# SUM-PRODUCT ESTIMATES APPLIED TO WARING'S PROBLEM MOD P

**Todd Cochrane**
*Department of Mathematics, Kansas State University, Manhattan, KS 66506*
cochrane@math.ksu.edu

**Christopher Pinner**
*Department of Mathematics, Kansas State University, Manhattan, KS 66506*
pinner@math.ksu.edu

*Received: 4/2/08, Revised: 9/3/08, Accepted: 10/10/08, Published: 10/27/08*

## Abstract

Let $\gamma(k,p)$ denote Waring's number (mod $p$) and $\delta(k,p)$ denote the $\pm$ Waring's number (mod $p$). We use sum-product estimates for $|nA|$ and $|nA-nA|$, following the method of Glibichuk and Konyagin, to estimate $\gamma(k,p)$ and $\delta(k,p)$. In particular, we obtain explicit numerical constants in the Heilbronn upper bounds: $\gamma(k,p) \le 83\ k^{1/2}$, $\delta(k,p) \le 20\ k^{1/2}$ for any positive $k$ not divisible by $(p-1)/2$.

## 1. Preliminaries

Let $p$ be a prime and $k$ a positive integer. The smallest $s$ such that the congruence

$$x_1^k + x_2^k + \cdots + x_s^k \equiv a \pmod p \tag{1.1}$$

is solvable for all integers $a$ is called Waring's number (mod $p$), denoted $\gamma(k,p)$. Similarly, the smallest $s$ such that

$$\pm x_1^k \pm x_2^k + \cdots \pm x_s^k \equiv a \pmod p, \tag{1.2}$$

is solvable for all $a$ is denoted $\delta(k,p)$. If $d = (k, p-1)$ then clearly $\gamma(d,p) = \gamma(k,p)$ and so we assume henceforth that $k|p-1$. If $A$ is the multiplicative subgroup of $k$-th powers in $\mathbb{Z}_p^*$ then we write

$$\gamma(A,p) = \gamma(k,p), \qquad \delta(A,p) = \delta(k,p).$$

Cauchy [4] established the uniform bound $\gamma(k,p) \le k$ with equality if $k = p-1$ or $(p-1)/2$, and many improvements to this bound have been made since then; see [6] for references. Heilbronn [11] made the following conjectures: Let $t = |A| = (p-1)/k$.

I: For any $\varepsilon > 0$, $\gamma(k,p) \ll_\epsilon k^\varepsilon$ for $t > c_\varepsilon$.

II: For $t > 2$, $\gamma(k,p) \ll k^{1/2}$.

The first conjecture was proved by Konyagin [13] and the second by Cipra and the authors [6]. For $t = 3, 4, 6$ it was shown [6] that

$$\sqrt{2k} - 1 \leq \gamma(k,p) \leq 2\sqrt{k}, \tag{1.3}$$

and thus the exponent $1/2$ is sharp. Indeed, the exact value of $\gamma(k,p)$ was determined for these three cases. The purpose of this paper is to show how sum-product estimates can be used to obtain explicit constants in the Heilbronn upper bounds.

**Theorem 1.1.** *For $t > 2$ we have the uniform upper bound $\gamma(k,p) \leq 83\ k^{1/2}$.*

The proof of the theorem (Section 9) uses the sum-product method of Glibichuk and Konyagin [9] for $t \geq 34$ (Sections 6,7) and the lattice method of Bovey [3] for $t < 34$ (Section 8). An explicit version of the first Heilbronn conjecture is given in Corollary 7.1. For delta we obtain $\delta(k,p) \leq 20\ k^{1/2}$; Corollary 10.3. We also explore the relationship between $\gamma(k,p)$ and $\delta(k,p)$ (Section 4) proving in particular,

$$\gamma(k,p) \leq 2 \lceil \log_2(\log_2(p)) \rceil\, \delta(k,p).$$

Bovey [3] proved the weaker bound $\gamma(k,p) \leq \delta(k,p) \log p$. We leave open the following

**Question 1.** Does there exist a constant $C$ such that $\gamma(k,p) \leq C\ \delta(k,p)$?

## 2. Sum-Product Estimates

For any subsets $S$, $T$ of $\mathbb{Z}_p$ let

$$S + T = \{s + t : s \in S, t \in T\}, \quad ST = \{st : s \in S, t \in T\},$$

$$S - T = \{s - t : s \in S, t \in T\}, \quad nS = S + S + \cdots + S \quad (n-\text{times}).$$

Note that $(nS)T \subset n(ST)$. We let $nST$ denote the latter, $n(ST)$. If $A$ is a multiplicative subgroup of $\mathbb{Z}_p^*$ then for any $\ell$, $A^\ell = A$, $nA^\ell = nA$ and $(nA)(mA) \subset nmA$. The basic strategy for bounding Waring's number is to first obtain good lower bounds for $|nA|$ and then apply the following lemma to sets of the form $nA$, $mA$ to obtain all of $\mathbb{Z}_p$.

**Lemma 2.1.** *Let $A$, $B$ be subsets of $\mathbb{Z}_p$ and $m$ a positive integer.*

*a) If $0 \notin A$ and $|B||A|^{1-\frac{2}{m}} > p$ then $mAB = \mathbb{Z}_p$.*

*b) If $|B||A| \geq 2p$ then $8AB = \mathbb{Z}_p$.*

Part (a) was proven by Bourgain [1, Lemma 1] for the case $m = 3$. We prove the general case in Section 3. Part (b) is due to Glibichuk and Konyagin [9, Lemma 2.1]. It follows from (b) that if $|nA| \geq \sqrt{2p}$ (for a multiplicative group $A$) then $\gamma(A, p) \leq 8n^2$.

We shall make frequent use of the Cauchy-Davenport inequality,

$$|S + T| \geq \min\{|S| + |T| - 1, p\},$$

for any $S, T \subset \mathbb{Z}_p$, and its corollary

$$|nS| \geq \min\{n(|S| - 1) + 1, p\}.$$

Another key tool we need is Rusza's triangle inequality (see, e.g., Nathanson [15, Lemma 7.4]).

$$|S + T| \geq |S|^{1/2}|T - T|^{1/2}, \tag{2.1}$$

for any $S, T \subset \mathbb{Z}_p$, and its corollary

$$|nS| \geq |S|^{\frac{1}{2^{n-1}}}|S - S|^{1-\frac{1}{2^{n-1}}} \geq |S - S|^{1-\frac{1}{2^n}}, \tag{2.2}$$

for any positive integer $n$.

In Section 5 we obtain lower bounds for $|A - A|$ and $|A + A|$ using the method of Stepanov. Next we obtain lower bounds for $|nA - nA|$ (Section 6), followed by lower bounds for $|nA|$ (Section 7).

## 3. Proof of Lemma 2.1(a)

Let $a \in \mathbb{Z}_p$ and $N$ denote the number of $2m$-tuples $(x_1, \ldots, x_m, y_1, \ldots y_m) \in \mathbb{Z}_p^{2m}$ with $x_1y_1 + \cdots + x_my_m = a$. We first note that

$$\sum_{\lambda \in \mathbb{Z}_p} \left| \sum_{x \in A} \sum_{y \in B} e_p(\lambda(xy)) \right|^2 = \sum_{x_1, x_2 \in A} \sum_{y_1, y_2 \in B} \sum_{\lambda \in \mathbb{F}_p} e_p(\lambda(x_1y_1 - x_2y_2))$$
$$= p|\{(x_1, x_2, y_1, y_2) : x_1, x_2 \in A, y_1, y_2 \in B, x_1y_1 = x_2y_2\}| \leq p|A|^2|B|,$$

the last inequality following from the assumption that $0 \notin A$ (and thus $x_1y_1 = x_2y_2$ implies $y_1 = x_1^{-1}x_2y_2$.) Now,

$$pN = |A|^m|B|^m + \sum_{\lambda \neq 0} \sum_{x_i \in A} \sum_{y_i \in B} e_p(\lambda(x_1y_1 + \cdots + x_my_m - a)) \tag{3.1}$$

$$= |A|^m|B|^m + \sum_{\lambda \neq 0} e_p(-\lambda a) \left( \sum_{x \in A} \sum_{y \in B} e_p(\lambda xy) \right)^m. \tag{3.2}$$

By the Cauchy-Schwarz inequality, for $\lambda \neq 0$,

$$\left|\sum_{x\in A, y\in B} e_p(\lambda xy)\right| \leq \sum_{y\in B}\left|\sum_{x\in A} e_p(\lambda xy)\right| \leq |B|^{1/2}\left(\sum_{y\in B}\left|\sum_{x\in A} e_p(\lambda xy)\right|^2\right)^{1/2}$$
$$\leq |B|^{1/2}\left(\sum_{y\in \mathbb{F}_p}\left|\sum_{x\in A} e_p(\lambda xy)\right|^2\right)^{1/2} = |B|^{1/2}(p|A|)^{1/2},$$

and so by the note above,

$$\left|\sum_{\lambda\neq 0} e_p(-\lambda a)\left(\sum_{x\in A}\sum_{y\in B} e_p(\lambda xy)\right)^m\right| \leq (|A||B|p)^{\frac{m-2}{2}}\sum_{\lambda\in\mathbb{Z}_p}\left|\sum_{x\in A}\sum_{y\in B} e_p(\lambda(xy))\right|^2$$
$$\leq |A|^{\frac{m}{2}+1}|B|^{\frac{m}{2}}p^{\frac{m}{2}}.$$

We conclude from (3.2) that $N$ is positive provided that

$$|A|^m|B|^m > |A|^{\frac{m}{2}+1}|B|^{\frac{m}{2}}p^{\frac{m}{2}},$$

yielding the result of the theorem.

## 4. Relations Between $\gamma(k, p)$ and $\delta(k, p)$

**Theorem 4.1.** *Let $A$ be the set of nonzero $k$-th powers in $\mathbb{Z}_p$ with $k|(p-1)$, $k \neq p-1$.*

*a)* $\gamma(k,p) \leq 3\left\lceil \log_2\left(\frac{3\log p}{\log|A|}\right)\right\rceil \delta(k,p)$.

*b)* $\gamma(k,p) \leq 3\left(\log_2(\delta(k,p)) + 4\right)\delta(k,p)$.

*c)* $\gamma(k,p) \leq 2\left\lceil \log_2(\log_2(p))\right\rceil \delta(k,p)$.

*d)* $\gamma(k,p) \leq (p_{min}-1)\delta(k,p)$, *where $p_{min}$ is the minimal prime divisor of $|A|$.*

*e) If $|A|$ is even then $\delta(k,p) = \gamma(k,p)$. If $|A|$ is odd, then $\delta(k,p) = \gamma(\frac{k}{2}, p)$.*

*Proof.* a) Put $A_0 = A \cup \{0\}$, $\delta = \delta(k,p)$. Since $\delta A_0 - \delta A_0 = \mathbb{Z}_p$ we obtain from (2.2)

$$|j\delta A_0| \geq |\delta A_0 - \delta A_0|^{1-1/2^j} = p^{1-1/2^j} \tag{4.1}$$

for any positive integer $j$. Hence if $j > \log_2\left(\frac{3\log p}{\log|A|}\right)$ we have $|j\delta A_0||A|^{\frac{1}{3}} > p$, and by Lemma 2.1(a), $3(j\delta A_0)A = \mathbb{Z}_p$, that is, $3j\delta A_0 = \mathbb{Z}_p$.

b) This follows from part (a) and the trivial bound $(2|A|+1)^\delta \geq p$, when $|A| \geq 2$.

c) If $j \geq \log_2(\log_2(p))$ then $p^{1/2^j} \leq 2$ and so by (4.1) $|j\delta A| \geq p/2$, and thus $2j\delta A = \mathbb{Z}_p$.

d) Let $q$ be the minimal prime divisor of $|A|$. Then $A$ has a subgroup $G$ of order $q$ and $\sum_{x \in G} x = 0$ so that $-1$ is a sum of $q-1$ elements of $A$.

e) If $|A|$ is even then $-1$ is a $k$-th power, and so $\gamma(k,p) = \delta(k,p)$. If $|A|$ is odd then $k$ must be even (for $p \neq 2$) and $A \cup (-A)$ is the set of $k/2$-th powers. □

## 5. Lower Bounds for $|A + A|$ and $|A - A|$

We give two estimates for $|A + A|$ and $|A - A|$ with $A$ a multiplicative subgroup of $\mathbb{Z}_p$, the first effective when $|A| \geq p^{2/3}$ and the second when $|A| < p^{2/3}$. Throughout this section $A \pm A$ will denote either one of these two sets.

**Theorem 5.1.** *If $A$ is a multiplicative subgroup of $\mathbb{Z}_p^*$ then*

$$|A \pm A| \geq p \left(1 + \frac{p^2}{|A|^3}\right)^{-1}.$$

*In particular $|A \pm A| \geq \frac{p}{2}$ if $|A| \geq p^{2/3}$.*

*Proof.* Let $N$ denote the number of solutions of the congruence $x_1 \pm x_2 \equiv y_1 \pm y_2 \pmod p$ with $x_1, x_2, y_1, y_2 \in A$, and $N_a$ the number of solutions of $x_1 \pm x_2 \equiv a \pmod p$, $x_1, x_2 \in A$, for $a \in \mathbb{Z}_p$. By the Cauchy-Schwarz inequality $|A|^2 = \sum_a N_a \leq |A \pm A|^{1/2} N^{1/2}$. The lower bound for $|A \pm A|$ then follows from the estimate of Hua and Vandiver [12] and Weil [16], $N \leq \frac{|A|^4}{p} + |A|p$. □

**Theorem 5.2.** *(a) Let $A$ be a multiplicative subgroup of $\mathbb{Z}_p^*$ and $\sigma$ be a positive integer. If $4\sigma(4\sigma-2) \leq |A| \leq \frac{p}{4\sigma-2}$, then $|A \pm A| \geq (\sigma+1)|A|$. (b) In particular, if $A$ is a multiplicative subgroup of $\mathbb{Z}_p^*$ with $|A| < p^{2/3}$, we have*

$$|A \pm A| \geq \tfrac{1}{4}|A| \left(\sqrt{|A|+1} + 1\right) > \tfrac{1}{4}|A|^{3/2}.$$

The theorem is a refinement of a special case of Bourgain, Glibichuck and Konyagin [2, Lemma 7] which gives $|A - A| \geq \frac{1}{9}|A|^{3/2}$ for $|A| < p^{1/2}$. The case $\sigma = 1$ is comparable to what one obtains from the Cauchy-Davenport Theorem, $|2A| \geq \min\{p, 2|A|\}$, for any multiplicative subgroup $A$. If 0 is included there is the stronger result $|2A_0| \geq \min\{p, 3|A| + 1\}$, for any multiplicative subgroup $A$ with $|A| \geq 2$, where $A_0 = A \cup \{0\}$; see [15, Theorem 2.8].

It is plain that the exponent $3/2$ in the lower bound of the theorem cannot be improved if we allow $|A|$ to approach $p^{2/3}$ in size, but we are lead to ask the following questions.

**Question 2.** For $|A| < p^{1/2}$ can the exponent $3/2$ in the theorem be improved?

**Question 3.** For $|A| \gg p^{2/3}$ do we have $A + A \supset \mathbb{Z}_p^*$, that is, $\gamma(A,p) \leq 2$? (Note, 0 may not be in $A + A$ even when $|A| = \frac{p-1}{2}$.) It is known that $\gamma(A,p) \leq 2$ for $|A| > p^{3/4}$.

*Proof of Theorem 5.2.* We use the Stepanov method as developed by Heath-Brown and Konyagin [10]. Let $A$ be a multiplicative subgroup of $\mathbb{Z}_p$ with $t = |A|$ and $\sigma$ be a positive integer. Suppose that $4\sigma(4\sigma - 2) \leq |A| \leq \frac{p}{4\sigma-2}$. We proceed with a proof by contradiction. Assume that $|A \pm A| < (\sigma + 1)t$. Write $A \pm A$ as a union of disjoint cosets of $A$ in $\mathbb{Z}_p^*$,

$$A \pm A = Ax_1 \cup Ax_2 \cdots \cup Ax_s \cup \{0\},$$

where the $\{0\}$ is omitted if $0 \notin A + A$. In particular,

$$|A \pm A| = st + 1 \text{ or } st, \tag{5.1}$$

and so $s \leq \sigma$.

For any coset $Ax_j$ let

$$N_j = |\{x \in A : x \pm 1 \in Ax_j\}| = |\{(x,y) \in A \times A : x \pm y = x_j\}|.$$

Now for any $x \in A$, $x \neq \mp 1$, $x \pm 1 \in Ax_j$ for some $j$ and so

$$\sum_{j=1}^{s} N_j = t - 1 \text{ or } t. \tag{5.2}$$

The next lemma is extracted from the proof of [14, Lemma 3.2].

**Lemma 5.1.** *Let $a, b, d$ be positive integers such that $sad + \frac{1}{2}sd(d-1) < ab^2$, $ab \leq t$, $tb \leq p$. Then*

$$\sum_{j=1}^{s} N_j \leq \frac{a - 1 + 2t(b-1)}{d}.$$

*Proof.* The lower case $a, b, d$ in the lemma correspond to the upper case $A, B, D$ in [14]. In equation (3.11) of [14] we actually have $sad + \frac{1}{2}sd(d-1) < ab^2$ by summing over $k$ in the preceding line of their proof. □

We apply the lemma with $a = 4s$, $b = 4s - 2$, $d = 8s - 5$. Then

$$sad + \frac{1}{2}sd(d-1) = 64s^3 - 64s^2 + 15s,$$

while

$$ab^2 = 64s^3 - 64s^2 + 16s,$$

so the first hypothesis holds. Next, $ab = 4s(4s-2) \le 4\sigma(4\sigma-2) \le t$. Finally, since $t \le \frac{p}{4\sigma-2}$ we have $tb \le \frac{p}{4\sigma-2}(4\sigma-2) = p$. Thus, by the lemma,

$$\sum_{j=1}^{s} N_j \le \frac{4s-1+2t(4s-3)}{8s-5} = t-1-\frac{t+6-12s}{8s-5} < t-1,$$

the latter inequality following from $12s-6 \le 4s(4s-2) \le t$. This contradicts the inequality in (5.2).

For part (b) simply choose $\sigma = [\frac{1}{4}(\sqrt{t+1}+1)]$ and observe that $t < p^{2/3}$ implies $t \le \frac{p}{4\sigma-2}$. □

## 6. Lower Bounds for $|nA - nA|$, Part I

We follow the method of Glibichuk and Konyagin [9], which builds upon ideas in [2]. For any subsets $X, Y$ of $\mathbb{Z}_p$ let

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

The key lemma is

**Lemma 6.1.** *[9, Lemma 3.2] For $X, Y \subset \mathbb{Z}_p$ with $|Y| > 1$ and $\frac{X-X}{Y-Y} \ne \mathbb{Z}_p$ we have*

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

*Proof.* If $\frac{X-X}{Y-Y} \ne \mathbb{Z}_p$ then there exist $x_1, x_2 \in X$, $y_1, y_2 \in Y$ such that $\frac{x_1-x_2}{y_1-y_2} + 1 \notin \frac{X-X}{Y-Y}$. But then the mapping from $X \times Y$ into $2XY - 2XY + Y^2 - Y^2$ given by

$$(x, y) \to (y_1 - y_2)x + (x_1 - x_2 + y_1 - y_2)y,$$

is clearly one-to-one and the lemma follows. □

We also use the elementary

**Lemma 6.2.** *Let $A$ be a multiplicative subgroup of $\mathbb{Z}_p^*$ and $X, Y$ be subsets of $\mathbb{Z}_p$ such that $AX \subset X$, $AY \subset Y$. Then*

$$\left| \frac{X-X}{Y-Y} \right| \le \frac{|X-X|(|Y-Y|-1)}{|A|}.$$

*Proof.* If $c = (x_1-x_2)/(y_1-y_2)$ for some $x_1, x_2 \in X$, $y_1 \ne y_2 \in Y$, then $c = (ax_1 - ax_2)/(ay_1 - ay_2)$ for any $a \in A$. □

For $k \in \mathbb{N}$, let

$$a_k = \frac{4^k - 1}{3}, \qquad b_k = \frac{4^k + 8}{6},$$

so that $a_1 = 1$, $a_2 = 5$, $a_3 = 21$, $a_4 = 85$, $b_1 = 2$, $b_2 = 4$, $b_3 = 12$, $b_4 = 44$, and for $k \geq 1$,

$$a_{k+1} = 4a_k + 1, \qquad b_{k+1} = 8a_{k-1} + 4. \tag{6.1}$$

Put

$$A_k = (a_k A - a_k A), \qquad B_k = (b_k A - b_k A).$$

**Theorem 6.1.** *Let $A$ be a multiplicative subgroup of $\mathbb{Z}_p^*$.*

*a) For $k \geq 1$, $|A_k| \geq |A - A||A|^{k-1}$ if $k = 1$ or $|A_{k-1} - A_{k-1}||A - A| < p|A|$.*

*b) For $k \geq 3$, $|B_k| \geq |A - A|^2|A|^{k-3}$ if $|A_{k-2} - A_{k-2}||2A - 2A| < p|A|$.*

*Proof of Theorem 6.1.* a) The statement is trivial for $k = 1$. For $k > 1$, put $X = A_{k-1}$, $Y = A$. The hypothesis $|A_{k-1} - A_{k-1}||A - A| < p|A|$ implies, by Lemma 6.2, that $\frac{X-X}{Y-Y} \neq \mathbb{Z}_p$. Noting that by relation (6.1)

$$2XY - 2XY + Y^2 - Y^2 = 2A_{k-1} - 2A_{k-1} + A - A = (4a_{k-1} + 1)A - (4a_{k+1} + 1)A = A_k,$$

we obtain $|A_k| \geq |A_{k-1}||A|$ by Lemma 6.1. The theorem now follows by induction on $k$.

b) Put $X = A_{k-2}$, $Y = A - A$. Under the assumption of the theorem $(X - X)/(Y - Y) \neq \mathbb{Z}_p$. Now, by relation (6.1), $2XY - 2XY + Y^2 - Y^2 \subseteq (8a_{k-2} + 4)A - (8a_{k-2} + 4)A = B_k$, and so by Lemma 6.1 we have $|B_k| \geq |A_{k-2}||A - A|$. Part (b) follows from the bound in part (a). □

**Theorem 6.2.** *Let $A$ be a multiplicative subgroup of $\mathbb{Z}_p^*$ and $\lambda$ be a positive real number such that $|A - A| \geq \lambda|A|^{3/2}$.*

*a) For $k \geq 1$, $|A_k| \geq \min\{3^{1/3}p^{2/3}, \lambda|A|^{k+\frac{1}{2}}\}$.*

*b) For $k \geq 3$, $|B_k| \geq \min\{3^{3/7}p^{4/7}, \lambda^2|A|^k\}$.*

*Proof.* a) The result is immediate for $k = 1$ or $|A| = 1$, so we assume $k \geq 2$ and $|A| \geq 2$. If $|A_{k-1} - A_{k-1}||A - A| < p|A|$ the inequality follows from Theorem 6.1. Otherwise, $|A_{k-1} - A_{k-1}| \geq p|A|/|A - A|$. Then

$$|A_k| = |a_k A - a_k A| \geq |4a_{k-1}A - 4a_{k-1}A| \geq |A_{k-1} - A_{k-1}| \geq \frac{p|A|}{|A - A|} \geq \frac{p}{|A - A|^{1/2}}.$$

Also by the Cauchy-Davenport relation $|A_k| \geq |A_2| = |5A - 5A| \geq 3|A - A|$ (for $|A| > 1$). Thus $|A_k|^3 \geq (p^2/|A - A|)(3|A - A|) = 3p^2$ and the result follows.

b)We may assume $|A| > 1$. If $|A_{k-2} - A_{k-2}||2A - 2A| < p|A|$ the result follows from Theorem 6.1. Assume that $|A_{k-2} - A_{k-2}||2A - 2A| \geq p|A|$. Then

$$\begin{aligned}|B_k| = |b_kA - b_kA| &\geq |8a_{k-1}A - 8a_{k-a}A| \geq |32a_{k-2}A - 32a_{k-2}A| \geq |A_{k-2} - A_{k-2}| \\ &\geq \frac{p|A|}{|2A - 2A|} \geq \frac{p}{|2A - 2A|^{3/4}}.\end{aligned}$$

Also $|B_k| \geq |12A - 12A| > 3|2A - 2A|$ and so $|B_k|^7 \geq (p^4/|2A - 2A|^3)3^3|2A - 2A|^3$. □

Thus with $\lambda = \frac{1}{4}$ (as given by Lemma 5.2) we have for any multiplicative subgroup $A$ of $\mathbb{Z}_p^*$,

$$\begin{aligned}|A - A| &\geq \min\{\tfrac{1}{4}|A|^{3/2}, p/2\} \\ |3A - 3A| &\geq \min\{|A|^2, 2p^{2/3}\} \\ |5A - 5A| &\geq \min\{\tfrac{1}{4}|A|^{5/2}, 3^{1/3}p^{2/3}\} \\ |12A - 12A| &\geq \min\{\tfrac{1}{16}|A|^3, 3^{3/7}p^{4/7}\} \\ |21A - 21A| &\geq \min\{\tfrac{1}{4}|A|^{7/2}, 3^{1/3}p^{2/3}\} \\ |44A - 44A| &\geq \min\{\tfrac{1}{16}|A|^4, 3^{3/7}p^{4/7}\} \\ |85A - 85A| &\geq \min\{\tfrac{1}{4}|A|^{9/2}, 3^{1/3}p^{2/3}\}\end{aligned}$$

The bound for $|A - A|$ is from Theorems 5.1 and 5.2. The bound for $|3A - 3A|$ follows from Lemma 6.1 when $|A - A|^2 < p|A|$ and from the Cauchy-Davenport inequality otherwise. Further lower bounds on $|nA - nA|$ are given in Section 10.

## 7. Lower Bounds for $|nA|$

For $k \in \mathbb{N}$, put $m_k = \frac{1}{3}4^{k+1} + k - \frac{13}{3}$ and $n_k = \frac{2}{3}4^{k+1} + k - \frac{14}{3}$, so that $m_1 = 2$, $m_2 = 19$, $m_3 = 84$, $n_1 = 7$, $n_2 = 40$, $n_3 = 169$.

**Theorem 7.1.** *Suppose that $A$ is a multiplicative subgroup of $\mathbb{Z}_p^*$ and $\lambda$ is a positive real number such that $|2A| \geq \lambda|A|^{3/2}$ and $|A - A| \geq \lambda|A|^{3/2}$. Then for any $k \in \mathbb{N}$,*

$$\begin{aligned}a)\quad |m_kA| &\geq \min\{\sqrt{2p},\ \alpha_k|A|^{k+\frac{1}{2}}\}, \\ b)\quad |n_kA| &\geq \min\{\sqrt{2p},\ \beta_k|A|^{k+1}\},\end{aligned}$$

*where $\alpha_k = \lambda^{\frac{5}{3} - \frac{8}{3\cdot 4^k}}$, $\beta_k = \lambda^{\frac{4}{3} - \frac{4}{3\cdot 4^k}}$.*

Observing that $3A = \mathbb{Z}_p$ when $|A| > p^{2/3}$ (see, e.g., [7]) and that by Theorem 5.2 we can take $\lambda = 1/4$ for $|A| < p^{2/3}$ , we obtain in particular that for any multiplicative subgroup $A$

of $\mathbb{Z}_p^*$,

$$\begin{aligned}
|2A| &\geq \min\{.25|A|^{3/2}, p/2\} \\
|4A| &\geq \min\{|A|^{3/2}, p^{5/8}\} \\
|7A| &\geq \min\{.25|A|^2, \sqrt{2p}\} \\
|19A| &\geq \min\{.125|A|^{5/2}, \sqrt{2p}\} \\
|40A| &\geq \min\{.177|A|^3, \sqrt{2p}\} \\
|84A| &\geq \min\{.106|A|^{7/2}, \sqrt{2p}\} \\
|169A| &\geq \min\{.163|A|^4, \sqrt{2p}\}.
\end{aligned}$$

The estimate for $|4A|$ comes from $|4A| \geq |A|^{1/2}|3A - 3A|^{1/2} \geq |A|^{3/2}$ for $|A - A|^2 < p|A|$, $|4A| \geq |A - A|^{15/16} \geq (p|A|)^{15/32} \geq p^{5/8}$, otherwise.

In comparison [9, Lemma 5.3] has $|13A| \geq \frac{3}{8}|A|^{13/7}$ for $|A|^2 \leq \frac{p-1}{2}$, $|53A| \geq \frac{3}{8}|A|^{20/7}$ for $|A|^3 \leq \frac{p-1}{2}$, $|213A| \geq \frac{3}{8}|A|^{27/7}$ for $|A|^4 < \frac{p-1}{2}$, etc.

*Proof of Theorem 7.1.* The inequalities $|m_kA| \geq \frac{1}{2}|A|^{k+\frac{1}{2}}$ and $|n_kA| \geq \frac{1}{2}|A|^{k+1}$ follow immediately from the Cauchy-Davenport estimates of $|m_kA|$ and $|n_kA|$ for $|A| < 5$ and so we assume $|A| \geq 5$.

We prove parts (a) and (b) simultaneously by induction on $k$. First note that the validity of part (a) for $k$ implies the validity of part (b) for $k$. If $|m_kA| \geq \sqrt{2p}$ then trivially $|n_kA| \geq \sqrt{2p}$. Otherwise $|m_kA| \geq \alpha_k|A|^{k+\frac{1}{2}}$. Then since $n_k = m_k + a_{k+1}$ we have by Rusza's inequality (2.1): $|n_kA| \geq |m_kA|^{1/2}|a_{k+1}A - a_{k+1}A|^{1/2} \geq |m_kA|^{1/2}|A_{k+1}|^{1/2}$.

If $|A_k - A_k||A - A| < p|A|$ then by Theorem 6.1 and the bound in part (a),

$$|n_kA| \geq \lambda^{\frac{5}{6}-\frac{4}{3\cdot 4^k}}|A|^{\frac{k}{2}+\frac{1}{4}}|A - A|^{1/2}|A|^{k/2} \geq \beta_k|A|^{k+1}.$$

If $|A_k - A_k||A - A| \geq p|A|$ then, in particular, $|2a_kA - 2a_kA| = |A_k - A_k| \geq p^{1/2}|A|^{1/2}$ and $|2a_kA|^2|A| \geq p$. Thus

$$\begin{aligned}
|n_kA| &\geq |3(2a_kA)| \geq |2a_kA|^{1/4}|2a_kA - 2a_kA|^{3/4} \geq |2a_kA|^{1/4}p^{3/8}|A|^{3/8} \\
&= (|2a_kA|^2|A|)^{1/8}|A|^{1/4}p^{3/8} \geq |A|^{1/4}p^{1/2} \geq \sqrt{2p}.
\end{aligned}$$

For $k = 1$ we have $|m_1A| = |2A|$ and so the inequality in (a) is trivial. Suppose the theorem is true for $k - 1$. Note that for $k \geq 2$, $m_k = n_{k-1} + b_{k+1}$ and so by inequality (2.1)

$$|m_kA| \geq |n_{k-1}A|^{1/2}|b_{k+1}A - b_{k+1}A|^{1/2} = |n_{k-1}A|^{1/2}|B_{k+1}|^{1/2}. \tag{7.1}$$

If $|A_{k-1} - A_{k-1}||2A - 2A| < p|A|$ then, by Theorem 6.1(b) and the induction assumption we have

$$\begin{aligned}
|m_kA| &\geq \lambda^{\frac{2}{3}-\frac{2}{3\cdot 4^{k-1}}}|A|^{\frac{k}{2}}|A - A||A|^{\frac{k-2}{2}} \\
&\geq \lambda^{\frac{2}{3}-\frac{8}{3\cdot 4^k}+1}|A|^{k+\frac{1}{2}} = \alpha_k|A|^{k+\frac{1}{2}}.
\end{aligned}$$

If $|A_{k-1}-A_{k-1}||2A-2A| \geq p|A|$ then, in particular, $|2a_{k-1}A-2a_{k-1}A| \geq p^{1/2}|A|^{1/2}$ and $|2a_{k-1}A|^2|A|^3 \geq p$. Thus

$$\begin{aligned}|m_kA| &\geq |4(2a_{k-1}A)| \geq |2a_{k-1}A|^{1/8}|2a_{k-1}A-2a_{k-1}A|^{7/8} \geq |2a_{k-1}A|^{1/8}p^{7/16}|A|^{7/16}\\ &\geq (|2a_{k-1}A|^2|A|^3)^{1/16}|A|^{1/4}p^{7/16} \geq |A|^{1/4}p^{1/2} \geq \sqrt{2p}.\end{aligned}$$

□

**Theorem 7.2.** *Put* $\gamma_k = \left(\frac{2}{\alpha_k^2}\right)^{1/(2k+1)}$, $\delta_k = \left(\frac{2}{\beta_k^2}\right)^{1/(2k+2)}$. *Let $A$ be a multiplicative subgroup of $\mathbb{Z}_p^*$ and $k \in \mathbb{N}$.*

*a) If $|A| \geq \gamma_k p^{1/(2k+1)}$, then $8m_k^2A = \mathbb{Z}_p$.*

*b) If $|A| \geq \delta_k p^{1/(2k+2)}$, then $8n_k^2A = \mathbb{Z}_p$.*

*Proof.* Under the given hypotheses, it follows from Theorem 7.1 that $|m_kA| \geq \sqrt{2p}$ and $|n_kA| \geq \sqrt{2p}$, and so by Lemma 2.1 (b) the theorem follows. □

Letting $\lambda = 1/4$ we obtain the following for any multiplicative subgroup $A$ of $\mathbb{Z}_p^*$:

$$\begin{aligned}8A &= \mathbb{Z}_p \quad \text{for } |A| > p^{1/2}\\ 32A &= \mathbb{Z}_p \quad \text{for } |A| > 3.18p^{1/3}\\ 392A &= \mathbb{Z}_p \quad \text{for } |A| > 2.38p^{1/4}\\ 2888A &= \mathbb{Z}_p \quad \text{for } |A| > 2.64p^{1/5}\\ 12800A &= \mathbb{Z}_p \quad \text{for } |A| > 2p^{1/6}\\ 56448A &= \mathbb{Z}_p \quad \text{for } |A| > 2.11p^{1/7}\\ 228488A &= \mathbb{Z}_p \quad \text{for } |A| > 1.72p^{1/8}.\end{aligned}$$

The result for $8A$ is due to Glibichuk [8, Corollary 4]. Note that $m_k \leq 1.0005\frac{4^{k+1}}{3}$ and $n_k \leq 1.00013\frac{2\cdot 4^{k+1}}{3}$ for any $k \geq 1$. Define $c_1 = c_2 = 1$ and

$$c_\ell = \begin{cases}\gamma_{\frac{\ell-1}{2}} & \text{if } \ell \geq 3 \text{ is odd}\\ \delta_{\frac{\ell-2}{2}} & \text{if } \ell \geq 4 \text{ is even}\end{cases}.$$

Then we obtain from Theorem 7.2 that for $\ell \geq 2$,

$$|A| \geq c_\ell p^{1/\ell} \quad \Longrightarrow \quad 57 \cdot 4^{\ell-2}A = \mathbb{Z}_p. \tag{7.2}$$

**Corollary 7.1.** *For any prime $p$, $\ell \geq 2$ and multiplicative subgroup $A$ of $\mathbb{Z}_p^*$ with $c_\ell p^{1/\ell} \leq |A| < c_{\ell-1}p^{1/(\ell-1)}$, we have $\gamma(A,p) \leq 14.25\ p^{\frac{\ln 4}{\ln(|A|/c_{\ell-1})}}$.*

*Proof.* $|A| \geq c_\ell p^{1/\ell}$ and so $\frac{57}{16}\cdot 4^\ell A = \mathbb{Z}_p$. We also have $(\ell-1)\ln(|A|/c_{\ell-1}) \leq \ln p$. Thus $\gamma(A,p) \leq \frac{57}{16}\cdot 4^{1+\frac{\ln p}{\ln(|A|/c_{\ell-1})}} \leq 14.25p^{\frac{\ln 4}{\ln(|A|/c_{\ell-1})}}$. □

## 8. Bovey's Method for Small $|A|$.

For small $|A|$ we use a method of Bovey to bound $\delta(k,p)$ and $\gamma(k,p)$. Let $t = |A|$ so that $tk = (p-1)$ and put $r = \phi(t)$. Let $R$ be a primitive $t$-th root of one $\pmod p$, that is, a generator of the cyclic group $A$, and $\Phi_t(x)$ be the $t$-th cyclotomic polynomial over $\mathbb{Q}$ of degree $r$ and $\omega$ be a primitive $t$-th root of unity over $\mathbb{Q}$. In particular, $\Phi_t(R) \equiv 0 \pmod p$. Let $f : \mathbb{Z}^r \to \mathbb{Z}[\omega]$ be given by

$$f(x_1, x_2, \ldots, x_r) = x_1 + x_2\omega + \cdots + x_r\omega^{r-1}.$$

Then $f$ is a one-to-one $\mathbb{Z}$-module homomorphism.

Consider the linear congruence

$$x_1 + Rx_2 + R^2x_3 + \cdots + R^{r-1}x_r \equiv 0 \pmod p. \tag{8.1}$$

By the box principle, we know there is a nonzero solution of (8.1) in integers $v_1 = (a_1, a_2, \ldots, a_r)$ with $|a_i| \le [p^{1/r}] \le (p-1)^{1/r}$, $1 \le i \le r$. For $2 \le i \le r$ set $v_i = f^{-1}(\omega^{i-1}f(v_1))$. Then $v_1, \ldots, v_r$ form a set of linearly independent solutions of (8.1) and by [3, Lemma 3]

$$\delta(k,p) \le \frac{1}{2}\sum_{i=1}^{t} \|v_i\|_1,$$

where $\|(x_1, x_2, \ldots, x_t)\|_1 = \sum_{i=1}^{t} |x_i|$. To determine the latter sum we start with the system

$$\begin{array}{ccccccc}
a_1 & + & a_2\omega & + & \ldots & + & a_r\omega^{r-1} \\
a_1\omega & + & a_2\omega^2 & + & \ldots & + & a_r\omega^{r} \\
a_1\omega^2 & + & a_2\omega^3 & + & \ldots & + & a_r\omega^{r+1} \\
a_1\omega^3 & + & a_2\omega^4 & + & \ldots & + & a_r\omega^{r+2} \\
a_1\omega^4 & + & a_2\omega^5 & + & \ldots & + & a_r\omega^{r+3} \\
\ldots & & & & & & \ldots \\
a_1\omega^{r-1} & + & a_2\omega^{r} & + & \ldots & + & a_r\omega^{2r-2}
\end{array}$$

and then reduce the higher powers of $\omega$ to powers less than $r$ using $\Phi_t$ or any other relation that is convenient. Note that for $0 \le i \le r-1$, $\omega^i$ occurs $i+1$ times in the array, while for $r \le i \le 2r-2$, $\omega^i$ occurs $2r-1-i$ times. If $\omega^i$ can be expressed as a sum/difference of $w_i$ powers of $\omega$ less than $r$ then we will call $w_i$ the weight of $\omega^i$ in the above system. We see that

$$\delta(k,p) \le \frac{1}{2}\left(\sum_{i=1}^{r} i + \sum_{i=r}^{2r-2} w_i(2r-1-i)\right)(p-1)^{1/r}.$$

In passing from $\delta(k,p)$ to $\gamma(k,p)$ we use the relation of Theorem 4.1 (d),

$$\gamma(k,p) \le (p_{min}-1)\delta(k,p). \tag{8.2}$$

where $p_{min}$ is the minimal prime divisor of $t$. To illustrate the method we consider a few special cases.

Case 1. Suppose $t$ is a prime power $q^\alpha$ so that $r = q^\alpha - q^{\alpha-1}$. Then $\omega^{r+q^{\alpha-1}} = 1$ and $\omega^r = -\sum_{i=0}^{q-2} \omega^{q^{\alpha-1}i}$. It follows that $w_i = q-1$ for $i = r, \dots, r+q^{\alpha-1}-1$ and that $w_i = 1$ for $i = r+q^{\alpha-1}, \dots, 2r-2$. Thus

$$\delta(k,p) \le \frac{1}{2}\left(\sum_{i=1}^{r} i + \sum_{i=r}^{r+q^{\alpha-1}-1} (2r-1-i)(q-1) + \sum_{i=r+q^{\alpha-1}}^{2r-2} (2r-1-i)\right)(p-1)^{1/r} \quad (8.3)$$

and so

$$\delta(k,p) \le \frac{1}{4}q^{\alpha-1}\left(q^{\alpha-1}(4q^2-11q+8)-(q-2)\right)(p-1)^{1/r} < t^{2+\frac{1}{r}}\ k^{1/r},$$

$$\gamma(k,p) \le \frac{1}{4}(q-1)q^{\alpha-1}\left(q^{\alpha-1}(4q^2-11q+8)-(q-2)\right)(p-1)^{1/r} < t^{3+\frac{1}{r}}\ k^{1/r}.$$

In particular, for $t = 2^\alpha$, we have $\delta(k,p) \le \frac{t^2}{8}(p-1)^{1/r}$, and for prime $t = q$

$$\delta(k,p) \le (t^2-3t+2.5)(p-1)^{1/(t-1)}, \quad \gamma(k,p) \le (t-1)(t^2-3t+2.5)(p-1)^{1/(t-1)}. \quad (8.4)$$

Case 2. Suppose $t = 2q$ where $q$ is a prime, so that $r = q-1$ and we have $\omega^q = -1$, $\omega^{q-1} = -1+\omega-\cdots+\omega^{q-2}$. We obtain

$$\sum_{i=1}^{r} \|v_i\|_1 \le \left(\frac{t^2}{2} - 3t + 5\right)(p-1)^{2/(t-2)},$$

$\delta(k,p) \le (.25t^2 - 1.5t + 2.5)(p-1)^{2/(t-2)}$ and $\gamma(k,p) \le (.25t^2 - 1.5t + 2.5)(p-1)^{2/(t-2)}$.

Case 3. $t = 21$, $r = 12$. We have $\omega^{12} = \omega^{11} - \omega^9 + \omega^8 - \omega^6 + \omega^4 - \omega^3 + \omega - 1$, and $\omega^{14} = -\omega^7 - 1$. Thus $\omega^{13} = \omega^{11} - \omega^{10} + \omega^8 - \omega^7 - \omega^6 + \omega^5 - \omega^3 + \omega^2 - 1$ giving it a weight of 9. $\omega^{14}$ to $\omega^{18}$ each have weight 2, $\omega^{19}$ weight 9, $\omega^{20}$ weight 8, $\omega^{21}$ and $\omega^{22}$ each of weight 1. Altogether we get

$$\sum_{i=1}^{r} \|v_i\|_1 \le (1+\cdots+12+8\cdot11+9\cdot10+2(9+\cdots+5)+9\cdot4+8\cdot3+1(2+1))p^{1/12} = 389p^{1/12},$$

$\delta(k,p) \le 194.5p^{1/12}$ and $\gamma(k,p) \le 389p^{1/12}$.

In a similar manner we obtain the following table of upper bounds for $\delta(k,p)$ and $\gamma(k,p)$. The values for $t = 3, 4$ and 6 were determined in [6]. The $p$'s appearing in the table may be replaced by $(p-1)$.

| $t$ | $\delta(k,p)$ | $\gamma(k,p)$ | $t$ | $\delta(k,p)$ | $\gamma(k,p)$ |
|---|---|---|---|---|---|
| 2 | $(p-1)/2$ | $(p-1)/2$ | 21 | $194.5p^{1/12}$ | $389p^{1/12}$ |
| 3 | $2\sqrt{k}$ | $2\sqrt{k}-1$ | 22 | $90.5p^{1/10}$ | $90.5p^{1/10}$ |
| 4 | $2\sqrt{k}-1$ | $2\sqrt{k}-1$ | 23 | $462.5p^{1/22}$ | $10175p^{1/22}$ |
| 5 | $12.5p^{1/4}$ | $50p^{1/4}$ | 24 | $43p^{1/8}$ | $43p^{1/8}$ |
| 6 | $\frac{2}{3}\sqrt{6k}$ | $\frac{2}{3}\sqrt{6k}$ | 25 | $327.5p^{1/20}$ | $1310p^{1/20}$ |
| 7 | $30.5p^{1/6}$ | $183p^{1/6}$ | 26 | $132.5p^{1/12}$ | $132.5p^{1/12}$ |
| 8 | $8p^{1/4}$ | $8p^{1/4}$ | 27 | $220.5p^{1/18}$ | $441p^{1/18}$ |
| 9 | $24p^{1/6}$ | $48p^{1/6}$ | 28 | $124.5p^{1/12}$ | $124.5p^{1/12}$ |
| 10 | $12.5p^{1/4}$ | $12.5p^{1/4}$ | 29 | $756.5p^{1/28}$ | $21182p^{1/28}$ |
| 11 | $90.5p^{1/10}$ | $905p^{1/10}$ | 30 | $74p^{1/8}$ | $74p^{1/8}$ |
| 12 | $10.5p^{1/4}$ | $10.5p^{1/4}$ | 31 | $870.5p^{1/30}$ | $26115p^{1/30}$ |
| 13 | $132.5p^{1/12}$ | $1590p^{1/12}$ | 32 | $128p^{1/16}$ | $128p^{1/16}$ |
| 14 | $30.5p^{1/6}$ | $30.5p^{1/6}$ | 33 | $583.5p^{1/20}$ | $1167p^{1/20}$ |
| 15 | $74p^{1/8}$ | $148p^{1/8}$ | 34 | $240.5p^{1/16}$ | $240.5p^{1/16}$ |
| 16 | $32p^{1/8}$ | $32p^{1/8}$ | 35 | $1233p^{1/24}$ | $4932p^{1/24}$ |
| 17 | $240.5p^{1/16}$ | $3848p^{1/16}$ | 36 | $97.5p^{1/12}$ | $97.5p^{1/12}$ |
| 18 | $24p^{1/6}$ | $24p^{1/6}$ | 37 | $1260.5p^{1/36}$ | $45378p^{1/36}$ |
| 19 | $306.5p^{1/18}$ | $5517p^{1/18}$ | 38 | $306.5p^{1/18}$ | $306.5p^{1/18}$ |
| 20 | $51.5p^{1/8}$ | $51.5p^{1/8}$ | | | |

## 9. Proof of Theorem 1.1

Let $t = |A| > 2$. As noted in (1.3), for $t = 3, 4$, $\gamma(k,p) \le 2\sqrt{k}$ and so we may assume $t \ge 5$. The inequality $\gamma(k,p) \le [k/2]+1$ of S. Chowla, Mann and Strauss [5], implies the theorem for $k \le 27551$ and so we assume $k > 27551$. The first step is to prove the theorem for $t < 34$ using the table from the previous section. Suppose $t$ is a prime. Then by (8.4),

$$\gamma(k,p) \le (t-1)(t^2-3t+2.5)t^{1/(t-1)}k^{1/(t-1)} \le 83\ k^{1/2},$$

provided that $k > 10^6$, $t < 34$. For $k < 10^6$, $p < 4 \cdot 10^7 < 2^{2^5}$ and so by Theorem 4.1 (c), $\gamma(k,p) \le 10\delta(k,p)$. Thus we get the improved (for $t > 10$) upper bound

$$\gamma(k,p) \le 10(t^2-3t+2.5)t^{1/(t-1)}k^{1/(t-1)}.$$

With the aid of a calculator one can check that the latter quantity is less than $83k^{1/2}$ for $t \le 31$ and $k \ge 27552$.

For nonprime values of $t < 34$, we turn to the table in the previous section. We note that if $\gamma(k,p) \le C(p-1)^{1/r}$ then $\gamma(k,p) \le 83\ k^{1/2}$ provided that $k > (C/83)^{2r/(r-2)}t^{2/(r-2)}$. Using the values of $C$ in the table one checks that the statement is valid for $k > 27551$.

Finally, suppose that $t \geq 34$ and that $k > 27551$. If $t > c_6 p^{1/6}$ we have by Theorem 7.2, $\gamma(k,p) \leq 12800 < 83\ k^{1/2}$. Next, assume $t < c_6 p^{1/6} = 2p^{1/6}$. Say $c_\ell p^{1/\ell} \leq t < c_{\ell-1} p^{1/(\ell-1)}$ for some $\ell \geq 7$. Then by Corollary 7.1, and noting that $2.102 > c_7 > c_6 > c_8 > c_9 \ldots$ we have

$$\begin{aligned}\gamma(k,p) &\leq 14.25\ p^{\frac{\ln 4}{\ln(t/c_7)}} \leq 14.25 \cdot (t+1/k)^{\frac{\ln 4}{\ln(t/c_7)}} k^{\frac{\ln 4}{\ln(t/c_7)}} \\ &\leq 14.25\,(34+1/27552)^{\frac{\ln 4}{\ln(34/c_7)}}\, k^{\frac{\ln 4}{\ln(34/c_7)}} \leq 83\ k^{.499}.\end{aligned}$$

## 10. Lower Bounds for $|nA - nA|$, Part II

The lower bounds on $|A_k|$ and $|B_k|$ established in Section 6 were sufficient for yielding good upper bounds on $\gamma(k,p)$. One can achieve slightly better upper bounds on $\delta(k,p)$ by using the following variant of Theorem 6.1.

**Theorem 10.1.** *For any multiplicative subgroup $A$ of $\mathbb{Z}_p^*$,*

*a)* $|3A - 3A| \geq \begin{cases} \frac{1}{2}\min\{|A|^2, p+1\} & \text{for any } A \\ |A|^2 & \text{for } |A| \leq p^{1/3}. \end{cases}$

*b) For $k \geq 1$,* $|A_k| \geq \begin{cases} \frac{3}{8}\min\{|A-A||A|^{k-1}, \frac{p+1}{2}\} \\ |A-A||A|^{k-1} & \text{for } |A| < p^{\frac{1}{k+2}}. \end{cases}$

*c) For $k \geq 3$,* $|B_k| \geq \begin{cases} \min\{\frac{3}{16}|A-A|^2|A|^{k-3}, \frac{p+1}{2}\}, \\ |A-A|^2|A|^{k-3} & \text{for } |A| < p^{\frac{1}{k+4}}. \end{cases}$

The theorem follows from a couple of lemmas of Glibichuk and Konyagin.

**Lemma 10.1.** *[9, Corollary 3.5] For $X, Y \subset \mathbb{Z}_p$ with $|Y| > 1$,*

$$|2XY - 2XY + Y^2 - Y^2| > \frac{|X||Y|(p-1)}{|X||Y| + p - 1}.$$

(Although their lemma is stated with a nonstrict inequality, the proof makes it clear that it is strict.)

The following lemma is the same as Glibichuk and Konyagin [9, Lemma 5.1] applied to a slightly different set $A_k$.

**Lemma 10.2.** *Suppose $A$ is a multiplicative subgroup of $\mathbb{Z}_p^*$ with $|A| \geq 5$. For any $k$ and real number $U$ with $0 \leq U \leq |A-A||A|^{k-1}$ we have*

$$|A_k| \geq U - \frac{5}{4}\frac{U^2}{p-1}.$$

*Proof.* The proof is by induction on $k$, with $k = 1$ being trivial. We use Lemma 10.1 with $X = A_{k-1}$, $Y = A$. Noting that $2XY - 2XY + Y^2 - Y^2 = 2A_{k-1} - 2A_{k-1} + A - A = A_k$, as above, we obtain

$$|A_k| \geq \frac{|A_{k-1}||A|(p-1)}{|A_{k-1}||A| + p - 1}, \tag{10.1}$$

and the proof proceeds identically as in [9]. □

*Proof of Theorem 10.1.* a) Put $X = Y = A$ in 10.1 to get $|3A-3A| \geq \frac{|A|^2(p-1)}{|A|^2+p-1}$. If $|A|^2 \leq p-1$ then $|3A - 3A| \geq \frac{1}{2}|A|^2$, while if $|A|^2 > p - 1$ then $|3A - 3A| > \frac{1}{2}(p - 1)$. If $|A|^3 < p$ then $|\frac{A-A}{A-A}| \leq |A|^3 < p$ and so Lemma 6.1 gives $|3A - 3A| \geq |A|^2$.

b) Put $U = \min\{|A-A||A|^{k-1}, \frac{p-1}{2}\}$. Then by Lemma 10.2, $|A_k| \geq \frac{3}{8}\min\{|A-A||A|^{k-1}, \frac{p-1}{2}\}$, provided that $|A| \geq 5$. For $|A| = 1, 2, 3, 4$ the inequality follows from the Cauchy-Davenport bound $|A_k| \geq \min\{p, 2a_k(|A|-1)+1\}$ and $|A-A| = 1, 3, 7, 9$ for $|A| = 1, 2, 3, 4$ respectively.

The second inequality is proven by induction on $k$, the case $k = 1$ being trivial. Suppose the statement is true for $k - 1$ and let $|A|^{k+2} < p$. Put $X = A_{k-1}$, $Y = A$. If $|X - X| < |A - A||A|^{k-1}$, in which case $|X - X||A - A|/|A| < p$, we can apply Theorem 6.1 to get the result. If $|X - X| \geq |A - A||A|^{k-1}$ then since $A_k \supset X - X$ the result is immediate.

c) Suppose $k \geq 3$. If $|A| = 1$ the bound is trivial, so assume $|A| > 1$. Put $X = A_{k-2}$, $Y = A - A$. Then

$$2XY - 2XY + Y^2 - Y^2 = 8\frac{4^{k-2}-1}{3}A - 8\frac{4^{k-2}-1}{3}A + 4A - 4A = B_k,$$

and so by Lemma 10.1

$$|B_k| \geq \min\left\{\frac{|A_{k-2}||A-A|}{2}, \frac{p+1}{2}\right\}$$

and the result follows from the bound in part (b).

Suppose now that $|A|^{k+4} < p$. If $|A_{k-2}-A_{k-2}| < |A-A|^2|A|^{k-3}$, in which case $|X-X||Y-Y|/|A| < p$, then the result follows from Theorem 6.1. Otherwise $|B_k| \geq |A_{k-2} - A_{k-2}| \geq |A - A|^2|A|^{k-3}$. □

**Corollary 10.1.** *Let $A$ be a multiplicative subgroup of $\mathbb{Z}_p^*$ with $|A| > 1$ and $\lambda < 1$ be a positive real with $|A - A| \geq \lambda|A|^{3/2}$.*

*a) For $k \geq 1$ if $|A| \geq (\frac{8}{3\lambda})^{2/(2k+1)}p^{2/(2k+1)}$ then $2a_kA - 2a_kA = \mathbb{Z}_p$.*

*b) For $k \geq 3$, if $|A| > (\frac{8}{3\lambda^2})^{1/k}p^{1/k}$ then $2b_kA - 2b_kA = \mathbb{Z}_p$.*

*Proof.* a) As seen in (10.1), $|A_k| > \min\left\{\frac{|A_{k-1}||A|}{2}, \frac{p}{2}\right\}$. Under the given hypotheses we have, by Theorem 10.1,

$$|A||A_{k-1}| \geq \min\left\{\frac{3}{8}\lambda|A|^{k+\frac{1}{2}}, \frac{3}{8}\frac{p+1}{2}|A|\right\} \geq p,$$

for $|A|>5$. Thus $|A_k|>\frac{p}{2}$ and $2A_k=\mathbb{Z}_p$. If $|A|=2,3$, or 4 then the corollary follows readily from the Cauchy-Davenport inequality, $|2a_kA-2a_kA|\geq\min\{p,4a_k(|A|-1)+1\}$. For $|A|=5$ the conditions require $k\geq 3$. Using the bound for $\delta(A,p)$ from the table in Section 8 ($t=5$), we get

$$\delta(A,p)\leq 12.5p^{1/4}\leq 12.5(3\lambda/8)^{1/4}5^{\frac{2k+1}{8}}\leq 12\cdot 5^{k/4}\leq\frac{2}{3}(4^k-1)=2a_k.$$

b) Under the given hypothesis $\frac{3}{16}\lambda^2|A|^k>\frac{p}{2}$ and so by Theorem 10.1, $|B_k|>\frac{p}{2}$. Thus $2B_k=\mathbb{Z}_p$. $\square$

Thus we obtain (with $\lambda=.25$)

$$\begin{aligned}
4A-4A&=\mathbb{Z}_p &&\text{for}\quad |A|>\sqrt{p}\\
10A-10A&=\mathbb{Z}_p &&\text{for}\quad |A|>2.58p^{2/5}\\
16A-16A&=\mathbb{Z}_p &&\text{for}\quad |A|>3.18p^{1/3}\\
42A-42A&=\mathbb{Z}_p &&\text{for}\quad |A|>1.97p^{2/7}\\
88A-88A&=\mathbb{Z}_p &&\text{for}\quad |A|>2.56p^{1/4}\\
170A-170A&=\mathbb{Z}_p &&\text{for}\quad |A|>1.70p^{2/9}\\
344A-344A&=\mathbb{Z}_p &&\text{for}\quad |A|>2.12p^{1/5}\\
682A-682A&=\mathbb{Z}_p &&\text{for}\quad |A|>1.54p^{2/11}\\
1368A-1368A&=\mathbb{Z}_p &&\text{for}\quad |A|>1.87p^{1/6}.
\end{aligned}$$

The result for $4A-4A$ is due to Glibichuk [8]. The result for $16A-16A$ is obtained from $|A-A|\geq .25|A|^{3/2}\geq\sqrt{2p}$ for $|A|>3.18p^{1/3}$, and thus $8(A-A)(A-A)=\mathbb{Z}_p$.

Put

$$d_\ell=(8/(3\lambda))^{1/\ell}\text{ for }\ell=3/2,5/2,7/2,\ldots. \tag{10.2}$$

Applying Corollary 10.1 (a) with $k=\ell-\frac{1}{2}$ we see that if $|A|\geq d_\ell p^{1/\ell}$ then $\delta(A,p)\leq 4a_k=\frac{4}{3}(4^k-1)=\frac{2}{3}4^\ell-\frac{4}{3}$. We deduce

**Corollary 10.2.** *For any prime p and multiplicative group A with $d_\ell p^{1/\ell}\leq|A|\leq d_{\ell-1}p^{1/(\ell-1)}$ for some half integer $\ell\geq 5/2$, we have*

$$\delta(A,p)\leq\tfrac{8}{3}\;p^{\frac{\ln 4}{\ln(|A|/d_{\ell-1})}}.$$

**Corollary 10.3.** *For $t>2$ we have the uniform upper bound, $\delta(k,p)\leq 20k^{1/2}$.*

*Proof.* For $k\leq 1595$ the result follows from $\delta(k,p)\leq[k/2]+1\leq 20k^{1/2}$. Suppose that $k>1595$. We note that $\delta(k,p)\leq C(p-1)^{1/r}$ implies $\delta(k,p)\leq 20k^{1/2}$ provided that $k>(C/20)^{2r/(r-2)}t^{2/(r-2)}$. Using the values of $C$ given in the table in Section 6 we see that the latter holds for $t<29$, $k>1595$. Next, if $t>1.70p^{2/9}$ then $\delta(k,p)\leq 340\leq 20k^{1/2}$ for

$k > 1595$. Otherwise, $d_\ell p^{1/\ell} \le t \le d_{\ell-1} p^{1/\ell-1}$ for some half integer $\ell \ge 11/2$. If $29 \le t < 50$ then we can take $\lambda = .28$ in the definition of $d_\ell$ (10.2) since

$$\frac{|A-A|}{|A|^{3/2}} \ge \frac{2t-1}{t^{3/2}} \ge \frac{99}{50^{3/2}} \ge .28,$$

and get $d_{9/2} = 1.6501\ldots$. Thus by Corollary 10.2

$$\delta(k,p) \le \tfrac{8}{3}\ (29 + \tfrac{1}{1595})^{\frac{\ln 4}{\ln(29/1.6502)}} k^{\frac{\ln 4}{\ln(29/1.6502)}} \le 14k^{.49}.$$

Finally, if $t \ge 50$ then we take $\lambda = .25$, $d_{9/2} = 1.70$, and get

$$\delta(k,p) \le \tfrac{8}{3}\ (50 + \tfrac{1}{1595})^{\frac{\ln 4}{\ln(50/1.70)}} k^{\frac{\ln 4}{\ln(50/1.70)}} \le 14k^{.41}.$$

$\square$

## References


[1] J. Bourgain, *Mordell's exponential sum estimate revistited*, J. Amer. Math. Soc. 18, no. 2 (2005), 477-499.

[2] J. Bourgain, A.A. Glibichuk and S.V. Konyagin, *Estimates for the number of sums and products and for exponential sums in fields of prime order*, J. London Math. Soc. (2) 73 (2006), 380-398.

[3] J. D. Bovey, *A new upper bound for Waring's problem (mod p)*, Acta Arith. 32 (1977), 157-162.

[4] A. Cauchy, *Recherches sur les nombres*, J. Ecole Polytechnique 9 (1813), 99-116.

[5] S. Chowla, H. B. Mann and E. G. Straus, *Some applications of the Cauchy-Davenport theorem*, Norske Vid. Selsk. Forh. Trondheim 32 (1959), 74-80.

[6] 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.

[7] T. Cochrane and C. Pinner, *Small values for Waring's number modulo p*, preprint.

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

[9] 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.

[10] D. R. Heath-Brown and S. Konyagin, *New bounds for Gauss sums derived from kth powers, and for Heilbronn's exponential sum*, Quart. J. Math. 51 (2000), 221-235.

[11] H. Heilbronn, *Lecture Notes on Additive Number Theory mod p*, California Institute of Technology (1964).

[12] 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.

[13] 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.

[14] S. V. Konyagin and I. E. Shparlinski, *Character sums with exponential functions and their applications*, Cambridge Univ. Press, Cambridge, 1999.

[15] M.B. Nathanson, *Additive Number Theory, Inverse Problems and the Geometry of Sumsets*, Graduate Texts in Mathematics 165, Springer, New York, 1996.

[16] A. Weil, *Number of solutions of equations in finite fields,* Bull. AMS 55 (1949), 497-508.