SUMSETS IN THE SET OF SQUARES

CHRISTIAN ELSHOLTZ AND LENA WURZINGER

Abstract. We study sumsets $\mathcal{A}+\mathcal{B}$ in the set of squares $\mathcal{S}$ (and, more generally, in the set of k-th powers $\mathcal{S}_k$, where $k \geq 2$ is an integer). It is known by a result of Gyarmati that $\mathcal{A}+\mathcal{B} \subset \mathcal{S}_k \cap [1,N]$ implies that $\min(|\mathcal{A}|,|\mathcal{B}|) = O_k(\log N)$. Here we study how the upper bound on $|\mathcal{B}|$ decreases, when the size of $|\mathcal{A}|$ increases (or vice versa). In particular, if $|\mathcal{A}| \geq Ck^{\frac{1}{m}} m (\log N)^{\frac{1}{m}}$, then $|\mathcal{B}| = O_k(m^2 \log N)$, for sufficiently large N, a positive integer m and an explicit constant $C > 0$. For example, with $m \sim \log\log N$ this gives: If $|\mathcal{A}| \geq C_k \log\log N$, then $|\mathcal{B}| = O_k(\log N (\log\log N)^2)$.

1. Introduction

1.1. **Sumsets in sets of arithmetic interest.** An important topic in additive combinatorics is the study of large sumsets

$$\mathcal{A}+\mathcal{B} = \{a+b : a \in \mathcal{A}, b \in \mathcal{B}\}$$

contained in sets $\mathcal{C}$ of special arithmetic interest, such as the set of primes, squares, pure powers, squarefree numbers and others. Most sets $\mathcal{C}$ cannot be written as a sumset in a nontrivial way, i.e. with $|\mathcal{A}|, |\mathcal{B}| \geq 2$. Wirsing [33] proved that most sets $\mathcal{C}$ cannot even be asymptotically written as a nontrivial sumset $\mathcal{A}+\mathcal{B}$, i.e. where the symmetric difference between $\mathcal{C}$ and $\mathcal{A}+\mathcal{B}$ is finite.

1.2. **The set of squares.** For the set of squares there are several reasons why it cannot be written as a sumset, some are elementary, some are deep: For any two elements $a_1, a_2 \in \mathcal{A}$ there can only be finitely many corresponding squares $a_i + b_j$, as the difference between consecutive squares increases, but $(a_2+b_j)-(a_1+b_j)$ does not. Less trivially, if there are infinitely many values x such that all of a_1+x, a_2+x, a_3+x are squares, then the elliptic curve $y^2 = (a_1+x)(a_2+x)(a_3+x)$ would contain infinitely many integral points (x,y), contradicting a famous theorem of Siegel [30].

Date: April 5, 2026.

2020 *Mathematics Subject Classification.* primary: 11P70; secondary: 11L40, 11N36.

Sárközy [24] raised the question if the set of quadratic residues modulo primes can be written as a nontrivial sumset, and conjectured that this is impossible. This question was taken up in particular by Shparlinski [29], Shkredov [27], and Hanson and Petridis [19].

In this paper, we study sumsets $\mathcal{A} + \mathcal{B}$ in the set of integer squares $\mathcal{S} = \{1, 4, 9, \ldots\}$, as well as more generally in the set of k-th integer powers $\mathcal{S}_k$, where $k \geq 2$ is an integer.

According to Guy [17, sections D14 and D15], Erdős and Leo Moser asked about integers whose pairwise sums are all squares. Examples with 5 positive integers are due to Jean Lagrange e.g.

$$\{7442, 28658, 148583, 177458, 763442\}.$$

No example with 6 positive integers seems to be known. Leo Moser, John Leech and others also asked about sumsets of two distinct sets of integers. The following results are known:

When $|\mathcal{A}| = 2$ or $|\mathcal{A}| = 3$, then there exist arbitrarily large sets $\mathcal{B}$ such that $\mathcal{A} + \mathcal{B} \subset \mathcal{S}$. In fact, according to [23, Theorem 4], for the case $|\mathcal{A}| = 2$, a set $\mathcal{B} \subset [1, N]$ can be almost as large as the maximal value of the divisor function in $[1, N]$. That is, $|\mathcal{B}|$ is infinitely often as large (but also not much larger than)

$$\exp((\log 2 - o(1)) \log N / \log \log N).$$

Here and throughout the paper we use Landau's notation.

For the case $|\mathcal{A}| = 3$, it has been shown in [10] that it is possible to have $\mathcal{B} \subset [1, N]$ with $|\mathcal{B}| \geq C(\log N)^{\frac{15}{17}}$ for suitable $C > 0$. By contrast, it is conjectured that for $|\mathcal{A}| \geq 4$, the set $\mathcal{B}$ is bounded by an absolute constant: In [1, comment after Theorem 4.6] the authors explain that this follows from the Bombieri-Lang conjecture. For related work see [3, 28].

Also iterated sumsets have been studied in the set of squares. Let $\mathcal{H} = a_0 + \{0, a_1\} + \cdots + \{0, a_d\}$ denote a Hilbert cube in the set of squares. Solymosi [31] conjectured that the maximal possible value d is absolutely bounded, which again follows from the Bombieri-Lang conjecture. Unconditionally, Dietmann and Elsholtz [8, 9] proved that for Hilbert cubes in $\mathcal{S} \cap [1, N]$ the dimension is bounded by $d = O(\log \log N)$, improving on an earlier result of Hegyvári and Sárközy [20], and generalising a result of Csikvári [6].

Gyarmati [18] provided a significant upper bound for the size of the smaller set.

Theorem (Theorem 9 in [18]). *Let $\mathcal{A}, \mathcal{B} \subset [1, N]$ with $\mathcal{A} + \mathcal{B} \subset \mathcal{S}_k$. Then, for sufficiently large N, the following holds:* $\min(|\mathcal{A}|, |\mathcal{B}|) \leq 4k \log N$.

We are interested in how the size of one of the sets influences the upper bound on the other set. In this direction we prove the following results:

Theorem 1. *There exist constants $C_1, C_2 > 0$ such that the following holds. Let $\mathcal{A}, \mathcal{B} \subset [1, N]$ with $\mathcal{A} + \mathcal{B} \subset \mathcal{S}_k$, where $k \geq 2$ is a positive integer, and $\mathcal{S}_k$ denotes the set of all k-th powers. Moreover, let m be a positive integer. If*

$$|\mathcal{B}| \geq C_1 m^2 k \log N,$$

then

$$|\mathcal{A}| \leq C_2 m k^{\frac{1}{m}} (\log N)^{\frac{1}{m}}.$$

For sufficiently large N, $C_1 = 2304, C_2 = 1152$ are admissible. (When $m \to \infty$, then C_2 can be chosen close to 24.)

This improves upon Gyarmati [18] in the asymmetric case. In particular, when $|\mathcal{B}|$ is larger than $\log N$ by a small factor, then the upper bound on $|\mathcal{A}|$ drops quickly towards $O(\log \log N)$. By contraposition the opposite also holds, i.e. when $|\mathcal{A}|$ is bounded from below, then the corresponding upper bound on $|\mathcal{B}|$ follows.

A natural threshold in Theorem 1 for the size of m is $\log \log N$, as for larger m both bounds on $|\mathcal{A}|, |\mathcal{B}|$ get worse. In particular, with $m = \lfloor \log \log N \rfloor$ this implies the following special case:

Theorem 2. *Let $\mathcal{A}, \mathcal{B} \subset [1, N]$ with $\mathcal{A} + \mathcal{B} \subset \mathcal{S}_k$, where $k \geq 2$ is a positive integer, and $\mathcal{S}_k$ denotes the set of all k-th powers. Then there are positive constants c_1, c_2 (depending on k) such that the following holds. Suppose that*

$$|\mathcal{A}| > c_1 \log \log N.$$

Then

$$|\mathcal{B}| \leq c_2 \log N (\log \log N)^2.$$

Other special cases, when $|\mathcal{B}|$ is slightly larger than $\log N$, follow from the corollaries below.

Corollary 1. *Let $\mathcal{A}, \mathcal{B} \subset [1, N]$ with $\mathcal{A} + \mathcal{B} \subset \mathcal{S}_k$, where $k \geq 2$ is a positive integer, and $\mathcal{S}_k$ denotes the set of all k-th powers. Let $h(N) = o(\log \log N)$. There are constants c_1, c_2 (depending on k) such that, if*

$$|\mathcal{B}| \geq c_1 \frac{\log N (\log \log N)^2}{h(N)^2},$$

then

$$|\mathcal{A}| \leq c_2 \frac{\log \log N}{h(N)} \exp(h(N)).$$

Corollary 2. *Let $\mathcal{A}, \mathcal{B} \subset [1, N]$ with $\mathcal{A} + \mathcal{B} \subset \mathcal{S}_k$, where $k \geq 2$ is a positive integer, and $\mathcal{S}_k$ denotes the set of all k-th powers. Let $\epsilon, \delta > 0$ and assume that*

$$|\mathcal{A}| \geq \epsilon (\log N)^{\delta}.$$

Then

$$|\mathcal{B}| = O_{\epsilon,\delta}(\log N).$$

In particular, if m is a positive integer such that $\frac{1}{m} < \delta$, then for sufficiently large N (in terms of ϵ and k), we have

$$|\mathcal{B}| \leq C m^2 k \log N,$$

with $C > 0$ a positive constant independent of ϵ, δ and k.

Another measure of the size of the sets is the product $|\mathcal{A}||\mathcal{B}|$. In the symmetric case $|\mathcal{A}| = |\mathcal{B}|$ one also has $|\mathcal{A}||\mathcal{B}| = O_k((\log N)^2)$ by Gyarmati's result. Here we prove in a quite large range on the sizes of the sets related upper bounds:

Corollary 3. *Let $\mathcal{A}, \mathcal{B} \subset [1, N]$ with $\mathcal{A}+\mathcal{B} \subset \mathcal{S}_k$ such that $|\mathcal{B}| \geq |\mathcal{A}| \geq 3kC_2 \log\log N$, or, more generally, such that $|\mathcal{A}| \in [3kC_2 \log\log N, 8 \log N]$, where N is sufficiently large and C_2 is defined as in Theorem 1. Then*

$$|\mathcal{A}||\mathcal{B}| = O_k((\log N)^2).$$

Moreover, if one of the sets is of size $C_1 m^2 \log N$ (with C_1 and m as in Theorem 1), then

$$|\mathcal{A}||\mathcal{B}| = O_k(m^3 (\log N)^{1+\frac{1}{m}}).$$

1.3. **Strategy and tools for the proof.**

1.3.1. *Proof strategy.* Sieve methods usually deduce bounds on the counting function, when restrictions on the number of residue classes modulo primes are known. In the case of binary sumsets, the following strategy has been proved useful, see [11] for sumsets in the set of primes. For one of the two sets, say the first set, one uses an "inverse sieve" to deduce information about the distribution of residue classes modulo primes from the counting function. If this set is smaller than $O(\sqrt{N})$, then one might use Gallagher's larger sieve [16].

This information on the distribution of residue classes of the first set is converted to information about the residue classes of the second set. In this paper we take particular emphasis on this conversion of information. This is where we introduce the Weil inequality and Burgess type estimates to the topic. This local information modulo primes on the second set then gives, by another sieve application, an upper bound

on the size of the second set. In this case this second sieve is also Gallagher's larger sieve, whereas in the case of primes [11] it was the usual large sieve in Montgomery's form.

1.3.2. *Methods of proof.* We first collect some general bounds on the problem of sumsets in the set of k-th powers modulo p and later apply a sieve method to obtain a result in the integer case.

The following inequalities concerning sumsets $\mathcal{A}_p + \mathcal{B}_p$ contained in the quadratic residues (which can easily be adapted to allow for zero to also be represented by the sumset) are known:

Lemma 1. *Let p be a prime. Then the following inequalities concerning $\mathcal{A}_p + \mathcal{B}_p$ contained in the set of quadratic residues hold.*

- *Erdős and Shapiro* [15]*: $|\mathcal{A}_p||\mathcal{B}_p| \le p$.*
- *Hanson and Petridis* [19, Theorem 1.2][1]*: $|\mathcal{A}_p||\mathcal{B}_p| \le \frac{p-1}{2}$ for $p \ge 3$.*

Lemma 2 (See Sárközy [24], Conrad [5], Peralta [22])**.** *We have*

$$|\mathcal{A}_p| \le \frac{p}{2^{|\mathcal{B}_p|}} + |\mathcal{B}_p|\sqrt{p}.$$

In particular, if $|\mathcal{B}_p| \ge \frac{1}{2\log 2}\log p$, then $|\mathcal{A}_p| = O(\sqrt{p}\log p)$.

Lemma 3 (Weil, see [26])**.** *Let χ be a multiplicative character of order $d > 1$ of $\mathbb{Z}/p\mathbb{Z}$. Assume that $g(x) \in (\mathbb{Z}/p\mathbb{Z})[x]$ has r distinct zeros in the algebraic closure of $\mathbb{Z}/p\mathbb{Z}$ and that it is not a constant multiple of the d-th power of a polynomial over $\mathbb{Z}/p\mathbb{Z}$. Then the following bound holds:*

$$\left|\sum_{x\in\mathbb{Z}/p\mathbb{Z}} \chi(f(x))\right| \le (r-1)\sqrt{p}.$$

We now adapt a result of Treviño [32, Theorem 1.1] and obtain the following Burgess-type result [2] concerning sums of the form

$$\sum_{x=0}^{p-1}\left|\sum_{a\in\mathcal{A}_p}\chi(a+x)\right|^{2m},$$

where $\mathcal{A}_p \subset \mathbb{Z}/p\mathbb{Z}$ and χ is a nonprincipal character of order k. A precursor of Burgess [2] is Davenport and Erdős [7].

[1]This follows from their formula $|\mathcal{A}_p||\mathcal{B}_p| \le d + |\mathcal{A}_p \cap (-B_p)|$ with $d = (p-1)/2$ and $\mathcal{A}_p \cap (-B_p) = \emptyset$.

In the mentioned sources, only sums with $\mathcal{A}_p$ being an interval were considered. However, the proofs only utilise estimates on the cardinality of the set

$$\{(a_1,\dots,a_{2m}) \in \mathcal{A}_p^{2m} : \\ (x+a_1)\cdots(x+a_m)(x+a_{m+1})^{d-1}\cdots(x+a_{2m})^{d-1} \text{ is a square}\},$$

which just depends on the cardinality of $\mathcal{A}_p$ and not on its structure, so they can easily be extended to general sets $\mathcal{A}_p$. (For comparison, recall that well known results by Chang [4] require intervals.) Our considerations lead to the following adaptation of Treviño [32, Theorem 1.1]. We first state the estimates in a sharper form, as this might be useful in another context, and then simplify the bounds for our specific application.

Lemma 4 (see Theorem 1.1 in [32])**.** *Let m be a positive integer, let p be a prime and let $\mathcal{A}_p \subset \mathbb{Z}/p\mathbb{Z}$. Furthermore, denote by χ a nonprincipal character. Then, if $m \le 9|\mathcal{A}_p|$, the following estimate holds:*

$$\sum_{x=0}^{p-1}\Big|\sum_{a\in\mathcal{A}_p}\chi(a+x)\Big|^{2m} < \frac{(2m)!}{2^m m!}p|\mathcal{A}_p|^m + (2m-1)\sqrt{p}|\mathcal{A}_p|^{2m}.$$

For an application to sumsets in the set of squares, we only need the result of Lemma 4 in the special case where χ is the Legendre character, which we will discuss separately below. As demonstrated by our subsequent proof, the condition that $m \le 9|\mathcal{A}_p|$ can be omitted in this case.

Lemma 5. *Let $m \ge 1, k \ge 2$ be positive integers, let $p \ge 3$ be a prime, let $\mathcal{A}_p \subset \mathbb{Z}/p\mathbb{Z}$, and denote by χ the Legendre symbol. Furthermore, let*

$$S_{\mathcal{A}_p}(x) = \sum_{a\in\mathcal{A}_p}\chi(a+x).$$

Then, for $\sqrt{p}-(2m-1) \ge 0$, the following estimate holds:

$$\sum_{x=0}^{p-1}|S_{\mathcal{A}_p}(x)|^{2m} \le \frac{(2m)!}{2^m m!}|\mathcal{A}_p|^m\sqrt{p}(\sqrt{p}-(2m-1)) + (2m-1)\sqrt{p}|\mathcal{A}_p|^{2m}.$$

Moreover, we also have the following bound:

$$\sum_{x=0}^{p-1}\big|S_{\mathcal{A}_p}(x)\big|^{2m} < \frac{(2m)!}{2^m m!}p|\mathcal{A}_p|^m + (2m-1)\sqrt{p}|\mathcal{A}_p|^{2m}.$$

We now derive bounds on the cardinality of sumsets in the k-th powers modulo primes from Lemmas 4 and 5.

Lemma 6. *Let k be a positive integer, let p be a prime such that $p \equiv 1 \mod k$, and let $\mathcal{A}_p + \mathcal{B}_p \subseteq \mathcal{R}_k \cup \{0\}$, where $\mathcal{R}_k$ denotes the set of k-th powers modulo p. If $m \leq 9|\mathcal{A}_p|$, then*

$$|\mathcal{B}_p|(|\mathcal{A}_p| - 1)^{2m} \leq \frac{(2m)!}{2^m m!}|\mathcal{A}_p|^m p + (2m-1)|\mathcal{A}_p|^{2m}\sqrt{p}.$$

If $k = 2$, the condition that $m \leq 9|\mathcal{A}_p|$ can be omitted.

Proof. We choose a nonprincipal character χ whose order divides k. We note that the group of characters modulo p is isomorphic to $(\mathbb{Z}/p\,\mathbb{Z})^\times$, and that $|(\mathbb{Z}/p\,\mathbb{Z})^\times| = p - 1$ is divisible by k. Hence such a character exists, for instance by Cauchy's theorem.

Now, an application of Lemma 4 (or Lemma 5 in the case $k = 2$) yields the claimed inequality. □

We now use the bound $\frac{(2m)!}{2^m m!} \leq m^m$ to obtain a simplified version of Lemma 6, which we will use for our proof. Actually, Stirling's formula gives $\frac{(2m)!}{2^m m!} \sim \sqrt{2}\, m^m (\frac{2}{e})^m$. However, in our application, this small loss gives essentially the same result as Lemma 6, up to a small multiplicative constant.

Lemma 7. *Let $m \geq 1, k \geq 2$ be positive integers, let p be a prime, and assume that $p \equiv 1 \mod k$ and that $\mathcal{A}_p + \mathcal{B}_p \subseteq \mathcal{R}_k \cup \{0\}$, where $\mathcal{R}_k$ denotes the set of k-th powers modulo p. If $m \leq 9|\mathcal{A}_p|$ or if $k = 2$, then*

$$|\mathcal{B}_p|(|\mathcal{A}_p| - 1)^{2m} \leq m^m|\mathcal{A}_p|^m p + 2m|\mathcal{A}_p|^{2m}\sqrt{p}.$$

Eventually we employ Gallagher's larger sieve to prove the main result, i.e. Theorem 1. The sieve transforms the local information modulo primes of one of the two sets $\mathcal{A}$ or $\mathcal{B}$ into an upper bound of the other set.

Lemma 8 (Gallagher's larger sieve, [16])**.** *Let $\mathcal{A}$ be a set of positive integers with counting function $\mathcal{A}(N) = \sum_{a\in\mathcal{A}, a\leq N} 1$ and let $\mathcal{P}'$ be a set of primes. Suppose that for $p \in \mathcal{P}'$, $\mathcal{A}$ intersects at most $\nu(p)$ residue classes modulo p. Then, provided the denominator is positive, the following bound holds:*

$$\mathcal{A}(N) \leq \frac{-\log N + \sum_{p\in\mathcal{P}'} \log p}{-\log N + \sum_{p\in\mathcal{P}'} \log p/\nu(p)}.$$

1.4. **Comparison with sumsets in the primes.** Let us summarize what is known in the case of sumsets in the set of primes $\mathcal{P}$. If $\mathcal{A}+\mathcal{B} \subset \mathcal{P}$, then the counting functions $\mathcal{A}(N) = \sum_{a\in\mathcal{A}, a\leq N} 1$ and $\mathcal{B}(N)$ satisfy $\mathcal{A}(N)\,\mathcal{B}(N) = O(N)$ (proved by Wirsing, for details see [13]). It seems

surprising that one cannot rule out the possibility of sumsets in the set of primes, where the summands are two sets of integers of size about $\sqrt{N}$. For ternary sumsets the situation is better, here it can be proved that the set of primes cannot asymptotically be decomposed into three sumsets, see [11].

The asymmetric binary case, when one of the sets is much smaller than the second one, has attracted attention: When $|\mathcal{A}| = k$ is finite, then an upper bound on $\mathcal{B}(N) = O_k(\frac{N}{(\log N)^k})$ follows from a small sieve argument. Quite recently, V. Kuperberg [21] extended this using the small sieve up to $k = o((\log N)^{1/4})$. Upper bounds by means of the large sieve have been given by Elsholtz [11, 12, 13, 14]: In particular: if $\mathcal{A}(N)$ increases more quickly, e.g. $(\log N)^r, r \geq 1$, then

$$\mathcal{B}(N) = O_r\left(\frac{N^{\frac{1}{2}+\frac{1}{r+1}}}{\exp\left(c_r \log N \log\log\log N/\log\log N\right)}\right)$$

can be proved, i.e. when r increases, then the upper bound $\mathcal{B}(N)$ tends quite quickly to the threshold $\sqrt{N}$. The special case $r = 1$ has recently found an unexpected application to the complexity of primes, see [25].

From this one observes a striking asymmetry: a quite small set $\mathcal{A}$ forces the second set $\mathcal{B}$ to be almost as small as in the symmetric case when $\mathcal{A}(N) = \mathcal{B}(N) = O(\sqrt{N})$. Our main result, Theorem 1, proves a corresponding asymmetry in the case of the squares.

2. Proofs

2.1. **Character sum estimates.** As mentioned earlier, while Treviño [32, Theorem 1.1] only formulates Lemma 4 in the case where $\mathcal{A}_p$ is an interval, the proof in [32] only depends on the cardinality of the interval and does not rely on any relations between its elements. In order to demonstrate this, we give a proof in the special case of the Legendre character, which we stated earlier as Lemma 5.

Proof of Lemma 5. We expand the inner sum using the multiplicativity of the Legendre symbol and change the order of summation.

$$\begin{aligned}\sum_{x=0}^{p-1}\left|\sum_{a\in\mathcal{A}_p}\chi(a+x)\right|^{2m} &= \sum_{x=0}^{p-1}\sum_{(a_1,\ldots,a_{2m})\in\mathcal{A}_p^{2m}}\chi\left((x+a_1)\cdots(x+a_{2m})\right)\\ &= \sum_{(a_1,\ldots,a_{2m})\in\mathcal{A}_p^{2m}}\sum_{x=0}^{p-1}\chi\left((x+a_1)\cdots(x+a_{2m})\right).\end{aligned}$$

Now, we partition $\mathcal{A}_p^{2m}$ into two sets: $\mathcal{A}_p^{2m} = \mathcal{T} \cup (\mathcal{A}_p^{2m} \setminus \mathcal{T})$, where

$$(x+a_1)\cdots(x+a_{2m})$$

is a square in $(\mathbb{Z}/p\,\mathbb{Z})[x]$ if and only if $(a_1,\ldots,a_{2m}) \in \mathcal{T}$.

Thus we can use Weil's Lemma 3 in order to bound all summands not in $\mathcal{T}$:

$$\sum_{\substack{(a_1,\ldots,a_{2m})\\ \in \mathcal{A}_p^{2m}\setminus\mathcal{T}}} \left| \sum_{x=0}^{p-1} \chi\left((x+a_1)\cdots(x+a_{2m})\right) \right| \leq (2m-1)\sqrt{p}(|\,\mathcal{A}_p|^{2m} - |\,\mathcal{T}|).$$

For the remaining summands, we apply a trivial estimate:

$$\sum_{(a_1,\ldots,a_{2m})\in\mathcal{T}} \left| \sum_{x=0}^{p-1} \chi\left((x+a_1)\cdots(x+a_{2m})\right) \right| \leq |\,\mathcal{T}|p.$$

Adding the two bounds yields

$$\sum_{x=0}^{p-1} \left| \sum_{a\in\mathcal{A}_p} \chi(a+x) \right|^{2m} \leq (2m-1)\sqrt{p}|\,\mathcal{A}_p|^{2m} + \sqrt{p}(\sqrt{p}-(2m-1))|\,\mathcal{T}|.$$

We note that if $(a_1,\ldots,a_{2m}) \in \mathcal{T}$, then each a_i appears an even number of times in $(a_1,\ldots,a_{2m})$. Given an element $(c_1,\ldots,c_m) \in \mathcal{A}_p^m$, we create an element $(a_1,\ldots,a_{2m})$ in $\mathcal{T}$ as follows: We choose indices $i_1 < \ldots < i_m$ and set $a_{i_j} = c_j$ for $j = 1,\ldots,m$. For the remaining m spots $a_{k_1},\ldots,a_{k_m}$, we choose some permutation σ of $\{1,\ldots,m\}$ and set $a_{k_i} = c_{\sigma(i)}$.

For $(c_1,\ldots,c_m) \in \mathcal{A}_p^m$, we have at most $\binom{2m}{m}m!$ different choices, and iterating over all of $\mathcal{A}_p^m$, each $(a_1,\ldots,a_{2m}) \in \mathcal{T}$ gets created at least 2^m times (since for all $a_i = a_j$, either i or j can be chosen first.) Thus

$$|\,\mathcal{T}| \leq \frac{1}{2^m}\frac{(2m)!}{m!}|\,\mathcal{A}_p|^m. \tag{1}$$

Hence, if $\sqrt{p}-(2m-1) \geq 0$, we have the following bound:

$$\sum_{x=0}^{p-1} \left| \sum_{a\in\mathcal{A}_p} \chi(a+x) \right|^{2m} \leq \frac{(2m)!}{2^m m!}|\,\mathcal{A}_p|^m\sqrt{p}(\sqrt{p}-(2m-1)) + (2m-1)\sqrt{p}|\,\mathcal{A}_p|^{2m}.$$

Furthermore, bounding $(\sqrt{p}-(2m-1))|\,\mathcal{T}|$ by $\sqrt{p}|\,\mathcal{T}|$ and then applying inequality (1) gives the second claimed inequality. □

2.2. **Application of sieve methods.** Throughout this section, let $N \in \mathbb{N}$ be a positive integer, and let $\mathcal{A}, \mathcal{B} \subset [1, N]$ such that

$$\mathcal{A} + \mathcal{B} \subset \mathcal{S}_k,$$

where $\mathcal{S}_k$ denotes the set of k-th powers for an integer $k \geq 2$. Moreover, for any prime number $p \equiv 1 \bmod k$, we define

$$\nu_{\mathcal{A}}(p) = |\, \mathcal{A} \bmod p|$$
$$\nu_{\mathcal{B}}(p) = |\, \mathcal{B} \bmod p|.$$

By Lemma 7, we know that

$$\nu_{\mathcal{B}}(p)(\nu_{\mathcal{A}}(p) - 1)^{2m} \leq m^m \nu_{\mathcal{A}}(p)^m p + 2m\nu_{\mathcal{A}}(p)^{2m}\sqrt{p}$$

if $\nu_{\mathcal{A}}(p) \geq \frac{1}{9}m$. We note that the two terms on the right are equal if

$$\nu_{\mathcal{A}}(p) = \frac{m\ \sqrt[2m]{p}}{\sqrt[m]{2m}},$$

and we remark that $\sqrt[m]{2m} = \exp(\frac{\log 2 + \log m}{m}) \in [1, 2]$. We hence observe that

$$\nu_{\mathcal{B}}(p)(\nu_{\mathcal{A}}(p) - 1)^{2m} \leq 4m\nu_{\mathcal{A}}(p)^{2m}\sqrt{p}$$

for $\nu_{\mathcal{A}}(p) \geq m\ \sqrt[2m]{p}$.

Proof of Theorem 1. Let

$$\mathcal{M} = \left\{p \in \mathcal{P}' : \nu_{\mathcal{A}}(p) \geq 4m\ \sqrt[2m]{p}\right\},$$

where $\mathcal{P}' = \{p \text{ prime} : p \equiv 1 \bmod k\}$ denotes the set of primes congruent to 1 modulo k, and let

$$y = (48m\varphi(k)\log N)^2,$$

where φ denotes the Euler totient function. Further, assume that $|\,\mathcal{B}| > 2304m^2 \log N$.

By the prime number theorem for arithmetic progressions, we have

$$\sum_{\substack{p \in \mathcal{P}' \\ p \leq y}} \log p \sim \frac{1}{\varphi(k)} y.$$

Thus, one of the following two cases has to hold (for sufficiently large N).

Case 1: The following inequality holds:

$$\sum_{\substack{p \in \mathcal{M} \\ p \leq y}} \log p \geq \frac{y}{2\varphi(k)}.$$

Case 2: The following inequality holds:

$$\sum_{\substack{p\notin\mathcal{M}\\ p\le y}}\log p\ge\frac{y}{4\varphi(k)}.$$

We start with

Case 1: We assume that

$$\sum_{\substack{p\in\mathcal{M}\\ p\le y}}\log p\ge\frac{y}{2\varphi(k)}.$$

For $p\in\mathcal{M}$, we have (by definition of $\mathcal{M}$ and in view of Lemma 7)

$$\nu_{\mathcal{B}}(p)(\nu_{\mathcal{A}}(p)-1)^{2m}\le 4m\nu_{\mathcal{A}}(p)^{2m}\sqrt{p}.$$

Hence

$$\begin{aligned}\nu_{\mathcal{B}}(p)\le 4m\left(\frac{\nu_{\mathcal{A}}(p)}{\nu_{\mathcal{A}}(p)-1}\right)^{2m}\sqrt{p}&=4m\left(1+\frac{1}{\nu_{\mathcal{A}}(p)-1}\right)^{2m}\sqrt{p}\\&\le 4m\left(1+\frac{2}{\nu_{\mathcal{A}}(p)}\right)^{2m}\sqrt{p}\\&\le 4m\left(1+\frac{1}{2m\sqrt[2m]{p}}\right)^{2m}\sqrt{p}\\&\le 4m\left(1+\frac{1}{2m}\right)^{2m}\sqrt{p}\\&<12m\sqrt{p},\end{aligned}$$

as $\left(1+\frac{1}{2m}\right)^{2m}=\exp\left(2m\log\left(1+\frac{1}{2m}\right)\right)<3$. Now, by the hypothesis of case 1,

$$\sum_{\substack{p\in\mathcal{M}\\ p\le y}}\frac{\log p}{\nu_{\mathcal{B}}(p)}\ge\sum_{\substack{p\in\mathcal{M}\\ p\le y}}\frac{\log p}{12m\sqrt{p}}\ge\sum_{\substack{p\in\mathcal{M}\\ p\le y}}\frac{\log p}{12m\sqrt{y}}\ge\frac{1}{12m}\frac{\sqrt{y}}{2\varphi(k)}\ge 2\log N.$$

Thus, by Gallagher's larger sieve,

$$|\mathcal{B}|\le\frac{(1+o(1))y/\varphi(k)}{-\log N+\sum_{\substack{p\in\mathcal{M}\\ p\le y}}\frac{\log p}{\nu_{\mathcal{B}}(p)}}\le\frac{(1+o(1))y/\varphi(k)}{\frac{1}{4\cdot 12m\varphi(k)}\sqrt{y}}\le 2304\ m^2k\log N.$$

This contradicts our assumption on the cardinality of $\mathcal{B}$.

Case 2: Suppose that

$$\sum_{\substack{p\notin\mathcal{M}\\ p\le y}}\log p\ge\frac{y}{4\varphi(k)}.$$

For all $p \notin \mathcal{M}$, we have $\nu_{\mathcal{A}}(p) \le 4m \sqrt[2m]{p}$. Hence by the hypothesis of case 2,

$$\sum_{\substack{p \notin \mathcal{M} \\ p \le y}} \frac{\log p}{\nu_{\mathcal{A}}(p)} \ge \sum_{\substack{p \in \mathcal{M} \\ p \le y}} \frac{\log p}{4m \sqrt[2m]{p}}$$

$$\ge \sum_{\substack{p \in \mathcal{M} \\ p \le y}} \frac{\log p}{4m \sqrt[2m]{y}} \ge \frac{1}{4m} \frac{y^{1-\frac{1}{2m}}}{4\varphi(k)} \ge \log N + \frac{1}{24m\varphi(k)} y^{1-\frac{1}{2m}}$$

for all sufficiently large y.

Now, by Gallagher's larger sieve,

$$\begin{aligned} |\mathcal{A}| &\le \frac{(1+o(1))y/\varphi(k)}{-\log N + \sum_{\substack{p \notin \mathcal{M} \\ p \le y}} \frac{\log p}{\nu_{\mathcal{A}}(p)}} \\ &\le \frac{(1+o(1))y}{\frac{1}{24m} y^{1-\frac{1}{2m}}} \\ &= 24\ m\ y^{\frac{1}{2m}}(1+o(1)) \\ &\le 24\ mk^{1/m}\ (48m)^{\frac{1}{m}} (\log N)^{\frac{1}{m}} \\ &\le 1152\ mk^{\frac{1}{m}}\ (\log N)^{\frac{1}{m}}. \end{aligned}$$

□

Proof of Theorem 2. This follows from the contrapositive of Theorem 1 by choosing

$$m = \lfloor \log \log N \rfloor.$$

□

Proof of Corollary 1. This follows from the contrapositive of Theorem 1 by choosing

$$m = \left\lfloor \frac{\log \log N}{h(N)} \right\rfloor.$$

□

Proof of Corollary 2. We choose an integer m in such a way that

$$\frac{1}{m} < \delta.$$

Then for all sufficiently large N we have

$$|\mathcal{A}| \ge \epsilon (\log N)^{\delta} > C_2 mk^{\frac{1}{m}} (\log N)^{\frac{1}{m}}$$

with C_2 as in Theorem 1. Hence (for all sufficiently large N) the contrapositive of Theorem 1 implies that

$$|\mathcal{B}| \le C_1 m^2 k \log N,$$

where C_1 is the same constant as in Theorem 1. □

Proof of Corollary 3. For the first part of Corollary 3, we start out with considerations for sufficiently large N which are similiar to those in the proof of Theorem 2: as $\mathcal{B}$ is bounded from below by

$$3kC_2 \log\log N > 3kC_2 \lfloor \log\log N \rfloor \exp(\log\log N / \lfloor \log\log N \rfloor),$$

we also know by (the contrapositive of) Theorem 1 that $\mathcal{A}$ is bounded from above by

$$|\mathcal{A}| \leq C_1 (\log\log N)^2 k \log N.$$

Moreover, $|\mathcal{A}| \geq 3kC_2 \log\log N$ by assumption. Therefore there exists some integer $m \in [1, 2k \log\log N]$ such that

$$C_2 m^2 k^{\frac{1}{m}} \log N \leq |\mathcal{A}| \leq C_2 (m+1)^2 k^{\frac{1}{m}} \log N.$$

Now another application of Theorem 1 gives

$$|\mathcal{A}| \leq C_1 m^2 k \log N.$$

We multiply the upper bounds on $|\mathcal{A}|$ and $|\mathcal{B}|$, which yields the bound

$$|\mathcal{A}||\mathcal{B}| \ll_k m^3 (\log N)^{1+\frac{1}{m}}.$$

As remarked earlier, we have $m \in [1, 2k \log\log N]$, so we can further estimate

$$|\mathcal{A}||\mathcal{B}| \ll_k m^3 (\log N)^{1+\frac{1}{m}} \ll_k (\log N)^2.$$

The case $|\mathcal{A}| \in [3kC_2 \log\log N, 8 \log N]$ as well as the second statement follow analogously. □

3. Acknowledgements

This manuscript grew out of the second author's MSc Thesis at TU Graz [34]. C. Elsholtz is supported by a joint FWF-ANR project ArithRand, grant numbers FWF I 4945-N and ANR-20-CE91-0006. Both authors would like to thank Igor Shparlinski for drawing our attention to related character sum estimates. Furthermore we would like to thank the referee for a careful reading of the paper.

References

1. N. Alon, O. Angel, I. Benjamini, and E. Lubetzky, *Sums and products along sparse graphs*, Israel J. Math. **188** (2012), 353–384.
2. D. A. Burgess, *On character sums and primitive roots*, Matematika **7** (1963), no. 4, 3–16.
3. L. Caporaso, J. Harris, and B. Mazur, *Uniformity of rational points*, J. Amer. Math. Soc. **10** (1997), no. 1, 1–35.
4. M.-C. Chang, *On a question of Davenport and Lewis and new character sum bounds in finite fields*, Duke Math. J. **145** (2008), no. 3, 409–442.

5. K. Conrad, *Quadratic residue patterns modulo a prime*, `https://kconrad.math.uconn.edu/blurbs/ugradnumthy/QuadraticResiduePatterns.pdf`, 2014.
6. P. Csikvári, *Subset sums avoiding quadratic nonresidues*, Acta Arith. **135** (2008), no. 1, 91–98.
7. H. Davenport and P. Erdős, *The distribution of quadratic and higher residues*, Publ. Math. Debrecen **2** (1952), no. 3-4, 252–265.
8. R. Dietmann and C. Elsholtz, *Hilbert cubes in progression-free sets and in the set of squares*, Israel J. Math. **192** (2012), no. 1, 59–66.
9. ———, *Hilbert cubes in arithmetic sets*, Rev. Mat. Iberoam. **31** (2015), no. 4, 1477–1498.
10. A. Dujella and C. Elsholtz, *Sumsets being squares*, Acta Math. Hungar **141** (2013), no. 4, 353–357.
11. C. Elsholtz, *The inverse Goldbach problem*, Mathematika **48** (2001), no. 1-2, 151–158.
12. ———, *Upper bounds for prime k-tuples of size log N and oscillations*, Arch. Math. (Basel) **82** (2004), no. 1, 33–39.
13. ———, *Additive decomposability of multiplicatively defined sets*, Funct. Approx. Comment. Math. **35** (2006), 61–77.
14. C. Elsholtz and A. J. Harper, *Additive decompositions of sets with restricted prime factors*, Trans. Amer. Math. Soc. **367** (2015), no. 10, 7403–7427.
15. P. Erdős and H. N. Shapiro, *On the least primitive root of a prime*, Pacific J. Math. **7** (1957), 861–865.
16. P. X. Gallagher, *A larger sieve*, Acta Arith. **18** (1971), 77–81.
17. R. K. Guy, *Unsolved problems in number theory*, third ed., Problem Books in Mathematics, Springer-Verlag, New York, 2004.
18. K. Gyarmati, *On a problem of Diophantus*, Acta Arith. **97** (2001), 53–65.
19. B. Hanson and G. Petridis, *Refined estimates concerning sumsets contained in the roots of unity*, Proc. Lond. Math. Soc. (3) **122** (2021), no. 3, 353–358.
20. N. Hegyvári and A. Sárközy, *On Hilbert cubes in certain sets*, Ramanujan J. **3** (1999), no. 3, 303–314.
21. V. Kuperberg, *Sums of singular series with large sets and the tail of the distribution of primes*, Q. J. Math. **74** (2023), no. 4, 1457–1479.
22. R. Peralta, *On the distribution of quadratic residues and nonresidues modulo a prime number*, Math. Comp. **58** (1992), no. 197, 433–440.
23. J. Rivat, A. Sárközy, and C. L. Stewart, *Congruence properties of the Ω-function on sumsets*, Illinois J. Math. **43** (1999), no. 1, 1–18.
24. A. Sárközy, *On additive decompositions of the set of quadratic residues modulo p*, Acta Arith. **155** (2012), 41–51.
25. J. Schlage-Puchta, *Alternating state complexity of the set of primes and square-free integers*, 2023.
26. W. M. Schmidt, *Equations over finite fields. An elementary approach*, Lecture Notes in Mathematics, Vol. 536, Springer-Verlag, Berlin-New York, 1976.
27. I. Shkredov, *Sumsets in quadratic residues*, Acta Arith. **164** (2014), 221–243.
28. I. Shkredov and J. Solymosi, *The uniformity conjecture in additive combinatorics*, SIAM J. Discrete Math. **35** (2021), no. 1, 307–321.
29. I. E. Shparlinski, *Additive decompositions of subgroups of finite fields*, SIAM J. Discrete Math. **27** (2013), no. 4, 1870–1879.

30. C. L. Siegel (under the pseudonym X), *The integer solutions of the equation* $y^2 = ax^n + bx^{n-1} + \cdots + k$. *(Extract from a letter to Prof. L. J. Mordell.)*, J. Lond. Math. Soc. **1** (1926), 66–68.
31. J. Solymosi, *Elementary additive combinatorics*, Additive combinatorics, CRM Proc. Lecture Notes, vol. 43, Amer. Math. Soc., Providence, RI, 2007, pp. 29–38.
32. E. Treviño, *The least k-th power non-residue*, J. Number Theory **149** (2015), 201–224.
33. E. Wirsing, *Ein metrischer Satz über Mengen ganzer Zahlen*, Arch. Math. (Basel) **4** (1953), 392–398.
34. L. Wurzinger, *Sumsets in multiplicatively defined sets*, Master's thesis, Graz University of Technology, 2023.

Institut für Analysis und Zahlentheorie, Technische Universität Graz, Kopernikusgasse 24, A-8010 Graz, Austria
Email address: elsholtz@math.tugraz.at

Institute of Science and Technology Austria, Am Campus 1, A-3400 Klosterneuburg, Austria
Email address: lena.wurzinger@ist.ac.at