Week 7: Mock Putnam 7

1: For any positive integer m, what is the remainder when $\prod_{1\le a\le m, \gcd(a,m)=1} a$ is divided by m?

2: Find all integers m, n such that $0 \le n \le 139^{2024}$ and

$$420^{69}(m^2-1) - 2m + 6 = 4\binom{139^{2024}}{n}.$$

3: Let $x^n + a_1 x^{n-1} + \cdots + a_n$ be a polynomial in $\mathbb{C}[x]$ with roots $r_1, \ldots, r_n \in \mathbb{C}$. Prove that

$$\sum_{i=1}^{n} |r_i|^2 \le n - 1 + \sum_{i=1}^{n} |a_i|^2.$$

4: Prove that the set of prime divisors of $2^{2^n} + 69$ for $n \in \mathbb{N}$ is infinite.

5: Let (a_n) be a sequence of positive real numbers such that $\sum_{n=1}^{\infty} a_n$ diverges. Let $s_n = \sum_{k=1}^{n} a_k$ be the partial sums. For which values of $p > 0$ does $\sum_{n=1}^{\infty} \frac{a_n}{s_n^p}$ converge?

6: Let $A_1 = \emptyset$ and $B_1 = \{0\}$ and for $n \ge 1$,

$$A_{n+1} = \{1 + b : b \in B_n\}, \qquad B_{n+1} = (A_n \backslash B_n) \cup (B_n \backslash A_n).$$

Find all positive integers n such that $B_n = \{0\}$.

Week 7: Sketch of proofs

1: Answer.

- If $m = 1$, then the answer is 0.
- If $m = 2, 4$ or $m = p^k, 2p^k$ for some odd prime p and $k > 0$, then the answer is $m - 1$.
- Otherwise the answer is 1.

Working mod m, it suffices to compute $L_m = \prod_{a \in (\mathbb{Z}/m\mathbb{Z})^\times} a$. For convenience, we will assume $m > 2$, as the case $m = 1$ and $m = 2$ are trivial.

First pair the elements of $(\mathbb{Z}/m\mathbb{Z})^\times$ with their inverses. Since $(a^{-1})^{-1} = a$ for any $a \in (\mathbb{Z}/m\mathbb{Z})^\times$, we can partition $(\mathbb{Z}/m\mathbb{Z})^\times$ into the set $H = \{a \in (\mathbb{Z}/m\mathbb{Z})^\times : a^2 = 1\}$ and several sets of size 2 of form $\{a, a^{-1}\}$ for some $a \in (\mathbb{Z}/m\mathbb{Z})^\times$ such that $a^{-1} \neq a \iff a^2 \neq 1$. Clearly, the product of all elements in the sets of size 2 is 1, so the formula for L_m simplifies to

$$L_m = \prod_{a \in H} a.$$

Notice that for each $a \in H$, we also have $-a \in H$. Also, since $m > 2$, there exists no element $a \in (\mathbb{Z}/m\mathbb{Z})^\times$ such that $a = -a$. (In $\mathbb{Z}/m\mathbb{Z}$, this would yield $a \in \{0, m/2\}$ if m is even and $a = 0$ if m is odd.) As a result, H can be partitioned into pairs $(a_1, -a_1), (a_2, -a_2), \ldots, (a_k, -a_k)$, where $2k = |H|$. Then we would get

$$L_m = \prod_{j=1}^{k} a_j \cdot (-a_j) = \prod_{j=1}^{k} (-1) = (-1)^k = (-1)^{|H|/2}.$$

It remains to determine when $|H|/2$ is odd and when it is even.

We first prove that $|H|/2$ is odd if and only if $H = \{\pm 1\}$. Indeed, suppose that $a \in H$ and $a \neq \pm 1$. Then $\{\pm 1, \pm a\}$ is a subgroup of H of order 4, and so $4 \mid |H|$, which means $|H|/2$ is even. Conversely, if $H = \{\pm 1\}$, then $|H|/2 = 1$. Thus, $L_m = -1$ if the only $a \in (\mathbb{Z}/m\mathbb{Z})^\times$ such that $a^2 = 1$ are $a = \pm 1$, and $L_m = 1$ otherwise. Finally, we determine when the former holds and when the latter holds.

First suppose that $m = cd$ for some $c, d > 2$ with $\gcd(c, d) = 1$. Then by Chinese remainder theorem, there exists an integer a such that $a \equiv -1 \pmod{c}$ and $a \equiv 1 \pmod{d}$. Note that $a \not\equiv \pm 1 \pmod{m}$ since $c, d > 2$. But the above gives $a^2 \equiv 1 \pmod{m}$. This yields $L_m = 1$. This case holds when m has at least two odd prime factors, or if m is divisible by 4 and also has an odd prime factor. It remains to check the case where m is either a prime power or 2 times an odd prime power.

If $m = 2^k$ for $k = 1, 2$, then it is easy to check that $a^2 \equiv 1 \pmod{m}$ implies $a \equiv \pm 1 \pmod{m}$, and thus $L_{2^k} = -1$. If $k \geq 3$, then $(2^{k-1} + 1)^2 \equiv 1 \pmod{2^k}$ with $1 < 2^{k-1} + 1 < 2^k - 1$, which means $L_{2^k} = 1$. If $m = p^k$ for some odd prime p, then $a^2 \equiv 1 \pmod{p^k}$ implies $p^k \mid (a - 1)(a + 1)$.

Then p divides one of $a-1$ or $a+1$. But p cannot divide both of them, since then p would divide $(a+1)-(a-1)=2$. By checking p-adic valuation, p^k must divide either $a-1$ or $a+1$. This yields $a \equiv \pm 1 \pmod{p^k}$. Thus this gives us $L_{p^k} = -1$.

Finally, suppose that $m = 2p^k$ for some odd prime p. By Chinese remainder theorem, $(\mathbb{Z}/m\mathbb{Z})^\times \cong (\mathbb{Z}/2\mathbb{Z})^\times \times (\mathbb{Z}/p^k\mathbb{Z})^\times \cong (\mathbb{Z}/p^k\mathbb{Z})^\times$, which has size 2 by the previous argument. Thus $L_{2p^k} = -1$.

Extra. In fact, the above method allows us to compute $L_G := \prod_{a \in G} a$ for any finite abelian group G. If the 2-torsion subgroup $G[2] := \{a \in G : a^2 = 1\}$ has size 2, then $G[2] = \{1, c\}$ for some $c \in G$, and we would get $L_G = c$. Otherwise, $L_G = 1$.

2: Answer. $m = 1$ and $n \in \{0, 139^{2024}\}$.

By Kummer's theorem, if $0 < n < 139^{2024}$, then

$$\nu_{139}\binom{139^{2024}}{n} = \frac{s_{139}(n) + s_{139}(139^{2024} - n) - 1}{138} > 0.$$

Thus 139 divides the right hand side. On the other hand, since $69 = \frac{139-1}{2}$ and $420 = 3 \cdot 139 + 3$,

$$420^{69} \equiv 3^{69} \equiv \left(\frac{3}{139}\right) = -\left(\frac{139}{3}\right) = -\left(\frac{1}{3}\right) = -1 \pmod{139}.$$

Thus we get

$$-(m^2-1) - 2m + 6 \equiv 0 \pmod{139} \iff (m+1)^2 \equiv 8 \pmod{139}.$$

Then $8 = 2^3$ is a quadratic residue mod 139. However, since $139 \equiv 3 \pmod 8$,

$$\left(\frac{2^3}{139}\right) = \left(\frac{2}{139}\right) = -1.$$

Thus 8 is not a quadratic residue mod 139. Contradiction!

The remaining case is $n \in \{0, 139^{2024}\}$. The right hand side equals 4, so $420^{69}(m^2-1) = 2m - 6 + 4 = 2(m-1)$, which implies either $m = 1$ or $420^{69}(m+1) = 2$. The second equation has no solution since $420^{69} > 2$.

3: Consider the companion matrix of $P(X) = X^n + a_1 X^{n-1} + \cdots + a_n$:

$$M = \begin{pmatrix} 0 & 0 & 0 & \cdots & a_n \\ 1 & 0 & 0 & \cdots & a_{n-1} \\ 0 & 1 & 0 & \cdots & a_{n-2} \\ \vdots & \vdots & \vdots & \ddots & \vdots \\ 0 & 0 & 0 & \cdots & a_1 \end{pmatrix}.$$

We now consider the square of the unitary norm of M, $\mathrm{Tr}(M^*M)$ in two ways.

First, by directly looking at the entries of M, we get

$$\mathrm{Tr}(M^*M) = \sum_{i,j} |M_{ij}|^2 = n - 1 + \sum_{i=1}^{n} |a_i|^2.$$

Second, by Schur decomposition, there exists a unitary matrix U and an upper triangular matrix T such that $M = UTU^*$. In particular, $M^*M = (UT^*U^*)(UTU^*) = U(T^*T)U^*$. Since U is unitary, this means M^*M is (unitarily) similar to T^*T, so

$$\mathrm{Tr}(M^*M) = \mathrm{Tr}(T^*T) = \sum_{i,j} |T_{ij}|^2 \geq \sum_{i=1}^{n} |T_{ii}|^2.$$

The Schur decomposition also implies that M is (unitarily) similar to T, so M and T has the same characteristic polynomial, $x^n + a_1 x^{n-1} + \ldots + a_n$. Since T is upper triangular, the diagonals of T are the roots of this polynomial in some order. In other words, there exists a permutation σ of $\{1, 2, \ldots, n\}$ such that $T_{ii} = r_{\sigma(i)}$ for each $i \leq n$. As a result,

$$n - 1 + \sum_{i=1}^{n} |a_i|^2 = \mathrm{Tr}(M^*M) \geq \sum_{i=1}^{n} |T_{ii}|^2 = \sum_{i=1}^{n} |r_{\sigma(i)}|^2 = \sum_{i=1}^{n} |r_i|^2.$$

This is the desired inequality; we are done.

4: Suppose for the sake of contradiction that such set is finite, and let $p_1, p_2, \ldots, p_N$ be its elements. First, for any $m, n \in \mathbb{N}$, notice that

$$2^{2^{n+m}} \equiv (-69)^{2^m} \equiv 69^{2^m} \pmod{2^{2^n} + 69}.$$

Thus $\gcd(2^{2^n} + 69, 2^{2^{n+m}} + 69) \leq K$ for any $m, n \in \mathbb{N}$ with $m \leq N$, where $K = 69^{2^N} + 69$.

Choose a positive integer n_0 such that $2^{2^{n_0}} + 69 > K^N$. By our initial assumption, for any $n \in \mathbb{N}$, we can write $2^{2^n} + 69 = p_1^{r_1} p_2^{r_2} \ldots p_N^{r_N}$ for some $r_1, r_2, \ldots, r_n \geq 0$. If $n \geq n_0$, then $2^{2^n} + 69 \geq K^N$, so $p_i^{r_i} > K$ for some i. That is, there exists $i \leq N$ and $r \geq 0$ such that $p_i^r > K$ and $p_i^r \mid 2^{2^n} + 69$. By pigeonhole principle, there exists $m \leq N$, $i \leq N$, and $r_1, r_2 \geq 0$ such that $p_i^{r_1}, p_i^{r_2} > K$, $p_i^{r_1} \mid 2^{2^{n_0}} + 69$, and $p_i^{r_2} \mid 2^{2^{n_0+m}} + 69$. Then

$$\gcd(2^{2^{n_0}} + 69, 2^{2^{n_0+m}} + 69) \geq p_i^{\min\{r_1, r_2\}} > K.$$

But from the first paragraph, the left hand side is less than or equal to K since $m \leq N$. Contradiction!

5: Answer. $p > 1$ no matter what (a_n) is.

First suppose that $p > 1$. Since $s_n < s_{n+1}$ for each $n \geq 1$ and $s_n \to \infty$ as $n \to \infty$,

$$\sum_{n=1}^{\infty} \frac{a_n}{s_n^p} = \frac{a_1}{s_1^p} + \sum_{n=2}^{\infty} \int_{s_{n-1}}^{s_n} \frac{dx}{s_n^p} \leq \frac{a_1}{a_1^p} + \sum_{n=2}^{\infty} \int_{s_{n-1}}^{s_n} \frac{dx}{x^p} = \frac{1}{a_1^{p-1}} + \int_{a_1}^{\infty} \frac{dx}{x^p} = \frac{p}{p-1} a_1^{-(p-1)} < \infty.$$

Conversely, we now show that $p = 1$ does not work (and thus any $p \leq 1$ does not work either). By MVT or looking at Maclaurin series expansion, one can see that there exists a positive real number $R < 1$ such that $\exp(-2x) \leq 1 - x$, or $-2x \leq \ln(1-x)$ for any $x \in [0, R]$. Now suppose for the sake of contradiction that $\displaystyle\sum_{n=1}^{\infty} \frac{a_n}{s_n}$ converge. That means there exists $N \geq 2$ such that $a_n/s_n \leq R$ for all $n \geq N$. In this case, we get

$$-\frac{a_n}{2s_n} \leq \ln\left(1 - \frac{a_n}{s_n}\right) = \ln \frac{s_{n-1}}{s_n} = \ln s_{n-1} - \ln s_n.$$

Summing from $n = N$ to infinity yields

$$-\frac{1}{2}\sum_{n=N}^{\infty} \frac{a_n}{s_n} \leq s_{N-1} - \lim_{n\to\infty} \ln s_n = -\infty$$

since $s_n \to \infty$ as $n \to \infty$. This contradicts our initial assumption. We are done.

6: Answer. Powers of 2.

By induction on n, one can see that A_n and B_n are finite sets for each $n \geq 1$.

For each finite set S, denote the polynomial

$$P_S(X) = \sum_{k\in S} X^k \in \mathbb{F}_2[X].$$

Then the recursive definition of A_{n+1} and B_{n+1} yields the recursive formula on the pair (P_{B_n}, P_{A_n}), given by $(P_{B_1}, P_{A_1}) = (1, 0)$ and $(P_{B_{n+1}}, P_{A_{n+1}}) = (P_{B_n} + P_{A_n}, XP_{B_n})$ for each n. If we let $T = \begin{pmatrix} 1 & 1 \\ X & 0 \end{pmatrix} \in M_2(\mathbb{F}_2[X])$, we get

$$\begin{bmatrix} P_{B_{n+1}} \\ P_{A_{n+1}} \end{bmatrix} = T \begin{bmatrix} P_{B_n} \\ P_{A_n} \end{bmatrix}.$$

By induction on n, we get

$$\begin{bmatrix} P_{B_n} \\ P_{A_n} \end{bmatrix} = T^n \begin{bmatrix} 0 \\ 1 \end{bmatrix},$$

and thus P_{B_n} is the $(1,2)$-entry $(T^n)_{12}$ of T^n. The goal is to find all $n \geq 1$ such that $(T^n)_{12} = 1$.

The characteristic polynomial of T, in variable y, is $y^2 + y + X$, which is irreducible in $\mathbb{F}_2(X)[y]$. Thus, for any $n \geq 1$, there exists a **unique** pair $(P, Q) \in \mathbb{F}_2[X]^2$ such that $T^n = PT + Q$. By induction on n, we get in fact $T^n = P_nT + Q_n$ for $n \geq 1$.

First, observe that for any $n \geq 1$,

$$P_{2n}T + Q_{2n} = (P_nT + Q_n)^2 = P_n^2T^2 + Q_n^2 = P_n^2T + (XP_n^2 + Q_n^2).$$

Thus we have the formula $P_{2n} = P_n^2$ for each n. Thus, if we write $n = 2^km$ where k is a non-negative integer and m is an odd positive integer, we have $P_n = P_m^{2^k}$. Clearly, this means $P_n = 1$ if and only if $P_m = 1$. It remains to show that if n is odd, then $P_n = 1$ if and only if $n = 1$. Direct computation yields $P_1 = 1$, so it remains to show that $P_n = 1$ implies $n = 1$.

Recall the equality $T^n = P_n T + Q_n$. Since $\det(T) = X$, we have $\det(P_n T + Q_n) = X^n$ for each n. If $P_n = 1$, then

$$X^n = \det(T + Q_n) = \det \begin{bmatrix} Q_n + 1 & 1 \\ X & Q_n \end{bmatrix} = (Q_n + 1)Q_n - X,$$

and thus $X^n + X = (Q_n + 1)Q_n = Q_n^2 + Q_n$. If $n > 1$, then the right hand side is non-zero, so Q_n is non-constant. Computing degree yields $n = 2\deg(Q_n)$, which is a contradiction, since n is odd. We are done.