Week 1

Pigeonhole Principle

1. (2016A5) Suppose that G is a finite group generated by the two elements g and h, where the order of g is odd. Show that every element of G can be written in the form $g^{m_1}h^{n_1}g^{m_2}h^{n_2}\cdots g^{m_r}h^{n_r}$ with $1 \leq r \leq |G|$ and $m_1, n_1, \dots, m_r, n_r \in \{-1, 1\}$.

2. Let $S = \{105, 106, \dots, 210\}$. Find the minimum value of n such that any n element subset T of S contains at least two elements that are not coprime.

Mock Putnam problems

A1 Prove that for each $n \geq 2$, there is a set S of n positive integers such that $(a-b)^2 \mid ab$ for every distinct $a, b \in S$.

A3 Let $p(x) = x^n + a_1x^{n-1} + \cdots a_n$ and $q(x) = x^m + b_1x^{m-1} + \cdots + b_m$ be polynomials with real coefficients. Suppose $q(x)|p(x)$ as polynomials. Suppose for some $k = 1, \dots, m$, we have $|b_k| > 2025^k\binom{m}{k}$. Prove that there exists $j = 1, \dots, n$ such that $|a_j| > 2024$.

A5 Suppose $p > n > m^2$, with p prime, and let $0 < a_1 < a_2 < \cdots < a_m < p$ be integers. Prove that there is an integer x, with $0 < x < p$ for which the m numbers

$$(xa_i \bmod p) \bmod n, \text{ for } 1 < i < m$$

are pairwise distinct.

A6 (2024 B6) For any real number a and $x \in (0, 1]$, define

$$F_a(x) = \sum_{n=1}^{\infty} n^a e^{2n} x^{n^2}.$$

Find a real number c such that

$$\lim_{x \to 1^-} F_a(x)e^{-1/(1-x)} = \begin{cases} 0 & \text{if } a < c, \\ \infty & \text{if } a > c. \end{cases}$$

1. (2016A5) Suppose that G is a finite group generated by the two elements g and h, where the order of g is odd. Show that every element of G can be written in the form $g^{m_1}h^{n_1}g^{m_2}h^{n_2}\cdots g^{m_r}h^{n_r}$ with $1 \le r \le |G|$ and $m_1, n_1, \ldots, m_r, n_r \in \{-1, 1\}$.

   Suppose we have an expression of the form $g^{m_1}h^{n_1}g^{m_2}h^{n_2}\cdots g^{m_r}h^{n_r}$ where $r > |G|$. Then using the standard method of $s_1 = g^{m_1}h^{n_1}, s_2 = g^{m_1}h^{n_1}g^{m_2}h^{n_2}, \ldots, s_r = g^{m_1}h^{n_1}g^{m_2}h^{n_2}\cdots g^{m_r}h^{n_r}$, we see that two of them are the same. Suppose $1 \le i < j \le r$ with $s_i = s_j$. Then

   $$g^{m_1}h^{n_1}g^{m_2}h^{n_2}\cdots g^{m_r}h^{n_r} = g^{m_1}h^{n_1}g^{m_2}h^{n_2}\cdots g^{m_i}h^{n_i}g^{m_{j+1}}h^{n_{j+1}}\cdots g^{m_r}h^{n_r}$$

   can be expressed in the desired form with less than r elements. In other words, it suffices to prove the given statement without any condition on r.

   Consider the set S of elements of the form $g^{m_1}h^{n_1}g^{m_2}h^{n_2}\cdots g^{m_r}h^{n_r}$ for any $r \ge 1$. Then S is closed under multiplication, and so is a subgroup of G because G is finite. From $gh \in S$, we get $h^{-1}g^{-1} \in S$, and then from $g^{-1}h \in S$, we get $g^{-2} \in S$. Since g has odd order, g is contained in the subgroup generated by g^{-2}. So $g \in S$ and then $h \in S$. So $S = G$.

2. Let $S = \{105, 106, \ldots, 210\}$. Find the minimum value of n such that any n element subset T of S contains at least two elements that are not coprime.

   Let P be the set of all primes in S. The "best" set should contain $P \cup \{2^7, 5^3, 11^2, 13^2\}$ along with some composite numbers whose prime divisors belong to $\{3, 7, 17, 19, \ldots, 103\}$. Since $17 \cdot 19$ is too large, we can add at most 2 more numbers, say $3^2 \cdot 19 = 171$ and $7 \cdot 17 = 119$. Hence the answer should be $\#P + 7$.

   For any $d \in \mathbb{N}$, let $A_d = \{n \in S\colon d \mid n\}$. Any composite number in S is in $A_2 \cup A_3 \cup A_5 \cup A_7 \cup A_{11} \cup A_{13}$. By inclusion-exclusion,

   $$\begin{aligned} |A_2 \cup A_3 \cup A_5 \cup A_7| &= |A_2| + |A_3| + |A_5| + |A_7| - |A_6| - |A_{10}| - |A_{14}| \\ &- |A_{15}| - |A_{21}| - |A_{35}| + |A_{30}| + |A_{42}| + |A_{70}| + |A_{105}| - |A_{210}| \\ &= 53 + 36 + 22 + 16 - 18 - 11 - 8 - 8 - 6 - 4 + 4 + 3 + 2 + 2 - 1 \\ &= 82. \end{aligned}$$

   The remaining composites belong to

   $$(A_{11} \cup A_{13}) \backslash (A_2 \cup A_3 \cup A_5 \cup A_7) = \{11^2, 11 \cdot 13, 11 \cdot 17, 11 \cdot 19\} \cup \{13^2\}.$$

   Hence $|P| = 106 - 82 - 5 = 19$. Now given 26 elements, there are at least 7 composites. At least 2 of which belong to the same set among

   $$A_2,\ A_3,\ A_5,\ A_7,\ \{11^2, 11 \cdot 13, 11 \cdot 17, 11 \cdot 19\},\ \{13^2\}.$$

Mock Putnam problems

A1 Prove that for each $n \ge 2$, there is a set S of n positive integers such that $(a-b)^2 \mid ab$ for every distinct $a, b \in S$.

Start with $a_1, \ldots, a_n$ with $(a_i - a_j)^2 \mid a_i a_j$. If $a_i \mid N$ for all i, then the same is true for $a_1 + N, \ldots, a_n + N$. Let $b = \mathrm{lcm}_i a_i$ and let $N = b(\mathrm{lcm}_i(a_i - b)^2 - 1)$. Then $a_1 + N, \ldots, a_n + N, b + N$ does the job.

A3 Let $p(x) = x^n + a_1x^{n-1} + \cdots a_n$ and $q(x) = x^m + b_1x^{m-1} + \cdots + b_m$ be polynomials with real coefficients. Suppose $q(x)|p(x)$ as polynomials. Suppose for some $k = 1, \ldots, m$, we have $|b_k| > 2025^k\binom{m}{k}$. Prove that there exists $j = 1, \ldots, n$ such that $|a_j| > 2024$.

The condition on $|b_k|$ implies that $q(x)$ has a root r with $|r| > 2025$. Then r is also a root of $p(x)$. Suppose $|a_j| \leq 2024$ for all j. Then

$$0 = |p(r)| \geq |r|^n - 2024(|r|^{n-1} + \cdots + 1) > 0.$$

A5 Suppose $p > n > m^2$, with p prime, and let $0 < a_1 < a_2 < \cdots < a_m < p$ be integers. Prove that there is an integer x, with $0 < x < p$ for which the m numbers

$$(xa_i \bmod p) \bmod n, \text{ for } 1 < i < m$$

are pairwise distinct.

For any $0 < a < b < p$, we let x be randomly chosen from $1, 2, \ldots, p-1$ and let

$$X(a,b) = \begin{cases} 1 & \text{if } (xa \bmod p) \bmod n = (xb \bmod p) \bmod n, \\ 0 & \text{otherwise.} \end{cases}$$

Then $X(a,b) = 1$ if and only if $x(a-b)\%p$ or $p - x(a-b)\%p$ is divisible by n. Hence

$$E(X(a,b)) = \frac{1}{p-1}\left(2\left\lfloor\frac{p}{n}\right\rfloor\right) \leq \frac{2(p-1)}{(p-1)n} = \frac{2}{n}.$$

We now let

$$Y = \sum_{1 \leq i < j \leq m} X(a_i, a_j)$$

so by the linearity of expectation, we have

$$E(Y) < \frac{m(m-1)}{2}\frac{2}{n} < 1.$$

Hence, $\Pr(Y = 0) > 0$.

A6 (2024 B6) For any real number a and $x \in (0,1]$, define

$$F_a(x) = \sum_{n=1}^{\infty} n^a e^{2n} x^{n^2}.$$

Find a real number c such that

$$\lim_{x \to 1^-} F_a(x)e^{-1/(1-x)} = \begin{cases} 0 & \text{if } a < c, \\ \infty & \text{if } a > c. \end{cases}$$

Let $y = 1/(1-x)$, so $x = 1 - \frac{1}{y}$ and we are letting $y \to \infty$. For a fixed y, the term x^{n^2} is approaching 0 as $n \to \infty$. So we should estimate $(1 - \frac{1}{y})^{n^2}$ in a way that suggests that it is small when n is large and y is fixed. We have

$$(1 - \frac{1}{y})^{n^2} = e^{n^2 \ln(1-y^{-1})} \approx e^{-n^2y^{-1}}.$$

More precisely, for any $\delta > 0$, we may take y large enough so that

$$e^{-n^2y^{-1}-\delta n^2y^{-2}} < (1-\frac{1}{y})^{n^2} < e^{-n^2y^{-1}}.$$

Then we have

$$F_a(x) \approx \sum_{n=1}^{\infty} n^a e^{-n^2y^{-1}+2n-y} = \sum_{n=1}^{\infty} n^a e^{-y^{-1}(n-y)^2}.$$

This is similar to the moments of a Gaussian distribution, which suggests that the main contribution comes from $|n-y| < y^{1/2+\epsilon}$. More precisely, we first note that for $n \approx y + y^{1/2}$, we have $e^{-y^{-1}(n-y)^2} \approx e^{-1}$ from which we see that $F_a(x) \gg y^a$. Hence we may assume $a < 0$. Now let $\epsilon > 0$ be arbitrary and small. Then we have

$$\sum_{|n-y|>y^{1/2+\epsilon}} n^a e^{-y^{-1}(n-y)^2} \ll \int_{|z|>y^{1/2+\epsilon}} e^{-\frac{z^2}{y}} dz =: I(y,\epsilon).$$

There are many ways to show $I(y,\epsilon)$ is small. For example,

$$I(y,\epsilon)^2 \leq \int_{y^{1/2+\epsilon}}^{\infty} \int_0^{2\pi} re^{-\frac{r^2}{y}} dr d\theta \ll e^{-y^{\epsilon}}.$$

For $|n-y| < y^{1/2+\epsilon}$, we have

$$n^a e^{-y^{-1}(n-y)^2} \ll y^a$$

which gives the upper bound

$$\sum_{|n-y|<y^{1/2+\epsilon}} n^a e^{-y^{-1}(n-y)^2} \ll y^{a+1/2+\epsilon}.$$

For $|n-y| \in (y^{1/2}, 2y^{1/2})$, we have

$$n^a e^{-y^{-1}(n-y)^2} \gg y^a$$

which gives the lower bound

$$\sum_{|n-y|<y^{1/2+\epsilon}} n^a e^{-y^{-1}(n-y)^2} \ll y^{a+1/2}.$$

In conclusion, we have

$$y^{a+1/2} + e^{-y^{\epsilon}} \ll F_a(x) \ll y^{a+1/2+\epsilon} + e^{-y^{\epsilon}}.$$

Hence we have $F_a(x) \to 0$ if $a < -1/2$ and $F_a(x) \to \infty$ if $a > -1/2$, as $y \to \infty$.