#A35 INTEGERS 23 (2023)

DOUBLING CONSTANT FOR SUBGROUPS OF $\mathbb{Z}_P^*$

Albert Cochrane
Department of Mathematics, Kansas State University Manhattan, Kansas
albertc@ksu.edu

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

Craig Spencer
Department of Mathematics, Kansas State University, Manhattan, Kansas
cvs@math.ksu.edu

Received: 3/14/22, Accepted: 4/17/23, Published: 4/24/23

Abstract

For any prime p and $t|(p-1)$, let A be the multiplicative subgroup of $\mathbb{Z}_p^*$ of order t, and $2A = A + A$, a union of λ_A cosets of A, together with $\{0\}$ in case t is even. For fixed n, we characterize all A for which $\lambda_A = n$. For $n = 1, 2, 3, 4$ we provide, with proof, a complete list of all such groups, while for $n = 5$ to 10 we make a conjecture based on our data. A has maximal doubling if $\lambda_A = \min(k, \lceil t/2 \rceil)$. We show A has maximal doubling if $t < \log_3 p$. Finally, we find all groups A contained in an arithmetic progression of length at most $\frac{3}{2}|A|$, generalizing a result of Chowla, Mann and Straus.

1. Introduction

Let p be a prime, $\mathbb{Z}_p = \mathbb{Z}/\mathbb{Z}p$, $\mathbb{Z}_p^* = \mathbb{Z}_p \setminus \{0\}$, and A be the multiplicative subgroup of $\mathbb{Z}_p^*$ of order $t = |A|$. Put $k := (p-1)/t$, so that A is the group of k-th powers in $\mathbb{Z}_p^*$. For convenience, we identify A with the ordered triple (k, t, p), and write

$$A \sim (k, t, p), \quad \text{to mean} \quad A \subseteq \mathbb{Z}_p^*, \quad |A| = t, \quad k = (p-1)/t.$$

Define

$$2A = A + A := \{a_1 + a_2 : a_1, a_2 \in A\},$$

and for any $x \in \mathbb{Z}_p^*$, define xA to be the coset $xA := \{xa : a \in A\}$. Throughout the paper, $2A$ always denotes the sum set $A + A$, not the coset where 2 is viewed

DOI: 10.5281/zenodo.7859042

as an element of $\mathbb{Z}_p^*$. Note that $2A$ is invariant under multiplication by elements of A, and so it is a union of cosets of A together possibly with 0. Since $-1 \in A$ if and only if t is even, we have $0 \in 2A$ if and only if t is even. Thus, letting $\lambda = \lambda_A$ denote the number of distinct cosets in $2A$,

$$|2A| = \begin{cases} \lambda|A|, & \text{if } t \text{ is odd;} \\ \lambda|A| + 1, & \text{if } t \text{ is even.} \end{cases} \tag{1.1}$$

The *doubling constant* for A is the ratio $\frac{|2A|}{|A|} = \lambda$ or $\lambda + \frac{1}{t}$, for t odd or even respectively.

The first objective of this paper is to determine all groups A for which $\lambda_A = n$, where n is a fixed natural number. The results were largely discovered by analyzing the computer generated data presented in Section 8, part of which can be found in the first author's thesis [5].

The problem of describing subsets S of additive groups with small doubling, $|2S| \leq K|S|$ with K a fixed constant, has received much attention. Freiman [9] gave a description of such sets in $\mathbb{Z}$ in terms of general arithmetic progressions. Ruzsa [18, 19], and Green and Ruzsa [11] generalized Freiman's Theorem to abelian groups while Breuillard, Green and Tao [3] addressed the problem for the case of non-abelian groups. In Section 11 we make use of quantitative results of Freiman [8], and Hamoudine and Rodseth [12] on small doubling, for the problem at hand.

Heath-Brown and Konyagin [14], Cochrane and Pinner [7], Shkredov [20] and Hart [13] established the following lower bounds on $|2A|$:

$$\begin{aligned} &|2A| \gg |A|^{\frac{3}{2}}, \quad \text{for } |A| < p^{2/3} \quad [14]; \\ &|2A| \geq \tfrac{1}{4}|A|^{\frac{3}{2}}, \quad \text{for } |A| < p^{2/3} \quad [7]; \\ &|2A| \gg_{\varepsilon} |A|^{\frac{8}{5}-\varepsilon}, \quad \text{for } |A| < p^{\frac{5}{9}-\varepsilon} \quad [20] \text{ and } [13]. \end{aligned}$$

It is elementary that $|2A| \leq \frac{t(t+1)}{2}$ since there are $\binom{t}{2}$ ways of adding distinct elements of A, and an additional t ways of adding an element to itself. If t is even, there are $\frac{t}{2}$ sums with $a_1 + a_2 = 0$, and so $|2A| \leq \frac{t(t+1)}{2} - (\frac{t}{2} - 1) = \frac{t^2}{2} + 1$. We say that the group A has *maximal doubling* if this upper bound is attained, or if $2A \supseteq \mathbb{Z}_p^*$, that is,

$$|2A| = \begin{cases} \min(\frac{t(t+1)}{2},\ p-1), & \text{for odd } t; \\ \min(\frac{t^2}{2}+1,\ p), & \text{for even } t. \end{cases}$$

Thus, A has maximal doubling if and only if

$$\lambda_A = \min\left(k, \lceil t/2 \rceil\right). \tag{1.2}$$

The second objective of this paper is to characterize when a subgroup A has maximal doubling. To do this, for fixed t we define the set of primes

$$\mathcal{P}_t := \{p \in \mathcal{P} : p \equiv 1 \bmod t \text{ and } p | R(f(x), \Phi_t(x)) \text{ for some } f(x)\}, \tag{1.3}$$

where $\mathcal{P}$ is the set of primes, $\Phi_t(x)$ the t-th cyclotomic polynomial and $f(x)$ runs through all polynomials of the form $f(x) = x^{k_1} + x^{k_2} - x^{l_1} - x^{l_2}$, $0 \le k_1, k_2, l_1, l_2 < t$, such that the resultant $R(f(x), \Phi_t(x))$ is nonzero. In particular, $\mathcal{P}_t$ is a finite set. Groups $A \sim (k, t, p)$ for which $p \in \mathcal{P}_t$, fail to have maximal combinatorial doubling, that is, $\lambda_A < \lceil t/2 \rceil$; see Lemma 3.

For groups of small size, maximal doubling can be characterized as follows.

Theorem 1. *Let $A \sim (k, t, p)$ be a group with $t \le \sqrt{2(p-1)}$. Then A has maximal doubling if and only if $p \notin \mathcal{P}_t$.*

If $t > \sqrt{2(p-1)}$, then necessarily $p \in \mathcal{P}_t$, and maximal doubling is equivalent to the statement $2A \supseteq \mathbb{Z}_p^*$.

A subgroup always has maximal doubling if t is sufficiently large or sufficiently small relative to p, as the next theorem indicates.

Theorem 2. *The following hold:*

(i) If $A \sim (k, t, p)$ is a group with $t > p^{3/4}$ then $2A \supseteq \mathbb{Z}_p^*$.

(ii) If $A \sim (k, t, p)$ is a group with $t < \log_3 p$, then $\lambda_A = \lceil t/2 \rceil$.

Part (i) of the theorem can be deduced from results of Weil [22], and Hua and Vandiver [15] on the number of solutions to the equation $x^k + y^k = c$ over $\mathbb{Z}_p$. We provide another proof here. Most likely, the size $p^{3/4}$ can be substantially reduced.

Question 1.1. Does there exist an absolute constant c_1 such that if $t > c_1 \sqrt{p \log p}$, then $2A \supseteq \mathbb{Z}_p^*$?

The size $\sqrt{p \log p}$ is motivated by the comment after (1.4). We have shown that one can take $c_1 = 2$ for any group with $p < 2.5 \cdot 10^6$, except for $A \sim (115, 6532, 751181)$, which requires $c_1 = 2.049$; see Table 6. In part (ii) of Theorem 2, the $\log_3 p$ can likely be improved to $\log_2 p$; see Conjecture 5.1.

Maximal doubling is very common for multiplicative subgroups. Even when it does not occur, it is reasonable to ask the following.

Question 1.2. Does there exist an absolute constant c_2 such that uniformly

$$|2A| \ge c_2 \cdot \min\left(\frac{t^2}{2},\ p - 1\right),$$

for any subgroup A?

Our computations have shown that for $p < 2.5 \cdot 10^6$ we can take $c_2 = 1/2$ for all but six groups, the worst case requiring $c_2 = .458$; see Table 5. We know of no example of a group with $p > 246241$ requiring a value of $c_2 < 1/2$.

An ideal exponential sum bound of the sort conjectured in [16], say

$$\left|\sum_{x\in A} e_p(ax)\right| \le c'\sqrt{t\log p},$$

for all a with $p \nmid a$, where c' is a constant and $e_p(ax) = e^{\frac{2\pi iax}{p}}$, together with (9.2) and (9.5), yields the slightly weaker result

$$|2A| \ge \min\left(\frac{t^2}{c'\log p}, \frac{p}{2}\right). \tag{1.4}$$

This implies in particular that $|2A| > p/2$ for $t > (c'/2)^{\frac{1}{2}}\sqrt{p\log p}$.

2. Solving $|2A| = n|A|$ for a Fixed Value of n

We now fix a positive integer n, and determine the subgroups A such that $\lambda_A = n$, that is, $|2A| = n|A|$ or $n|A| + 1$. To get our feet wet, consider the cases $n = 1$ and $n = 2$. It is easy to see that $\lambda_A = 1$ if and only if $t = 1$, 2 or $p - 1$, that is, $A = \{1\}$, $\{1, -1\}$ or $\mathbb{Z}_p^*$. These happen to be the only subgroups that are arithmetic progressions [4]. Next, for $n = 2$ we obtain

Theorem 3. *Let A be a multiplicative subgroup of $\mathbb{Z}_p^*$ with $p > 5$. Then:*

(i) $|2A| = 2|A|$ *if and only if* $t = 3$*, or* t *is odd and* $k = 2$*;*

(ii) $|2A| = 2|A| + 1$ *if and only if* $t = 4$*, or* t *is even and* $k = 2$.

Let us examine the cases where $n = 2$, identified by the theorem. If $k = 2$, then A is the group of squares mod p, $t = \frac{p-1}{2}$ and by the Cauchy-Davenport Theorem, $|2A| \ge |A| + |A| - 1 = p - 2$. Thus for $p > 5$, $|2A| = 2t = p - 1$, if t is odd; $|2A| = 2t + 1 = p$, if t is even. If $t = 3$, say $A = \langle\omega\rangle = \{1, \omega, \omega^2\}$, then

$$2A = \{2, 2\omega, 2\omega^2, 1 + \omega, 1 + \omega^2, \omega + \omega^2\}, \qquad |2A| = 6;$$

while if $t = 4$, say $A = \langle\omega\rangle = \{\pm 1, \pm\omega\}$, then

$$2A = \{0, \pm 2, \pm 2\omega, \pm(1 + \omega), \pm(1 - \omega)\}, \qquad |2A| = 9.$$

It is routine to verify that the elements listed in the displayed sets above are distinct.

For general n it is convenient to classify groups into one of three types.

Type-1 groups: $p \notin \mathcal{P}_t$. For such groups, we have $\lambda_A = \lceil t/2 \rceil$.

Type-2 groups: $p \in \mathcal{P}_t$ and $2A \supseteq \mathbb{Z}_p^*$. In this case, $\lambda_A = k$.

Type-3 groups: $p \in \mathcal{P}_t$ and $2A \not\supseteq \mathbb{Z}_p^*$. In this case, $\lambda_A < k$.

Type-1 and Type-2 groups have maximal doubling, while Type-3 groups do not. For Type-3 groups we define

$$\mathcal{S}_n := \{A : \lambda_A = n \text{ and } A \text{ does not have maximal doubling}\}.$$

Here, A is a subgroup of an arbitrary $\mathbb{Z}_p^*$. The following proposition is immediate.

Proposition 1. *A subgroup $A \sim (k,t,p)$ has $\lambda_A = n$ if and only if*

(i) $t = 2n$ or $2n-1$ and $p \notin \mathcal{P}_t$ (Type 1),

(ii) $k = n$, $p \in \mathcal{P}_t$ and $2A \supseteq \mathbb{Z}_p^*$ (Type 2), or

(iii) $A \in \mathcal{S}_n$ (Type 3).

Types 1 and 2 provide three infinite families of subgroups with $\lambda_A = n$. On the other hand, there are at most finitely many Type-3 groups with $\lambda_A = n$.

Theorem 4. *For any positive integer n, $\mathcal{S}_n$ is a finite set. Indeed, for any $A \in \mathcal{S}_n$ we must have $p \in \mathcal{P}_t$ and either*

$$n+1 \le k \le 4n-3 \quad \textit{and} \quad 2n+1 \le t < nk^2/(k-n), \textit{ or}$$
$$2n+1 \le t \le 8n(2n-1)-1.$$

As noted above, $\mathcal{S}_1 = \emptyset$, and Theorem 3 gives $\mathcal{S}_2 = \emptyset$, that is, $\lambda_A = 2$ if and only if $\lceil t/2 \rceil = 2$ or $k = 2$ ($p > 5$). For $n = 3, 4$ we have (see Section 10)

$$\begin{aligned} \mathcal{S}_3 &= \{(4,7,29),(4,10,41),(5,8,41),(6,7,43)\}, \\ \mathcal{S}_4 &= \{(5,12,61),(5,14,71),(5,20,101),(6,10,61),(12,9,109),(14,9,127)\}. \end{aligned} \tag{2.1}$$

For $5 \le n \le 10$ we have also, almost certainly, determined $\mathcal{S}_n$ (see Table 4), but the technology/run-time required to verify that the sets we found are complete is presently outside of our reach. From Proposition 1, Theorem 2 (i), and the data in Tables 1 and 2, we can now completely classify all groups with $|2A| = 3|A|$, $3|A|+1$, $4|A|$ or $4|A|+1$.

Corollary 1. *Let A be a multiplicative subgroup of $\mathbb{Z}_p^*$ of order t, $k = (p-1)/t$ and λ_A be as defined in* (1.1)*. The following hold:*

(i) $\lambda_A = 3$ if and only if $t = 5$ or 6 and $p > 13$ (Type 1), $k = 3$ and $p \ge 31$ (Type 2), or $A \in \mathcal{S}_3$ (Type 3);

(ii) $\lambda_A = 4$ if and only if $t = 7$ or 8 and $p > 43$ (Type 1), $k = 4$ and $p \ge 37$ (Type 2), or $A \in \mathcal{S}_4$ (Type 3).

3. Solving $|2A| \geq n|A|$ and Arithmetic Progressions

Consider the related problem of determining all subgroups A with $|2A| \geq n|A|$ for a given positive integer n. If $|2A| \geq n|A|$ then necessarily

$$2n - 1 \leq |A| \leq \frac{p-1}{n}, \tag{3.1}$$

that is, $t \geq 2n-1$ and $k \geq n$, since $|2A| \leq \min(\frac{t(t+1)}{2}, p)$. Conversely, if A is a subgroup with maximal doubling, then (3.1) is sufficient for $|2A| \geq n|A|$. Thus (3.1) is necessary and sufficient for $|2A| \geq n|A|$ for all but a finite number of subgroups belonging to $\cup_{i=1}^{n-1} \mathcal{S}_i$.

Since $\mathcal{S}_1 = \mathcal{S}_2 = \emptyset$ we have $|2A| \geq 3|A|$ if and only if

$$5 \leq |A| \leq \frac{p-1}{3}.$$

An interesting consequence of this fact is the following corollary. Chowla, Mann and Straus [4] established that the only multiplicative subgroups of $\mathbb{Z}_p^*$ that are arithmetic progressions are the trivial cases where $t = 1, 2$ or $p-1$. Recall, an *almost arithmetic progression* is an arithmetic progression with one element deleted, but not itself an arithmetic progression.

Corollary 2. *Let A be a multiplicative subgroup of $\mathbb{Z}_p^*$ of order t. Then A is contained in an arithmetic progression of length at most $\frac{3}{2}t$ if and only if*

- *(i) $t = 1, 2$ or $p - 1$, whence A is an arithmetic progression; or*
- *(ii) $(k, t, p) = (2, 3, 7)$, $A = \{1, 2, 4\}$, whence A is an almost arithmetic progression; or*
- *(iii) $(k, t, p) = (2, 6, 13), (2, 8, 17), (3, 4, 13)$ or $(4, 4, 17)$, whence A is contained in a progression of length exactly $\frac{3}{2}t$, but not contained in any shorter length progression.*

4. Proof of Theorem 1

Lemma 1. *Let z be a complex number of modulus 1 such that $z^a + z^b = z^c + z^d$ for some integers a, b, c, d. Then $z^a + z^b = 0$ or $\{z^a, z^b\} = \{z^c, z^d\}$ (as multi-sets).*

Proof. Conjugating the given equation and inserting $\overline{z} = z^{-1}$ yields $\frac{z^a+z^b}{z^{a+b}} = \frac{z^c+z^d}{z^{c+d}}$. Thus either $z^a + z^b = 0$ or $z^{a+b} = z^{c+d}$. In the latter case, $(x - z^a)(x - z^b) = (x - z^c)(x - z^d)$ (with x an indeterminate) and so by uniqueness of factorization, $\{z^a, z^b\} = \{z^c, z^d\}$. $\square$

Let $\Phi_t(x)$ be the t-th cyclotomic polynomial, of degree $\phi(t)$, and $f(x)$ a polynomial of the form

$$f(x) := x^{k_1} + x^{k_2} - x^{l_1} - x^{l_2}, \qquad 0 \le k_1, k_2, l_1, l_2 < t. \tag{4.1}$$

Lemma 2. *Suppose that $f(x)$ is a polynomial of the type (4.1) with $\{k_1, k_2\} \neq \{l_1, l_2\}$, so that $f(x)$ is not identically zero. Suppose further that for even t, we do not have $|k_2 - k_1| = |l_2 - l_1| = t/2$. Then $(\Phi_t(x), f(x)) = 1$.*

Proof. Let α be a primitive t-th root of unity in $\mathbb{C}$. Since $\Phi_t(x)$ is irreducible, it suffices to show that $f(\alpha) \neq 0$. Suppose to the contrary that $f(\alpha) = 0$. Then $\alpha^{k_1} + \alpha^{k_2} = \alpha^{l_1} + \alpha^{l_2}$, and so by Lemma 1, either $\{k_1, k_2\} = \{l_1, l_2\}$, or $\alpha^{k_1} + \alpha^{k_2} = \alpha^{l_1} + \alpha^{l_2} = 0$, whence $\alpha^{k_1 - k_2} = \alpha^{l_1 - l_2} = -1$. The latter implies that t is even and $|k_1 - k_2| = |l_1 - l_2| = t/2$. □

Lemma 3. *For any group $A \sim (k, t, p)$, $\lambda_A = \lceil t/2 \rceil$ if and only if $p \notin \mathcal{P}_t$, where $\mathcal{P}_t$ is the set of primes in (1.3).*

Proof. First note that the generators of A are just the zeros of $\Phi_t(x)$ in $\mathbb{Z}_p$. Let ω be a generator of A and consider solving the equation

$$\omega^{k_1} + \omega^{k_2} = \omega^{l_1} + \omega^{l_2}, \tag{4.2}$$

with $0 \le k_1, k_2, l_1, l_2 < t$, $\{k_1, k_2\} \neq \{l_1, l_2\}$. If t is even, we have a trivial class of solutions

$$\omega^{k_1} + \omega^{k_1 + t/2} = \omega^{l_1} + \omega^{l_1 + t/2} = 0.$$

Otherwise, with $f(x) := x^{k_1} + x^{k_2} - x^{l_1} - x^{l_2}$, we have $(f(x), \Phi_t(x)) = 1$ by Lemma 2, and so the resultant $R = R(f, \Phi_t)$ is a nonzero integer. If ω is a solution of (4.2), that is, a zero of f mod p, then ω is a common zero of f and Φ_t mod p, and so $R = 0$ in the field $\mathbb{Z}_p$, that is, $p|R$. In particular, if $p \nmid R(f, \Phi_t)$ for all such $f(x)$, then all of the distinct looking sums $\omega^{k_1} + \omega^{k_2}$ actually give distinct values mod p, with the exception of the sums equalling 0 with $k_1 = k_2 \pm \frac{t}{2}$. Thus, if $p \notin \mathcal{P}_t$, then $\lambda_A = \lceil t/2 \rceil$.

Conversely, if $\lambda_A = \lceil t/2 \rceil$, then (4.2) can only have trivial solutions for any generator ω of A. Thus, for any $f(x) = x^{k_1} + x^{k_2} - x^{l_1} - x^{l_2}$, with $R(f, \Phi_t) \neq 0$ in $\mathbb{Z}$, we must also have $R(f, \Phi_t) \neq 0$ in $\mathbb{Z}_p$. Therefore, $p \notin \mathcal{P}_t$. □

Proof of Theorem 1. Suppose that $A \sim (k, t, p)$ is a group with $t \le \sqrt{2(p-1)}$. Then $\frac{t}{2} \le k$, that is, $\lceil t/2 \rceil \le k$, and so by (1.2) A has maximal doubling if and only if $\lambda_A = \lceil t/2 \rceil$. By Lemma 3, such is the case if and only if $p \notin \mathcal{P}_t$. □

5. Proof of Theorem 2

Let $\mathcal{P}_t$ be the set of primes in (1.3) and put

$$P_t = \max\{p : p \in \mathcal{P}_t\}.$$

For $t = 1, 2, 3$, $\mathcal{P}_t = \emptyset$, and so P_t is undefined. We can estimate P_t by bounding $|R(f, \Phi_t)|$ where f is any polynomial of the type (4.1). Since $\Phi_t(x) = \prod_{(i,t)=1}(x - \alpha^i)$, where α is a primitive t-th root of unity, we have

$$R := R(f, \Phi_t) = \prod_{\substack{i=1 \\ (i,t)=1}}^{t} f(\alpha^i) = \prod_{\substack{i=1 \\ (i,t)=1}}^{t} \left(\alpha^{ik_1} + \alpha^{ik_2} - \alpha^{il_1} - \alpha^{il_2}\right),$$

and so trivially $|R| \le 4^{\phi(t)}$. The next lemma sharpens this estimate.

Lemma 4. *Let t be a positive integer with $t \ge 4$.*

- *(i) If t is odd then $P_t < 3^{\phi(t)}$.*
- *(ii) If t is even then $P_t \le \frac{3^{\phi(t)+1}-1}{2}$, with equality if $t = 2q$ for some prime q such that $\frac{3^q-1}{2}$ is a prime.*

The case of equality in part (ii) is easy to see. If $t = 2q$ with q a prime, $p = \frac{3^q-1}{2}$ and A is the group of t-th powers in $\mathbb{Z}_p^*$, then $1, -1$ and $3 \in A$ and we have the nontrivial collision $3 + (-1) = 1 + 1$, meaning $p \in \mathcal{P}_t$. The first few cases of equality occur when $q = 7, 13, 71$ and 103. We believe that the upper bound for odd t can be improved.

Conjecture 5.1. For all $t \ge 4$ we have $P_t \le (2^t + 1)/3$, with equality if and only if t is an odd prime and $(2^t + 1)/3$ is a prime.

For even $t \ge 10$, the upper bound on P_t in Lemma 4 (ii) is stronger than the bound in the conjecture. Again, the case of equality in the conjecture is easy to see. If t is an odd prime, $p = (2^t + 1)/3$ and A is the group of t-th powers, then $1, -2, 4 \in A$, and we have the nontrivial collision $4 + (-2) = 1 + 1$, meaning $p \in \mathcal{P}_t$; see also Example 6.1. Conversely, if $P_t = (2^t + 1)/3$, then $(2^t + 1)/3$ is a prime, and this implies in turn that t is an odd prime. We have verified the conjecture on a computer for $t \le 223$.

Proof of Theorem 2. Part (i) actually requires Lemma 6, proven later, but we will include it here for convenience. By (9.1), if

$$t \ge \left((p - 1 - t)(p - 1)^2\right)^{1/4},$$

then $2A \supseteq \mathbb{Z}_p^*$. This is slightly stronger than the statement in part (i). Part (ii) is immediate from Lemma 4. Indeed, if $t < \log_3 p$, then $p > 3^t > \frac{3}{2}3^{\phi(t)}$. Therefore $p \notin \mathcal{P}_t$, and so A has maximal doubling, that is, $\lambda_A = \lceil \frac{t}{2} \rceil$. □

Proof of Lemma 4. To establish the upper bounds in parts (i) and (ii), we must show that any prime factor p of a nonzero resultant of the form $R(f, \Phi_t)$, with f as in (4.1), is bounded above by $3^{\phi(t)}$ for odd $t > 3$, $\frac{3}{2}3^{\phi(t)}$ for even $t > 2$. Equivalently, if (4.2) has a nontrivial solution, then p is bounded as such. The trivial solutions to (4.2) are $\{k_1, k_2\} = \{l_1, l_2\}$, and in the case t is even, $|k_1 - k_2| = |l_1 - l_2| = t/2$. For a nontrivial solution, either $k_1 \neq k_2$ or $l_1 \neq l_2$, say without loss of generality that $k_1 < k_2$. Dividing by ω^{k_1} yields a nontrivial solution to (4.2) of the type

$$1 + \omega^d = \omega^a + \omega^b, \tag{5.1}$$

for some integers a, b, d with $1 \leq d < t$, $d \neq t/2$, $0 < a \leq b < t$, and $a, b \neq d$. Replacing ω with ω^i, for an appropriate i with $(i, t) = 1$, we may assume that $d|t$. Thus we may assume

$$d|t, \quad d < t/2, \quad 0 < a \leq b < t, \quad |a - b| \neq t/2, \quad a \neq d, b \neq d. \tag{5.2}$$

Suppose now that (a, b, d) is a triple satisfying (5.2), for which (5.1) holds true, and consider the following cases.

(i) If $a = b = t/2$, (5.1) becomes $-3 = \omega^d$, which implies that $\mathrm{ord}_p(-3) = t/d$, and thus $p|\Phi_{t/d}(-3)$.

(ii) If $a = t/2$ and $b \neq t/2$ or vice versa, then (5.1) becomes

$$2 = \omega^b - \omega^d, \quad d|t, \quad d < t/2, \quad b \neq t/2, \quad b \neq d, \quad |d - b| \neq t/2. \tag{5.3}$$

We may restrict our attention to the case where $(b, d) = 1$. Indeed, if $(b, d) = e > 1$ then (5.3) represents a nontrivial collision for elements of a subgroup of A of order t/e, and so we can appeal to the bound on p for groups of size t/e. Set $f(x) := x^b - x^d - 2$. Then,

$$f(\alpha^i)f(\alpha^{-i}) = 6 + 2\alpha^{di} + 2\alpha^{-di} - 2\alpha^{bi} - 2\alpha^{-bi} - \alpha^{(b-d)i} - \alpha^{(d-b)i}. \tag{5.4}$$

By the arithmetic-geometric mean inequality,

$$R^2 = \prod_{(i,t)=1} f(\alpha^i)f(\alpha^{-i}) \leq \left(\frac{1}{\phi(t)} \sum_{(i,t)=1} f(\alpha^i)f(\alpha^{-i}) \right)^{\phi(t)}. \tag{5.5}$$

Using the Ramanujan sum formula,

$$\frac{1}{\phi(t)} \sum_{(i,t)=1} \alpha^{ai} = \frac{\mu(t/(t,a))}{\phi(t/(t,a))},$$

we get from (5.4),

$$\frac{1}{\phi(t)} \sum_{(i,t)=1} f(\alpha^i)f(\alpha^{-i}) = \Sigma_1 := 6 + 4\frac{\mu(t/d)}{\phi(t/d)} - 4\frac{\mu(t/(t,b))}{\phi(t/(t,b))} - 2\frac{\mu(t/(t,d-b))}{\phi(t/(t,d-b))}.$$

We claim that for $t \neq 30$, $\Sigma_1 \leq 9$, whence we conclude from (5.5), that $R \leq 3^{\phi(t)}$ as desired. For $t = 30$, we can have $\Sigma_1 = 9.25$, for example when $(d, b) = (3, 10)$, but one can check numerically that the prime factors of R never exceed $3^{\phi(t)}$.

To prove the claim, we begin with a computer computation verifying the claim for $t \leq 72$. Henceforth, we assume that $t > 72$. By the constraint in (5.3), all three values $\frac{t}{d}, \frac{t}{(t,b)}, \frac{t}{(t,d-b)}$ are at least 3. Furthermore, since $(b, d) = 1$, the values $d, (t, b)$ and $(t, d-b)$ are pairwise relatively prime, implying that $d(t, b)(t, d-b)|t$. In particular,

$$d(t, b)(t, d-b) \leq t. \tag{5.6}$$

If $t/(t, b) = 3$ then by (5.6) and $t > 72$,

$$t/(t, d-b) \geq (t, b) = t/3 > 24, \quad \text{and} \quad t/d \geq (t, b) > 24,$$

and thus since $\phi(n) \geq 8$ for $n > 24$, $\Sigma_1 \leq 6 + \frac{1}{2} + 2 + \frac{1}{4} = 8.75$. If $t/(t, d-b) = 3$ then in the same manner $t/(t, b) > 24$, $t/d > 24$, and $\Sigma_1 \leq 6 + \frac{1}{2} + \frac{1}{2} + 1 = 8$. If $t/(t, b) = 4$, then $t/d, t/(t, d-b) \geq (t, b) = t/4 > 18$ and since $\phi(n) \geq 8$ for $n > 18$, $\Sigma_1 \leq 6 + \frac{1}{2} + 0 + \frac{1}{4} = 6.75$. Similarly, if $t/(t, d-b) = 4$, then $\Sigma_1 \leq 6 + \frac{1}{2} + \frac{1}{2} = 7$. If $t/(t, b) = 5$, then $t/d > 14$ and $t/(t, d-b) > 14$ whence their totient values are at least 6, and $\Sigma_1 \leq 6 + \frac{2}{3} + 1 + \frac{1}{3} = 8$, while if $t/(t, d-b) = 5$, then $t/d > 14$, $t/(t, b) > 14$ and $\Sigma_1 \leq 6 + \frac{2}{3} + \frac{2}{3} + \frac{1}{2} < 7.84$.

We are left with considering the case where both $t/(t, b) \geq 6$ and $t/(t, d-b) \geq 6$. Since $-\frac{\mu(n)}{\phi(n)} \leq \frac{1}{6}$ for $n \geq 6$, we get $\Sigma_1 \leq 6 + 2 + \frac{2}{3} + \frac{1}{3} = 9$, establishing the claim.

(iii) Suppose next that we have (5.1) with $a - d = \pm t/2$, so that it becomes $1 + \omega^d = -\omega^d + \omega^b$, or $2 = \omega^{b-d} - \omega^{-d}$, an equation of the type already considered in case (ii), upon replacing ω with ω^{-1}.

(iv) Suppose finally that we have (5.1) with

$$d|t, \quad d < t/2, \quad 0 < a \leq b < t, \quad a, b \notin \{d, t/2\}, \quad |a - d| \neq t/2. \tag{5.7}$$

Let $f(x) = 1 + x^d - x^a - x^b$, with a, b and d satisfying (5.7). As in case (ii) we obtain

$$\begin{aligned}\frac{1}{\phi(t)} \sum_{(i,t)=1} f(\alpha^i) f(\alpha^{-i}) = 4 &+ 2\frac{\mu(t/d)}{\phi(t/d)} + 2\frac{\mu(t/(t, a-b))}{\phi(t/(t, a-b))} - 2\frac{\mu(t/(t, a))}{\phi(t/(t, a))} \\ &- 2\frac{\mu(t/(t, a-d))}{\phi(t/(t, a-d))} - 2\frac{\mu(t/(t, b))}{\phi(t/(t, b))} - 2\frac{\mu(t/(t, b-d))}{\phi(t/(t, b-d))}.\end{aligned}$$

Plainly, the maximum possible value of the third term $2\frac{\mu(t/(t,a-b))}{\phi(t/(t,a-b))}$ occurs when $a = b$. Thus by replacing a with b in the case where

$$-2\frac{\mu(t/(t, a))}{\phi(t/(t, a))} - 2\frac{\mu(t/(t, a-d))}{\phi(t/(t, a-d))} < -2\frac{\mu(t/(t, b))}{\phi(t/(t, b))} - 2\frac{\mu(t/(t, b-d))}{\phi(t/(t, b-d))},$$

or b with a in the opposite case, we obtain a larger value for the sum. Hence, we may assume that $a = b$ in determining an upper bound, whence the sum simplifies to

$$\frac{1}{\phi(t)}\sum_{(i,t)=1} f(\alpha^i)f(\alpha^{-i}) = \Sigma_2 := 6 + 2\frac{\mu(t/d)}{\phi(t/d)} - 4\frac{\mu(t/(t,b))}{\phi(t/(t,b))} - 4\frac{\mu(t/(t,d-b))}{\phi(t/(t,d-b))}.$$

Again, by (5.7), $\frac{t}{d}, \frac{t}{(t,b)}, \frac{t}{(t,d-b)}$ are all at least 3, and we may assume that $(d, b) = 1$ so that (5.6) holds. We claim that for $t \neq 15$, $\Sigma_2 \leq 9$. For $t = 15$, Σ_2 can be as large as 9.25, for example when $(d, b) = (1, 6)$, but its prime divisors are all less than $3^{\phi(t)}$.

The proof of the claim follows the argument of case (ii). A computer is used to verify the claim for $t \leq 72$. Assume now that $t > 72$. If $t/(t, b) = 3$ or $t/(t, d-b) = 3$ then the other two ratios exceed 24 and we get $\Sigma_2 \leq 6 + \frac{1}{4} + 2 + \frac{1}{2} = 8.75$. If $t/(t, b) = 4$ or $t/(t, d - b) = 4$, then the other two ratios exceed 18 and $\Sigma_2 \leq 6 + \frac{1}{4} + 0 + \frac{1}{2} = 6.75$. If $t/(t, b) = 5$ or $t/(t, d - b) = 5$, then the other two ratios exceed 14 and $\Sigma_2 \leq 6+\frac{1}{3}+1+\frac{2}{3} = 8$. Finally, if both $t/(t, b) \geq 6$ and $t/(t, d-b) \geq 6$, then using $-\frac{\mu(n)}{\phi(n)} \leq \frac{1}{6}$ for $n \geq 6$, $\Sigma_2 \leq 6 + 1 + \frac{2}{3} + \frac{2}{3} < 8.34$, establishing the claim.

For odd t, only case (iv) can hold, and we get $P_t \leq R \leq 3^{\phi(t)}$ establishing part (i) of the lemma. For even t we conclude that either $P_t \leq \Phi_{t/d}(-3)$ for some divisor $d|t$, or $P_t \leq R \leq 3^{\phi(t)}$. The upper bound in part (ii) now follows from the upper bound on $\Phi_t(-3)$ in Lemma 12. □

6. Examples of Resultants

Example 6.1. Let $t > 2$ and $f(x) = 1 + x - 2x^2 = (1 - x)(1 + 2x)$. Then

$$\begin{aligned} R(f, \Phi_t) &= \prod_{(i,t)=1} (1 - \alpha^i)(1 + 2\alpha^i) \\ &= \prod_{(i,t)=1} (1 - \alpha^i)(-\alpha^i)(-2 - \alpha^{-i}) = \Phi_t(1)\Phi_t(0)\Phi_t(-2). \end{aligned}$$

Now $\Phi_t(0) = 1$,

$$\Phi_t(1) = \begin{cases} q, & \text{if } t = q^l \text{ for some prime } q; \\ 1, & \text{if } t \text{ is not a prime power.} \end{cases}$$

Thus for any prime $p \equiv 1 \bmod t$, $p|R$ if and only if $p|\Phi_t(-2)$. In this case, $-2, 4 \in A$, and we have the nontrivial collision $1 + 1 = -2 + 4$ of elements in A. By the upper bound on $\Phi_t(-2)$ in Lemma 12,

$$p \leq \begin{cases} \frac{3}{2}\, 2^{\phi(t)}, & \text{if } t \text{ is odd;} \\ 2^{\phi(t)+1}, & \text{if } t \text{ is even.} \end{cases}$$

If $\Phi_t(-2)$ is itself a prime p with $p \equiv 1 \bmod t$, then $P_t \geq \Phi_t(-2)$. If t is a prime, then $\Phi_t(-2) = \frac{2^t+1}{3}$, the value in Conjecture 5.1. The first few such (t,p) prime pairs are

$$(t,p) = (3,3),(5,11),(7,43),(11,683),(13,2731),(17,43691),$$
$$(19,174763),(23,2796203),(31,715827883).$$

In each case, $p = P_t$; see Table 1.

Example 6.2. Suppose that $t = 3q$, with q a prime, $q \equiv 1 \bmod 3$, $f(x) = 1+x-2x^q$. Put $\alpha = e^{2\pi i/t}$, $\alpha_3 = \alpha^q = -\frac{1}{2} + \frac{\sqrt{3}}{2}i$. Then

$$\begin{aligned} R = R(f,\Phi_t) &= \prod_{(j,t)=1} \left(1+\alpha^j - 2\alpha^{qj}\right) \\ &= \prod_{\substack{(j,t)=1 \\ j\equiv 1 \pmod 3}} \left(1-2\alpha_3+\alpha^j\right) \prod_{\substack{(j,t)=1 \\ j\equiv 2 \pmod 3}} \left(1-2\overline{\alpha_3}+\alpha^j\right). \end{aligned}$$

Plainly, the two products have the same absolute value. Setting

$$P(x) := \frac{x^q-\alpha_3}{x-\alpha_3} = \prod_{\substack{(j,t)=1 \\ j\equiv 1 \pmod 3}} (x-\alpha^j),$$

we see that with $z = -2+\sqrt{3}\,i$,

$$\begin{aligned} |R| &= \prod_{\substack{(j,t)=1 \\ j\equiv 1 \pmod 3}} \left|1-2\alpha_3+\alpha^j\right|^2 = |P(-1+2\alpha_3)|^2 = |P(-2+\sqrt{3}\,i)|^2 \\ &= \frac{\left|z^q-\alpha_3\right|^2}{\left|z-\alpha_3\right|^2} = \frac{7^q - 2\mathcal{R}(\overline{\alpha}_3 z^q)+1}{|-\frac{3}{2}-\frac{\sqrt{3}}{2}i|^2} = \frac{7^q - 2\mathcal{R}(\overline{\alpha}_3 z^q)+1}{3} \approx \frac{7}{3}\,7^{\phi(t)/2}. \end{aligned}$$

7. Computing $|2A|$

Lemma 5. *If $A = \langle\omega\rangle$ is a subgroup of $\mathbb{Z}_p^*$ of order t, then*

$$A+A = \bigcup_{i=0}^{\frac{t-1}{2}} (1+\omega^i)A, \quad \textit{for odd } t;$$
$$A+A = \bigcup_{i=0}^{\frac{t}{2}-1} (1+\omega^i)A \cup \{0\}, \quad \textit{for even } t.$$

Note, the $i=0$ term in the union is the coset $(1+1)A$, not to be confused with the sum set $2A$. The cosets listed in this decomposition are all nonzero, that is, $1+\omega^i \neq 0$, but they need not be distinct. If the cosets are distinct, then A has maximal doubling.

Proof. Let $\omega^j + \omega^l$, with $0 \le j \le l < t$, be a typical element of $A + A$. Then, with $i = l - j$,

$$\omega^j + \omega^l = \omega^j(1 + \omega^i) \in (1 + \omega^i)A.$$

If $i > t/2$ we can replace i with $t - i$, noting that $(1 + \omega^i)A = (1 + \omega^{t-i})A$. The lemma now follows from the fact that $0 \in A + A$ if and only if t is even. □

To compute $|2A|$, let $\eta : \mathbb{Z}_p^*/A \to \mathbb{Z}_p^*$ be the mapping $\eta(xA) = x^t$. Since η is one-to-one, it follows from Lemma 5 that

$$\lambda_A = \#\{(1 + \omega^i)^t : 0 \le i \le \lfloor \tfrac{t-1}{2} \rfloor\}, \tag{7.1}$$

where ω is any generator of A.

8. Data for Small Values of t and p

Computers were used to generate data for all groups with $p < 2.5 \cdot 10^6$ and for all groups with $t \le 223$. Only partial data is displayed here due to the excessive length of the full data set. The value 223 was chosen as the stopping point for t in order to prove that our determination of $\mathcal{S}_4$ was complete. Recall the definition of Type-1, Type-2 and Type-3 groups given in Section 2.

8.1. Table 1

For a fixed t, we computed all possible resultants $R(f(x), \Phi_t(x))$, where $f(x) = 1 + x^d - x^a - x^b$, with $d|t$, and $1 \le a \le b < t$; see (5.2). For each nonzero resultant, we determined the prime divisors p with $p \equiv 1 \bmod t$, thus forming the set $\mathcal{P}_t$. The primes are listed in Table 1 for $4 \le t \le 18$. The extended table (not displayed) gives $\mathcal{P}_t$ for $4 \le t \le 223$.

8.2. Table 2

For each $p \in \mathcal{P}_t$ and subgroup A of $\mathbb{Z}_p^*$ of order t, we computed λ_A using (7.1). Table 2 provides a list of all such λ_A, for groups with $k > 2$. Parentheses have been placed around primes for which $2A \supseteq \mathbb{Z}_p^*$, that is, $\lambda_A = k$ (Type-2 group). The extended table gives all λ_A values for groups with $t \le 223$.

8.3. Table 3

Table 3 gives all possible values of λ_A for a fixed t for Type-1, Type-2 and Type-3 groups respectively. Recall, Type-1 means $\lambda_A = \lceil t/2 \rceil$, Type-2 means $\lambda_A = k$, $p \in \mathcal{P}_t$, and Type-3 means $\lambda_A < k$, $p \in \mathcal{P}_t$.

t	$\mathcal{P}_t$
2	$\emptyset$
3	$\emptyset$
4	5
5	11
6	$7, 13$
7	$29, 43$
8	$17, 41$
9	$19, 37, 109, 127$
10	$11, 31, 41, 61$
11	$23, 67, 89, 199, 397, 683$
12	$13, 37, 61, 73$
13	$53, 79, 131, 157, 313, 521, 1613, 2003, 2731$
14	$29, 43, 71, 113, 127, 239, 547, 1093$
15	$31, 61, 151, 181, 211, 241, 271, 331, 421, 541, 1321, 1381$
16	$17, 97, 113, 193, 257, 337$
17	$103, 137, 239, 307, 409, 443, 613, 647, 919, 953, 1021, 1429, 2857, 3571,$ $15641, 17783, 25229, 26317, 43691$
18	$19, 37, 73, 109, 127, 163, 199, 307, 757$

Table 1: $\mathcal{P}_t$ sets for $t \leq 18$

t	p	$\|2A\|$
5	none	
6	none	
7	29, 43	$3\|A\|$
8	41	$3\|A\| + 1$
9	(37),109,127	$4\|A\|$
10	(31), 41	$3\|A\| + 1$
10	61	$4\|A\| + 1$
11	67, 89, 199, 397, 683	$5\|A\|$
12	(37)	$3\|A\| + 1$
12	61	$4\|A\| + 1$
12	73	$5\|A\| + 1$
13	(53)	$4\|A\|$
13	79	$5\|A\|$
13	131, 157, 313, 521, 1613, 2003, 2731	$6\|A\|$
14	(43)	$3\|A\| + 1$
14	71	$4\|A\| + 1$
14	113,127,239	$5\|A\| + 1$
14	547,1093	$6\|A\| + 1$
15	(61)	$4\|A\|$
15	181,211,331	$6\|A\|$
15	151,241,271,421,541,751,1321,1381	$7\|A\|$
16	97,113	$5\|A\| + 1$
16	257,337	$6\|A\| + 1$
16	193	$7\|A\| + 1$

Table 2: Doubling constants for Type-2 and Type-3 groups, $k > 2$

t	Type-1 λ_A	Type-2 λ_A	Type-3 λ_A
2	1	-	-
3	2	-	-
4	2	1	-
5	3	2	-
6	3	1,2	-
7	4	-	3
8	4	2	3
9	5	2,4	4
10	5	1,3	3,4
11	6	2	5
12	6	1,3	4,5
13	7	4	5,6
14	7	2,3	4-6
15	8	2,4	6,7
16	8	1	5-7
17	9	6	5-8
18	9	1,2,4	5-8
19	10	-	6-9
20	10	2,3	4,7-9
21	11	2,6	8,9,10
22	11	1,3,4	6-10
23	12	2	5,8-11
24	12	3,4,8	7,9-11
25	13	4,6	8-12
26	13	2,3,5	5,8-12
27	14	4,6	9,11-13
28	14	1,4,7	8-13
29	15	2	7,9,11-14
30	15	1,2,5-8	7,10-14
31	16	-	8,9,12-15
32	16	3,6	7,9,11-15
33	17	2,6	8,10,11,13-16
34	17	3,4,7	8,10,12-16
35	18	2,6,8	10,12,14-17
36	18	1-3,5,11	10,11,13-17
37	19	4	5,13,15-18
38	19	5,6	10-12,14-18
39	20	2,4,8	11,14-19
40	20	1,6,7	8,10-15,17-19
41	21	2	14,16,18-20
42	21	1,3,5,9	7,9,10-14,16-20
43	22	4	8,15-21
44	22	2,8,9	12,13,15-21
45	23	4,6	11,14,16-22
46	23	1,3	5,9,10,13,14,16-22
47	24	6	12,14,16-23

Table 3: Possible values of λ_A for given t

n	$\|\mathcal{S}_n\|$	k-range	t-range	p-range
2	0	-	-	-
3	4	4-6	7-10	29-43
4	6	5-14	9-20	61-127
5	18	6-62	11-46	67-683
6	19	7-210	13-70	127-2731
7	27	8-92	15-95	151-1381
8	40	9-2570	17-64	211-43691
9	56	10-9198	19-118	271-174763
10	61	11-4358	21-128	331-91309

Table 4: Description of $\mathcal{S}_n$ sets

8.4. Table 4

Recall, $\mathcal{S}_n$ is the set of all Type-3 groups having $\lambda_A = n$. In Table 4 we describe the sets $\mathcal{S}_n$ for $n \leq 10$. For $n = 2, 3$ and 4, the sets are given explicitly in (2.1), and we prove that these are the full sets in Section 10. For $5 \leq n \leq 10$, we have determined what we believe to be the full set based on computations up to $p = 2.5 \cdot 10^6$. In Table 4 we just display the cardinality of each of the sets, as well as the range of k, t and p values for the groups in the set.

Conjecture 8.1. For $n \leq 10$ there are no elements of $\mathcal{S}_n$ with $p > 174763$.

8.5. Table 5

Next, we seek an optimal constant c such that uniformly

$$\lambda_A \geq c \cdot \min\left(\lceil t/2 \rceil,\ k\right). \tag{8.1}$$

To do this, we define for any group A, the value

$$C_A := \max\left(\frac{\lambda_A}{\lceil t/2 \rceil}, \frac{\lambda_A}{k}\right),$$

so that

$$\lambda_A = C_A \min\left(\lceil t/2 \rceil,\ k\right),$$

and

$$|2A| \geq C_A \min\left(\frac{|A|^2}{2}, p-1\right).$$

For groups with maximal doubling, $C_A = 1$. In general, C_A represents the fraction of maximum possible doubling for the group A.

Table 5 contains a list of all groups A with $p < 2.5 \cdot 10^6$ having $C_A \leq .5$, as well as groups with $p < 3361$ having record breaking small values of C_A. The values

p	k	t	λ_A	$\lambda_A/\lceil t/2\rceil$	λ_A/k	C_A
29	4	7	3	3/4	3/4	.750
113	7	16	5	5/8	5/7	.714
113	8	14	5	5/7	5/8	.714
137	8	17	5	5/9	5/8	.625
229	12	19	6	3/5	1/2	.600
577	18	32	9	9/16	1/2	.562
757	21	36	10	5/9	10/21	.555
1151	23	50	12	12/25	12/23	.521
3361	40	84	20	10/21	1/2	.500
3511	39	90	19	19/45	19/39	.487
4051	45	90	22	22/45	22/45	.488
5857	61	96	22	11/24	22/61	.458
10303	101	102	25	25/51	25/101	.490
12301	82	150	35	7/15	35/82	.466
16111	90	179	45	1/2	1/2	.500
246241	456	540	125	25/54	125/456	.462

Table 5: Minimal values of C_A.

of C_A have been rounded down to three places. Thus for all groups in this range, we can take $c = .458$ in (8.1), and for all but six groups we can take $c = 1/2$. In particular, for all but these six groups we have

$$|2A| \geq \frac{1}{2} \cdot \min\left(\frac{|A|^2}{2},\ p-1\right).$$

8.6. Table 6

Finally we determine the largest subgroup A of $\mathbb{Z}_p^*$ such that $2A$ fails to contain $\mathbb{Z}_p^*$. If $t < \sqrt{2(p-1)}$ then we are guaranteed that $2A \not\supseteq \mathbb{Z}_p^*$. Also, by Theorem 2, if $t > p^{3/4}$ then $2A \supseteq \mathbb{Z}_p^*$. Thus, it is enough to consider groups of size $\sqrt{2(p-1)} \leq t \leq p^{3/4}$. For each prime p we determined the maximal t, denoted t_{max}, such that $2A \not\supseteq \mathbb{Z}_p^*$. In Table 6 we list all p and t_{max} such that the ratio

$$r_{max} := \frac{t_{max}}{\sqrt{p \log p}}$$

is greater than 1.7, with p running from 2 to $2.5 \cdot 10^6$. The ratio was rounded up to three decimal places. Thus, for instance, for any subgroup A with $p < 2.5 \cdot 10^6$ we have $2A \supseteq \mathbb{Z}_p^*$ provided that

$$|A| > 1.89\sqrt{p \log p},$$

p	t_{max}	k	λ_A	r_{max}
10781	539	20	19	1.704
29581	986	30	29	1.787
33791	1090	31	30	1.837
93809	1804	52	51	1.741
171673	2488	69	68	1.730
240007	3077	78	77	1.785
450077	4246	106	105	1.755
461801	4618	100	99	1.882
473971	4270	111	110	1.716
751181	6532	115	114	2.049
931537	6469	144	143	1.808
942049	6542	144	143	1.818
962921	6335	152	151	1.740
1105171	6698	165	164	1.708
1318553	7666	172	171	1.779
1630927	8237	198	197	1.706
1852621	8822	210	209	1.707
1879049	9736	193	192	1.869
2101051	10150	207	206	1.836
2161829	10102	214	213	1.800
2189153	9773	224	223	1.729

Table 6: Largest A with $2A \not\supseteq \mathbb{Z}_p^*$

with the one exception $A \sim (115, 6532, 751181)$. We have included in the table the associated k and λ_A values for these groups. As expected, all of these groups have *almost maximal doubling*, that is, $\lambda_A = k - 1$.

9. Proof of Theorem 4

We start with two lemmas that provide sufficient conditions for $|2A| \geq n|A|$.

Lemma 6. *For any multiplicative subgroup A of $\mathbb{Z}_p^*$, with $|A| = t$, $k = (p-1)/t$, and any positive integer $n \leq k$, we have $|2A| \geq n|A|$ provided that*

$$t \geq \frac{(n-1)k^2}{k-(n-1)}.$$

Taking $n = k$ we see that $|2A| \geq p - 1$ provided that

$$t \geq (k-1)k^2, \qquad \text{or equivalently,} \qquad p \geq (k-1)k^3 + 1. \tag{9.1}$$

Similarly, taking $n = \lceil k/2 \rceil$, we see that $|2A| \ge \frac{p-1}{2}$ provided that

$$p \ge \begin{cases} \left(\frac{k-2}{k+2}\right) k^3 + 1, & \text{if } k \text{ is even;} \\ \left(\frac{k-1}{k+1}\right) k^3 + 1, & \text{if } k \text{ is odd.} \end{cases}$$

In particular, $|2A| \ge p - 1$ if $t > p^{3/4}$, and $|2A| \ge \frac{p-1}{2}$ if $t > p^{2/3}$.

Proof. It is well known that

$$|2A| \ge t^4/E_A, \tag{9.2}$$

where E_A is the additive energy of A,

$$E_A := \#\{(x_1, x_2, x_3, x_4) : x_i \in A, 1 \le i \le 4, x_1 + x_2 = x_3 + x_4\}.$$

For even t we can do slightly better. For $0 \le c < p - 1$, let n_c denote the number of $(x_1, x_2) \in A \times A$ with $x_1 + x_2 = c$. Then

$$E_A = t^2 + \sum_{c=1}^{p-1} n_c^2, \quad \text{and} \quad \sum_{c=1}^{p-1} n_c = t^2 - t.$$

By the Cauchy-Schwarz inequality,

$$t^2 - t \le (|2A| - 1)^{1/2} \left(\sum_{c=1}^{p-1} n_c^2 \right)^{1/2} = (|2A| - 1)^{1/2} (E_A - t^2)^{1/2},$$

and so for even t,

$$|2A| \ge \frac{t^2(t-1)^2}{E_A - t^2} + 1. \tag{9.3}$$

Letting $\lambda = \lambda_A$, the number of cosets in $2A$, we have by (9.2) and (9.3),

$$\lambda_A \ge \begin{cases} t^3/E_A, & \text{if } t \text{ is odd;} \\ t(t-1)^2/(E_A - t^2), & \text{if } t \text{ is even.} \end{cases} \tag{9.4}$$

Define

$$\Phi_A = \max_{p \nmid a} \left| \sum_{x \in A} e_p(ax) \right|,$$

where $e_p(ax) = e^{2\pi i a x/p}$. The following estimate is well known; see eg. [6, Equation (11)]:

$$E_A \le \frac{|A|^4}{p} + |A| \Phi_A^2. \tag{9.5}$$

Using the Gauss sum bound $\Phi_A \le \sqrt{p-1}$ and $tk = p - 1$, we have

$$E_A \le \frac{t^4}{p} + t(p-1) < \frac{t^3}{k} + t^2 k. \tag{9.6}$$

In order to have $\lambda_A \geq n$, it is enough to have $\lambda_A > n-1$. For odd t, by (9.4) and (9.6), it suffices to have

$$\frac{t^3}{\frac{t^3}{k} + t^2 k} \geq n-1, \tag{9.7}$$

which simplifies to the statement of the lemma. Similarly, for even t it suffices to have

$$\frac{t(t-1)^2}{\frac{t^3}{k} + t^2 k - t^2} \geq n-1. \tag{9.8}$$

For $n \geq 3$, we claim this is implied by the inequality in (9.7). Indeed, for $n \geq 3$, (9.7) implies

$$tk \geq 2(t+k^2). \tag{9.9}$$

The left-hand side of (9.8) is greater than or equal to the left-hand side of (9.7) if

$$\left(1 - \frac{1}{t}\right)^2 \geq 1 - \frac{k}{t+k^2}.$$

Dropping the $\frac{1}{t^2}$ term on the left-hand side, we see that it suffices to have $\frac{2}{t} \leq \frac{k}{t+k^2}$, the condition in (9.9). The statement of the lemma is trivial if $n=1$ or 2. $\square$

We also need the following result of Cochrane and Pinner [7].

Lemma 7 ([7], Theorem 5.2)**.** *Let n be a positive integer, and A a subgroup of $\mathbb{Z}_p^*$ with $t \geq 8(n-1)(2n-3)$ and $k \geq 4n-6$. Then $|2A| \geq n|A|$.*

Proof of Theorem 4. Let n be a fixed positive integer and A a subgroup of $\mathbb{Z}_p^*$ not having maximal doubling, with $\lambda_A = n$. We may assume $n \geq 2$. Since A does not have maximal doubling, $t > 2n$ and $k > n$. Applying Lemma 7 with n replaced by $n+1$, we deduce from $|2A| < (n+1)|A|$ that either

$$n+1 \leq k \leq 4n-3, \quad \text{or} \quad 2n+1 \leq t \leq 8n(2n-1)-1.$$

By Lemma 6, applied with n replaced by $n+1$, for each value of k in the range $n+1 \leq k \leq 4n-3$, we must have $t < \frac{nk^2}{k-n}$. Finally, since A does not have maximal doubling, we have $p \in \mathcal{P}_t$ by Lemma 3. $\square$

10. Determination of the Sets $\mathcal{S}_n$ for $n = 2, 3$ and 4

Consider first the case $n=2$, and let A be a Type-3 group with $\lambda_A = 2$. By Theorem 4, either $3 \leq k \leq 5$ and $5 \leq t < 2k^2/(k-2)$, or $5 \leq t \leq 47$. In the first case, if $k = 3, 4$ or 5, then $t \leq 17, 15, 16$ respectively. Thus in both cases we must have $5 \leq t \leq 47$. Table 3 reveals that there are no Type-3 groups in this range with $\lambda_A = 2$. Thus $\mathcal{S}_2 = \emptyset$.

Next consider $n = 3$. Then by Theorem 4, either $4 \le k \le 9$ and $7 \le t \le 3k^2/(k-3)$, or $7 \le t \le 119$. The first case implies that $t \le 48$, and so in both cases, $7 \le t \le 119$. Again, the extended Table 3 reveals that the only Type-3 groups with $\lambda_A = 3$ occur when $t = 7, 8$ or 10. The specific groups can then be read from Table 2:

$$\mathcal{S}_3 = \{(4,7,29),(4,10,41),(5,8,41),(6,7,43)\}.$$

For $n = 4$, we have either $5 \le k \le 13$ and $t < 4k^2/(k-4)$, or $9 \le t \le 223$. In both case we get $t \le 223$. The extended tables reveal the six groups

$$\mathcal{S}_4 = \{(5,12,61),(5,14,71),(5,20,101),(6,10,61),(12,9,109),(14,9,127)\}.$$

For $n = 5$ we would need data for groups as large as $t = 359$, which would require more computation time than we think is worthwhile. It is better to find an improvement of Lemma 7 first.

11. Another Proof of Theorem 3

In this section, we appeal to inverse results from additive combinatorics to give a second proof of Theorem 3 that only requires computational information for groups with $t \le 13$ or $p < 2500$. This section also lays the groundwork for the proof of Corollary 2.

Recall, a subset of $\mathbb{Z}_p$ of the form $\{a, a+d, a+2d, \ldots, a+(\ell-1)d\}$, with $a, d \in \mathbb{Z}_p$, $d \ne 0$, is called an *arithmetic progression* or *d-progression* of length ℓ. It is elementary that if A and B are arithmetic progressions with the same difference, then $|A+B| = \min(|A|+|B|-1, p)$. Vosper [21] established the following inverse result.

Theorem 5 ([21])**.** *Suppose that A, B are subsets of $\mathbb{Z}_p$ with $|A|, |B| \ge 2$, and $|A+B| = |A|+|B|-1 \le p-2$. Then A and B are arithmetic progressions with the same difference.*

A set S is called an *almost arithmetic progression*, or *almost progression* if S is an arithmetic progression with one term removed, but not itself an arithmetic progression. It is elementary that if A and B are almost progressions with the same difference, then $|A+B| \le |A|+|B|+1$. Hamoudine and Rodseth [12] established the following inverse characterization.

Theorem 6 ([12])**.** *Suppose that A, B are subsets of $\mathbb{Z}_p$ with $|A|, |B| \ge 3$, and that*

$$7 \le |A+B| = |A|+|B| \le p-4.$$

Then A and B are arithmetic progressions or almost arithmetic progressions with the same difference d.

In particular, either one of A and B is a d-progression while the other is an almost d-progression, or

$$A = \{a, a+2d, a+3d, \ldots, a+|A|d\}, \quad \text{and} \quad B = \{b, b+2d, b+3d, \ldots, b+|B|d\}.$$

for some $a, b, d \in \mathbb{Z}_p$.

Freiman [8] proved the following inverse theorem (cf. [17, Theorem 2.11]).

Theorem 7 ([8])**.** *Let A be a subset of $\mathbb{Z}_p$ and r be an integer with $0 \le r \le \frac{2}{5}|A|-2$. If $|A+A| = 2|A|-1+r$ and $|A| \le p/35$, then A is contained in an arithmetic progression with $|A|+r$ elements.*

We immediately deduce the following lemma, part (i) from Theorem 6, and part (ii) from Theorem 7.

Lemma 8. *Let A be a subset of $\mathbb{Z}_p$.*

(i) If $4 \le |A| \le (p-1)/3$ and $|2A| = 2|A|$ then A is an almost progression of the form $A = \{a, a+2d, a+3d, \ldots, a+|A|d\}$.

(ii) If $10 \le |A| \le p/35$, and $|2A| = 2|A|+1$, then A is contained in an arithmetic progression with $|A|+2$ elements.

Proof of Theorem 3. Suppose that $t \ge 5$, $k \ge 3$, and $\lambda_A = 2$. From Table 2 we see that $t \ge 14$. Computational data also show that $p > 2500$. By Lemma 6, we must have $t < 2k^2/(k-2)$, and consequently, $p = kt+1 < 2k^3/(k-2)+1$. Since $p > 2500$ we must have $k \ge 35$.

Suppose now that $t \ge 14$, $k \ge 35$, and that $|2A| = 2|A|$ or $2|A|+1$. Then, by Lemma 8, A is contained in an arithmetic progression of length at most $t+2$. It follows that the set $3A-3A := A+A+A-A-A-A$ is contained in an arithmetic progression of length at most $6(t+2)-5 = 6t+7$ and so $|3A-3A| \le 6t+7$. On the other hand, a result of Glibichuk and Konyagin [10, Corollary 3.6] (see also [2]) gives,

$$|3A-3A| \ge \min\left(\tfrac{t^2}{2}, \tfrac{p-1}{2}\right).$$

Thus, either $6t+7 \ge \frac{1}{2}t^2$, that is, $t \le 13$, or $6t+7 \ge \frac{p-1}{2}$, that is, $k \le 12 + \frac{14}{t} \le 13$, contradicting $t \ge 14$, $k \ge 35$. □

12. Proof of Corollary 2, Part I: Almost Arithmetic Progressions

Chowla, Mann and Straus [4] proved the following.

Lemma 9 ([4])**.** *If A is a multiplicative subgroup of $\mathbb{Z}_p^*$ with $3 \leq |A| < p-1$ then A is not an arithmetic progression.*

Thus, a subgroup of $\mathbb{Z}_p^*$ is an arithmetic progression if and only if $t = 1, 2$ or $p-1$. As the first step towards proving Corollary 2, we prove the following characterization of almost arithmetic progressions.

Lemma 10. *If p is a prime with $p \neq 7$, then no subgroup of $\mathbb{Z}_p^*$ is an almost arithmetic progression. For $p = 7$, the subgroup $\{1, 3, 4\}$ of $\mathbb{Z}_7^*$ is the unique subgroup that is an almost arithmetic progression.*

We need the following.

Lemma 11. *If A is a multiplicative subgroup of $\mathbb{Z}_p^*$ that is an almost arithmetic progression of the type*

$$a, a+d, \ldots, a+(r-1)d, a+(r+1)d, \ldots, a+td,$$

for some $a, d \in \mathbb{Z}_p^*$ and positive integers r, t with $1 \leq r < t$, then

$$p | (t^3 - t^2 + 12rt - 12r^2).$$

We note that Lemma 9 is an immediate consequence of the $r = 0$ version of this lemma. The proof we give here follows the argument in [4] (see also [17]) for the proof of Lemma 9.

Proof. Since A is not an arithmetic progression we know $3 \leq t < p-1$. It is elementary that for any subgroup A of $\mathbb{Z}_p^*$ with $t \geq 3$, $\sum_{x \in A} x = 0$ and $\sum_{x \in A} x^2 = 0$. Then

$$\begin{aligned}
0 &= \sum_{x \in A} \sum_{y \in A} (x-y)^2 = \sum_{i=0}^{t} \sum_{j=0}^{t} ((a+id)-(a+jd))^2 - 2\sum_{i=0}^{t} ((a+id)-(a+rd))^2 \\
&= d^2 \left(\sum_{i=0}^{t} \sum_{j=0}^{t} (i-j)^2 - 2\sum_{i=0}^{t} (i-r)^2 \right) \\
&= d^2 \left(2t \sum_{i=0}^{t} i^2 - 2\Big(\sum_{i=0}^{t} i \Big)^2 + 4r \sum_{i=0}^{t} i - 2(t+1)r^2 \right) \\
&= d^2 \left(\tfrac{1}{3} t^2 (t+1)(2t+1) - \tfrac{1}{2} (t(t+1))^2 + 2rt(t+1) - 2(t+1)r^2 \right) \\
&= \tfrac{1}{6} d^2 (t+1)(t^3 - t^2 + 12rt - 12r^2).
\end{aligned}$$

Since $p \geq 5$ and $p \nmid d^2(t+1)$, the lemma follows. $\square$

Proof of Lemma 10. Suppose that A is a subgroup of $\mathbb{Z}_p^*$ that is an almost arithmetic progression. In particular, $t \geq 3$ and $p \geq 7$. Since A is contained in an arithmetic progression of length $t+1$ we have

$$|2A| \leq 2(t+1) - 1 < 3t = 3|A|,$$

and so $|2A| = 2|A|$ or $2|A| + 1$. By Theorem 3, $t = 3$ or 4, or $k = 2$. If $t = 3$, then by Lemma 11, we have

$$p|6(2r^2 - 6r - 3),$$

for some $r \in \{0, 1, 2\}$, implying that $p = 7$ and $A = \{1, 2, 4\}$. For $t = 4$, we get similarly that

$$p|12(r^2 - 4r - 4),$$

for some $r \in \{0, 1, 2, 3\}$, but there are no such primes with $p \equiv 1 \bmod 4$.

If $k = 2$, then the set of squares mod p is contained in an arithmetic progression $\{a + dj : 0 \leq j \leq t\}$ of length $t + 1 = \frac{p+1}{2}$, for some $a, d \in \mathbb{Z}_p^*$, which implies that $\left(\frac{a+dj}{p}\right) = 1$ for all but one value of $j \in [0, (p-1)/2]$. Therefore,

$$\left|\sum_{j=0}^{(p-1)/2} \left(\frac{a + dj}{p}\right)\right| \geq \frac{p-3}{2}.$$

On the other hand, by the Polya-Vinogradov estimate (see [1, Lemma 3.1] for the numeric version stated here), for any arithmetic progression I,

$$\left|\sum_{x \in I} \left(\frac{x}{p}\right)\right| \leq \tfrac{4}{\pi^2}\sqrt{p}\,\log(3p). \tag{12.1}$$

Together, these inequalities imply that $p \leq 13$. By Lemma 11, for $p = 13$, $t = 6$ we must have $13|(r^2 - 6r - 15)$ for some r with $1 \leq r < 6$, which does not occur. For $p = 11$, $t = 5$ we must have $11|(3r^2 - 15r - 25)$ for some r with $1 \leq r < 5$, which also does not occur. This leaves $p = 7, 5$ or 3, cases we have already accounted for. $\square$

13. Proof of Corollary 2, Part II

If $p \leq 7$ then every subgroup of $\mathbb{Z}_p^*$ is accounted for in parts (i) and (ii) of the corollary, and so we may assume that $p > 7$. Suppose that A is a subgroup of $\mathbb{Z}_p^*$ contained in an arithmetic progression B of length $\lfloor \frac{3}{2}t \rfloor$. Then $|2A| \leq |2B| \leq 2|B| - 1 \leq 3t - 1$, and so by Theorem 3, it follows that $k \leq 2$ or $t \leq 4$. The cases $k = 1$, $t = 1$ and $t = 2$ are trivial. We consider the remaining cases in turn.

Suppose that $k = 2$, that is, A is the group of squares. Since A is contained in an arithmetic progression B with $|B| = \lfloor \frac{3}{2}t \rfloor = \lfloor \frac{3}{4}(p-1) \rfloor$, the complementary set $B^c = \mathbb{Z}_p \setminus B$ is an arithmetic progression of length $|B^c| = p - |B| = \lceil \frac{1}{4}(p+3) \rceil$ consisting entirely of quadratic nonresidues together possibly with zero. Let $B^c =$

$\{a + dj : 1 \leq j \leq M\}$, with $M = \lceil \frac{1}{4}(p+3) \rceil$, for some $a, d \in \mathbb{Z}_p$, $d \neq 0$. Therefore,

$$\left| \sum_{j=1}^{M} \left(\frac{a+dj}{p} \right) \right| \geq M - 1 \geq \frac{1}{4}(p-1). \tag{13.1}$$

Combining this with the Polya-Vinogradov upper bound (12.1), we conclude that $p < 80$. For $p < 80$, a computer is used to compute all possible sums of the type (13.1). By factoring out d, one can assume that $d = 1$, saving computing time. The only sums satisfying (13.1) with $7 < p < 80$ occur when $p = 13$ and 17. For $p = 13$ we have

$$A = \{1, 3, 4, 9, 10, 12\} \subset \{1 + 3k : 0 \leq k \leq 8\} = \{1, 4, 7, 10, 0, 3, 6, 9, 12\},$$

while for $p = 17$,

$$A = \{1, 2, 4, 8, 9, 13, 15, 16\} \subset \{9 + 3k : 0 \leq k \leq 11\}.$$

If in either case, $p = 13$ or $p = 17$, A was contained in an arithmetic progression of shorter length than the one given, then the complementary set would be a longer progression of nonresidues than actually occurs for $p = 13$ or 17.

Suppose now that $t = 3$. Then $\lfloor \frac{3}{2} t \rfloor = 4$, and so A is contained in a progression of length 4. Then A is either an arithmetic progression or an almost arithmetic progression, and so by Lemmas 9 and 10, $A = \{1, 2, 4\}$ in $\mathbb{Z}_7^*$.

Finally, suppose that $t = 4$. In particular, $p \equiv 1 \bmod 4$. In this case, the assumption is that A is contained in a progression of length 6, say

$$a, a + d, a + 2d, a + 3d, a + 4d, a + 5d,$$

for some $a, d \in \mathbb{Z}_p$, $d \neq 0$. Consider all possible ways of forming A by deleting two elements from the progression. If either element is one of the extremities, a or $a + 5d$, then A is either a progression or an almost progression, cases already dealt with. Consider in turn the other $\binom{4}{2} = 6$ possibilities.

(i) $A = \{a, a + 3d, a + 4d, a + 5d\}$. Then forming the sum $\sum_{x \in A} \sum_{y \in A} (x - y)^2$, we get $0 = 56d^2$, implying that $p = 7$, contradicting $p \equiv 1 \bmod 4$.

(ii) $A = \{a, a + 2d, a + 4d, a + 5d\}$. Forming the same sum, we get $0 = 59d^2$, implying that $p = 59$, again in violation of $p \equiv 1 \bmod 4$.

(iii) $A = \{a, a + 2d, a + 3d, a + 5d\}$. This time we get $0 = 52d^2$, implying that $p = 13$. For $p = 13$, we see that

$$A = \{1, 5, 8, 12\} \subset \{8 + 2k : 0 \leq k \leq 5\} = \{8, 10, 12, 1, 3, 5\}.$$

A is not contained in any shorter progression, since it is not an almost arithmetic progression, by Lemma 10.

(iv) $A = \{a, a+d, a+4d, a+5d\}$. Then $0 = 68d^2$ and so $p = 17$. For $p = 17$, we have

$$A = \{1, 4, 13, 16\} \subset \{1 + 3k : 0 \le k \le 5\} = \{1, 4, 7, 10, 13, 16\}.$$

Again, A is not contained in any shorter progression.

(v) $A = \{a, a+d, a+3d, a+5d\}$. Then $0 = 59d^2$, which as we saw above cannot occur.

(vi) $A = \{a, a+d, a+2d, a+5d\}$. Then $0 = 56d^2$, which also cannot occur.

14. Estimation of $\Phi_t(n)$

Lemma 12. *For any positive integers $n > 1$, $t > 2$ we have*

$$\begin{aligned} (a) \quad & \Phi_t(n) < \frac{n}{n-1}\ n^{\phi(t)}, \quad \textit{for } t \textit{ odd;} \\ & \Phi_t(n) < \frac{n+1}{n}\ n^{\phi(t)}, \quad \textit{for } t \textit{ even.} \end{aligned}$$

$$\begin{aligned} (b) \quad & \Phi_t(-n) < \frac{n+1}{n}\ n^{\phi(t)}, \quad \textit{for } t \textit{ odd;} \\ & \Phi_t(-n) < \frac{n}{n-1}\ n^{\phi(t)}, \quad \textit{for } t \textit{ even.} \end{aligned}$$

To prove the lemma we need the following lemma.

Lemma 13. *Let $\mathcal{P}$ be the set of primes and x a positive real with $0 < x \le \frac{1}{2}$. Then*

$$\begin{aligned} (i) \quad & \prod_{p \in \mathcal{P}} (1 + x^p) < 1 + x; \\ (ii) \quad & \prod_{p \in \mathcal{P}} (1 - x^p) > 1 - x. \end{aligned}$$

Proof. (i) Noting that $\log(1+x) < x - \frac{3}{8}x^2$ for $0 < x \le \frac{1}{2}$, we have for $0 < x \le \frac{1}{2}$,

$$\begin{aligned} \sum_{p \in \mathcal{P}} \log(1 + x^p) &< \log((1+x^2)(1+x^3)) + \sum_{\substack{p \ge 5 \\ p \in \mathcal{P}}} \left(x^p - \frac{3}{8}x^{2p}\right) \\ &< \log((1+x^2)(1+x^3)) + \sum_{\substack{n \ge 5 \\ n \text{ odd}}} \left(x^n - \frac{3}{8}x^{2n}\right) \\ &= \log((1+x^2)(1+x^3)) + \frac{x^5}{1-x^2} - \frac{3}{8}\frac{x^{10}}{1-x^4} < \log(1+x), \end{aligned}$$

the last inequality being verified on a calculator for $0 < x \le \frac{1}{2}$.

(ii) For the lower bound in (ii), we first observe that $\log(1-x) > -x - 2x^2$ for $0 < x \le \frac{1}{2}$, and so

$$\sum_{\substack{p\ge 5\\ p\in\mathcal{P}}} \log(1-x^p) > -\sum_{\substack{p\ge 5\\ p\in\mathcal{P}}} \left(x^p + 2x^{2p}\right) > -\frac{x^5}{1-x^2} - \frac{2x^{10}}{1-x^4},$$

and

$$\sum_{p\in\mathcal{P}} \log(1-x^p) > \log((1-x^2)(1-x^3)) - \frac{x^5}{1-x^2} - \frac{2x^{10}}{1-x^4} > \log(1-x),$$

the last inequality being verified on a calculator for $0 < x \le \frac{1}{2}$. □

Proof of Lemma 12. It suffices to prove parts (a) and (b) for the case of odd square-free t. The inequalities for even square-free t follow from the formula

$$\Phi_{2t}(x) = \Phi_t(-x),$$

for t odd. For a general positive integer t, we write $t = t_1 t_2$ with t_1 the radical of t (the product of its distinct prime divisors), and deduce the inequalities from the formula

$$\Phi_t(x) = \Phi_{t_1}(x^{t_2}).$$

(a) Let $t = q_1 q_2 \cdots q_r$, with the q_i distinct odd primes. Suppose that r is odd. Let $\omega = \omega(d)$ denote the number of distinct prime divisors of d, and for any non-negative integer j, set

$$\prod_{\omega=j} := \prod_{d\mid t,\ \omega(d)=j} .$$

Then

$$\begin{aligned}
\Phi_t(n) &= \prod_{d\mid t} (n^d - 1)^{\mu(t/d)} = n^{\phi(t)} \prod_{d\mid t} \left(1 - \frac{1}{n^d}\right)^{\mu(t/d)} \\
&= n^{\phi(t)} \frac{\prod_{\omega=r}\left(1-\frac{1}{n^d}\right)\prod_{\omega=r-2}\left(1-\frac{1}{n^d}\right)\cdots\prod_{\omega=1}\left(1-\frac{1}{n^d}\right)}{\prod_{\omega=r-1}\left(1-\frac{1}{n^d}\right)\prod_{\omega=r-3}\left(1-\frac{1}{n^d}\right)\cdots\prod_{\omega=2}\left(1-\frac{1}{n^d}\right)\left(1-\frac{1}{n}\right)} \\
&< n^{\phi(t)} \frac{\prod_{\omega=r-2}\left(1-\frac{1}{n^d}\right)}{\prod_{\omega=r-1}\left(1-\frac{1}{n^d}\right)} \frac{\prod_{\omega=r-4}\left(1-\frac{1}{n^d}\right)}{\prod_{\omega=r-3}\left(1-\frac{1}{n^d}\right)} \cdots \frac{\prod_{\omega=1}\left(1-\frac{1}{n^d}\right)}{\prod_{\omega=2}\left(1-\frac{1}{n^d}\right)} \frac{1}{\left(1-\frac{1}{n}\right)}.
\end{aligned}$$

We claim that for $l = 0$ to $r-1$,

$$\prod_{\omega=l+1} \left(1 - \frac{1}{n^d}\right) > \prod_{\omega=l} \left(1 - \frac{1}{n^d}\right). \tag{14.1}$$

Indeed, applying Lemma 13 (ii) with $x = \frac{1}{n^d}$,

$$\prod_{\omega=l+1}\left(1-\frac{1}{n^d}\right) > \prod_{\substack{d|t\\ \omega(d)=l}}\prod_{j=1}^{r}\left(1-\frac{1}{n^{dq_j}}\right) > \prod_{\substack{d|t\\ \omega(d)=l}}\left(1-\frac{1}{n^d}\right) = \prod_{\omega=l}\left(1-\frac{1}{n^d}\right).$$

Thus, for odd r we get $\Phi_t(n) < n^{\phi(t)}\frac{n}{n-1}$.

Next, if r is even, we write

$$\begin{aligned}\Phi_t(n) &= \prod_{d|t}(n^d-1)^{\mu(t/d)} = n^{\phi(t)}\prod_{d|t}\left(1-\frac{1}{n^d}\right)^{\mu(t/d)}\\ &< n^{\phi(t)}\frac{\prod_{\omega=r-2}\left(1-\frac{1}{n^d}\right)}{\prod_{\omega=r-1}\left(1-\frac{1}{n^d}\right)}\cdots\frac{\prod_{\omega=2}\left(1-\frac{1}{n^d}\right)}{\prod_{\omega=3}\left(1-\frac{1}{n^d}\right)}\frac{\left(1-\frac{1}{n}\right)}{\prod_{\omega=1}\left(1-\frac{1}{n^d}\right)},\end{aligned}$$

which, by (14.1), yields $\Phi_t(n) < n^{\phi(t)}$.

(b) Again, let $t = q_1q_2\cdots q_r$, with the q_i distinct odd primes. Suppose that r is odd. Then

$$\begin{aligned}\Phi_t(-n) &= \prod_{d|t}(-n^d-1)^{\mu(t/d)} = n^{\phi(t)}\prod_{d|t}\left(1+\frac{1}{n^d}\right)^{\mu(t/d)}\\ &= n^{\phi(t)}\frac{\prod_{\omega=r}\left(1+\frac{1}{n^d}\right)}{\prod_{\omega=r-1}\left(1+\frac{1}{n^d}\right)}\frac{\prod_{\omega=r-2}\left(1+\frac{1}{n^d}\right)}{\prod_{\omega=r-3}\left(1+\frac{1}{n^d}\right)}\cdots\frac{\prod_{\omega=1}\left(1+\frac{1}{n^d}\right)}{\left(1+\frac{1}{n}\right)}.\end{aligned}$$

We claim that for $l = 0$ to $r-1$,

$$\prod_{\omega=l+1}\left(1+\frac{1}{n^d}\right) < \prod_{\omega=l}\left(1+\frac{1}{n^d}\right). \tag{14.2}$$

Indeed, applying Lemma 13 with $x = \frac{1}{n^d}$,

$$\prod_{\omega=l+1}\left(1+\frac{1}{n^d}\right) < \prod_{\substack{d|t\\ \omega(d)=l}}\prod_{j=1}^{r}\left(1+\frac{1}{n^{dq_j}}\right) < \prod_{\substack{d|t\\ \omega(d)=l}}\left(1+\frac{1}{n^d}\right) = \prod_{\omega=l}\left(1+\frac{1}{n^d}\right).$$

Thus, for odd r we get $\Phi_t(-n) < n^{\phi(t)}$.

Next, if r is even, we write

$$\begin{aligned}\Phi_t(-n) &= \prod_{d|t}(-n^d-1)^{\mu(t/d)} = n^{\phi(t)}\prod_{d|t}\left(1+\frac{1}{n^d}\right)^{\mu(t/d)}\\ &= n^{\phi(t)}\frac{\prod_{\omega=r}\left(1+\frac{1}{n^d}\right)}{\prod_{\omega=r-1}\left(1+\frac{1}{n^d}\right)}\ \frac{\prod_{\omega=r-2}\left(1+\frac{1}{n^d}\right)}{\prod_{\omega=r-3}\left(1+\frac{1}{n^d}\right)}\cdots\frac{\prod_{\omega=2}\left(1+\frac{1}{n^d}\right)}{\prod_{\omega=1}\left(1+\frac{1}{n^d}\right)}\left(1+\frac{1}{n}\right),\end{aligned}$$

which, by (14.2), yields the inequality of the lemma. □

References

[1] J. Bourgain, T. Cochrane, J. Paulhus and C. Pinner, On the parity of k-th powers mod p, a generalization of a problem of Lehmer, *Acta Arith.* **147** (2011), no. 2, 173-203.

[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), no. 2, 380–398.

[3] E. Breuillard, B. Green and T. Tao, Small doubling in groups, in *Erdös Centennial, Bolyai Soc. Math. Stud.*, 25, János Bolyai Math. Soc., Budapest, 2013, 129-151.

[4] 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.

[5] A. Cochrane, *Sumset Growth for Multiplicative Subgroups of a Finite Field*, Masters Thesis, Kansas State University, 2021.

[6] T. Cochrane, D. Hart, C. Pinner and C. Spencer, Waring's number for large subgroups of $\mathbb{Z}_p^*$, *Acta Arith.* **163** (2014), no. 4, 309-325.

[7] T. Cochrane and C. Pinner, Sum-product estimates applied to Waring's problem mod p, *Integers* **8** (2008), #A46, 18 pp.

[8] G. A. Freiman, Inverse problems of additive number theory. On the addition of sets of residues with respect to a prime modulus, *Soviet Math. Dokl.* **2** (1961), 1520-1522.

[9] G. A. Freiman, *Foundations of a Structural Theory of Set Addition*, Amer. Math. Soc., Providence, R. I., 1973. Translated from the Russian, Translations of Mathematical Monographs, Vol 37.

[10] A. A. Glibichuk and S.V. Konyagin, Additive properties of product sets in fields of prime order, in *Additive Combinatorics*, CRM Proc. Lecture Notes, 43, Amer. Math. Soc., Providence, RI, 2007, 279–286.

[11] B. Green and I. Z. Rusza, Freiman's theorem in an arbitrary abelian group, *J. London Math. Soc.* **75** (2007), no. 1, 163-175.

[12] Y. O. Hamidoune and O. J. Rodseth, An inverse theorem mod p, *Acta Arith.* **92** (2000), no. 3, 251-262.

[13] D. Hart, A note on sumsets of subgroups in $\mathbb{Z}_p^*$, *Acta Arith.* **161** (2013), no. 4, 387-395.

[14] 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.

[15] 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.

[16] H. L. Montgomery, R. C. Vaughan and T. D. Wooley, Some remarks on Gauss sums associated with k-th powers, *Math. Proc. Camb. Phil. Soc.* **118** (1995), no. 1, 21-33.

[17] M. B. Nathanson, *Additive Number Theory: Inverse Problems and the Geometry of Sumsets*, Springer, New York, 1996.

[18] I. Z. Ruzsa, Sums of finite sets, in *Number Theory* (New York, 1991–1995), Springer, New York, 1996, 281–293.

[19] I. Z. Ruzsa, An analog of Freiman's theorem in groups, in *Structure Theory of Set Addition*, Asterisque 258:xv, 1999, 323–326.

[20] I. D. Shkredov, Some new inequalities in additive combinatorics, *Moscow J. of Combinatorics and Number Theory* **3** (2013), no. 3-4, 189-239.

[21] A. G. Vosper, The critical pairs of subsets of a group of prime order, *J. London Math. Soc.* **31** (1956), 200-205.

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