, & \text{for } |A| &\ll p^{23171\dots}. \end{aligned}$$

This process can be continued to generate further lower bounds on $|nA|$. For example, using the lower bounds for $|3A|$, $|4A|$, and $|8A| \geq |3A|^{\frac{1}{2}}|5A-5A|^{\frac{1}{2}}$, $|9A| \geq |4A|^{\frac{1}{2}}|5A-5A|^{\frac{1}{2}}$ one obtains lower bounds for $|8A|$, $|9A|$ respectively. See also [2] for further lower bounds of this type.

8. AN APPLICATION OF THE GLIBICHUK-KONYAGIN $8AB$ THEOREM

The following lemma is due to Glibichuk [5], and Glibichuk and Konyagin [6]. See also Glibichuk and Rudnev [7] for a variation.

Lemma 8.1. *Let A, B be subsets of \mathbb{Z}_p such that $|A||B| \geq 2p$. Then $8AB = \mathbb{Z}_p$. Moreover if A is symmetric ($A = -A$) or antisymmetric ($A \cap -A = \emptyset$) then it suffices to have $|A||B| \geq p$.*

Let A be the multiplicative group of nonzero k -th powers, so that $(nA)(mA) \subseteq (nm)A$ for any positive integers m, n . Thus, by Lemma 8.1, if $|A||2A| \geq 2p$ then $16A = \mathbb{Z}_p$, while if $|2A||2A| \geq 2p$ then $32A = \mathbb{Z}_p$. Using $|2A| \gg |A|^{\frac{8}{5}-\epsilon}$ we see that it suffices to have $|A| \gg p^{\frac{5}{13}+\epsilon}$, $|A| \gg p^{\frac{5}{16}+\epsilon}$, respectively. The $16A$ bound is slightly weaker than what we obtained from Theorem 6.1. Similarly if $|A||3A| \geq 2p$ then $24A = \mathbb{Z}_p$; if $|2A||3A| \geq 2p$ then $48A = \mathbb{Z}_p$. Using $|3A| \gg |A|^{\frac{9}{5}-\epsilon}$, $|2A| \gg |A|^{\frac{8}{5}-\epsilon}$, we obtain the bounds for $s = 24, 48$ in Table 1.

Using $|2A| \gg |A|^{\frac{8}{5}-\epsilon}$, $|3A| \gg |A|^{\frac{9}{5}-\epsilon}$, $|4A| \gg |A|^2$ (for $|A| \ll p^{1/2}$) we obtain in a similar manner the bounds for $s = 64, 96, 128$ in Table 1.

If $|7A||7A| \geq 2p$ then $392A = \mathbb{Z}_p$. Using the lower bound in Lemma 7.8 for $|7A|$, we see that it suffices to have $|A| \gg p^{\frac{5}{21}+\epsilon}$. Finally, if $|19A||19A| \geq 2p$ then $2888A = \mathbb{Z}_p$. Using the lower bound in Lemma 7.8 for $|19A|$ we see that it suffices to have $|A| \gg p^{\frac{10}{53}+\epsilon}$. Clearly, one can continue obtaining further examples of this type, but our interest in this paper is small s .

9. APPENDIX: PROOF OF LEMMA 4.1

The lemma is an easy consequence of the following double Hölder inequality.

Lemma 9.1. *For any nonnegative real numbers a_i, b_i , $1 \leq i \leq n$, and any positive real number ℓ , we have*

$$\sum_{i=1}^n a_i b_i \leq \left(\sum_{i=1}^n a_i \right)^{1-\frac{1}{\ell}} \left(\sum_{i=1}^n a_i^2 \right)^{\frac{1}{2\ell}} \left(\sum_{i=1}^n b_i^{2\ell} \right)^{\frac{1}{2\ell}}.$$

Proof. By Hölder's inequality, we have

$$(35) \quad \sum_{i=1}^n a_i b_i \leq \left(\sum_{i=1}^n a_i^{\frac{2\ell}{2\ell-1}} \right)^{1-\frac{1}{2\ell}} \left(\sum_{i=1}^n b_i^{2\ell} \right)^{\frac{1}{2\ell}}.$$

By another application of Hölder, we note that

$$\begin{aligned} \sum_{i=1}^n a_i^{\frac{2\ell}{2\ell-1}} &= \sum_{i=1}^n a_i^{\frac{2\ell-2}{2\ell-1}} a_i^{\frac{2}{2\ell-1}} \\ &\leq \left(\sum_{i=1}^n a_i^{\frac{2\ell-2}{2\ell-1} \frac{2\ell-1}{2\ell-2}} \right)^{\frac{2\ell-2}{2\ell-1}} \left(\sum_{i=1}^n a_i^{\frac{2}{2\ell-1} (2\ell-1)} \right)^{\frac{1}{2\ell-1}} \\ &= \left(\sum_{i=1}^n a_i \right)^{\frac{2\ell-2}{2\ell-1}} \left(\sum_{i=1}^n a_i^2 \right)^{\frac{1}{2\ell-1}}. \end{aligned}$$

Inserting the latter bound into (35) yields the lemma. \square

Proof of Lemma 4.1. Since B is A -invariant we have

$$\begin{aligned} |A| \left(\sum_{x \in B} e_p(\lambda x) \right)^j &= \sum_{y \in A} \left(\sum_{x \in B} e_p(\lambda y x) \right)^j \\ &= \sum_{x_1 \in B} \cdots \sum_{x_j \in B} \sum_{y \in A} e_p(\lambda y(x_1 + \cdots + x_j)) \\ &= \sum_{b=0}^{p-1} n(b) \sum_{y \in A} e_p(\lambda y b), \end{aligned}$$

where

$$n(b) = |\{(x_1, \dots, x_j) : x_i \in B, 1 \leq i \leq j, x_1 + \cdots + x_j = b\}|.$$

By Lemma 9.1 and the elementary identities,

$$\sum_{b=0}^{p-1} n(b) = |B|^j, \quad \sum_{b=0}^{p-1} n(b)^2 = T_j(B),$$

we obtain, for $\lambda \neq 0$,

$$\begin{aligned} |A| \left| \sum_{x \in B} e_p(\lambda x) \right|^j &\leq \left(\sum_{b=0}^{p-1} n(b) \right)^{1-\frac{1}{\ell}} \left(\sum_{b=0}^{p-1} n(b)^2 \right)^{\frac{1}{2\ell}} \left(\sum_{b=0}^{p-1} \left| \sum_{y \in A} e_p(\lambda y b) \right|^{2\ell} \right)^{\frac{1}{2\ell}} \\ &= |B|^{j(1-\frac{1}{\ell})} T_j(B)^{\frac{1}{2\ell}} (T_\ell(A)p)^{\frac{1}{2\ell}}. \end{aligned}$$

Dividing by $|A|$ and taking the j -th root of both sides yields the lemma. \square

REFERENCES

- [1] J. Bourgain and S. V. Konyagin, *Estimates for the number of sums and products and for exponential sums in fields of prime order*, C.R. Acad. Sci., Paris 337, no. 2, (2003), 75-80.
- [2] J. A. Cipra, T. Cochrane, C. Pinner, *Heilbronn's conjecture on Waring's Number (mod p)*, J. Number Theory 125, no. 2, (2007), 289-297.
- [3] T. Cochrane and C. Pinner, *Sum-product estimates applied to Waring's problem mod p* , Integers 8 (2008), A46, 1-18.
- [4] ———, *Explicit bounds on monomial and binomial exponential sums*, Q.J. Math. 62 (2011) no. 2, 323-349.
- [5] A. A. Glibichuk, *Combinatorial 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.

- [6] A. A. Glibichuk and S. V. Konyagin, *Additive properties of product sets in fields of prime order*, Additive combinatorics, 279-286, CRM Proc. Lecture Notes, 43, Amer. Math. Soc., Providence, RI, 2007.
- [7] A. A. Glibichuk and M. Rudnev, *On additive properties of product sets in an arbitrary finite field*, (English summary) J. Anal. Math. 108 (2009), 159-170.
- [8] D. Hart, *A note on subgroups of \mathbb{Z}_p^** , arXiv:1303.2729v1, Mar. 12 2013, 1-8.
- [9] D. R. Heath-Brown and S. V. Konyagin, *New bounds for Gauss sums derived from k th powers, and for Heilbronn's exponential sum*, Q. J. Math. 51 (2000), no. 2, 221-235.
- [10] L. K. Hua and H. S. Vandiver, *Characters over certain types of rings with applications to the theory of equations in a finite field*, Proc. Nat. Acad. Sci. U.S.A. 35 (1949), 94-99.
- [11] S. V. Konyagin, *On estimates of Gaussian sums and Waring's problem for a prime modulus*, Trudy Mat. Inst. Steklov 198 (1992), 111-124; translation in Proc. Steklov Inst. Math. 1994, 105-107.
- [12] ———, *Estimates for trigonometric sums over subgroups and for Gauss sums*. (Russian) IV International Conference "Modern Problems of Number Theory and its Applications": Current Problems, Part III (Russian) (Tula, 2001), 86-114, Mosk. Gos. Univ. im. Lomonosova, Mekh.-Mat. Fak., Moscow, 2002.
- [13] H. L. Montgomery, R. C. Vaughan, T. D. Wooley, *Some remarks on Gauss sums associated with k th powers*, Math. Proc. Cambridge Philos. Soc. 118 (1995), no. 1, 21-33.
- [14] O. Moreno and F. N. Castro, *On the calculation and estimation of Waring number for finite fields*, Séminaires et Congrès 11 (2005), 29-40.
- [15] M. B. Nathanson, *Additive Number Theory, Inverse Problems and the Geometry of Sumsets*, Graduate Texts in Mathematics 165, Springer, New York, 1996.
- [16] T. Schoen and I. D. Shkredov, *Additive properties of multiplicative subgroups of F_p* . Q. J. Math. 63 (2012), no. 3, 713-722.
- [17] ———, *Higher moments of convolutions*, J. Number Theory 133 (2013), no. 5, 1693-1737.
- [18] I. D. Shkredov, *Some new inequalities in additive combinatorics*, arXiv: 1208.2344v2, Aug. 23 2012, 1-35.
- [19] I. D. Shkredov and I. V. Vyugin, *On additive shifts of multiplicative subgroups*, Mat. Sb., 203:6 (2012), 81-100.
- [20] C. Small, *Waring's Problem mod n* , American Math. Monthly 84, no. 1, (1977), 12-25.
- [21] ———, *Solution of Waring's problem mod n* , American Math. Monthly 84, no. 5, (1977), 356-359.
- [22] A. Weil, *Number of solutions of equations in finite fields*, Bull. AMS 55 (1949), 497-508.

DEPARTMENT OF MATHEMATICS, KANSAS STATE UNIVERSITY, MANHATTAN, KS 66506
E-mail address: `cochrane@math.ksu.edu`

DEPARTMENT OF MATHEMATICS, KANSAS STATE UNIVERSITY, MANHATTAN, KS 66506
E-mail address: `dnhart@math.ksu.edu`

DEPARTMENT OF MATHEMATICS, KANSAS STATE UNIVERSITY, MANHATTAN, KS 66506
E-mail address: `pinner@math.ksu.edu`

DEPARTMENT OF MATHEMATICS, KANSAS STATE UNIVERSITY, MANHATTAN, KS 66506
E-mail address: `cvs@math.ksu.edu`