Homework #10
Combinatorial Number Theory (2025)

This homework is to be submitted on Moodle before next Tuesday at 23:59

E1. Let $N, d, r \in \mathbb{N}$ and consider the set

$$B = \{(n_1, \dots, n_d) \in [0, N/2)^d : n_1^2 + \dots + n_d^2 = r\},$$

viewed as a subset of $\mathbb{Z}_N^d$. Show that this set has no proper (i.e. nontrivial) arithmetic progressions of length 3, and can have cardinal as large as $(N/2)^d/(d^2N^2)$ for suitable choice of r.

> ***Solution:***
>
> First, we show that the set $B_r = \{(n_1, \dots, n_d) \in [0, N/2)^d : n_1^2 + \dots + n_d^2 = r\} \subset \mathbb{Z}_N^d$ contains no nontrivial arithmetic progression of length 3. Suppose $x, y, z \in B$ form a 3-term arithmetic progression in $\mathbb{Z}_N^d$. This means$x_i + z_i \equiv 2y_i \pmod N \qquad 1 \le i \le d$. Since each coordinate satisfies $0 \le x_i, z_i < N/2$, we have $x_i + z_i = 2y_i$ as integers.
>
> By the parallelogram law,
>
> $$2\|x\|_2^2 + 2\|z\|_2^2 = \|x+z\|_2^2 + \|x-z\|_2^2 = 4\|y\|_2^2 + \|x-z\|_2^2$$
>
> Using, $\|x\|_2 = \|y\|_2 = \|z\|_2 = r$ we obtain $\|x - z\| = 0$, i.e. $x = z$. Therefore the progression is trivial, and B contains no nontrivial 3-term arithmetic progression.
>
> We now show that $|B_r|$ can be as large as $(N/2)^d/(d^2N^2)$ for suitable r.
>
> The total number of points in $[0, N/2)^d$ is $(N/2)^d$. The possible values of $r = n_1^2 + \dots + n_d^2$ for $(n_1, \dots, n_d) \in [0, N/2)^d$ range from 0 to at most $d \cdot (N/2)^2$. By the pigeonhole principle, there exists some r such that
>
> $$|B_r| \ge \frac{(N/2)^d}{d \cdot (N/2)^2 + 1} > \frac{(N/2)^d}{dN^2}.$$