Introduction to the 4th autumn series

The problems of this year’s 4th autumn series deal with polynomials. This short text aims to overview their basic properties while also providing you with some common terminology to talk about them.

What is a polynomial?

An expression $P(x)$ written as

$$P(x) = a_n x^n + a_{n-1} x^{n-1} + \cdots + a_2 x^2 + a_1 x + a_0$$

is called a polynomial. The real numbers $a_n, a_{n-1}, \ldots, a_2, a_1, a_0$ are called the coefficients of $P(x)$. The individual expressions $a_k x^k$ (for $k = 0, 1, \ldots, n$) are called terms. The polynomial $P(x)$ is called constant, if all of its coefficients except $a_0$ are zero. The largest index $k$ such that $a_k \neq 0$ is called the degree of $P(x)$ and we denote it by $\deg P$.

Degree and roots

If $n$ is the degree of $P(x) = a_n x^n + \cdots + a_1 x + a_0$ and $m$ is the degree of $Q(x) = b_m x^m + \cdots + b_1 x + b_0$, what is the degree of their product

$$R(x) = P(x)Q(x) = (a_n x^n + \cdots + a_1 x + a_0)(b_m x^m + \cdots + b_1 x + b_0)$$?

If we multiply out the parentheses, we will get many new terms $a_k b_\ell x^{k+\ell}$, but the one with the greatest exponent will be $a_n b_m x^{n+m}$. This means:

**Fact.** If $R(x)$ is the product of polynomials $P(x)$ and $Q(x)$, then

$$\deg R = \deg P + \deg Q.$$

Any number $r$ that satisfies $P(r) = 0$ is called a root of $P$. For example, $P(x) = x^2 - 1$ has two roots 1 and −1, while $P(x) = 3x - 5$ has only a single root $\frac{5}{3}$. In general, a non-zero polynomial $P(x)$ can only have at most $\deg P$ different roots. Further, if we know all the roots, we can use them to express the polynomial as a nice product.

**Fact.** If $P(x)$ is a non-zero polynomial of degree $n$ and it has $n$ different roots $x_1, x_2, \ldots, x_n$, then we can write it as

$$P(x) = a(x - x_1)(x - x_2)\cdots(x - x_n)$$

for some number $a \neq 0$.

Notice that in this arrangement, if $x$ becomes greater that all the roots, then increasing $x$ increases all of the $x - x_i$, so $|P(x)|$ also increases and is thus unbounded. This holds even for polynomials that don’t have $n$ different roots:

**Fact.** Let $P(x)$ be a non-constant polynomial. Then $|P(x)|$ is unbounded. Expressed formally: for any constant $C$, there exists an $x$ such that $|P(x)| > C$.

Let us try and use these facts to solve a problem.

**Problem.** A polynomial $P(x)$ of degree $n$ that has $n$ distinct real roots $x_1, \ldots, x_n$ is called timely, if is satisfies $P(x_i + 1) = 1$ for each $i = 1, \ldots, n$. Find all timely polynomials.
Solution. All non-zero constant polynomials $P(x) = k \neq 0$ are timely, since there are no roots, and so the condition holds trivially. Further, polynomials of the form $x - a$ are also timely, since $P(a) = 0$ and $P(a + 1) = 1$. Let us now show that there are no timely polynomials beyond these.

Let $P(x)$ be any timely polynomial and suppose it is non-constant, i.e. $n \geq 1$. We can consider the polynomials $Q(x) = P(x + 1) - P(x)$ and $R(x) = Q(x) - 1$. Since $P(x)$ is timely, we have

$$R(x_i) = P(x_i + 1) - P(x_i) - 1 = 1 - 0 - 1 = 0,$$

so $R(x)$ has $n$ distinct roots $x_i$. But suppose that $P(x)$ is written as

$$P(x) = c_n x^n + c_{n-1} x^{n-1} + \cdots + c_1 x + c_0$$

for some $c_n \neq 0$. Then $P(x+1) = c_n (x+1)^n + c_{n-1} (x+1)^{n-1} + \ldots$ Multiplying out $c_{n-1} (x+1)^{n-1}$ will only give us terms of the term $c_{n-1} x^{n-1}$ and some other terms with exponents lower then $n-1$. Similarly, multiplying out $c_n (x+1)^n$ with the binomial theorem will give us $c_n x^n$, the next term will be $c_n n x^{n-1}$ and all the others will have exponents lower then $n-1$. Altogether, the first two terms of $P(x+1)$ are

$$P(x) = c_n x^n + (c_{n-1} + nc_n) x^{n-1} + \cdots$$

Finally, this means that the $x^n$ and $x^{n-1}$ terms of $Q(x) = P(x+1) - P(x) - 1$ are

$$Q(x) = c_n x^n - c_n x^n + (c_{n-1} + nc_n) x^{n-1} - c_{n-1} x^{n-1} + \cdots = 0x^n + nc_n x^{n-1} + \cdots$$

Since $n$ and $c_n$ are non-zero, we have $\deg Q = n - 1$.

Now suppose for the sake of a contradiction that $n \geq 2$. Then $Q(x)$ is non-constant and subtracting the constant 1 will not change its degree, so $R(x) = Q(x) - 1$ also has $\deg R = n - 1 \geq 1$. Thus $R(x)$ is non-zero. But earlier we showed that $R(x)$ has $n$ distinct roots. This would contradict the fact that a non-zero $R(x)$ has at most $\deg R$ roots.

So it must be the case that $n \leq 1$, and so we are left to sort out the case $n = 1$. We can then write $P(x) = kx - a$,

$$Q(x) = P(x+1) - P(x) = k(x+1) - kx - a + a = k$$

and $R(x) = Q(x) - 1 = k - 1$. So $R(x)$ is constant, but we know it has a root $x_1$. This means that $R(x)$ has to be a constant zero, and so $k = 1$. This leads back to $P(x) = x - a$, which is what we wanted to show.

Polynomials with integer coefficients and divisibility

When all the coefficients of a polynomial are integers, it allows us to say some interesting things about divisibility. As a reminder: we say that an integer $a$ divides another integer $b$ if there exists an integer $c$ such that $b = ac$. This relation is denoted $a \mid b$.

A well-known algebraic identity tells us that

$$a^n - b^n = (a - b) \cdot (a^{n-1} + a^{n-2} b + \cdots + ab^{n-2} + b^{n-1}) ,$$

which means that $a - b \mid a^n - b^n$ for all integers $a, b$. Then if $P(x) = c_n x^n + \cdots + c_1 x + c_0$ is a polynomial with integer coefficients, we can rearrange the difference $P(a) - P(b)$ into the individual differences of terms $c_k a^k - c_k b^k$. Each of these is divisible by $a - b$, giving us:

**Fact.** If $P(x)$ is a polynomial with integer coefficients and $a$ and $b$ are integers, then

$$a - b \mid P(a) - P(b).$$
Sometimes, it can be useful to think of this in a slightly different way: whenever integers $x$ and $y$ give the same remainder modulo an integer $m$, then the values $P(x)$ and $P(y)$ also give the same remainder modulo $m$.

**Problem.** Let $P(x)$ be a polynomial with integer coefficients that satisfies $P(0) = P(1) = 1$. Prove that $P(x)$ has no integer roots.

**Solution.** Suppose for the sake of contradiction that $P$ has an integer root $r$. This $r$ is either even or odd. If it is even, plugging $a = r$, $b = 0$ into the previous fact tells us that

$$r - 0 \mid P(r) - P(0) = 0 - 1 = -1.$$  

But $r$ is even, so it cannot divide an odd number, so this is a contradiction.

Similarly, if $r$ is odd, plugging in $a = r$, $b = 1$ tells us that

$$r - 1 \mid P(r) - P(1) = 0 - 1.$$

Again, an even number cannot divide an odd number. Altogether, we have shown that $P(x)$ cannot have an integer root.