Exercise Set #10
Combinatorial Number Theory (2025)

E1. For $f, g, h : \mathbb{Z}_N \to \mathbb{C}$, define

$$\Gamma(f,g,h) = \frac{1}{N^2} \sum_{n,m \in \mathbb{Z}_N} f(n)g(m)h(n+m).$$

(i) Prove

$$\Gamma(f,g,h) = \sum_{\xi \in \mathbb{Z}_N} \hat{f}(\xi)\hat{g}(\xi)\hat{h}(-\xi).$$

(ii) Suppose $\|f\|_\infty, \|g\|_\infty, \|h\|_\infty \leq 1$. Show that

$$|\Gamma(f,g,h)\| \leq \min\{\|\hat{f}\|_\infty, \|\hat{g}\|_\infty, \|\hat{h}\|_\infty\}.$$

E2. By a *randomly generated* subset of $\mathbb{Z}_N$ we mean a set A where each $n \in \mathbb{Z}_N$ has a 50% probability of being an element in A. Imagine flipping a coin N times and including the number n in A if the nth coin flip is "heads" and excluding the number n from A if the nth coin flip is "tails". The next problem says that, almost surely, a randomly generated set is pseudorandom.

Let $\epsilon > 0$. Prove that the probability that a randomly generated subset of $\mathbb{Z}_N$ is ϵ-pseudorandom converges to 1 as $N \to \infty$.
Hint: Use Hoeffding's inequality: For independent random variables $X_1, \ldots, X_k$ with $|X_i| \leq 1$,

$$\mathbb{P}\left[|S_k - \mathbb{E}\left[S_k\right]| \geq t\right] \leq 2\exp\left(-\frac{t^2}{2k}\right),$$

where $S_k = \sum_{i=1}^k X_i$.

E3. Prove *Dirichlet's approximation theorem*: for any $\alpha \in \mathbb{R}$ and any $Q \in \mathbb{N}$, there exist $p, q \in \mathbb{Z}$ with $1 \leq q \leq Q$ such that

$$\left|\alpha - \frac{p}{q}\right| \leq \frac{1}{qQ}.$$