Week 4

Polynomials

1. Let p be a prime and let $h(x) \in \mathbb{Z}[x]$ such that h induces a bijection on the residue classes mod p^2. Show that h also induces a bijection on the residue classes mod p^n for all $n \geq 2$.

2. Let $p(x)$ be a nonconstant real polynomial. For any positive integer n, let $q_n(x) = (x+1)^n p(x) + x^n p(x+1)$. Does there exists a choice for $p(x)$ so that there are infinitely many n such that all the roots of $q_n(x)$ are real?

3. Let $f(x)$ be a monic real polynomial of degree n. Show that f can be written as the average of two monic real polynomials g, h of degree n having all real roots.

4. Let $n \geq 1$ and let $\zeta = e^{2\pi i/n}$. Does there exist a polynomial $P(x)$ of degree at most $n-2$ with coefficients in $\mathbb{C}$ and constants $a, b \in \mathbb{C}$ with $b \neq 0$ such that $P(k) = a + b\zeta^k$ for $k = 1, \ldots, n$.

5. Find all integers $m, n > 2$ such that $k^n + k^2 - 1 \mid k^m + k - 1$ for infinitely many integers k.

6. Let $n \geq 2$ be an integer. We say two polynomials $P(x), Q(x)$ with real coefficients are block-similar if for any $j = 1, \ldots, n$,

   $$\{P(2026j), P(2026j-1), \ldots, P(2026j-2025)\} = \{Q(2026j), Q(2026j-1), \ldots, Q(2026j-2025)\}$$

   are sets of size 2026. Prove that there do not exist distinct polynomials P, Q of degrees at most n that are block-similar.

Polynomials

1. (Putnam 2008 B4) Let p be a prime and let $h(x) \in \mathbb{Z}[x]$ such that h induces a bijection on the residue classes mod p^2. Show that h also induces a bijection on the residue classes mod p^n for all $n \geq 2$.

   This is secretly Hensel. The assumption that $h : \mathbb{Z}/p^2\mathbb{Z} \to \mathbb{Z}/p^2\mathbb{Z}$ implies that h' is never 0 mod p.

2. (IMC 2017 P7) Let $p(x)$ be a nonconstant real polynomial. For any positive integer n, let $q_n(x) = (x+1)^n p(x) + x^n p(x+1)$. Does there exists a choice for $p(x)$ so that there are infinitely many n such that all the roots of $q_n(x)$ are real?

   For a polynomial $F(x) = Ax^m + Bx^{m-1} + Cx^{m-2} + \cdots$ to have all real roots $r_1, \ldots, r_m$, we have

   $$0 \leq r_1^2 + \cdots + r_m^2 = (r_1 + \cdots + r_m)^2 - 2(r_1 r_2 + r_1 r_3 + \cdots + r_{m-1} r_m) = \frac{B^2}{A^2} - 2\frac{C}{A}.$$

   That is, we need $B^2 - 2AC \geq 0$. Here, we scale $p(x)$ so that $p(x) = x^r + ax^{r-1} + bx^{r-2} + \cdots$. Then

   $$q_n(x) = 2x^{r+n} + (n + \cdots)x^{r+n-1} + (\frac{n^2}{2} + \cdots)x^{r+n-2} + \cdots$$

   where the $\cdots$ in the coefficients are lower degree terms in n with coefficients depending on $p(x)$. Then

   $$B^2 - 2AC = n^2 - 2n^2 + \cdots = -n^2 + \cdots$$

   which can be non-negative for only finitely many n.

3. (USAMO 2002 P3) Let $f(x)$ be a monic real polynomial of degree n. Show that f can be written as the average of two monic real polynomials g, h of degree n having all real roots.

   We seek for $r(x) \in \mathbb{R}[x]$ of degree $n-1$ such that $g = f + r$ and $h = f - r$ work. Such an $r(x)$ is determined by its value at n points, say by $r(1), \ldots, r(n)$ via Lagrange interpolation. If $g(1), g(2), \ldots, g(n)$ alternate signs, then g has one real root from each of $(1,2), (2,3), \ldots, (n-1, n)$, and then one more since the sum of the roots is real. Similarly for h. Hence we choose $r(1), \ldots, r(n)$ such that

   $$\begin{array}{lll} f(1) + r(1) > 0 & \text{and} & f(1) - r(1) < 0, \\ f(2) + r(2) < 0 & \text{and} & f(2) - r(2) > 0, \\ & \vdots & \end{array}$$

   This is possible by choosing $(-1)^{j-1} r(j)$ sufficiently large for $j = 1, \ldots, n$.

4. (Putnam 2008 A5) Let $n \geq 1$ and let $\zeta = e^{2\pi i/n}$. Does there exist a polynomial $P(x)$ of degree at most $n-2$ with coefficients in $\mathbb{C}$ and constants $a, b \in \mathbb{C}$ with $b \neq 0$ such that $P(k) = a + b\zeta^k$ for $k = 1, \ldots, n$.

   The $(n-1)$-th forward difference

   $$\sum_{j=0}^{n-1} (-1)^{n-1-j} \binom{n-1}{j} P(x+j) = 0.$$

Evaluate it at $x = 1$ gives

$$0 = \sum_{j=0}^{n-1} (-1)^{n-1-j} \binom{n-1}{j} (a + b\zeta^k) = b(\zeta - 1)^{n-1}$$

which is a contradiction.

5. (IMO 2002 P3) Find all integers $m, n > 2$ such that $k^n + k^2 - 1 \mid k^m + k - 1$ for infinitely many integers k.

   Let $g(x) = x^m + x - 1$ and $f(x) = x^n + x^2 - 1$. Divide f by g to get $f(x) = g(x)q(x) + r(x)$ with $q, r \in \mathbb{Z}[x]$ and $\deg r < \deg f$. If $f(k) \mid g(k)$, then $f(k) \mid r(k)$, but $f(k) > |r(k)|$ as $k \to \infty$. Hence in order for $f(k)| \mid r(k)$ for infinitely many k, we need $r(k) = 0$ for infinitely many k and so $r(x) = 0$ and $f(x) \mid g(x)$ in $\mathbb{Z}[x]$.

   Next we have

   $$g(x) - x^{m-n} f(x) = x - 1 - x^{m-n+2} + x^{m-n} = (x-1)(1 - x^{m-n}(x+1)).$$

   Since $f(1) \neq 0$, we see that $f(x)$ is coprime to $x - 1$. So we have $f(x) \mid x^{m-n+1} + x^{m-n} - 1$. Hence we have $m - n + 1 \geq n$. Since $f(1) = 1$ and $f(0) = -1$, there exists $\alpha \in (0, 1)$ such that $f(\alpha) = 0$, which also gives $\alpha^{m-n+1} + \alpha^{m-n} - 1 = 0$. Hence we have

   $$\alpha^n + \alpha^2 = 1 = \alpha^{m-n+1} + \alpha^{m-n}.$$

   Since $m - n + 1 \geq n$ and $m - n \geq n - 1 \geq 2$, we are forced into equality for both. Hence $n = 3$ and $m = 5$. Finally, one checks that

   $$x^5 + x - 1 = (x^3 + x^2 - 1)(x^2 - x + 1).$$

6. (IMO SL 2015 A6) Let $n \geq 2$ be an integer. We say two polynomials $P(x), Q(x)$ with real coefficients are block-similar if for any $j = 1, \ldots, n$,

   $$\{P(2026j), P(2026j-1), \ldots, P(2026j-2025)\} = \{Q(2026j), Q(2026j-1), \ldots, Q(2026j-2025)\}$$

   are sets of size 2026. Prove that there do not exist distinct polynomials P, Q of degrees at most n that are block-similar.

   For any $F \in \mathbb{R}[x]$ of degree $d \geq 0$, let $\Sigma_F(x)$ be the polynomial of degree $d + 1$ such that $\Sigma_F(m) = F(1) + \cdots + F(m)$ for every positive integer m. Then

   $$F(x) = \Delta\Sigma_F := \Sigma_F(x) - \Sigma_F(x - 1)$$

   since they agree on every positive integer.

   Let $k = 2026$. Then here $\Sigma_{P-Q}(x)$ has $n+1$ roots $0, k, 2k, \ldots, nk$. This forces $\deg \Sigma_{P-Q} \geq n+1$ so $\deg(P - Q) \geq n$. Since their degrees are at most n, we have equalities. Let

   $$T(x) = x(x - k)(x - 2k) \cdots (x - nk).$$

   Then by scaling P and Q, we have

   $$\Sigma_{P-Q} = T \qquad \text{and} \qquad P - Q = \Delta T = T(x) - T(x - 1).$$

Similarly, $\Sigma_{P^2-Q^2}$ also has $n+1$ roots $0, k, 2k, \ldots, nk$. So there is a polynomial G of degree $\deg(P^2-Q^2)+1-\deg T = \deg(P+Q)$ such that $\Sigma_{P^2-Q^2} = TG$. Then

$$\begin{aligned} P^2-Q^2 &= T(x)G(x) - T(x-1)G(x-1) \\ &= (T(x)-T(x-1))G(x) + T(x-1)(G(x)-G(x-1)) \end{aligned}$$

which should be divisible by $P-Q = T(x)-T(x-1)$. Hence

$$T(x)-T(x-1) \mid T(x-1)(G(x)-G(x-1)).$$

Since $\gcd(T(x)-T(x-1), T(x-1)) = \gcd(T(x), T(x-1)) = 1$ as they have distinct roots, we have $T(x)-T(x-1) \mid G(x)-G(x-1)$. Since $\deg G = \deg(P+Q) \le n < \deg T$, we conclude that $G(x)-G(x-1)=0$ so G is constant. Hence $P+Q$ is a constant. By shifting P and Q, we may assume that $P=-Q=\Delta T/2$.

Within each $[kj-(k-1), kj]$, we see that since P and $-P$ take the same values, if P is not 0 on all the integer points, then P must take both positive and negative values. In either case, P has at least 1 zero in $[kj-(k-1), kj]$ for each $j=1,\ldots,n$. Since P has degree n, it has exactly 1 zero in each such intervals. Let $m=k/2$. Then in particular, $P(1),\ldots,P(m)$ should have the same sign and $P(m+1),\ldots,P(2m)$ have the same sign.

We note that for $a=1,\ldots,k-1$, each of $T(a)$ has sign $(-1)^n$. Let $m=k/2$. Then

$$\begin{aligned} \frac{T(m)}{T(m-1)} &= \frac{m(-m)(-3m)\cdots(-(2n-1)m)}{(m-1)(-m-1)(-3m-1)\cdots(-(2n-1)m-1)} \\ &= \frac{m^2}{m^2-1}\frac{3m}{3m+1}\cdots\frac{(2n-1)m}{(2n-1)m+1} \\ &\le \frac{m^2}{m^2-1}\frac{3m}{3m+1} \\ &< 1 \end{aligned}$$

since $3m^3 < 3m^3+m^2-3m-1$ for $m \ge 4$. Hence we have $T(m)/T(m-1) \in (0,1)$, which implies that $P(m) = T(m)-T(m-1)$ has a different sign from $T(m)$, but $P(1)=T(1)$ has the same sign as $T(m)$. So $P(1)$ and $P(m)$ have different signs, which is a contradiction.