6 Subsequence Sums III: length $= exp(G)$

In this section, we will study another restricted subsequence sum problem. If G is a group, the *exponent* of G, denoted $exp(G)$, is the smallest integer m so that the order of every element in G divides m. If G is a finite abelian group, then there exist positive integers $m_1, m_2, \ldots, m_d$ so that m_i divides m_{i+1} for $1 \leq i \leq d$ and so that $G \cong \mathbb{Z}_{m_1} \times \mathbb{Z}_{m_2} \ldots \mathbb{Z}_{m_d}$. In this case, $exp(G) = m_d$. The *exponent length Davenport constant*, denoted $D^{exp}(G)$, is the smallest integer ℓ so that every sequence of elements from G of length $\geq \ell$ has a subsequence of length $exp(G)$ with sum equal to 0. The goal of this section is to prove a lovely theorem of Reiher - conjectured by Kemnitz - that $D^{exp}(\mathbb{Z}_n \times \mathbb{Z}_n) = 4n - 3$. We begin with an observation (due to Kemnitz) which includes the trivial lower bound on $D^{exp}(\mathbb{Z}_n \times \mathbb{Z}_n)$ together with the useful fact that the general problem reduces to the special case when n is prime.

Observation 6.1

(i) $D^{exp}(\mathbb{Z}_n \times \mathbb{Z}_n) \geq 4n - 3$

(ii) *If* $D^{exp}(\mathbb{Z}_n \times \mathbb{Z}_n) = 4n - 3$ *holds for* n *prime, then it holds for all* n.

Proof: For part (i), consider the sequence consisting of $n - 1$ copies of the four elements $(0, 0)$, $(0, 1)$, $(1, 0)$ and $(1, 1)$. This sequence has no length n subsequence with zero sum, so $D^{exp}(\mathbb{Z}_n \times \mathbb{Z}_n) \geq 4n - 3$.

For part (ii), we proceed by induction on n. If $n = 1$ or n is prime, there is nothing to prove. Otherwise we may choose $a, b > 1$ with $ab = n$. Let $g_1, g_2, \ldots, g_{4n-3}$ be a sequence of elements in $\mathbb{Z}_n \times \mathbb{Z}_n$ and let $H \leq \mathbb{Z}_n \times \mathbb{Z}_n$ be a subgroup isomorphic to $\mathbb{Z}_a \times \mathbb{Z}_a$. By repeatedly applying the theorem for $\mathbb{Z}_b \times \mathbb{Z}_b \cong (\mathbb{Z}_n \times \mathbb{Z}_n)/H$ we may choose pairwise disjoint subsets $J_1, J_2, \ldots, J_{4a-3}$ of I so that $|J_i| = b$ and $\sum_{j \in J_i} g_j \in H$ (every subset of I of size $\geq 4b - 3$ contains such a set, so if we have chosen $J_1, J_2, \ldots, J_k$, we can always choose a suitable J_{k+1}, unless 4ab-3 - kb $= |I \setminus \cup_{i=1}^{k} J_i| < 4b - 3$ in which case $k > 4a - 4$). Now, applying the result for $\mathbb{Z}_a \times \mathbb{Z}_a$ to the sequence $\sum_{j \in J_1} g_j, \sum_{j \in J_2} g_j, \ldots \sum_{j \in J_{4a-3}} g_j$ gives us a sequence of length $n = ab$ with sum 0 as required. □

Now let us fix a prime p and a sequence $g_1, g_2, \ldots, g_{4p-3}$ of elements in $\mathbb{Z}_p$ where $g_i = (a_i, b_i)$. We let $I = \{1, 2, \ldots, 4p - 3\}$ denote the index set, and for any $J \subseteq I$ and any nonnegative integer k we let $(k|J)$ denote the number of subsets $J' \subseteq J$ with $|J'| = k$ so that

$\sum_{j\in J'} g_j = 0$. Through the remainder of this section, we shall use the symbol $\equiv$ to denote numbers which are equivalent modulo p. Our proof of Reiher's theorem will proceed with three lemmas which establish a number of equations (modulo p) concerning numbers of the form $(k|J)$. The only tool we require for this is the Chevalley-Warning theorem.

Lemma 6.2 *Let* $J \subseteq I$

(i) $-1 + (p|J) - (2p|J) + (3p|J) \equiv 0$ *if* $|J| > 3p - 3$

(ii) $-1 + (p|I) - (2p|I) + (3p|I) \equiv 0$

(iii) *If* $|J| = 3p - 2$ *or* $|J| = 3p - 1$, *then* $(p|J) \equiv 0$ *implies* $(2p|J) \equiv -1$

(iv) *If* $|J| = 3p$ *and* $(3p|J) = 1$, *then* $(p|J) > 0$

(v) $(p - 1|I) - (2p - 1|I) + (3p - 1|I) \equiv 0$

Proof: Consider the following family of polynomials over $\mathbb{Z}_p$.

$$\sum_{j\in J} x_j^{p-1} \qquad \sum_{j\in J} a_j x_j^{p-1} \qquad \sum_{j\in J} b_j x_j^{p-1}$$

It follows from the Chevalley-Warning theorem that whenever $|J| > 3p - 3$, the number of common solutions to the above polynomials is congruent to 0 modulo p. This gives us

$$\begin{aligned} 0 &\equiv 1 + (p-1)^p(p|J) + (p-1)^{2p}(2p|J) + (p-1)^{3p}(3p|J) \\ &\equiv 1 - (p|J) + (2p|J) - (3p|J). \end{aligned}$$

which completes the proof of (i). Parts (ii) and (iii) are immediate consequences of (i). Part (iv) follows from (iii) applied to a subset of J of size $3p - 1$ and the observation that $(p|J) = (2p|J)$ if $|J| = 3p$ and $(3p|J) = 1$. Part (v) follows from a similar argument to the first, applied to the following family of polynomials.

$$1 + \sum_{i\in I} x_i^{p-1} \qquad \sum_{i\in I} a_i x_i^{p-1} \qquad \sum_{i\in I} b_i x_i^{p-1}$$

This completes the proof. $\square$

Lemma 6.3

$$3 - 2(p - 1|I) - 2(p|I) + (2p - 1|I) + (2p|I) \equiv 0$$

Proof: Let $J \subseteq I$ satisfy $|J| = 3p-3$ and consider the following family of polynomials

$$y^{p-1} + \sum_{j\in J} x_j^{p-1} \qquad \sum_{j\in J} a_j x_j^{p-1} \qquad \sum_{j\in J} b_j x_j^{p-1}$$

Again by the Chevalley-Warning theorem, the number of common solutions to this family is 0 modulo p. The number of solutions with $y = 0$ has size $1+(p-1)^p(p|J)+(p-1)^{2p}(2p|J) \equiv 1-(p|J)+(2p|J)$ and the number with $y \neq 0$ has size $(p-1)^p(p-1|J)+(p-1)^{2p}(2p-1|J) \equiv -(p-1|J)+(2p-1|J)$. Thus, we have

$$0 \equiv 1 - (p-1|J) - (p|J) + (2p-1|J) + (2p|J).$$

Summing this identity over all subsets J of I of size $3p-3$ gives us

$$\begin{aligned} 0 &\equiv \sum_{J\subseteq I:|J|=3p-3} \Big(1 - (p-1|J) - (p|J) + (2p-1|J) + (2p|J)\Big) \\ &\equiv \tbinom{4p-3}{3p-3} - \tbinom{3p-2}{2p-2}(p-1|I) - \tbinom{3p-3}{2p-3}(p|I) + \tbinom{2p-2}{p-2}(2p-1|I) + \tbinom{2p-3}{p-3}(2p|I) \\ &\equiv 3 - 2(p-1|I) - 2(p|I) + (2p-1|I) + (2p|I). \end{aligned}$$

which completes the proof. □

Lemma 6.4 *If* $(p|I) = 0$, *then* $(p-1|I) \equiv (3p-1|I)$.

Proof: Let t denote the number of partitions of I into $\{A, B, C\}$ which satisfy $|A| = p-1$, $|B| = p-2$, $|C| = 2p$ and $\sum_{i\in A} g_i = 0$, $\sum_{i\in B} g_i = \sum_{i\in I} g_i$, and $\sum_{i\in C} g_i = 0$. We will first count t (modulo p) by running through all possible choices for A and applying part (iii) of Lemma 6.2. This gives us

$$t = \sum_A (2p|I \setminus A) \equiv \sum_A -1 \equiv -(p-1|I)$$

On the other hand, summing over all choices for B and applying part (iii) of Lemma 6.2 gives us

$$t = \sum_B (2p|I \setminus B) \equiv \sum_B -1 \equiv -(3p-1|I)$$

Combining these equations gives us the desired result. □

Theorem 6.5 (Reiher) $D^{exp}(\mathbb{Z}_n \times \mathbb{Z}_n) = 4n - 3$

Proof: By Observation 6.1 it suffices to prove that our sequence $g_1, g_2, \ldots, g_{4p-3}$ in $\mathbb{Z}_p$ contains a subsequence of length p with sum 0. Assume (for a contradiction) that this does not hold. Then adding the equations from (ii) and (v) of Lemma 6.2, the equation from Lemma 6.3 and the equation $0 \equiv (p-1|I) - (3p-1|I)$ from Lemma 6.4 we get

$$2 - (p|I) + (3p|I) \equiv 0$$

Part (iv) of Lemma 6.2 now gives us a contradiction. $\square$

Although the proof is a bit beyond our scope, we will mention the following interesting result concerning the exponent length Davenport constant.

Theorem 6.6 (Alon, Dubiner) *For every $d \geq 1$ there exists a constant c so that $D^{exp}(\mathbb{Z}_n^d) \leq cn$.*