SUMMER CAMP 2015 TRAINING: POLYNOMIALS

1. Polynomials and their roots

A polynomial $P(x)$ over $\mathbb{C}$ (or $\mathbb{R}, \mathbb{Q}, \mathbb{Z}, \dots$) of degree n is an expression of the form

$$a_n x^n + a_{n-1}x^{n-1} + \cdots + a_1 x + a_0$$

where $a_i \in \mathbb{C}$ (or $\mathbb{R}, \mathbb{Q}, \mathbb{Z} \dots$) and where $a_n \neq 0$. We write $n = \deg P$. By convention, the zero polynomial has degree 'negative infinity', so that its degree is smaller than that of any other polynomial. Polynomials can be subtracted, multiplied, and added together. For any polynomials $f(x), g(x)$ it is easy to see that

$$\deg\,(f+g) \leq \max(\deg\,f, \deg\,g).$$

Moreover, if f, g are non-zero polynomials, then

$$\deg\,fg = \deg\,f + \deg\,g.$$

We say that $f(x)$ divides $g(x)$— written $f \mid g$ — if there exists a polynomial $s(x)$ such that $f(x)s(x) = g(x)$. It turns out that just like for integers, one can talk about remainders for polynomials:

Lemma 1.1. *Let $f(x), g(x)$ be polynomials, such that $g(x) \neq 0$. Then there exits a unique pair of polynomials $r(x), s(x)$ with $\deg\,r < \deg\,g$, such that $f = sg + r$. We say that r is the remainder of f divided by g.*

Proof. Lets first prove uniqueness. So suppose there are two pairs $(s_1, r_1), (s_2, r_2)$ satisfying the conclusion of the lemma. Then subtracting, we get

$$0 = f - f = (s_1 - s_2)g + (r_1 - r_2),$$

and thus g divides $(r_1 - r_2)$. However, $\deg\,g < \deg\,(r_1 - r_2)$, and so $r_1 = r_2$. We then get $(s_1 - s_2)g = 0$, and $g \neq 0$,which means $s_1 = s_2$. So we have proved uniqueness.

To prove existence, we use induction on $\deg\,f$. If $\deg\,f < \deg\,g$ the result is obvious. So suppose we have proven the result for $\deg\,f < n$ and suppose that $\deg\,f = n \geq \deg\,g$. Write $f(x) = a_n x^n + \cdots + a_1 x + a_0$ and $g(x) = b_m x^m + \cdots + b_1 x + b_0$. Consider $h(x) = f(x) - a_n/b_m x^{n-m} \cdot g$. Then $h(x) = (a_{n-1} - a_n b_{m-1}/a_n)x^{n-1} + \dots$, and thus $\deg\,h < n$. Now, by induction, we can write $h = s_0 g + r$ for polyomials (s_0, r) with $\deg\,r < \deg\,g$. Thus, setting $s = s_0 + a_n/b_m x^{n-m}$, we have $f = sg + r$. This completes the induction.

∎

We say that a number r is a root of $P(x)$ if $P(r) = 0$. It is not hard to show that $P(r) = 0$ if and only if $(x - r)|P(x)$.

1.1. **Polynomials over $\mathbb{C}$.** We write $\mathbb{C}[x]$ for the set of all polynomials with coefficients in $\mathbb{C}$ (and likewise for $\mathbb{Q}, \mathbb{Z}, \dots$). The most important theorem to know is the fundamental theorem of algebra:

Theorem 1.2. *Every polynomial $f(x) \in \mathbb{C}[x]$ of degree at least 1 has a complex root. That is, there is a $z \in \mathbb{C}$ such that $f(z) = 0$.*

We record the following important corollary:

Corollary 1.3. *Every polynomial $f(x) \in \mathbb{C}[x]$ can be factored into linear polynomials. That is, we can write $f(x) = c(x - z_1)(x - z_2) \cdots (x - z_n)$ and the constant c and the multiset $\{z_1, \dots, z_n\}$ is unique. That is, any degree n polynomial has n roots counted with multiplicity.*

Proof. Write $f(x) = a_n x^n + \cdots + a_1 x + a_0$. Looking at the leading coefficient, se must have $c = a_n$ so we may assume that $f(x)$ is monic. We proceed by induction on n, the case of $n = 1$ being immediate. Now, by the fundamental theorem of algebra, $f(x)$ has some root z_1 so we may write $f(x) = (x - z_1)g(x)$ for some polynomial $g(x)$ of degree $n - 1$. By induction, we can write $g(x) = (x - z_2) \cdots (x - z_n)$ and thue $f(x) = (x - z_1) \cdots (x - z_n)$ as desired.

To show uniqueness, suppose that

$$\prod_{i=1}^{n} (x - z_i) = \prod_{i=1}^{n} (x - w_i)$$

for different multisets $\{z_1, \dots, z_n\}$ and $\{w_1, \dots, w_n\}$. We may assume that none of the z_i equal any of the w_j or else we could divide out and get an equality between products of smaller degree. Plugging in $x = z_1$, we get $0 = \prod_{i=1}^{n} (z_1 - w_i)$, which is a contradiction.

□

1.2. **Polynomials over $\mathbb{R}$.** While polynomials in $\mathbb{R}$ can't be factored into linear polynomials, you have a theorem that is almost as good.

Theorem 1.4. *Every polynomial$f(x) \in \mathbb{R}[x]$ can be factored uniquely as*

$$f(x) = c \prod_{i=1}^{k} (x - r_i) \prod_{i=1}^{m} Q_i(x)$$

where c, r_i are real and $Q_i(x) \in \mathbb{R}[x]$ are monic quadratic polynomials with complex roots.

Proof. Again,we may assume that f is monic, so that $c = 1$. Using the fundamental theorem of algebra, we can write $f(x) = \prod_{i=1}^{n} (x - z_i$ where the z_i are complex numbers. Now, recall that complex conjugation is the operation which takes $a + bi$ to $\overline{a + bi} = a - bi$. Since f has real coefficients, and these are preserved by complex conjugation, we have

$$f(\overline{z}) = \sum_{i=0}^{n} a_n \overline{z}^n = \sum_{i=0}^{n} \overline{a_n z^n} = \overline{f(z)}.$$

Thus, if z is a complex root then so is $\overline{z}$. More generally, if $(x-z)^m|f(x)$ then $(x-\overline{z})^m|f(x)$ so complex conjugate roots occur with equal multiplicity.

Thus, we may write

$$f(x) = \prod_{i=1}^{k}(x-r_i) \cdot \prod_{i=1}^{m}(x-z_i)(x-\overline{z_i})$$

where $z_i = a_i + b_i$ is not a real number. Now let $Q_i(x) = (x-z_i)(x-\overline{z_i}) = x^2 = -2a_x + a_i^2 + b_i^2$. The proof of uniqueness is left as an exercise!

□

The above is an extremely useful fact! As practise, try proving the following:

(Hard) Exercise: Let $P(x)$ be a polynomial over the real numbers such that for any $r \in \mathbb{R}$, $P(r) \geq 0$. Prove that there are two real polynomials S, T such that

$$P(x) = S(x)^2 + T(x)^2.$$

1.3. **Polynomials over $\mathbb{Q}$.** There are many more polynomials over $\mathbb{Q}$ then over $\mathbb{R}$ and $\mathbb{C}$ that cannot be factored into smaller degree polynomials. We call such polynomials *irreducible.* It can be hard to decide if a given polynomial is irreducible. These are similar to prime numbers, since everything can be factored into them. We will prove this theorem, but first a couple lemmas:

Lemma 1.5. *If $f(x), g(x)$ are two polynomials, there exists a monic polynomial $h(x)$, called the greatest common divisor of f and g (written gcd(f,g)), such that for any polynomial $t(x)$, r divides h if and only if t divides both f and g. Moreover, we can write $h = af + bg$ for some polynomials a, b.*

Proof. We do induction on the $n+m$, where $n = \deg f, m = \deg g$. The case of $n=0, m=0$ being obvious, since f, g are just scalars and $h=1$.

Now for the induction step, suppose wlog $n \geq m$. Then we can write $f = gs + r$ for polynomials r, s with $\deg r < m$. Now, note that for any polynomial t, it divides both f and g if and only if it divides both g and r. By induction, g and r have a greatest common divisor h, and the same h will therefore be the gcd of f and g. Moreover, $h = a_0 r + b_0 g$ for some polynomials a_0, b_0 by induction, so then

$$h = a_0(f - gs) + b_0 g = a_0 f + (b_0 - a_0 s)g,$$

so we can take $a = a_0, b = b_0 - a_0 s$.

□

Lemma 1.6. *If $f(x)$ is irreducible, and $f|gh$ then f divides at least one of g and h.*

Proof. Suppose f does not divide either g or h. Let $t = \gcd(g, f)$. Then $gcd(f, g)$ is some polynomial dividing f, but can't be equal to f since f does not divide t. Now since f is irreducible, $gcd(f, g)$ must be 1. Thus, we can write $1 = af + bg$ for polynomials a, b. Multiplying by h, we get $h = afh + bgh$. Now, if f divided gh, then f would divide $afh + bgh$, and thus f would divide h, which is a contradiction. □

Theorem 1.7. *Every non-zero monic polynomial $f(x) \in \mathbb{Q}[x]$ can be factored uniquely as $f(x) = \prod_{i=1}^{n} Q_i(x)$ where $Q_i(x)$ are monic irreducible polynomials.*

Proof. To prove that such a factorization exists, we can induct on the degree n on $f(x)$. For $n = 0$ the theorem is obvious. For higher n, just pick an divisor $g(x)$ of $f(x)$ of minimal degree. Then $g(x)$ must be irredudicibile. now we can write f/g as a product of irreducible polynomials, and since $f = f/g \cdot g$ we are done.

To prove uniqueness, suppose we had $\prod_{i=1}^{n} Q_i(x) = \prod_{i=1}^{m} R_j(x)$ where the Q_i and R_j are distinct. Then Q_1 divides the right hand side, and so by repeated application of lemma 1.6 it must divdide some R_j. Wlog $Q_1|R_1$. But R_1 is irreducible, and thus $Q_1 = R_1$, which is a contradiction. □

1.4. **Polynomials over $\mathbb{Z}$.** Over the integers, polynomials are a little trickier. basically, since $\mathbb{Z}$ has a rich structure of factoring, factorig in $\mathbb{Z}[x]$ is like worrying about $\mathbb{Q}[x]$ and $\mathbb{Z}$ simultaneously. The following fact — named Gauss' lemma — is super useful for working with polynomials over $\mathbb{Z}$:

Lemma 1.8. *Let $f(x)$ be an integer polynomial, and $g(x), h(x)$ be polynomials over $\mathbb{Q}$ such that $f(x) = g(x)h(x)$. Then there exists a rational non-zero number c such that $cg(x)$ and $h(x)/c$ are integer polynomials, and $f(x) = cg(x) \cdot h(x)/c$. In other words, any factorization over $\mathbb{Q}$ secretly comes from a factorization over $\mathbb{Z}$.*

Proof. By first scaling g and shrinking h, we may assume that the coefficients of g are integers. Now, take c to be the reciprocal of the gcd of all the coefficients of g. Let $h_0 = h/c$, and assume for the sake of contradiction that h_0 does not have integer coefficients.

Write $h_0(x) = \sum_{i=0}^{n} a_i x^i$ and $g_0(x) = \sum_{j=0}^{m} b_j x^j$ where a_n, b_m are non-zero. Let p be a prime that occurs in the denominator of at least one of the a_i. Let p^m be the highest power of p dividing the denominators of any of the a_i, and Let k be the smallest integer such that p^m divides the denominator of a_k and l be the smallest integer such that p does not divide b_l.

Now, the $k + l$'th coefficient of f is equal to

$$\sum_{i \leq k+l} a_i b_{k+l-i}.$$

The sum on the RHS only has one term $a_k b_l$ such that p^m divides the denominator, and thus $k+l$'th coefficient of f has denominator divisible by p^m. But it is an integer! This is a contradiction.

$\square$

(Hard) Excercise: $a_0, \ldots, a_{n-1}$ are positive integers such that a_0 is prime and $|a_0| > \sum_{i=1}^{n-1} |a_i|$. Prove that $f(x) = x^n + a_{n-1}x^{n-1} + a_{n-2}x^{n-2} + \cdots + a_1 x + a_0$ is irreducible.

1.5. **Polynomials over $\mathbb{F}_p$.** For a prime number p, one can also consider polynomials $f(x)$ with coefficients in $\mathbb{F}_p$. In fact, if $F(x) \in \mathbb{Z}[x]$ then one can obtain a polynimial $f(x)$with coefficients in $\mathbb{F}_p$by simply reducing the coefficients of $F(x)$ modulo p. Then any factorization of $F(x)$ becomes a factorization of $f(x)$ and so if f is irreducible then so is F. The following factorization can be extremely useful (and follows from Fermat's little theorem):

$$x^p - x = x(x-1)(x-2)\cdots(x-(p-1)) \mod p.$$

Exercise: find a polynomial with integer coefficients which is irreducible, but is reducible modulo every prime number p.

2. Useful tips

(1) For any polynomial $P(x)$, $(x-y)$ divides $P(x) - P(y)$. This is extremely useful, especially with integer polynomials!
(2) Let $P(x) = x^n + \cdots + a_1 x + a_0$ be a polynomial with roots $z_1, \ldots, z_n$, and let $S_m = \sum_{i=1}^n z_i^m$. Then the S_i satisfy the following simple recurrence relation: $S_{i+n} = -a_{n-1}S_{i+n-1} - \cdots - a_1 S_{i+1} - a_0 s_0$.
(3) If a monic integer polynomial $P(x)$ is such that all its roots α have absolute value at most 1, then in fact all its roots have absolute value equal to 1 and the constant term is 1. Moreover, all the roots of $P(x)$ are roots of unity **(Hard) Exercise: Prove this!**.
(4) A real polynomial has its non-real roots in complex-conjugate pairs. In particular, the number of non-real roots is even!

3. Problems

(1) A polynomial $P(x)$ of degree 10 satisfies $P(k) = \frac{k}{k+1}$ for $k = 0, 1, \ldots, 10$. Find $P(11$.
(2) Let a, b, c be distinct integers, and $P(x)$ a polynomial with integer coefficients. Prove that $P(a) = b, P(b) = c, P(c) = a$ cannot all be true.
(3) Let $n > 1$ be a positive integer. $P(x)$ is a degree n polynomial with positive integer coefficients. Ley $P^{(2)}(x) = P(P(x))$ and $P^{(m+1)}(x) = P(P^{(m)}(x))$ for $n \geq 2$. For some $k > 1$. For any $k \geq 1$, prove that $P^{(k)}(x) = x$ has at most n integer solutions.

(4) Let $p(x)$ be a polynomial with integer coefficients. Determine if there always exists a positive integer k such that $p(x) - k$ is irreducible.
(5) Let $f(z)$ be a monic polynomial with complex coefficients. Prove that we can find a complex number w with $|w| = 1$ and $|f(w)| \geq 1$.
(6) Prove that $x^n - x - 1$ is irreducible over the integers for all $n \geq 2$.
(7) Let $P(x)$ be a non-constant polynomial with integer coefficients. Prove that there is no function T from the set of integers into the set of integers such that the number of integers x with $T^{(n)}(x) = x$ is equal to $P(n)$ for every positive integer n, where $T^{(n)}$ denotes the n-fold application of T.
(8) Let $P(x), Q(x)$ be real monic polynomials. Prove that the sum of the squares of the coefficients of $P(x)Q(x)$ is at least as large as $P(0)^2 + Q(0)^2$.
(9) Let $f(x)$ be a monic irreducible polynomial with integer coefficients such that $|f(0)|$ is not a perfect square. Prove that $f(x^2)$ is also irreducible.
(10) Find all two variable polynomials $P(x, y)$ such that for any real numbers a, b, c we have
$$P(ab, c^2 - 2) + P(ac, b^2 - 2) + P(bc, a^2 - 2) = 0.$$
(11) Do there exist positive integers a, b, c such that for every $n > 2$, there exist a polynomial $P_n(x) = x^n + \cdots + ax^2 + bx + c$ with integer coefficients such that $P_n(x)$ has n integer roots (counted with multiplicity)?
(12) Let $P(x)$ be a polynomial with integer coefficients such that $P(n) > n$ for all positive integers n. Suppose that for every positive integer m, there exists a k such that $P^{(k)}(1)$ is divisible by m. Prove that $P(x) = x + 1$.
(13) Let $a_1 \geq a_2 \geq \cdots \geq a_n > 0$ be ;positive integers. Prove that $x^n - a_1x^{n-1} - a_2x^{n-2} - \cdots - a_n$ is irreducible over the integers.
(14) Let $P(x)$ be a monic polynomial with integer coefficients. Determine if there always exists a positive integer k such that $P(x) - k$ is irreducible.
(15) Let $P(x) = x^n + a_1x^{n-1} + \cdots + a_n$ be a monic polynomial with integer coefficients of degree $n \geq 3$ such that a_n is even, and for all $1 \leq k \leq n-1$, $a_k + a_{n-k}$ is even. Suppose $P(x) = R(x)Q(x)$ where R, Q have integer coefficients such that the coefficients of R are all odd, and $\deg R \geq \deg Q$. Prove that $P(x)$ has an integer root.
(16) A nonconstant polynomial f with integer coefficients has the property such that for each prime p, there exists a prime q and integer m such that $f(p) = q^m$. Prove that $f(x) = x^n$ for some positive integer n.
(17) Does there exists an infinite sequence of pariwise coprime positive integers $a_0, a_1, \ldots, a_n, \ldots$ such that for each n, the polynomial $\sum_{i=0}^{n} a_i x^n$ is irreducible?