Appendix 15A: Summing sets (mod p)

We have seen in Lemma 15.3.1 that if we add two finite sets of integers A and B then $|A+B| \geq |A|+|B|-1$. Moreover much of the rest of chapter 15 has focussed on the expansion properties of adding the same set to itself several times. Here we focus on summing sets (mod n).

Theorem 15.8 (Cauchy-Davenport)**.** *Let p be a prime, and suppose that A and B are non-empty subsets of $\mathbb{Z}/p\mathbb{Z}$. Then*

$$|A+B| \geq \min(|A|+|B|-1, p).$$

Proof. The theorem is unaffected by translating A and B, that is replacing A by $A+x$ and B by $B+y$. Sometimes it will be convenient to perform such translations.

Another useful transformation is to replace the pair of sets A, B by their *union* $U := A \cup B$ and their *intersection* $I := A \cap B$. Note that $|U|+|I| = |A|+|B|$ and $U + I \subseteq A + B$, so that $|A+B| \geq |U+I|$. Therefore if we can prove the theorem for the pair I, U then it follows for the original pair A, B.

Suppose without loss of generality that $|A| \geq |B|$. By translating A and B appropriately we may assume that $0 \in A, B$. We will prove our result by induction on $|B|$. If $|B| = 1$ then the result is trivial. If $|B| > 1$ and there exist $a \in A, b \in B$ for which $B-b \not\subseteq A-a$ then the result follows by applying the induction hypothesis to the pair $I = (A-a) \cap (B-b)$, $U = (A-a) \cup (B-b)$, since in this case $|I| < |B|$. Hence we may assume that $B - b \subseteq A - a$, and therefore that $B - b + a \subseteq A$ for all $a \in A$ and $b \in B$. Taking the union over all $a \in A, b \in B$ we deduce that $B - B + A \subseteq A$.

From this we see that $2B - 2B + A = B - B + (B - B + A) \subseteq B - B + A \subseteq A$, and then, by induction, that $kB - kB + A \subseteq A$ for all $k \geq 1$. Since $0 \in B$ we deduce that if H is the subgroup of $\mathbb{Z}/p\mathbb{Z}$ generated additively by B then $A + H = A$. But there are only two subgroups of $\mathbb{Z}/p\mathbb{Z}$: either $H = \{0\}$, or $H = \mathbb{Z}/p\mathbb{Z}$. In the first

case we have $B = \{0\}$ since $B \subseteq H$. The theorem is trivial in this case. In the second case we have $A = \mathbb{Z}/p\mathbb{Z}$, in which case the result is also trivial. □

Exercise 15.7.4. Suppose that A is a subset of $\mathbb{Z}/p\mathbb{Z}$ with at least two elements. Show that if $n \geq \frac{p-1}{|A|-1}$ then $nA = \mathbb{Z}/p\mathbb{Z}$.

Exercise 15.7.5. Use Theorem 15.8 to show that if A and B are finite sets of integers then $|A + B| \geq |A| + |B| - 1$.

We can try to modify this argument to work in $\mathbb{Z}/n\mathbb{Z}$ or other additive groups G. Some care is needed here for, if H is a subgroup of G then $H + H = H$, so there is no expansion. Moreover if $A = A_0 + H$ and $B = B_0 + H$ are unions of cosets of H (with A_0 and B_0 minimal), then $A + B = (A_0 + B_0) + H$, and therefore

$$|A + B| - |A| - |B| = |H|(|A_0 + B_0| - |A_0| - |B_0|);$$

in the particular case that $|A_0| = |B_0| = 1$, we obtain $|A + B| = |A| + |B| - |H|$.

To state the best possible result in general finite additive groups G, we need to define the *stabilizer* of A, a subset of G, to be

$$\mathrm{Stab}(A) := \{g \in G : g + A = A\}.$$

One can see that $H := \mathrm{Stab}(A)$ is a subgroup of G, with the property that $A + H = A$, and so A is a union of cosets of $\mathrm{Stab}(A)$.

Theorem 15.9 (Kneser's Theorem)**.** *If A and B are finite subsets of an additive group G and $H = \mathrm{Stab}(A + B)$ then*

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

Exercise 15.7.6. Suppose that A is a subset of $\mathbb{Z}/N\mathbb{Z}$ and that A additively generates all of $\mathbb{Z}/N\mathbb{Z}$; that is, there exists r for which $rA = \mathbb{Z}/N\mathbb{Z}$. Prove that $NA = \mathbb{Z}/N\mathbb{Z}$.

Exercise 15.7.7. We give another proof of Theorem 14.5.

(a) Show that any sequence of $2m$ (not necessarily distinct) residues mod p either has $m + 1$ identical residues, or can be partitioned into m sets of two distinct residues.

(b) Prove that if $A_1, \dots A_{p-1}$ are subsets of $\mathbb{Z}/p\mathbb{Z}$ which each contain two distinct residues then $A_1 + \cdots + A_{p-1} = \mathbb{Z}/p\mathbb{Z}$.

(c) Deduce Theorem 14.5.