Math 96:
Polynomials Techniques

October 29th, 2021

Today we will discuss some techniques relating to polynomials that may prove useful on the Putnam Exam.

1 Basics

Recall that a polynomial is a function of the form $p(x) = a_d x^d + a_{d-1}x^{d-1} + \ldots + a_0$. Here the *degree* of $p(x)$ is d, or the largest power of x with a non-zero coefficient. You can also have polynomials in many variables. For example, a polynomial $p(x, y, z)$ is a function given by a sum of terms of the form $ax^i y^j z^k$ where i, j, k are non-negative integers. It is not hard to see that the sum or product of two polynomials is another polynomial.

2 Polynomials and Factorization

One of the most important features of polynomials is their factorization (i.e. the ability to write a polynomial as a product of simpler polynomials). It turns out that in many cases there is a theory of unique factorization of polynomials similar to unique factorization of integers.

In particular let R be either a field (like $\mathbb{R}, \mathbb{C}$, or $\mathbb{Q}$) or a ring with unique prime factorization (like $\mathbb{Z}$). We say that a polynomial (in any number of variables) with coefficients in R is *irreducible over R* if it cannot be written as a product of (non-constant) polynomials with coefficients in R. The important result here is that any polynomial with coefficients in R can be written as a product of polynomials that are irreducible over R and furthermore, this factorization is unique up to reordering the factors and multiplying them by constants.

If $p(x)$ is a polynomial in one variable, $p(x)$ has a linear factor $(x-r)$ if and only if r is a *root* of p (namely if and only if $p(r) = 0$). Note that if p has degree d (and we are in one of the cases where unique factorization into irreducibles holds), then p cannot have more than d linear factors, and thus cannot have more than d roots. This is a very useful fact as it implies that if p has more than d roots, it must be identically 0. In particular, if you want to show that two degree-d polynomials $p(x)$ and $q(x)$ are the same, it suffices to find $d+1$ values of x so that $p(x) = q(x)$ (as these x will be roots of $p - q$).

Finally, the Fundamental Theorem of Algebra says that for polynomials specifically over the complex numbers, any polynomial in one variable will always factor into linear factors. In particular, any polynomial $p(x)$ of degree-d will have *exactly* d roots (with multiplicity) and can be written $p(x) = a\prod_{i=1}^{d}(x - r_i)$. Over the real numbers, any polynomial will factor into linear and quadratic factors. In particular, any real polynomial of odd degree will have at least one root.

1956 B7: The polynomials $P(z)$ and $Q(z)$ with complex coefficients have the same set of numbers for their zeroes but possibly different multiplicities. The same is true for the polynomials $P(z) + 1$ and $Q(z) + 1$. Prove that $P(z) \equiv Q(z)$.

3 Coefficients and Symmetric Polynomials

How do the coefficients of a polynomial relate to its roots? Well if $p(x) = (x-r_1)(x-r_2)(x-r_3)\cdots(x-r_k)$, expanding out we find that

$$p(x) = x^k - \sigma_1 x^{k-1} + \sigma_2 x^{k-2} - \ldots \pm \sigma_k,$$

where $\sigma_t = \sum_{1 \le i_1 < i_2 < \ldots < i_t \le k} r_{i_1} r_{i_2} \cdots r_{i_k}$ is the t^{th} elementary symmetric polynomial in the roots.

In particular, $\sigma_1 = r_1 + r_2 + \ldots + r_k$ is the sum of the roots. This means that if you know the values of all but one of the roots, $r_1, r_2, \ldots, r_{k-1}$ it is relatively easy to solve for the last one $r_k = \sigma_1 - (r_1 + r_2 + \ldots + r_{k-1})$.

This gives rise to a common trick. Suppose you have a polynomial $p(x, y, z)$ in many variables, and that you have some root $p(x_0, y_0, z_0) = 0$, but want to find others. If p is a degree-2 polynomial in x, then thinking of y_0 and z_0 as constant, we have a quadratic polynomial in x ($p(x, y_0, z_0)$) which has one root (x_0), and so we can find another. If p is also quadratic in y or z, we can repeat this trick with other variables to find many roots.

Another variation of this trick applies to the arithmetic of Elliptic Curves. If $p(x, y)$ is a polynomial of degree-3 and we have two roots, then restricting ourselves to the line between those roots, we have a degree-3 polynomial in one variable with two roots, and so we can find the third.

1986 B5: Let $f(x, y, z) = x^2 + y^2 + z^2 + xyz$. Let $p(x, y, z), q(x, y, z), r(x, y, z)$ be polynomials with real coefficients satisfying

$$f(p(x, y, z), q(x, y, z), r(x, y, z)) = f(x, y, z).$$

Prove or disprove the assertion that the sequence p, q, r consists of some permutation of $\pm x, \pm y, \pm z$, with the number of minus signs 0 or 2.

4 Summation Polynomials

Note that

$$\sum_{i=1}^{n} 1 = n,$$

$$\sum_{i=1}^{n} i = n(n+1)/2,$$

$$\sum_{i=1}^{n} i^2 = n(n+1)(2n+1)/6.$$

In general, for any polynomial $p(x)$, there exists a polynomial $q(x)$ so that

$$\sum_{i=1}^{n} p(i) = q(n)$$

for all n. This can be shown in any given case by finding a q so that $q(n) - q(n-1) \equiv p(n)$ and $q(0) = 0$, and using induction. It can also be shown by writing $p(x)$ in terms of the polynomials $\binom{x}{k}$ and noting that

$$\sum_{i=1}^{n} \binom{i}{k} = \binom{n+1}{k+1}.$$

1981 B1: Find:

$$\lim_{n\to\infty} \left[\frac{1}{n^5} \sum_{h=1}^{n} \sum_{k=1}^{n} (5h^4 - 18h^2k^2 + 5k^4) \right].$$

5 Representations and Coefficients

There are several ways of writing down a polynomial. You can write it as a sum of coefficients. You can write it as a product over roots. But there are other ways, and for some applications being able to write it in a more convenient way may be crucial. For example instead of writing a polynomial in one variable in terms of powers of x, you can write it in terms of powers of $(x - r)$ like

$$p(x) = a_d(x - r)^d + a_{d-1}(x - r)^{d-1} + \ldots + a_0.$$

This is often useful when you want to know how the polynomial behaves near $x = r$. You can also write the polynomial in terms of binomial coefficients $\binom{x}{k}$ which is useful for computing summation polynomials.

2016 A1: Find the smallest positive integer j such that for every polynomial p with integer coefficients and for every integer k, the integer

$$p^{(j)}(k) = \frac{\partial^j p(x)}{\partial x^j}|_{x=k}$$

(the j^{th} derivative of p at k) is divisible by 2016.