Math 43900 Problem solving, Fall 2017, Lecture 4 exercises.

These problems are taken from the textbook, from Ravi Vakil's Putnam seminar notes, from David Galvin's problems and from Po-Shen Loh's Putnam seminar notes.

Polynomials

Useful facts

1. If $P(X)$ has root α then $X-\alpha \mid P(X)$, i.e., $P(X)=(X-\alpha)Q(X)$ for a polynomial $Q(X)$. The root α is a double root, i.e., it appears twice in the list of roots, if and only if $P(\alpha)=P'(\alpha)=0$.

2. If a polynomial with coefficients in $\mathbb{C}$ has infinitely many roots it must be the 0 polynomial. A variant is that if P, Q are complex polynomials with $P(z)=Q(z)$ for infinitely many values of z then $P=Q$.

3. If $P(X)$ and $Q(X)$ have the same (complex) roots then they differ by a scalar. In particular, if they have the same leading coefficient then $P=Q$.

4. Remember from the quadratic formula that if $X^2+aX+b=0$ has roots α and β then $\alpha+\beta=-a$ and $\alpha\beta=b$. If $P(X)=X^n+a_1X^{n-1}+a_2X^{n-2}+\cdots+a_{n-1}X+a_n$ has roots $\alpha_1,\ldots,\alpha_n$ then for $1\le r\le n$
$$(-1)^r a_r = \sum_{i_1<i_2<\ldots<i_r} \alpha_{i_1}\alpha_{i_2}\cdots\alpha_{i_r} (= s_r)$$
which specializes to $-a_1=\sum_i \alpha_i (= s_1)$, $a_2=\sum_{i<j}\alpha_i\alpha_j (= s_2)$, $-a_3=\sum_{i<j<k}\alpha_i\alpha_j\alpha_k (= s_3)$ and so on until $(-1)^n a_n = \prod \alpha_i (= s_n)$. The s_k are called the **elementary symmetric polynomials** in the roots.

5. If A and B are two polynomials then you can divide with remainder: $A(X)=B(X)\cdot Q(X)+R(X)$ with either $R(X)=0$ or $\deg R<\deg B$. Using divisibilities you can show that the gcd of A and B is the same as the gcd of B and R and then compute the gcd sequentially. We write (A,B) for the gcd.

6. This is Gauss' lemma: If A and B are integer polynomials and A/B is a polynomial (necessarily with rational coefficients) then it is an integer polynomial. In other words if $B \mid A$ as rational polynomials then $B \mid A$ as integral polynomials.

7. If a matrix has entries which are polynomials then the determinant of the matrix is also a polynomial. You can show this by induction using the fact that a determinant can be expanded in terms of rows and minors.

8. This is the important Eisenstein irreducibility criterion, which we'll prove when we do modular arithmetic. Suppose $P(X)=X^n+a_1X^{n-1}+\cdots+a_{n-1}X+a_n$ is an integral polynomial and p is a prime number such that $p \mid a_1,a_2,\ldots,a_n$ but $p^2 \nmid a_n$. Then $P(X)$ is an irreducible polynomial.

9. Finally an input from Galois theory that's useful: If a rational (or real or complex) polynomial $P(x_1,x_2,\ldots,x_n)$ doesn't depend on the ordering of the variables $x_1,\ldots,x_n$, i.e., no matter how you permute them the final expression is the same, then $P(x_1,\ldots,x_n)$ can be written as a polynomial rational (or real or complex) polynomial $Q(s_1,\ldots,s_n)$ where s_k are the elementary symmetric polynomials. E.g., $x_1^2x_2+x_1x_2^2+x_1^2x_3+x_1x_3^2+x_2^2x_3+x_2x_3^2=s_1s_2-3s_3$ (check this!).

Problems with roots

1. Suppose $P(X)$ is a monic polynomial with integer coefficients. Show that if $P(X)$ has a rational root α then α is in fact integral. [Roots of such polynomials are called algebraic integers.]

2. Let $P(X) = X^n + a_1X^{n-1} + \cdots + a_{n-1}X + a_n$. If $a_1 + a_3 + a_5 + \cdots$ and $a_2 + a_4 + \cdots$ are real numbers show that $P(1)$ and $P(-1)$ are real numbers as well. As a follow-up: let $\alpha_1, \ldots, \alpha_n$ be the roots of $P(X)$ and suppose that $Q(X) = X^n + b_1X^{n-1} + \cdots b_{n-1}X + b_n$ has roots $\alpha_1^2, \ldots, \alpha_n^2$. Show that $b_1 + b_2 + \cdots + b_n$ is a real numbers.

3. For which real values of p and q are the roots of the polynomial $X^3 - pX^2 + 11X - q$ three consecutive integers?

4. For which values of $n \geq 1$ do there exist polynomials $P(X)$ satisfying:

   (a) $P(k) = k$ for $1 \leq k \leq n$,

   (b) $P(0)$ is an integer, and

   (c) $P(-1) = 2017$?

5. (Putnam 2005) Find a non-zero polynomial $P(X, Y)$ such that $P(\lfloor t \rfloor, \lfloor 2t \rfloor) = 0$ for all real numbers t. (Here $\lfloor t \rfloor$ indicates the greatest integer less than or equal to t.)

6. If $P(X)$ is a real polynomial whose roots are all real and distinct and different from 0 show that $XP'(X) + P(X)$ is a real polynomial with distinct real roots which are different from 0. As a follow-up: show that $XP''(X) + 3XP'(X) + P(X)$ has distinct real roots. [Hint for the follow-up: apply the first part twice.]

Problems with divisibilities

1. (Useful) Show that if $m \mid n$ then $X^m - 1 \mid X^n - 1$. Also show that if $m \mid n$ are odd then $X^m + 1 \mid X^n + 1$. As a follow-up: show that if m and n are positive integers with gcd d then the polynomials $X^m - 1$ and $X^n - 1$ have gcd $X^d - 1$. [Hint: Show that if $m = nq + r$ is division with remainder then $X^m - 1 = (X^n - 1)Q(X) + X^r - 1$ is division with remainder.]

2. Show that in the product $(1 - X + X^2 - X^3 + \cdots + X^{100})(1 + X + X^2 + X^3 + \cdots + X^{100})$ when you expand and collect terms X only appears to even exponents.

3. Show that the polynomial $X^3 - 2$ is irreducible in $\mathbb{Z}[X]$.

4. Find all polynomials $P(X)$ satisfying $(X + 1)P(X) = (X - 2)P(X + 1)$.

5. Suppose p is a prime. Show that $P(X) = X^{p-1} + X^{p-2} + \cdots + X + 1 = \dfrac{X^p - 1}{X - 1}$ is an irreducible polynomial. [Hint: Look at $P(X + 1)$ and apply the Eisenstein irreducibility criterion.]

6. Show that $(X - 1)(X - 2) \cdots (X - n) - 1$ is irreducible in $\mathbb{Z}[X]$. [Hint: Show that if it factors as $P(X)Q(X)$ then $P + Q$ has roots $1, 2, \ldots, n$.]

7. Suppose p is a prime $\equiv 3 \pmod 4$. Show that $(X^2 + 1)^n + p$ is irreducible over $\mathbb{Z}$. [Hint: the condition on p implies that $X^2 + 1$ has no roots mod p.]

8. Let $P(X) \in \mathbb{Z}[X]$ be an irreducible polynomial such that $|P(0)|$ is not a perfect square. Show that $P(X^2)$ is also irreducible.