Problems 6 – polynomials

1. Prove that a polynomial with real coefficient $p(x)$ is nonnegative for all real values iff it is a sum of two squares (of polynomials with real coefficients).

Solution. A sum of squares is obviously nonnegative. The other part is more interesting.
Complex conjugation keeps the polynomial, so for each root above the complex line $a+ib$ there is corresponding complex conjugate root below the complex line $a-ib$. Also, each real root is of odd multiplicity, otherwise function to both side of this root wouldn't be positive.
Thus we can divide all the complex roots into pairs: $\alpha_1, \overline{\alpha_1}, \alpha_2, \overline{\alpha_2}, ..., \alpha_k, \overline{\alpha_k}$.
Hence the polynomial can be written as

$$p(x) = A(x-\alpha_1)(x-\alpha_2)\cdot...\cdot(x-\alpha_k)\cdot\left(x-\overline{\alpha_1}\right)\left(x-\overline{\alpha_2}\right)\cdot...\cdot\left(x-\overline{\alpha_k}\right),$$

where A is the highest coefficient. $(x-\alpha_1)(x-\alpha_2)\cdot...\cdot(x-\alpha_k)$ is a polynomial with complex coefficients, it can be written as $r(x)+\mathrm{i}q(x)$ where $r(x), q(x)$ are polynomials with real coefficients. So

$$p(x) = A\left(r(x)+\mathrm{i}q(x)\right)\left(\overline{r(x)+\mathrm{i}q(x)}\right) = A\left(r(x)+\mathrm{i}q(x)\right)\left(r(x)-\mathrm{i}q(x)\right) =$$

$$= A\left(\left(r(x)\right)^2+\left(q(x)\right)^2\right)$$

Since $p(x)$ is nonnegative so A should be nonnegative, so

$$p(x) = A\left(\left(r(x)\right)^2+\left(q(x)\right)^2\right) = \left(\sqrt{A}\cdot r(x)\right)^2+\left(\sqrt{A}\cdot q(x)\right)^2.$$

2. A polynomial with real coefficients of 2 variables $p(x,y)$ is always positive. Is it true that it is always bigger then some positive ε?

Solution. No. $p(x,y) = (1-xy)^2 + x^2$ is always positive, since both squares can't be 0 – if $x = 0$ then $1 - xy = 1$.
But if $1 - xy = 0$ and y is very large then x can be very small. Hence the polynomial accepts all positive values.

3. (a) Suppose that a polynomial with integer coefficients is can be decomposed into a product of two polynomials with rational coefficients. Show that it is decomposed into a product of two polynomials with integer coefficients.

(b) Suppose p is a prime number and a polynomial with integer coefficients

$$a_n x^n + a_{n-1}x^{n-1} + a_{n-2}x^{n-2} + \ldots + a_2 x^2 + a_1 x + a_0$$

has the following properties:

a_n is not divisible by p,

$a_{n-1}, a_{n-2}, \ldots, a_2, a_1, a_0$ are divisible by p,

but a_0 is not divisible by p^2.

In this case the polynomial is not decomposable into the product of two polynomials with integer coefficients.

Remark. (a) is called Gauss lemma, (b) – Eisenstein criterion.

Solution. (a) We can multiply our rational factors by an integer numbers so that they will become integer. So product of two integer polynomials is a given polynomial times integer number: $N \cdot s(x) = q(x) \cdot r(x)$.
We want to prove that we can get rid off that integer number. Suppose N has a prime factor p. We shall prove either all coefficients of $q(x)$ or all coefficients of $r(x)$ are divisible by p. So p can be cancelled out, and in this way N can be gradually reduced to 1.
Suppose not all coefficients of $q(x)$ and not all coefficients of $r(x)$ are divisible by p. Let $s(x) = a_n x^n + \ldots + a_2 x^2 + a_1 x + a_0$

$$q(x) = b_k x^k + \ldots + b_2 x^2 + b_1 x + b_0$$
$$r(x) = c_m x^m + \ldots + c_2 x^2 + c_1 x + c_0$$

Let b_v be the first coefficient of $q(x)$ which is not divisible by p, and c_w the first coefficient of $r(x)$ which is not divisible by p. Then $b_v c_w$ is not divisible by p, and for each $j \neq 0$ the number $b_{v+j}c_{w+j}$ is not divisible by p, so na_{v+w} is not divisible by p, which is impossible. QED.

Another way to formulate the solution – look at all those polynomial mod p. You will get $0 = q(x) \cdot r(x) \pmod p$. So either $0 = q(x)$ or $0 = r(x) \pmod p$.

(b) First solution.
Suppose our polynomial $s(x) = a_n x^n + \ldots + a_2 x^2 + a_1 x + a_0$ has a decomposition: $s(x) = q(x) \cdot r(x)$ where

$$q(x) = b_k x^k + \ldots + b_2 x^2 + b_1 x + b_0$$
$$r(x) = c_m x^m + \ldots + c_2 x^2 + c_1 x + c_0$$

So, $a_0 = b_0 c_0$ hence one of the numbers b_0, c_0 is divisible by p but not both. Without loss of generality assume that p divides b_0 and not c_0.
$a_1 = b_0 c_1 + b_1 c_0$ and p divides a_1 and $b_0 c_1$, so p divides also b_1.
$a_2 = b_0 c_2 + b_1 c_1 + b_2 c_0$ and p divides a_2 , $b_0 c_2$, $b_1 c_1$, so p divides also b_2.
And so forth, we proof in k steps that p divides b_k.

But then p would divide $a_n = b_k c_m$, which is impossible. QED.

Second solution. Write everything mod p. You get $a_n x^n = q(x) \cdot r(x) \pmod{p}$. This means only the first coefficient of q and only the first coefficient of r are nonzero mod p. Hence both b_0 and c_0 are divisible by p, so $a_0 = b_0 c_0$ is divisible by p^2.

Definition. A polynomial is called ***irreducible*** if it can't be presented as a product of two polynomials of degree>0. Of course, this definition depends on the field (for example, it can be irreducible over **Q** and split over **R**).

4. Determine whether the following polynomials are irreducible over **Q**:
(a) $2x^3+3x^2+5x+7$
(b) $x^4+19x^2+2x+99$
(c) x^8+x+1
*(d) $x^n+x^{n-1}+\ldots+x^2+x+1$ (here answer depends on n)

Solution. (a) Yes.
If a polynomial of degree 3 is split, the factors are of degrees 1 and 2. Hence it has a root (in the same field over which it splits).
There is a way to find all rational roots of a polynomial. Every rational number has a representation m/n, where m and n are coprime, m integer and n natural. Substitute it into our polynomial:

$$2(m/n)^3+3(m/n)^2+5(m/n)+7 = 0$$

Multiply it by n^{degree}, in our case n^3:

$$2m^3+3m^2n+5mn^2+7n^3 = 0$$

Now you have an equation in integer numbers. All terms in left hand side except the last one are divisible by m, and all terms the first one are divisible by n. So the last term $2m^3$ is divisible by n, and the first term $7n^3$ is divisible by m. But m and n are coprime, hence the 2 is divisible by n and 7 is divisible by m. So there is only finite number of numbers which can possibly be roots: 1, 7, -1, -7, ½ , -½, 7/2, -7/2.

Remark. That's the general principle: if polynomial with integer coefficients has a rational root, its nominator divides the free coefficient and its denominator divides the first coefficient, so the root can be found in finite number of verifications.

In our case, odd integer number is not an option, since value will be odd, and positive numbers are also out of question, so the two remaining possibilities

are -1/2 and -7/2. Of course, first gives positive value and second negative, so this polynomial has no rational roots.

(b) $x^4+19x^2+2x+99 = x^4 + 20x^2 + 100 - x^2 + 2x - 1 = (x^2 + 10)^2 - (x - 1)^2 =$
$= (x^2 + x + 9)(x^2 - x + 11)$

(c) x^8+x+1 . The answer – yes.
Consider number $\omega = \frac{-1+i\sqrt{3}}{2} = "\sqrt[3]{1}"$ (cube of this number is 1).
It is root of polynomial $x^3 - 1$ and since it isn't one it is even a root of $x^2 + x + 1$. But $\omega^8 + \omega + 1 = \omega^2 + \omega + 1 = 0$ so, our polynomial is not co-prime to $x^2 + x + 1$. Their greatest common divisor is a polynomial with coefficient in **Q**, since it is given by Euclidean algorithm, so it is of degree 2 and not 1, so it is $x^2 + x + 1$. Conclusion $x^8 + x + 1$ is divisible by $x^2 + x + 1$.
Perform long division to verify yourself, and you get a decomposition
$x^8 + x + 1 = \left(x^2 + x + 1\right)\left(x^6 - x^5 + x^3 - x^2 + 1\right)$.

(d) $x^n+x^{n-1}+\ldots+x^2+x+1$ is irreducible iff n+1 = p is prime.
If n+1 = k·m then
$x^n+x^{n-1}+\ldots+x^2+x+1 = (x^{(m-1)k}+\ldots+x^{2k}+x^k+1)(x^{k-1}+ x^{k-2}+\ldots+x^2+x+1)$.
The hard part is to prove irreducibility for primes.
The simplest prove uses a trick – shifting by 1. Denote $x = y + 1$.
This transformation doesn't influence irreducibility property. But

$$x^{p-1} + x^{p-2} + \ldots + x + 1 = \frac{x^p - 1}{x - 1} = \frac{(y+1)^p - 1}{y} = \frac{\sum_{j=1}^{p} \binom{p}{j} y^j}{y} = \sum_{j=1}^{p} \binom{p}{j} y^{j-1}$$

So, we have a polynomial with first coefficient 1, last coefficient p and all coefficients in the middle are divisible by p, so it is irreducible by Eisenstein's criterion (3b).

5. Proof that if two polynomials of degree less then N have the same values at N different points, then they coincide.

Solution. The difference of two such polynomials would be a polynomial with N roots, and a polynomial of degree less then N has less than N roots, unless it is constant 0.

Remark. Of course that problem was not a real challenge; it is a hint for the next problem. The inverse problem is bit more interesting: given N distinct points $x_1, x_2, \ldots x_N$, and n arbitrary values, $a_1, a_2, \ldots, a_N$, prove that there exists unique polynomial of degree < N such that $p(x_i) = a_i$. We have proven only uniqueness, there are different proofs for existance, from constructive ones to dimension counting.

6. Given two polynomials $p(z)$, $q(z)$ with complex coefficients. It is also given that for any complex number z ,

$$p(z) = 0 \text{ iff } q(z) = 0$$
$$p(z) = 1 \text{ iff } q(z) = 1$$

Prove that the polynomials are equal.

Solution. We may assume without loss of generality that deg p ≥ deg q.
A point z happens to be a root of multiplicity k of $p(z)$ iff it is a root of $p(z)$ and a root of degree $k - 1$ of polynomial $p'(z)$.
Total number of roots of $p(z)$ with multiplicities is its degree n.
Number of distinct roots of $p(z)$ is n minus total multiplicity of distinct roots of $p(z)$ as roots of $p'(z)$.
Number of distinct roots of $p(z) - 1$ is, for the same reason, n minus sum of multiplicities of roots of $p(z) - 1$ as roots of $p'(z)$. So, number of points in which $p(z)$ is 0 or 1 is at least $2n - \deg(p') = n + 1$.
So, p and q are both polynomials of degree less than $n + 1$, and they coincide in at least n points, hence they are equal.