Week 9: Mock Putnam 9

1: Prove that there does not exist rational numbers a, b, c such that $\cos(\pi/7) = a + \sqrt{b} + \sqrt[3]{c}$.

2: Let A be an $n \times n$ symmetric matrix with integer coordinates. Let $\mathbf{b} \in \mathbb{Z}^n$ be a vector whose entries are the diagonal entries of A. That is, the i-th entry of $\mathbf{b}$ is the (i,i)-entry of A. Prove that there exists $\mathbf{v} \in \mathbb{Z}^n$ such that every entry of $A\mathbf{v} - \mathbf{b}$ is even.

3: Find all positive integer solutions to $m^{n+1} - (m+1)^n = 69$, if any.

4: For a positive integer n and any point x in the unit square $[0,1] \times [0,1]$, let $Y_n(x)$ denote the random variable that is 1 if an odd number of $B(X_1, r_1), \ldots, B(X_n, r_n)$ contains x, and 0 if otherwise; where $B(X_i, r_i)$ is the open ball centered at X_i of radius r_i; where each X_i is independent and uniformly chosen in the unit square $[0,1]^2$ and each r_i is independent and uniformly chosen in $(0, \sqrt{3/(n\pi)})$. Find

$$\lim_{n\to\infty} E\left[\int_{[0,1]^2} Y_n(x)\, dx\right].$$

5: Let $f(x) : (1, \infty) \to \mathbb{R}$ be a differentiable function such that for all $x > 1$,

$$f'(x) = \frac{x^2 - f(x)^2}{x^2(1 + f(x)^{2024})}.$$

Prove that $\lim_{x\to\infty} f(x) = \infty$.

6: Let p be a prime and let $n \geq 1$. Let $A \subseteq \mathbb{Z}/p\mathbb{Z}$ be a subset with more than $p^{\frac{1}{2}+\frac{1}{2n}}$ elements. Prove that for any nonzero $\alpha \in \mathbb{Z}/p\mathbb{Z}$, there exist $a_1, \ldots, a_n, b_1, \ldots, b_n \in A$ such that $\alpha = a_1 b_1 + \cdots + a_n b_n$.

Week 9: Sketch of proofs

1: Let $\beta = -2\cos(\pi/7) = \zeta_7^4 + \zeta_7^{-4}$. We first show that the minimal polynomial of β is $f_\beta(X) = X^3 + X^2 - 2X - 1$. Note that it is irreducible, since it is monic of degree 3 with no integer roots. Now notice that

$$\beta^2 - 2 = \zeta_7 + \zeta_7^{-1}, \quad \beta^4 - 4\beta^2 + 2 = (\beta^2 - 2)^2 - 2 = \zeta_7^2 + \zeta_7^{-2}.$$

Thus we get

$$-1 = (\beta^4 - 4\beta^2 + 2) + (\beta^2 - 2) + \beta = \beta^4 - 3\beta^2 + \beta \iff \beta^4 - 3\beta^2 + \beta + 1 = 0.$$

Now notice that $X^4 - 3X^2 + X + 1 = (X - 1)(X^3 + X^2 - 2X - 1)$, and clearly $\beta \neq 1$. This shows that the minimal polynomial of β is f_β.

Now we claim that $\sqrt{b} \in \mathbb{Q}(\sqrt{b} + \sqrt[3]{c})$. Indeed, let $\alpha = \sqrt{b} + \sqrt[3]{c}$. Then we have

$$c = (\alpha - \sqrt{b})^3 = \alpha^3 - 3\alpha^2\sqrt{b} + 3\alpha b - b\sqrt{b} = (\alpha^2 + 3b)\alpha - (3\alpha^2 + b)\sqrt{b}.$$

If $3\alpha^2 + b \neq 0$, then this yields

$$\sqrt{b} = \frac{\alpha^3 + 3\alpha b - c}{3\alpha^2 + b} \in \mathbb{Q}(\alpha).$$

Otherwise we have $b = -3\alpha^2$ and so

$$c = -8\alpha^3 \iff \sqrt[3]{c} = -2\alpha = -2\sqrt{b} - 2\sqrt[3]{c} \iff 3\sqrt[3]{c} = -2\sqrt{b}.$$

Taking cubes yield $-8b\sqrt{b} = 27c \in \mathbb{Q}$, so we have $\sqrt{b} \in \mathbb{Q}$. Either way, the claim is proved.

Next, we show that in fact, $\sqrt{b} \in \mathbb{Q}$. Indeed, since $\sqrt{b} + \sqrt[3]{c} = \cos(\pi/7) - a = -\beta/2 - a$, the previous claim implies $\sqrt{b} \in \mathbb{Q}(\beta)$. Thus there exists a polynomial $f \in \mathbb{Q}[X]$ with $\deg(f) \leq \deg(f_\beta) - 1 = 2$ such that $f(\beta) = \sqrt{b}$. Clearly we are done if f is constant, so suppose for the sake of contradiction that f is non-constant. Then $f(\beta)^2 - b = 0$, and so $f_\beta(X) \mid f(X)^2 - b$. By computing degree, we necessarily have $\deg(f) = 2$. Write $f(X) = t(X^2 + uX + v)$ for some $t \in \mathbb{Q} \setminus \{0\}$ and $u, v \in \mathbb{Q}$. Then we have

$$(X^2 + uX + v)^2 = X^4 + 2uX^3 + (u^2 + 2v)X^2 + 2uvX + v^2 \equiv t^{-2}b \pmod{X^3 + X^2 - 2X - 1}.$$

Using the fact that $X^3 + X^2 - 2X - 1 \mid X^4 - 3X^2 + X + 1$, the above becomes

$$(3X^2 - X - 1) + 2u(-X^2 + 2X + 1) + (u^2 + 2v)X^2 + 2uvX + v^2 \equiv t^{-2}b \pmod{X^3 + X^2 - 2X - 1}.$$

The polynomial on the left hand side has degree at most 2, so we get equality:

$$(3X^2 - X - 1) + 2u(-X^2 + 2X + 1) + (u^2 + 2v)X^2 + 2uvX + v^2 = t^{-2}b.$$

Matching X^2-coefficient yield

$$3 - 2u + u^2 + 2v = 0 \iff u^2 - 2u - 1 + 2(v + 2) = 0,$$

Matching X-coefficient yield

$$-1 + 4u + 2uv = 0 \iff 2u(v + 2) = 1.$$

Thus we get

$$u^2 - 2u - 1 + 1/u = 0 \iff u^3 - 2u^2 - u + 1 = 0.$$

Impossible, since $X^3 - 2X^2 - X + 1$ is irreducible.

Since $\sqrt{b} \in \mathbb{Q}$, we get $\cos(\pi/7) - \sqrt[3]{c} \in \mathbb{Q}$. Recalling that $\beta = -2\cos(\pi/7)$, we get $\beta + 2\sqrt[3]{c} \in \mathbb{Q}$. Now let $q = \beta + 2\sqrt[3]{c}$. Since β is irrational, so is $\sqrt[3]{c}$. Thus the minimal polynomial of $-2\sqrt[3]{c}$ is $X^3 + 8c$. On the other hand, the minimal polynomial of $\beta - q$ is $f_\beta(X + q)$, so we get

$$f_\beta(X + q) = X^3 + 8c \implies f_\beta(X) = (X - q)^3 + 8c.$$

Matching X-coefficient yield $3q^2 = -2$, which is a contradiction.

2: We translate the problem over $\mathbb{F}_2$. Let A be an $n \times n$ symmetric matrix over $\mathbb{F}_2$. Define $\mathbf{b} \in \mathbb{F}_2^n$ by $b_i = A_{ii}$ for each $i \le n$. Our goal is to show that there exists $\mathbf{v} \in \mathbb{F}_2^n$ such that $A\mathbf{v} = \mathbf{b}$.

First, we show that for any $\mathbf{x} \in \mathbb{F}_2^n$, $A\mathbf{x} = 0$ implies $\mathbf{b}^T\mathbf{x} = 0$. We show more: $\mathbf{x}^T A\mathbf{x} = \mathbf{b}^T\mathbf{x}$. Indeed, expanding yields

$$\mathbf{x}^T A\mathbf{x} = \sum_{i=1}^{n}\sum_{j=1}^{n} x_i A_{ij} x_j = \sum_{i=1}^{n} A_{ii}x_i^2 + 2\sum_{1\le i<j\le n} A_{ij}x_i x_j = \sum_{i=1}^{n} A_{ii}x_i^2.$$

Since $b_i = A_{ii}$ for each $i \le n$ and $c^2 = c$ for each $c \in \mathbb{F}_2$, the right hand side is equal to $\mathbf{b}^T\mathbf{x}$.

Now suppose for the sake of contradicion that $A\mathbf{v} \neq \mathbf{b}$ for all $\mathbf{v} \in \mathbb{F}_2^n$. Let $\{\mathbf{a}_1, \mathbf{a}_2, \ldots, \mathbf{a}_k\}$ be a basis for the image of A. Then $\{\mathbf{a}_1, \mathbf{a}_2, \ldots, \mathbf{a}_k, \mathbf{b}\}$ is linearly independent, and so it extends to a basis for $\mathbb{F}_2^n$. Thus, there exists an invertible matrix whose i-th row is $\mathbf{a}_i$ for each $i \le k$ and whose $(k+1)$-th row is $\mathbf{b}$. We can pick $\mathbf{x} \in \mathbb{F}_2^n$ such that $\mathbf{a}_i^T\mathbf{x} = 0$ for each $i \le k$ and $\mathbf{b}^T\mathbf{x} = 1$. But since $\{\mathbf{a}_i : i \le k\}$ spans the image of A, we get $A\mathbf{x} = 0$ and $\mathbf{b}^T\mathbf{x} = 1$. Contradiction!

3: **Answer.** None.

Working mod m gives $-1 \equiv 69 \pmod{m}$, or $m \mid 70$. Working mod 3 yields $m^{n+1} \equiv (m+1)^n \pmod{3}$. Since m and $m+1$ cannot be both divisible by 3, this means m and $m+1$ are not divisible by 3, and so $m \equiv 1 \pmod{3}$. So far, this gives us $m \in \{1, 7, 10, 70\}$.

Working mod $m+1$ gives $(-1)^{n+1} \equiv 69 \pmod{m+1}$, so $m+1$ divides either 70 or 68. However, the three numbers 8, 11, and 71 does not divide both of 70 and 68. It remains to consider the case $m = 1$, which gives $1 - 2^n = 69$. But $69 > 1 > 1 - 2^n$; contradiction.

4: **Answer.** $\dfrac{1 - e^{-2}}{2}$.

For convenience, denote $c_n = \sqrt{3/(n\pi)}$. For each $X, x \in [0,1]^2$ and $r > 0$, let $\delta(X, x, r)$ be 1 if $|X - x| < r$ and 0 otherwise. From the definition, we have

$$Y_n(x) = \frac{1}{2}\left(1 - \prod_{i=1}^{n}(-1)^{\delta(X_i, x, r_i)}\right).$$

As a result, we have

$$\int_{[0,1]^2} Y_n(x)\, dx = \frac{1}{2} - \frac{1}{2}\int_{[0,1]^2} \prod_{i=1}^{n} (-1)^{\delta(X_i,x,r_i)}\, dx.$$

By linearity of expectation,

$$E\left[\int_{[0,1]^2} Y_n(x)\, dx\right] = \frac{1}{2} - \frac{1}{2}\int_{[0,1]^2} E\left[\prod_{i=1}^{n} (-1)^{\delta(X_i,x,r_i)}\right] dx.$$

Since the variables X_i and r_i are identical and independently distributed, we get

$$E\left[\prod_{i=1}^{n} (-1)^{\delta(X_i,x,r_i)}\right] = E\left[(-1)^{\delta(X,x,r)}\right]^n,$$

where X is a random uniformly chosen point in $[0,1]^2$ and r is a randomly chosen positive integer less than c_n. For $x \in [c_n, 1-c_n]^2$, we have

$$\Pr(\delta(X,x,r)=1) = c_n^{-1}\int_0^{c_n} \mathrm{Vol}\left(B_r(x)\cap[0,1]^2\right) dr = \frac{1}{n}.$$

So we have

$$E\left[(-1)^{\delta(X,x,r)}\right]^n = (1-\frac{1}{n}-\frac{1}{n})^n \to e^{-2}.$$

For $x \notin [c_n, 1-c_n]^2$, we have

$$\int_{x\in[0,1]^2\setminus[c_n,1-c_n]^2} E\left[(-1)^{\delta(X,x,r)}\right]^n dx \ll 1-(1-2c_n)^2 \to 0.$$

Therefore, the answer is $\frac{1}{2}(1-e^{-2})$.

5: We first notice that for any $x>1$, the given formula yields

$$-1 \le -\frac{1}{x^2} \le -\frac{f(x)^2}{x^2(1+f(x)^{2024})} \le f'(x) \le \frac{x^2}{x^2(1+f(x)^{2024})} \le 1.$$

That is, we have $|f'(x)| \le 1$ for all $x>1$. We also have $f'(x) \ge -x^{-2}$ for all $x>1$.

First consider the case where $|f(x_0)| < x_0$ for some $x_0 > 1$. We claim that $|f(x)| < x$ for all $x > x_0$. If not, then there exists $x_1 > x_0$ such that $|f(x_1)| \ge x_1$, and thus

$$|f(x_1)-f(x_0)| \ge |f(x_1)| - |f(x_0)| > x_1 - x_0 \implies \left|\frac{f(x_1)-f(x_0)}{x_1-x_0}\right| > 1.$$

By mean value theorem, there exists $c \in (x_0,x_1)$ such that $f'(c) = \dfrac{f(x_1)-f(x_0)}{x_1-x_0}$. The above inequality means $|f'(c)| > 1$ for some $c \in (x_0,x_1)$. Contradiction, since $|f'(x)| \le 1$ for all $x > 1$.

Since $|f(x)| < x$ for all $x > x_0$, we get $f'(x) > 0$ for all $x > x_0$. In particular, f is strictly increasing on (x_0, ∞). Thus, $\lim_{x\to\infty} f(x)$ exists and is either ∞ or a fixed real number, say L. If the latter holds, then we must have $f'(x) \to 0$ as $x \to \infty$. On the other hand,

$$\lim_{x\to\infty} f'(x) = \lim_{x\to\infty} \frac{x^2 - f(x)^2}{x^2(1 + f(x)^{2024})} = \lim_{x\to\infty} \frac{1 - (f(x)/x)^2}{1 + f(x)^{2024}} = \frac{1}{1 + L^{2024}} > 0.$$

Contradiction. Thus we get $f(x) \to \infty$ as $x \to \infty$.

Now consider the case where $|f(x)| \geq x$ for all $x > 1$. By continuity, we have either $f(x) \geq x$ for all $x > 1$ or $f(x) \leq -x$ for all $x > 1$. The former case immediately yields $\lim_{x\to\infty} f(x) = \infty$. In the latter case, we have $f(x) + x \leq 0$ for all $x > 1$. On the other hand, for all $x > 2$,

$$f'(x) + 1 \geq -\frac{1}{x^2} + 1 > \frac{3}{4} > 0.$$

So the function $g(x) = f(x) + x$ is bounded above but g' is bounded below by a positive real number. Contradiction!

6: We rewrite $\mathbb{Z}/p\mathbb{Z}$ as $\mathbb{F}_p$. For each $\alpha \in \mathbb{F}_p$, denote $e_p(\alpha) = e^{2\pi i\alpha/p}$. Notice the formula

$$\frac{1}{p} \sum_{c\in\mathbb{F}_p} e_p(c\alpha) = \begin{cases} 1, & \alpha = 0, \\ 0, & \alpha \neq 0. \end{cases}$$

Thus, the quantity

$$N_{A,\alpha} := \frac{1}{p} \sum_{\mathbf{a},\mathbf{b}\in A^n} \sum_{c\in\mathbb{F}_p} e_p(c(\mathbf{a}\cdot\mathbf{b} - \alpha))$$

counts the number of pairs $(\mathbf{a}, \mathbf{b})$ of vectors in A^n such that $\mathbf{a}\cdot\mathbf{b} = \alpha$. We can write

$$N_{A,\alpha} = \frac{|A|^{2n}}{p} + R, \qquad \text{where} \qquad R = \frac{1}{p} \sum_{\mathbf{a},\mathbf{b}\in A^n} \sum_{c\in\mathbb{F}_p^\times} e_p(c(\mathbf{a}\cdot\mathbf{b} - \alpha)).$$

We now apply Cauchy-Schwarz over $\mathbf{a}$ to get

$$\begin{aligned}
R^2 &\leq \frac{|A|^n}{p^2} \sum_{\mathbf{a}\in A^n} \left| \sum_{\mathbf{b}\in A^n} \sum_{c\in\mathbb{F}_p^\times} e_p(c(\mathbf{a}\cdot\mathbf{b} - \alpha)) \right|^2 \\
&= \frac{|A|^n}{p^2} \sum_{\mathbf{a}\in\mathbb{F}_p^n} \sum_{\mathbf{b}_1,\mathbf{b}_2\in A^n} \sum_{c_1,c_2\in\mathbb{F}_p^\times} e_p(\mathbf{a}\cdot(c_1\mathbf{b}_1 - c_2\mathbf{b}_2))\, e_p(\alpha(c_2 - c_1)) \\
&= \frac{|A|^n}{p^2} \sum_{\mathbf{b}_1,\mathbf{b}_2\in A^n} \sum_{c_1,c_2\in\mathbb{F}_p^\times} e_p(\alpha(c_2 - c_1)) \sum_{\mathbf{a}\in\mathbb{F}_p^n} e_p(\mathbf{a}\cdot(c_1\mathbf{b}_1 - c_2\mathbf{b}_2)) \\
&= |A|^n p^{n-2} \sum_{\mathbf{b}_1,\mathbf{b}_2\in A^n} \sum_{c_1,c_2\in\mathbb{F}_p^\times} e_p(\alpha(c_2 - c_1))\mathbf{1}_{c_1\mathbf{b}_1 = c_2\mathbf{b}_2}.
\end{aligned}$$

We write $c = c_1$ and $s = c_2/c_1$ so that

$$R^2 \;\; \leq \;\; |A|^n p^{n-2} \sum_{\mathbf{b}_1,\mathbf{b}_2 \in A^n} \sum_{c,s \in \mathbb{F}_p^\times} e_p(\alpha c(s-1)) \mathbf{1}_{\mathbf{b}_1 = s\mathbf{b}_2}.$$

Note that for a fixed s, the sum over c is almost a complete sum:

$$\sum_{c \in \mathbb{F}_p^\times} e_p(\alpha c(s-1)) = \begin{cases} -1 & \text{if } s \neq 1, \\ p-1 & \text{if } s = 1. \end{cases}$$

Hence

$$R^2 \;\; \leq \;\; |A|^n p^{n-2} \sum_{\mathbf{b}_2 \in A^n} (p-1) + (-1) \cdot |A^n \cap ((\mathbb{F}_p^\times \backslash \{1\}) \cdot \mathbf{b}_2)| \;\; < \;\; |A|^{2n} p^{n-1},$$

and so $R < |A|^n p^{n/2-1/2}$. The given bound on $|A|$ gives $|A|^n \geq p^{n/2+1/2}$, so

$$\frac{|A|^{2n}}{p} \geq |A|^n p^{n/2-1/2} > R$$

as desired.