# Budapest, Additive combinatorics summer 2024
# based on lectures by CE

1. Prove that the set $S = \left\{\sum_{i=0}^{r} a_i 5^i : a_i \in \{0,1,2\} \text{ and } |\{i : a_i = 1\}| = \lfloor \frac{r+1}{3} \rfloor\right\}$ is 3-progression-free. Work out the constant $C$ in $|S| \sim C\frac{3^r}{\sqrt{r}}$, where $r \to \infty$.

2. Is the set $S = \left\{\sum_{i=0}^{r} a_i 4^i : a_i \in \{0,1,2\} \text{ and } |\{i : a_i = 1\}| = \lfloor \frac{r+1}{3} \rfloor\right\}$ 3-progression-free?

3. Is the set $S \subset \mathbb{Z}_4^n$ proper-3-progression-free, where a proper arithmetic progression of length three consists of three distinct points? $S = \left\{\{a_1, \ldots, a_n\} : a_i \in \{0,1,2\} \text{ and } |\{i : a_i = 1\}| = \lfloor \frac{n}{3} \rfloor\right\}$.
(Give a proof or a counterexample).

4. Prove that the Salem-Spencer construction gives 3-progression-free sets.

$$S = \left\{ \sum_{i=0}^{r} a_i (2m-1)^i : a_i \in \{0,1,\ldots,(m-1)\} \text{ and for each } j \in \{0,1,\ldots,m-1\} \text{ there exists } r_j \text{ with:} \right.$$
$$\left. |\{i : a_i = j\}| = r_j \text{ and with } \sum_{j=0}^{m-1} r_i = r+1. \right\}$$

When applying it to progression-free sets of integers in the interval $[1, N]$, how should one choose $m$ and $r$ (roughly!) ?

5. (Done in lecture): Prove that in $\mathbb{Z}_5^2$ one can find 10 points which can be reduced", which has the consequence that in $\mathbb{Z}_5^{20n}$ one can choose all elements that have each of the 10 points exactly $n$ times in coordinates $i$ and $i+1$, ($i$ is odd, $i = 1, 3, \ldots, 20n-1$). Deduce that $r_3(\mathbb{Z}_5^{20n}) \gg (\sqrt{10} + o(1))^{20n}$, (write this estimate with binomial coefficients.)

6. A cap is a set which does not contain three distinct points on any line. Let $D = \{0,1,3,4,5\} \subset \mathbb{F}_{11}$. Let

$$S_D = \left\{ (a_1, \ldots, a_n) : \text{ for } |D|-1 \text{ values } d_j \in D \text{ one has that } |\{i : a_i = d_j\}| = \lfloor \frac{n}{5} \rfloor \right\}.$$

Prove that the set $S_D \subset \mathbb{F}_{11}^n$ is a cap.
(For simplicity one can assume that $5 \mid n$.)

(Modulo 11 there are other good digit sets, where digit 9 replaces another digit).
(More time consuming: modulo 17 find a maximal set of residue classes that define cap in $\mathbb{F}_{17}$,

Now let $D = \{0,1,2,3,4,5\}$. Prove that $T_D \subset \mathbb{F}_{11}^n$ is not a cap.

$$T_D = \left\{ (a_1, \ldots, a_n) : \text{ for } |D|-1 \text{ values } d_j \in D \text{ one has that } |\{i : a_i = d_j\}| = \lfloor \frac{n}{6} \rfloor \right\}$$

is not a cap.

7. On sums of two squares:
1) Read the Richards argument. Ian Richards, Advances in mathematics, 1982, On the gaps between numbers which are sums of two squares,
2) A key idea of the improvement is that not all primes $p \equiv 3 \bmod 4$ are needed, but that large primes $p = 11 \bmod 16$, and later some more, can be omitted from the product $P$. What are the size restrictions of these primes $p = 11 \bmod 16$ ?

8. Verify that all odd integers can be written as a sum of squares and a cube (which may be negative), by verifying the following identity:

$$2x + 1 = (x^3 - 3x^2 + x)^3 + (x^2 - x - 1)^2 - (x^2 - 2x)^3.$$

If you can find (not only verify!) such identities very fast, please contact me. Obviously, if one roughly knows how they might look like one can run over many potential cases. (CE).

9. Let $d$ be odd and composite, and let $q$ be the least prime factor of $d$. Then ther3 does not exist any $x \in \mathbb{Z}$ such that the value $p_d(x) = (c_q q)^q + x^d$ is a sum of two squares, where $c_q = 2$, when $q \equiv 3 \pmod 4$, and $c_q = 6$, when $q \equiv 1 \pmod 4$.
(The proof is elementary, uses congruence arguments, and factoring of the poylnomial, and needs some case study. The slides contained the special case $q = 3 \bmod 4$, then reducing to $z = 1 \bmod 4$. The case $q = 1 \bmod 4$ is similar.)

10. Let $(s_n)$ be the sequence of integers which are sums of two integer squares, in natural order. $(1, 2, 4, 5, 8, 9, 10, 12, \ldots)$. Prove that $s_n - s_{n-1} = O((s_n)^{1/4})$. (You can make the constant explicit.) Show that this implies that there exist many integers, which are sums of two squares, which have at least 75 percent of their binary bits as 1. Now assume that every interval of length $O((s_n)^{1/4+\delta})$ contains $O((s_n)^{1/4+\delta+o(1)})$ integers which are sums of two squares, (where $\delta > 0$ is small. (The counting function of integers $t \leq X$ which are sums of two squares is about $C\frac{X}{\sqrt{\log X}}$, so that this is a uniform distribution result.) Show that this implies that many integers which are sums of two squares have at least (almost) 7/8-th of their bits being 1. Recall that one can explicitly construct integers, which are sums of two squares, with almost all bits being 1.