CAUCHY-DAVENPORT THEOREM FOR ABELIAN GROUPS
AND DIAGONAL CONGRUENCES

TODD COCHRANE, MISTY OSTERGAARD, AND CRAIG SPENCER

Abstract. We prove an analogue of the Cauchy-Davenport Theorem and Chowla’s Theorem for sum sets in a general abelian group and give an application to diagonal congruences, establishing a best possible estimate for the distribution of solutions of a diagonal congruence \( \sum_{i=1}^n a_i x_i^k \equiv c \pmod{q} \) with an arbitrary modulus.

1. Main Theorem for Abelian Groups

The most significant result of this paper is a best possible estimate on the uniform distribution of points satisfying a diagonal congruence, which we present in Section 5. In order to prove the result we needed an appropriate generalization of the Cauchy-Davenport Theorem \([3, 7]\) to a general modulus that went beyond what Chowla’s Theorem \([4]\) provided. This led us to a variation of Kneser’s Theorem \([9]\) (Theorem 1.1 below) for abelian groups that we have not been able to find in the literature, and that we believe has interest in its own right. We start the paper with a discussion of this result.

For any subsets \( A_1, \ldots, A_n \) of an additive abelian group \( G \) we define

\[
A_1 + \cdots + A_n = \{ x_1 + \cdots + x_n : x_i \in A_i, 1 \leq i \leq n \},
\]

and write \( nA \) for the sum of \( n \) copies of a subset \( A \) of \( G \). The Cauchy-Davenport Theorem states that for cyclic groups \( G \) of prime order, we have

\[
|A_1 + \cdots + A_n| \geq \min\{|G|, |A_1| + \cdots + |A_n| - (n - 1)\},
\]

for any \( A_i \). Chowla \([4]\) extended this estimate to cyclic groups of arbitrary finite order for certain \( A_i \); see Section 4. With all the \( A_i \) equal, say \( A_i = A, 1 \leq i \leq n \), the inequality in (1.1) becomes

\[
|nA| \geq \min\{|G|, n|A| - (n - 1)\}.
\]

Olson \([11, \text{Theorem 2.2}]\) considered a general group \( G \), and proved that for any finite set \( A \) of generators of \( G \) with \( 0 \in A \) and any positive integer \( n \) we have either \( nA = G \) or

\[
|nA| \geq \begin{cases} 
\frac{n+1}{2} |A|, & \text{if } |A| \text{ is even;} \\
\frac{n+1}{2} |A| + \frac{n-1}{2}, & \text{if } |A| \text{ is odd.}
\end{cases}
\]

Our main theorem on groups is a generalization of Olson’s result for the case of abelian groups.

Date: October 27, 2017.
2010 Mathematics Subject Classification. Primary: 11D79, 11D72, 11P05.
Key words and phrases. Cauchy-Davenport Theorem; Diagonal congruences.
Theorem 1.1. Let \( n \geq 1 \) and \( A_1, \ldots, A_n \) be finite, nonempty subsets of an abelian group \( G \), such that no \( A_i \) is contained in a coset of a proper subgroup of \( G \). Then

\[
|A_1 + \cdots + A_n| \geq \min \left\{ |G|, \left( \frac{1}{2} + \frac{1}{2n} \right) \sum_{i=1}^{n} |A_i| \right\}.
\]

For infinite groups, the \( |G| \) on the right-hand side can be dropped. The lower bound is best possible without a further assumption as we see in Example 1.1 below. Without the assumption on the \( A_i \) not being contained in a coset of a proper subgroup the inequality can fail. For example, if each \( A_i \) is contained in a coset of some proper subgroup \( H \) of \( G \), then \( A_1 + \cdots + A_n \) is contained in a single coset of \( H \) and so its cardinality can never exceed \( |H| \). The \( n = 2 \) case of the theorem is given in [12, Theorem 4.6.1], while a weaker lower bound for general \( n \) is given in [12, Corollary 2.7.1].

By Theorem 1.1, for any finite subset \( A \) of an abelian group \( G \) that is not contained in a coset of a proper subgroup of \( G \), we have

\[
|nA| \geq \min \left\{ |G|, \left( \frac{n+1}{2} \right) |A| \right\},
\]

for any positive integer \( n \). Recalling that a subset \( S \) of \( G \) is called a basis of order \( n \) if \( nS = G \), we see that \( A \) is a basis of order \( \left[ \frac{|G|}{|A|} \right] - 1 \). The same estimate was obtained by Olson [11, Theorem 2.2], Hamidoune and Rödseth [8, Lemma 1], and Nathanson [10, Theorem 4.10], in the case where \( A \) is a set of generators for \( G \) with \( 0 \in A \). In the latter case, we certainly have that \( A \) is not contained in a coset of any proper subgroup of \( G \). The estimate in (1.4) recovers the result of Olson (1.2) for even \( |A| \). For odd \( |A| \), we give a small refinement of (1.2) in Proposition 3.1.

Example 1.1. Let \( H \) be a proper subgroup of \( G \), \( a \) an element of \( G \) with \( a \notin H \), and \( A = H \cup (H + a) \). Then for any positive integer \( n \),

\[
|nA| = |H \cup (H + a) \cup \cdots \cup (H + na)| \leq (n + 1)|H| = (\frac{1}{2} + \frac{1}{2n}) \sum_{i=1}^{n} |A|.
\]

If in addition, the order of \( a + H \) in \( G/H \) exceeds \( n \), then we have in fact equality, \( |nA| = \frac{n+1}{2}|A| \).

Remark 1.1. If we impose the stronger assumption that no \( A_i \) is contained in a union of \( \ell \) cosets of any proper subgroup of \( G \), then we obtain

\[
|A_1 + \cdots + A_n| \geq \min \left\{ |G|, \left( \frac{\ell}{\ell+1} + \frac{1}{(\ell+1)n} \right) \sum_{i=1}^{n} |A_i| \right\}.
\]

Notation: In what follows we let \( \mathbb{Z}_q \) denote the ring of integers mod \( q \).

2. Proof of Theorem 1.1

Let \( G \) be an abelian group. For any nonempty subset \( S \) of \( G \) we define the stabilizer of \( S \) to be the subgroup of \( G \) given by

\[
\text{stab}(S) := \{ x \in G : x + S \subseteq S \}.
\]

The set \( S \) is a union of cosets of \( \text{stab}(S) \). The following lemma, found in Nathanson [10] as a consequence of Kneser’s Theorem [9], is the key ingredient for proving the theorem. Kneser’s Theorem is just the case \( n = 2 \) of the lemma.
Lemma 2.1. [10, Theorem 4.4]. Let $n \geq 2$. If $A_1, \ldots, A_n$ are finite, nonempty subsets of an abelian group and $H$ is the stabilizer of $A_1 + \cdots + A_n$, then

$$|A_1 + \cdots + A_n| \geq |A_1| + \cdots + |A_n| - (n-1)|H|.$$ 

Proof of Theorem 1.1. For $1 \leq i \leq n$, let $A_i$ be a finite nonempty subset of an abelian group $G$ not contained in a coset of any proper subgroup of $G$. Set $H = \text{stab}(A_1 + \cdots + A_n)$. If $H = G$ then plainly $A_1 + \cdots + A_n = G$. Thus we may assume that $H$ is a proper subgroup of $G$. Applying Lemma 2.1 with $A_i$ replaced by $A_i + H$, and noting that

$$A_1 + \cdots + A_n = A_1 + \cdots + A_n + H = (A_1 + H) + \cdots + (A_n + H),$$

gives

$$|A_1 + \cdots + A_n| = |(A_1 + H) + \cdots + (A_n + H)| \geq |A_1 + H| + \cdots + |A_n + H| - (n-1)|H|.$$ 

Now for any $i$, $A_i + H$ is a union of cosets of $H$, say $r_i$ in number, so that $|A_i + H| = r_i|H|$. Plainly $r_i \geq 2$; otherwise $A_i$ is contained in a coset of $H$, contrary to assumption. We also note that $|A_i| \leq |A_i + H|$ and so $|H| \geq \frac{1}{r_i}|A_i|$. Thus,

$$|A_1 + \cdots + A_n| \geq r_1|H| + \cdots + r_n|H| - (n-1)|H|$$

$$= (r_1 - 1 + \frac{1}{r_1})|H| + \cdots + (r_n - 1 + \frac{1}{r_n})|H|$$

$$\geq \left(1 - \frac{1}{r_1} + \frac{1}{nr_1}\right)|A_1| + \cdots + \left(1 - \frac{1}{r_n} + \frac{1}{nr_n}\right)|A_n|$$

$$\geq \left(\frac{1}{2} + \frac{1}{2n}\right)|A_1| + \cdots + \left(\frac{1}{2} + \frac{1}{2n}\right)|A_n|$$

as desired. \qed

3. Refinement of Olson’s estimate

We observed in Example 1.1 that if $A$ is a union of two cosets of a proper subgroup then the lower bound $|nA| \geq \frac{n+1}{2}|A|$ is best possible. If $A$ is not such a set, we get a modest improvement.

Proposition 3.1. Let $A$ be a finite subset of an abelian group $G$ not contained in a coset of any proper subgroup of $G$ and not equal to a union of two cosets of a proper subgroup of $G$. Then for any $n \geq 2$ we have

$$|nA| \geq \min \{ |G|, \frac{n+1}{2}|A| + \frac{n+1}{2} \},$$

unless $|A| = 3$ with $n$ arbitrary; $|A| = 4$ and $n = 2$; or $|A| = 6$, $n = 2$ and $A$ is a union of three cosets of a subgroup of order $2$. In the latter cases, we have

$$|nA| \geq \min \{ |G|, \frac{n+1}{2}|A| + \frac{n-1}{2} \}.$$ 

In particular, if $A$ is any subset not contained in a coset of a proper subgroup of $G$ and $|A| > 3$ is odd then the estimate in (3.1) applies, yielding a small refinement of Olson’s estimate (1.2).
Proof. Following the proof of Theorem 1.1 with \( A_i = A, r_i = r, 1 \leq i \leq n \), we see that if \( |A| < |A + H| = r|H| \), then \( |H| \geq \frac{1}{r}(|A| + 1) \), and so

\[
|nA| \geq n (r - 1 + \frac{1}{n}) |H| \geq n (r - 1 + \frac{1}{n}) \frac{1}{r}(|A| + 1) \geq \frac{n+1}{n} |A| + \frac{n+1}{2}.
\]

Henceforth we may assume that \( |A| = |A + H| \), which implies that \( A \) is a union of \( r \) cosets of \( H \). By assumption, \( r \geq 3 \). If \( |H| = 1 \) then Lemma 2.1 gives \( |nA| \geq n|A| - (n - 1) \), and so (3.1) holds for \( |A| \geq \frac{3n-1}{n-1} \). There remains the cases \( |A| = 3 \) with arbitrary \( n \), and \( |A| = 4, n = 2 \), both of which satisfy

\[
n|A| - (n - 1) \geq \frac{n+1}{n} |A| + \frac{n+1}{2}.
\]

If \( |H| \geq 2 \) then since \( r \geq 3 \), Lemma 2.1 gives

\[
|nA| \geq n|A| - (n - 1)|H| \geq n|A| - (n - 1) \frac{|A|}{r} = (\frac{2}{r}n + \frac{1}{r}) |A|,
\]

which is greater than or equal to the lower bound in (3.1) for \( |A| \geq 3 \left( \frac{n+1}{n-1} \right) \). Since \( |H| \geq 2 \), we have \( |A| \geq 2r \geq 6 \) and so the latter inequality holds for \( n \geq 3 \). It also holds for \( n = 2 \) when \( |A| \geq 9 \). There remains the possibility that \( n = 2 \) and \( |A| = 6, 7 \) or 8. If \( |A| = 6 \), then \( r = 3, |H| = 2 \) and we have

\[
|2A| \geq 2|A| - 2 = 10 > \frac{3}{2}|A| + \frac{1}{2}.
\]

If \( |A| = 7 \) then \( |H| = 7 \) and \( A \) is a coset of \( H \), contrary to assumption. If \( |A| = 8 \) then \( |H| = 2 \); otherwise \( |H| = 8 \) or 4 and \( A \) is a union of one or two cosets of \( H \) contrary to assumption. Thus, \( |2A| \geq 2|A| - 2 = 14 \) and so (3.1) holds.

\[\square\]

Example 3.1. The following examples show that the estimate in (3.2) is best possible for each of the exceptional cases.

i) \( |A| = 3 \): Let \( A := \{0, 1, 2\} \subseteq \mathbb{Z}_m \) with \( m > 2n + 1 \). Then

\[
|nA| = 2n + 1 = \frac{n+1}{n} |A| + \frac{n-1}{2}.
\]

ii) \( |A| = 4, n = 2 \): Let \( A := \{0, 1, 2, 3\} \subseteq \mathbb{Z}_m \) with \( m > 6 \). Then

\[
|2A| = 7 = \frac{3}{2}|A| + 1.
\]

iii) \( |A| = 6, n = 2 \): Let \( A := \{0, 1, 2, 3, 4, 5\} \subseteq \mathbb{Z}_{16} \). Then

\[
|2A| = 10 = \frac{3}{2}|A| + 1.
\]

4. A Generalization of Chowla’s Theorem

Chowla established the following generalization of the Cauchy-Davenport theorem to modular rings with an arbitrary modulus.

Theorem 4.1. [4]. Let \( q \) be a positive integer, and \( A, B \) be finite subsets of \( \mathbb{Z}_q \) such that \( 0 \in A \), and for all nonzero \( a \in A \) we have \( (a, q) = 1 \). Then

\[
|A + B| \geq \min\{q, |A| + |B| - 1\}.
\]

The condition that every nonzero element of \( A \) is relatively prime to \( q \) can be restated, \( A \cap H = \{0\} \) for every proper subgroup \( H \) of \( \mathbb{Z}_q \). We generalize Chowla’s Theorem to abelian groups as follows.

Theorem 4.2. Let \( G \) be an abelian group and \( A \) be a finite subset of \( G \) containing zero. Suppose that for every proper subgroup \( H \) of \( G \) we have \( A \cap H = \{0\} \). Then for any finite subset \( S \) of \( G \) we have

\[
|A + S| \geq \min\{|G|, |A| + |S| - 1\}.
\]
Proof. By Kneser’s Theorem, letting $H = \text{stab}(A + S)$ we have

$$|A + S| \geq |A + H| + |S + H| - |H|.$$ 

If $H = G$ then $A + S = G$, and so we may assume that $H$ is a proper subgroup of $G$. Then by assumption, $A \cap H = \{0\}$, and so $|A + H| \geq |A \cup H| = |A| + |H| - 1$, and

$$|A + S| \geq |A| + |H| - 1 + |S| - |H| = |A| + |S| - 1. \quad \Box$$

5. Application to Diagonal Congruences

Consider the diagonal congruence

$$(5.1) \sum_{i=1}^{n} a_i x_i^k \equiv c \pmod{q},$$

where the $a_i$ are integers with $(a_i, q) = 1$, $1 \leq i \leq n$, and $c$ is any integer. In [12, Theorem 2.6.1] the second author established that for $n \geq 4k$ there always exists a solution of (5.1). Our interest here is obtaining a solution of this congruence in a cube $B$ of points in $\mathbb{Z}^n$ with side length $B$,

$$(5.2) B := \{ x \in \mathbb{Z}^n : C_i + 1 \leq x_i \leq C_i + B, 1 \leq i \leq n \},$$

$C_i \in \mathbb{Z}, 1 \leq i \leq n$.

**Theorem 5.1.** For any positive integer $k$, there exists a constant $N(k)$ such that if $n > N(k)$ and $B$ is a cube of side length $B > \max\{q^{1/k}, k\}$, then there is a solution of the diagonal congruence (5.1) in $B$.

The theorem is best possible up to the determination of $N(k)$ and improvement in the constant 1 in front of $q^{1/k}$. Indeed, consider the congruence

$$x_1^k + \cdots + x_n^k \equiv \lceil q/2 \rceil \pmod{q},$$

and box $B$ with $1 \leq x_i \leq B, 1 \leq i \leq n$. Plainly with $n = N(k)$ we will need $B \gg k^{q^{1/k}}$ in order to solve this congruence. For prime moduli $p$, it was shown by the authors [5] that for $n \geq \frac{1}{2}(k^2 + k + 2)$, there is a solution of (5.1) mod $p$ with $1 \leq x_i \ll p^{1/k}$.

Results of this type date back to the work of Pitman and Ridout [13] and Birch [2]. Schmidt [14] generalized their work to establish that for any positive integer $k$ and $n > N_0(k, \varepsilon)$, the homogeneous congruence

$$(5.3) a_1 x_1^k + \cdots + a_n x_n^k \equiv 0 \pmod{q},$$

has a solution with

$$1 \leq x_i \ll_{k, \varepsilon} q^{\frac{1}{k} + \varepsilon}.$$

Theorem 5.1 not only removes the $\varepsilon$ from Schmidt’s result, but it is also the first result of this type that deals with non-homogeneous congruences as well. Baker [1] obtained a nontrivial solution of the homogeneous congruence (5.3) with

$$\max |x_i| \ll_{k, n, \varepsilon} q^{\frac{1}{k} + \frac{1}{2n-2} + \varepsilon}.$$ 

Although not reaching the optimal size $q^{1/k}$, his inequality is effective when the number of variables is small. Further results of this type are discussed in the authors’ works [5, 6].
Proof. The key ingredient is an upper bound on the number $N_q(B)$ of solutions of the congruence

$$\sum_{i=1}^{n} a_i x_i^k \equiv \sum_{i=1}^{n} a_i y_i^k \pmod{q},$$

with $x, y \in B$. In [5] the authors established that for $n \geq \frac{1}{2}(k^2 + k + 2)$, we have

$$N_q(B) \leq c_k \left( \frac{B^{2n}}{q} + B^{2n-k} \right),$$

for some constant $c_k$ depending only on $k$. Letting $S_B$ denote the mod $q$ values of the diagonal form $\sum_{i=1}^{n} a_i x_i^k$ as $x$ runs through $B$,

$$S_B := \left\{ \sum_{i=1}^{n} a_i x_i^k \pmod{q} : x \in B \right\},$$

we deduce from the Cauchy-Schwarz inequality the lower bound

$$|S_B| \geq \frac{B^{2n}}{N_q(B)} \geq \frac{1}{2c_k} \min\{B^k, q\}.$$ (5.5)

Lemma 5.1. [12, Lemma 4.6.1] For any cube $B$ as in (5.2), and integers $a_i$ with $(a_i, q) = 1$, $1 \leq i \leq n$, the value set $S_B$ is contained in a coset of a proper additive subgroup of $\mathbb{Z}_q$ if and only if there exists a prime $p | q$, such that $x^k \pmod{p}$ is constant on every edge $[C_i + 1, C_i + B]$ of the cube.

Proof. Suppose that $S_B$ is contained in a coset $p\mathbb{Z}_q + l$ for some $p | q$, $p \neq 1$, and $l \in \mathbb{Z}$. We may assume that $p$ is a prime by enlarging the subgroup if necessary. Thus, for all $x \in B$, we have

$$\sum_{i=1}^{n} a_i x_i^k \equiv l \pmod{p}.$$ (5.4)

In particular, for $1 \leq i \leq n$, $x_i^k \pmod{p}$ must be constant on the interval $[C_i + 1, C_i + B]$. The converse is trivial.

We return to the proof of Theorem 5.1. Suppose that $B > \max\{q^{1/k}, k\}$. Let $A_1, A_2, \ldots, A_r$ be value sets of the type $S_B$, with $n \geq \frac{1}{2}(k^2 + k + 2)$. By (5.5), since $B > q^{1/k}$, we have $|A_i| \geq \frac{q}{2c_k}$, $1 \leq i \leq r$. We claim that for any prime divisor $p$ of $q$, $x_i^k$ is not constant mod $p$ on any edge of the cube $B$. Indeed, if $p \leq B$ then each edge contains a full set of residues mod $p$ and so $x_i^k$ takes on at least two distinct values mod $p$, while if $p > B$, then for fixed $a$, the congruence $x^k \equiv a \pmod{p}$ has at most $k < B$ solutions, and so again $x_i^k$ takes on at least two distinct values mod $p$ on each edge. Thus by Lemma 5.1, none of the sets $A_i$ are contained in a coset of a proper subgroup of $\mathbb{Z}_q$. By Theorem 1.1 it follows that for $r \geq 4c_k - 1$, we have $A_1 + \cdots + A_r = \mathbb{Z}_q$. Set $r = [4c_k] - 1$. If we start with a form in at least $\frac{1}{2}(k^2 + k + 2)$ variables, we may partition the variables into $r$ disjoint sets, each with at least $\frac{1}{2}(k^2 + k + 2)$ variables, and form $r$ value sets $A_1, \ldots, A_r$ of the type $S_B$, with $A_1 + \cdots + A_r = \mathbb{Z}_q$, completing the proof.

Remark 5.1. As seen in the proof, the constant $N(k)$ in Theorem 5.1 may be taken to be $2c_k(k^2 + k + 2)$ where $c_k$ is the constant in (5.4).
Remark 5.2. The $k$ appearing in the lower bound $\max\{q^{1/k}, k\}$ of Theorem 5.1 is necessary to deal with trivial cases such as

$$\sum_{i=1}^{n} a_i x_i^{p-1} \equiv c \pmod{p},$$

with $p$ an odd prime, $k = p - 1$. Plainly this congruence is not solvable for most choices of $c$ with $1 \leq x_i \leq p - 1$ for all $i$. On the other hand, $p^{1/k} < 2$. In order to guarantee solvability for all $c$ one needs an interval containing 0, that is, we need $B > k$.

Alternatively, one can drop the $k$, and insert the hypothesis that “for any prime divisor $p$ of $q$, $x^k \pmod{p}$ is not constant on any edge of $B$.” Such a version is stated in [12, Theorem 4.6.1].

References


Department of Mathematics, Kansas State University, Manhattan, KS 66506
E-mail address: cochrane@math.ksu.edu

Department of Mathematics, University of Southern Indiana, Evansville, IN 47712
E-mail address: M.Ostergaard@usi.edu

Department of Mathematics, Kansas State University, Manhattan, KS 66506
E-mail address: cvs@math.ksu.edu