MATH 298 A1-Sem - Fall 2020

Problem solving seminar

Contents

Wednesday, September 2, 2020

1 Polynomials

A polynomial of degree n with coefficients in $\mathbb{R}$ is a function $f : \mathbb{R} \longrightarrow \mathbb{R}$ given by

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

with $a_0, a_1, \ldots, a_n \in \mathbb{R}$ and $a_n \neq 0$. The set (or ring for those of you who know abstract algebra) of all such polynomials is denoted $\mathbb{R}[x]$. We will also consider polynomials with coefficients in $\mathbb{C}$ (respectively, $\mathbb{Q}$), the set of complex numbers (respectively, the set of rational numbers). These polynomials are defined in the same way and can be viewed as functions $\mathbb{C} \longrightarrow \mathbb{C}$ (respectively, $\mathbb{Q} \longrightarrow \mathbb{Q}$); the set of such polynomials is denoted $\mathbb{C}[x]$ (respectively, $\mathbb{Q}[x]$).

I think that many of you are already familiar with the Binomial Theorem (or Binomial Formula) which gives a formula for the power of a polynomial of degree one.

Theorem 1.1 (Binomial Theorem)**.** *If x and y are two variables (or if x and y are two elements of $\mathbb{R}$ or $\mathbb{C}$ or $\mathbb{Q}$, etc.), then*

$$(x+y)^n = \sum_{k=0}^{n} \binom{n}{k} x^k y^{n-k}.$$

Recall that for any two non-zero integers, we can perform division with remainder. It is possible also to do such division with polynomials.

Theorem 1.2 (Division of polynomials)**.** *Let $F = \mathbb{Q}, \mathbb{R}$ or $\mathbb{C}$. Let $f(x), g(x) \in F[x]$ with $g(x) \neq 0$. Then there exist unique polynomials $q(x), r(x) \in F[x]$ such that*

$$f(x) = g(x)q(x) + r(x)$$

and either $r(x) = 0$ or $\deg(r(x)) < \deg(g(x))$. $r(x)$ is called the remainder.

When $r(x) = 0$, we say that $g(x)$ divides $f(x)$, or that $f(x)$ is a multiple of $g(x)$.

Definition 1.3. *Let $F = \mathbb{R}, \mathbb{C}$ or $\mathbb{Q}$. A root x_0 of a polynomial $f(x)$ in $F[x]$ is an element of F such that $f(x_0) = 0$.*

One basic fact about roots of polynomials is given by the Root-Factor Lemma. You must have used it before even if you did not call it explicitly by this name.

Lemma 1.4 (Root-Factor Lemma)**.** *Let $F = \mathbb{Q}, \mathbb{R}, \mathbb{C}$. Let $f(x)$ be a polynomial in $F[x]$ and $a \in F$. Then $f(a) = 0$ if and only if $f(x) = (x-a)g(x)$ for some polynomial $g(x)$ in $F[x]$.*

Definition 1.5. *Suppose that $f(x) \in F[x]$ and $x_0 \in F$ where $F = \mathbb{Q}, \mathbb{R}$ or $\mathbb{C}$. If x_0 is a root of the polynomial $f(x)$, then x_0 is said to have multiplicity m if $(x - x_0)^m$ divides $f(x)$ in $F[x]$ but $(x - x_0)^{m+1}$ does not divide $f(x)$. In other words, x_0 is a root of multiplicity m if $f(x) = (x - x_0)^m g(x)$ and $g(x_0) \neq 0$.*

You all know the formula for finding the roots of a polynomial of degree 2 in $\mathbb{R}[x]$. I would like to point out that it is also valid over the complex numbers: if $a, b, c \in \mathbb{C}$ and $a \neq 0$, the roots in $\mathbb{C}$ of $ax^2 + bx + c = 0$ are given also by the formula

$$\frac{-b \pm \sqrt{b^2 - 4ac}}{2a}.$$

In particular, this works even when $a, b, c \in \mathbb{R}$ and $b^2 - 4ac < 0$. This raises the question of how to compute the square root of a complex number: we will return to this later, for the moment it is enough to understand that if $d \in \mathbb{R}, d > 0$, then $\sqrt{-d} = \sqrt{d}i$ where $i = \sqrt{-1}$.

There are similar formulas for roots of polynomials of degree 3 and 4 in $\mathbb{C}$, but they are a lot more complicated, so it's not worth trying to learn them by heart. It can also be proved that, for a polynomial of degree $\geqslant 5$, there is no formula for its roots in terms only of the four basic operations $+, -, \cdot, \div$ and radicals (square roots, cubic roots, etc.).

Theorem 1.6 (Fundamental Theorem of Algebra)**.** *Let $f(x)$ be a polynomial in the variable x with complex coefficients, so $f(x) = a_n x^n + a_{n-1} x^{n-1} + \cdots + a_1 x + a_0$ and $a_i \in \mathbb{C}$. (In particular, a_i could be in $\mathbb{R}$.) Suppose that $a_n \neq 0$. Then*

1. *$f(x)$ has at least one root in $\mathbb{C}$, that is, there exists $z \in \mathbb{C}$ such that $f(z) = 0$.*

2. *$f(x)$ can be factored as $f(x) = a_n(x - z_1)(x - z_2) \cdots (x - z_n)$ where $z_i \in \mathbb{C}$ for $i = 1, 2, \ldots, n$.*

More results will be presented later as needed. Now it's time to start looking at examples of problems about polynomials.

Example 1. Solve the equation

$$x^3 - 3x^2 + 4 = 0$$

given that two of its solutions are equal.

Solution: The polynomial $x^3 - 3x^2 + 4$ has degree 3 and its leading coefficient is 1, so it can be factored out as

$$x^3 - 3x^2 + 4 = (x - a)(x - b)(x - c)$$

where a, b and c are its roots in $\mathbb{C}$. (They will eventually turn out to be in $\mathbb{Z}$.) Since two of its roots are equal, we can assume that $b = c$. Expanding the right-hand side of the previous equation, we obtain:

$$x^3 - 3x^2 + 4 = (x - a)(x - b)(x - b) = (x - a)(x^2 - 2bx + b^2) = x^3 - (a + 2b)x^2 + (b^2 + 2ab)x - ab^2.$$

Comparing coefficients of x^2 and x on both sides, and comparing also the constant terms, we see that

$$\begin{aligned} -3 &= -(a+2b), && (1)\\ 0 &= b^2+2ab, && (2)\\ 4 &= -ab^2. && (3) \end{aligned}$$

The last equation shows that $a \neq 0$ and $b \neq 0$, so b can be cancelled in (2):

$$b^2+2ab = 0 \text{ and } b \neq 0 \Longrightarrow b+2a = 0 \Longrightarrow b = -2a.$$

Substituting $b = -2a$ into (1), we obtain $-3 = -a-2b = -a-2\cdot(-2a) = 3a$, so $a = -1$. Since $b = -2a$, $b = 2$.

Finally, it can be checked that

$$x^3-3x^2+4 = (x-(-1))(x-2)(x-2) = (x+1)(x-2)^2.$$

□

Since the roots of the polynomial x^3-3x^2+4 are all rational numbers (actually, integers), that equation can be solved using the Rational Root Test even without knowing that two of its solutions are equal.

Lemma 1.7 (Rational Root Test)**.** *Suppose that $f(x) = a_nx^n + a_{n-1}x^{n-1} + \cdots + a_1x + a_0 \in \mathbb{Z}[x]$, so the coefficients of $f(x)$ are integers. Suppose that $\frac{r}{s} \in \mathbb{Q}$ is a root of $f(x)$, where r and s are relatively prime integers and $s \neq 0$, so $f\left(\frac{r}{s}\right) = 0$ and $\gcd(r,s) = 1$. Then s divides a_n and r divides a_0. In particular, if $f(x)$ is a monic polynomial (that is, $a_n = 1$), then $s = \pm 1$ and $\frac{r}{s} = \pm r \in \mathbb{Z}$.*

Example 2. Apply the Rational Root Test to the polynomial x^3-3x^2+4 from Example 1.

Solution: If $f(x) = x^3-3x^2+4$ as in Example 1, then $a_n = 1$, so $f(x)$ is monic and thus the Rational Root Test tells us that any rational root of $f(x)$ must be an integer r that divides 4. The possible roots for $f(x)$ are thus $\pm 1, \pm 2$ and ± 4. One can then check that $f(-1) = 0$, $f(2) = 0$ and $f(r) \neq 0$ when $r = 1, -2$ and ± 4, so -1 and 2 are the only two roots of $f(x)$ in $\mathbb{Q}$.

The Rational Root Test does not tell us about the multiplicities of these roots though. Since the coefficients of $f(x)$ are all integers and $f(x)$ has two roots in $\mathbb{Z}$, it must actually have three roots in $\mathbb{Z}$, taking multiplicities into account. Therefore, either

$$f(x) = (x+1)^2(x-2) \text{ or } f(x) = (x+1)(x-2)^2.$$

Since $f(x) = x^3-3x^2+4$, it can be checked that the second factorization is the correct one. □

Wednesday, September 9, 2020

Example 3. Let $f(x) = a_n x^n + a_{n-1}x^{n-1} + \cdots + a_1 x + a_0$ with $a_i \in \mathbb{Z}$. Show that $f(x)$ does not have a root in $\mathbb{Z}$ if $f(0)$ and $f(1)$ are both odd.

Solution: $f(0) = a_0$, so a_0 is odd since $f(0)$ is odd.

$f(1) = a_n + a_{n-1} + \cdots + a_1 + a_0$, so $a_n + a_{n-1} + \cdots + a_1 + a_0$ is odd also and $a_n + a_{n-1} + \cdots + a_1$ must be even because a_0 is odd.

The shortest way to complete this solution is to use congruences modulo 2. If you don't know about these, you can skip this paragraph and read the alternative way to write the solution below. If $r \in \mathbb{Z}$, then

$$\begin{aligned} f(r) &= a_n r^n + a_{n-1}r^{n-1} + \cdots + a_1 r + a_0 \\ &\equiv a_n r + a_{n-1} r + \cdots + a_1 r + a_0 \bmod 2 \text{ since } r^k \equiv r \bmod 2 \text{ for all } k \geqslant 1; \\ &\equiv (a_n + a_{n-1} + \cdots + a_1) r + a_0 \bmod 2 \\ &\equiv a_0 \bmod 2 \text{ since } a_n + a_{n-1} + \cdots + a_1 \text{ is even;} \\ &\equiv 1 \bmod 2 \text{ since } a_0 \text{ is odd.} \end{aligned}$$

This proves that $f(r) \neq 0$, so the polynomial $f(x)$ does not have a root in $\mathbb{Z}$.

If you want to avoid congruences modulo 2, then it is possible to replace the computations in the previous paragraph by the following observation about multiplication of integers:

$$\text{even} \cdot \text{even} = \text{even}, \quad \text{even} \cdot \text{odd} = \text{even}, \quad \text{odd} \cdot \text{odd} = \text{odd}.$$

Therefore, if r is an even integer, then $a_i r^i$ is even for all i and $a_n r^n + a_{n-1}r^{n-1} + \cdots + a_1 r$ is even, so $a_n r^n + a_{n-1}r^{n-1} + \cdots + a_1 r + a_0$ is odd because a_0 is odd.

If r is odd, then $a_i r^i$ has the same parity as a_i: if a_i is even, $a_i r^i$ is even and if a_i is odd, then $a_i r^i$ is also odd. It follows that $a_n r^n + a_{n-1}r^{n-1} + \cdots + a_1 r$ has the same parity as $a_n + a_{n-1} + \cdots + a_1$, which is even, as observed above. Since a_0 is odd, $a_n + a_{n-1} + \cdots + a_1 + a_0$ is odd, hence $a_n r + a_{n-1} r + \cdots + a_1 r + a_0$ is odd and $f(r)$ is odd.

In conclusion, since $f(r)$ is always odd when r is an integer, $f(r)$ is never 0. □

By the Root-Factor Lemma, if $f(x_0) = 0$, then x_0 has multiplicity at least 1. There is a way to detect the multiplicity of a root using derivatives. For instance, if x_0 is a root of multiplicity 2 so that $f(x) = (x - x_0)^2 g(x)$ with $g(x_0) \neq 0$, then

$$f'(x) = 2(x - x_0)g(x) + (x - x_0)^2 g'(x), \quad f'(x_0) = 0,$$

and

$$f''(x) = 2g(x) + 4(x - x_0)g'(x) + (x - x_0)^2 g''(x), \quad f'(x_0) = 2g(x_0) \neq 0,$$

so x_0 is a root of $f'(x)$ but not of $f''(x)$. In general, we have the following result.

Lemma 1.8. *Suppose that $f(x) \in F[x]$ and $x_0 \in F$ where $F = \mathbb{Q}, \mathbb{R}$ or $\mathbb{C}$. Then x_0 is a root of $f(x)$ of multiplicity $m \iff f^{(k)}(x_0) = 0$ for $0 \leqslant k \leqslant m-1$ and $f^{(m)}(x_0) \neq 0$. Here, $f^{(k)}(x)$ is the k^{th}-derivative of $f(x)$ and, by convention, $f^{(0)}(x) = f(x)$.*

Example 4. Let $f(x) = x^n - nx + n - 1$, $n > 1$. What is the multiplicity of 1 as a root of $f(x)$?

Solution: $f'(x) = nx^{n-1} - n$ and $f'(1) = n - n = 0$, so 1 has multiplicity at least 2.

$f''(x) = n(n-1)x^{n-2}$, so $f''(1) \neq 0$ because $n > 1$: this implies that the multiplicity of 1 is at most 2. In conclusion, it must be exactly 2. □

Example 5. Let $f(x) = nx^{n+1} - (n+1)x^n + 1$. Show that $(x-1)^2$ divides $f(x)$.

Solution: Showing that $(x-1)^2$ divides $f(x)$ is the same as proving that 1 is a root of $f(x)$ of multiplicity $\geqslant 2$.

It is enough to check that $f'(1) = 0$.

$$f'(x) = n(n+1)x^n - (n+1)nx^{n-1} = n(n+1)x^{n-1}(x-1),$$

so $f'(1) = 0$.

1 is a root of multiplicity exactly 2 since

$$f''(x) = n(n+1)(n-1)x^{n-2}(x-1) + n(n+1)x^{n-1} = n(n+1)x^{n-2}((n-1)(x-1) + x)$$

and $f''(1) = n(n+1) \neq 0$. □

Example 6. Set

$$f(x) = 1 + x + \frac{x^2}{2!} + \frac{x^3}{3!} + \cdots + \frac{x^{n-1}}{(n-1)!} + \frac{x^n}{n!}.$$

Show that the polynomial $f(x)$ does not have a root of multiplicity $\geqslant 2$.

Solution: Suppose that x_0 is a root of $f(x)$, so $f(x_0) = 0$. x_0 has multiplicity exactly one if $f'(x_0) \neq 0$.

$$f'(x) = 0 + 1 + \frac{2x}{2!} + \frac{3x^2}{3!} + \cdots + \frac{nx^{n-1}}{n!} = 1 + x + \frac{x^2}{2!} + \cdots + \frac{x^{n-1}}{(n-1)!},$$

so $f'(x) = f(x) - \frac{x^n}{n!}$. Therefore,

$$f'(x_0) = f(x_0) - \frac{x_0^n}{n!} = -\frac{x_0^n}{n!}.$$

$x_0 \neq 0$ since $f(0) = 1$ and $f(x_0) = 0$. Therefore, $f'(x_0) = -\frac{x_0^n}{n!} \neq 0$, so x_0 has multiplicity exactly one. □

Wednesday, September 16, 2020

There are very explicit relations between the roots of a polynomial and the coefficients of a polynomial. Let $f(x) = a_n x^n + a_{n-1}x^{n-1} + \cdots + a_1 x + a_0$ be a polynomial in $F[x]$ where $F = \mathbb{Q}, \mathbb{R}$ or $\mathbb{C}$. Actually, since $\mathbb{Q} \subset \mathbb{R} \subset \mathbb{C}$, we can just assume that $f(x) \in \mathbb{C}[x]$. Moreover, let's assume that $f(x)$ is monic, so $a_n = 1$. By the Fundamental Theorem of Algebra, $f(x)$ can be decomposed as

$$f(x) = a_n x^n + a_{n-1}x^{n-1} + \cdots + a_1 x + a_0 = (x - z_1)(x - z_2)\cdots(x - z_n) \tag{4}$$

where $z_1, \ldots, z_n \in \mathbb{C}$ are its roots. The constant term on the right-hand side of (4) is $(-1)^n z_1 z_2 \cdots z_n$, so

$$a_0 = (-1)^n z_1 z_2 \cdots z_n. \text{ (Just set } x = 0 \text{ on both sides of (4).)}$$

At the other end, the coefficient of x^{n-1} is $-z_1 - z_2 - \cdots - z_n$, so

$$a_{n-1} = -z_1 - z_2 - \cdots - z_n.$$

To see this, not that, when expanding the right-hand side of (4), to obtain a multiple of x^{n-1}, you should select x in all the factors except one and for this factor you select the constant $-z_i$. If, instead, we select x in just one factor (say in $(x - z_i)$) and the constants $-z_j$ in all the other factors (so for $j \neq i$), then we obtain $a_1 x$, so

$$a_1 = (-1)^{n-1} z_1 z_2 \cdots z_n \left(\frac{1}{z_1} + \frac{1}{z_2} + \cdots + \frac{1}{z_n} \right).$$

The coefficient of x^{n-2} is

$$z_1 z_2 + \cdots + z_1 z_n + z_2 z_3 + \cdots + z_2 z_n + z_3 z_4 + \cdots + z_{n-1} z_n.$$

To see this, observe that, when expanding the right-hand side of (4), to obtain a multiple of x^{n-2}, you should select x in all the factors except two and for these two factors you select the constants $-z_i$ and $-z_j$ whose product is $z_i z_j$.

There are similar formulas for all the coefficients a_i which are called Viète's formulas:

$$\text{For } k = 0, 1, \ldots, n-1,\ a_{n-k} = (-1)^k \sum_{1 \leqslant i_1 < i_2 < \cdots < i_k \leqslant n} z_{i_1} z_{i_2} \cdots z_{i_k}.$$

What these formulas show is that the coefficients of $f(x)$ are polynomial functions of the roots of $f(x)$:

$$a_k = p_k(z_1, z_2, \ldots, z_n).$$

Moreover, these are symmetric polynomials in the sense that switching two variables in the polynomials doesn't change it:

$$a_k = p_k(z_1, \ldots, z_i, \ldots, z_j, \ldots, z_n) = p_k(z_1, \ldots, z_j, \ldots, z_i, \ldots, z_n).$$

This follows from the fact that the factors in (4) can be reordered and their product is still the same polynomial $f(x)$. The symmetry property can be seen directly for the formulas for $p_k(z_1, z_2, \ldots, z_n)$ when $k = 0, 1, n-1, n-2$ given above.

Symmetric polynomials are the polynomials invariant under permutations of the variables and are important in representation theory, combinatorics, algebraic geometry, etc. (Permutations are a central notion in group theory and you'll learn about them if you take MATH 328.)

Knowing how roots are related to coefficients can allow us to deduce formulas involving the roots even if we don't know what the roots are precisely. This is illustrated in the following examples.

Example 7. Let z_1, z_2, z_3 be the roots of $x^3 + 4x^2 + 8x + 3$.

(a) Find $\frac{1}{z_1} + \frac{1}{z_2} + \frac{1}{z_3}$.

(b) Determine $z_1^2 + z_2^2 + z_3^2$.

(c) Evaluate $(z_1 + z_2)(z_2 + z_3)(z_3 + z_1)$.

Solution: (a) Recall the formula above for a_1, which is:

$$a_1 = (-1)^{n-1} z_1 z_2 \cdots z_n \left(\frac{1}{z_1} + \frac{1}{z_2} + \cdots + \frac{1}{z_n} \right).$$

The product of the roots $z_1 z_2 \cdots z_n$ is equal to $(-1)^n a_0$, so

$$a_1 = -a_0 \left(\frac{1}{z_1} + \frac{1}{z_2} + \cdots + \frac{1}{z_n} \right).$$

In this particular example, $n = 3$, $a_1 = 8$ and $a_0 = 3$, so

$$8 = -3 \left(\frac{1}{z_1} + \frac{1}{z_2} + \frac{1}{z_3} \right)$$

and

$$\frac{1}{z_1} + \frac{1}{z_2} + \frac{1}{z_3} = -\frac{8}{3}.$$

(b) From Viete's formulas, we know that

$$x_1 + x_2 + x_3 = -4 \text{ and } x_1x_2 + x_2x_3 + x_3x_1 = 8, \tag{5}$$

but those formulas don't tell us anything about $x_1^2 + x_2^2 + x_3^2$, at least not directly. What we need is a way to relate $x_1^2 + x_2^2 + x_3^2$ to $x_1 + x_2 + x_3$ and to $x_1x_2 + x_2x_3 + x_3x_1$.

Let's try first the easier problem of relating $x_1^2 + x_2^2$ to $x_1 + x_2$ and to x_1x_2 :

$$(x_1 + x_2)^2 = x_1^2 + 2x_1x_2 + x_2^2, \text{ so } x_1^2 + x_2^2 = (x_1 + x_2)^2 - 2x_1x_2.$$

This suggests that we should consider $(x_1 + x_2 + x_3)^2$:

$$(x_1 + x_2 + x_3)^2 = (x_1 + x_2 + x_3)(x_1 + x_2 + x_3) = x_1^2 + x_2^2 + x_3^2 + 2x_1x_2 + 2x_2x_3 + 2x_3x_1,$$

so

$$(x_1 + x_2 + x_3)^2 - 2(x_1x_2 + x_2x_3 + x_3x_1) = x_1^2 + x_2^2 + x_3^2.$$

Therefore, from (5), it follows that

$$(-4)^2 - 2 \cdot 8 = x_1^2 + x_2^2 + x_3^2, \;\; 0 = x_1^2 + x_2^2 + x_3^2.$$

How can this be possible? If $x_1, x_2, x_3 \in \mathbb{R}$, then $x_1^2 + x_2^2 + x_3^2 = 0$ exactly when $x_1 = 0 = x_2 = x_3$; however, 0 is not a root of $x^3 + 4x^2 + 8x + 3$. The explanation is that two of x_1, x_2, x_3 are complex numbers (with non-zero imaginary parts). Recall that, since $x^3 + 4x^2 + 8x + 3$ has degree 3, it is known from calculus that it must have at least one root in $\mathbb{R}$.

(c) Since $a_2 = -(z_1 + z_2 + z_3)$ and $a_2 = 4$, it follows that $z_1 + z_2 = -z_3 - 4$, $z_2 + z_3 = -z_1 - 4$ and $z_3 + z_1 = -z_2 - 4$. Therefore, we have to evaluate

$$-(z_1 + 4)(z_2 + 4)(z_3 + 4),$$

so let's expand this:

$$\begin{aligned} -(z_1 + 4)(z_2 + 4)(z_3 + 4) &= -z_1z_2z_3 - 4(z_1z_2 + z_2z_3 + z_3z_1) - 16(z_1 + z_2 + z_3) - 64 \\ &= 3 - 4 \cdot 8 - 16 \cdot (-4) - 64 \text{ by Viète's formulas;} \\ &= -29 \end{aligned}$$

□

In Linear Algebra I, you learned how to find all the solutions of any system of linear equations. When the equations are not all linear, finding all the exact solutions is, in general, an impossible task. The next example is an exception and can be solved quickly using a clever observation.

Example 8. Solve the following system of polynomial equations in three variables:

$$x_1 + x_2 + x_3 = -3, \; x_1x_2 + x_2x_3 + x_3x_1 = 3, \;\; x_1x_2x_3 = -1.$$

Solution: By Viete's formulas, those equations are satisfied by the roots of the polynomial $x^3 + 3x^2 + 3x + 1$. By the Binomial Formula, this polynomial is equal to $(x + 1)^3$. Therefore,

$$(x + 1)^3 = (x + 1)(x + 1)(x + 1) = (x - x_1)(x - x_2)(x - x_3)$$

and it follows that the only solution is $x_1 = -1, x_2 = -1$ and $x_3 = -1$. □

As pointed out above, the polynomials in Viète's formulas are symmetric polynomials. A polynomial $f(x_1, \ldots, x_n)$ in n variables is said to be symmetric if

$$f(x_1, \ldots, x_i, \ldots, x_j, \ldots, x_n) = f(x_1, \ldots, x_j, \ldots, x_i, \ldots, x_n)$$

for any two distinct indices i and j. In other words, replacing x_i by x_j and x_j by x_i does not change the polynomial. For instance, the following polynomials are symmetric:

$$x_1x_2,\ x_1^2x_2 + x_1x_2^2,\ \ x_1^3x_2^3,\ \ x_1^2 + x_2^2 + x_3^2.$$

The notion of symmetry is important in mathematics and not just in geometry, but also in algebra. Even for polynomials, it can have more than one meaning. For instance, a polynomial $f(x)$ such that $f(-x) = f(x)$ can be viewed as symmetric with respect to the origin: actually, its values are symmetric with respect to the origin 0. In this case, $f(x)$ must be a polynomial with even powers of x only.

Example 9. Let $f(x) = (1 - x + x^2 - \cdots + x^{100})(1 + x + x^2 + \cdots + x^{100})$. Show that, after multiplying and collecting terms, only even powers of x will remain.

Solution: Observe that $f(-x) = (1+x+x^2+\cdots+x^{100})(1-x+x^2-\cdots+x^{100}) = f(x)$. This means that the polynomial $f(x)$ cannot contain odd powers of x with non-zero coefficients because $x^k \neq (-x)^k$ if k is odd. Therefore, $f(x)$ is a polynomial in x^2: in other words, only even powers of x remain in $f(x)$ after multiplying the two polynomials of degree 100. □

In general, if $g(x)$ is any polynomial and $f(x) = g(-x)g(x)$, then $f(x)$ is a polynomial in x^2, that is, with only even powers of x.

Wednesday, September 23, 2020

There is also the related notion of anti-symmetry, as defined in the next example.

Example 10. A polynomial $f(x, y)$ is antisymmetric if $f(x, y) = -f(y, x)$. Prove that every antisymmetric polynomial $f(x, y)$ has the form $f(x, y) = (x - y)g(x, y)$ where $g(x, y)$ is symmetric.

Solution: Let's divide $f(x, y)$ by $x - y$ with remainder $h(y)$, so

$$f(x, y) = (x - y)g(x, y) + h(y).$$

To see this, consider a monomial x^iy^j in $f(x, y)$, write x as $(x - y) + y$ and expand $((x - y) + y)^iy^j$ using the Binomial Formula:

$$\left(\sum_{k=0}^{i} \binom{k}{i} (x - y)^k y^{k-i}\right) y^j.$$

This shows that any monomial $x^i y^j$ can be replaced by a monomial in $(x-y)$ and y. Taking all those with $(x-y)^k$ and $k \geqslant 1$ gives the polynomial $(x-y)g(x,y)$. The remaining polynomials involve only y and form $h(y)$.

Then $f(x,y) = -f(y,x)$ and $f(x,y) = (x-y)g(x,y) + h(y) \Longrightarrow$

$$(x-y)g(x,y) + h(y) = -(y-x)g(y,x) - h(x). \tag{6}$$

Let us set $y = x$ to obtain $h(y) = -h(y)$, so $h(y) = 0$ and $f(x,y) = (x-y)g(x,y)$. Moreover, (6) now becomes $(x-y)g(x,y) = -(y-x)g(y,x)$, which simplifies to $g(x,y) = g(y,x)$: this means that $g(x,y)$ is a symmetric polynomial. □

Example 11. If the polynomial $f(x,y)$ is symmetric and $x-y$ divides $f(x,y)$, show that $(x-y)^2$ divides $f(x,y)$.

Solution: $x-y$ divides $f(x,y) \Longrightarrow f(x,y) = (x-y)h(x,y)$ for some polynomial $h(x,y)$.

$f(x,y)$ is symmetric $\Longrightarrow f(x,y) = f(y,x) \Longrightarrow (x-y)h(x,y) = (y-x)h(y,x) \Longrightarrow h(x,y) = -h(y,x)$, so $h(x,y)$ is anti-symmetric. By the previous example applied to $h(x,y)$ instead of $f(x,y)$, it follows that $h(x,y) = (x-y)g(x,y)$ for some symmetric polynomial $g(x,y)$.

$f(x,y) = (x-y)h(x,y)$ and $h(x,y) = (x-y)g(x,y) \Longrightarrow f(x,y) = (x-y)^2 g(x,y)$. □

Laurent polynomials are polynomials where negative powers of x are allowed. A Laurent polynomial can thus be written as

$$\begin{aligned}\sum_{i=-m}^{n} a_i x^i &= a_{-m}x^{-m} + a_{-m+1}x^{-m+1} + \cdots + a_{-1}x^{-1} + a_0 + \cdots + a_{n-1}x^{n-1} + a_n x^n \\ &= x^{-m}(a_{-m} + a_{-m+1}x + \cdots + a_{-1}x^{m-1} + a_0 x^m + \cdots + a_{n-1}x^{m+n-1} + a_n x^{m+n})\end{aligned}$$

For Laurent polynomials, we can consider a new symmetry, namely the map $x \leftrightarrow \frac{1}{x}$, and the polynomials that are invariant under this map. The Laurent polynomials $f(x)$ such that $f(x) = f\left(\frac{1}{x}\right)$ are called palindromic. (Recall that a palindrome is a word that reads backwards the same as forwards, e.g. radar, level.) More explicitly, a palindromic Laurent polynomial is of the form

$a_{-n}x^{-n} + a_{-n+1}x^{-n+1} + \cdots + a_{-1}x^{-1} + a_0 + a_1 x + \cdots + a_{n-1}x^{n-1} + a_n x^n$ where $a_i = a_{-i}$, $0 \leqslant i \leqslant n$.

For instance,

$$2x^4 + 5x^3 - 2x + 4 - 2x^{-1} + 5x^{-3} + 2x^{-4}$$

is a palindromic Laurent polynomial. It is also possible to talk about an ordinary polynomial $a_0 + a_1 x + a_2 x^2 + \cdots + a_{n-1}x^{n-1} + a_n x^n$ being palindromic if $a_k = a_{n-k}$ for $0 \leqslant k \leqslant n$, e.g. $x^5 + 6x^4 - 4x^3 - 4x^2 + 6x + 1$.

One way to obtain a palindromic Laurent polynomial is via $g\left(x+\frac{1}{x}\right)$ where $g(x)$ is an ordinary polynomial. Actually, any palindromic Laurent polynomial is of this form as the next example shows (although it is stated for palindromic ordinary polynomials).

Example 12. Let $f(x)=\sum_{i=0}^{n} a_i x^i$ be a palindromic polynomial. Show that

1. $x^n f\left(\frac{1}{x}\right)=f(x)$
2. If n is even, $f(x)=x^{\frac{n}{2}} g\left(x+\frac{1}{x}\right)$ for some ordinary polynomial $g(x)$ of degree $\frac{n}{2}$.

Solution: Since $f(x)$ is palindromic, $a_i=a_{n-i}$ for $i=0,1,\ldots,n$. Therefore,

$$\begin{aligned} x^n f\left(\frac{1}{x}\right) &= x^n \sum_{i=0}^{n} a_i x^{-i} = \sum_{i=0}^{n} a_i x^{n-i} \\ &= \sum_{i=0}^{n} a_{n-i} x^{n-i} \text{ since } a_i = a_{n-i}; \\ &= \sum_{k=0}^{n} a_j x^j \text{ after setting } j = n-i; \\ &= f(x) \end{aligned}$$

This proves the first identity.

The proof of the second statement is by induction on the degree of $f(x)$. Since n is even, $n=2m$ with $m \in \mathbb{Z}_{>0}$. Since $f(x)$ is palindromic, $x^{-m} f(x)$ is a palindromic Laurent polynomial, $a_n=a_0$ and

$$x^{-m} f(x) - a_n \left(x+\frac{1}{x}\right)^m$$

is also a palindromic Laurent polynomial. Let's denote it by $\widetilde{f}(x)$. The powers of x appearing in $x^m \widetilde{f}(x)$ are x^j with $1 \leqslant j \leqslant n-1$, so $x^m \widetilde{f}(x) = x h(x)$ for some polynomial $h(x)$ of degree $n-2$. Moreover, $h(x)$ is also palindromic since its coefficients are $a_{n-1},\ldots,a_1$, with a_1 its constant term. By induction, it follows that

$$h(x) = x^{\frac{n-2}{2}} k\left(x+\frac{1}{x}\right) \text{ for some ordinary polynomial } k(x) \text{ of degree } \frac{n-2}{2}.$$

Therefore,

$$\begin{aligned} x^{-m} f(x) - a_n \left(x+\frac{1}{x}\right)^m &= \widetilde{f}(x) = x^{-m+1} h(x) \\ &= x^{-m+1} x^{\frac{n-2}{2}} k\left(x+\frac{1}{x}\right) \\ &= x^{-m+1} x^{m-1} k\left(x+\frac{1}{x}\right) \\ &= k\left(x+\frac{1}{x}\right) \end{aligned}$$

It follows that

$$x^{-m}f(x) = a_n\left(x + \frac{1}{x}\right)^m + k\left(x + \frac{1}{x}\right)$$

and thus

$$f(x) = x^m g\left(x + \frac{1}{x}\right)$$

where

$$g(x) = a_n x^m + k(x).$$

□

If $f(x)$ is a palindromic polynomial of odd degree, say of degree $n = 2k + 1$, then

$$f(-1) = \sum_{i=0}^{n} a_i(-1)^i = \sum_{i=0}^{k}(a_i(-1)^i + a_{n-i}(-1)^{n-i}) = \sum_{i=0}^{k}(a_i - a_{n-i})(-1)^i = 0$$

because $a_i = a_{n-i}$ and $(-1)^n = -1$. This shows that $f(x)$ has a root on the unit circle, namely the root -1. When the degree of $f(x)$ is even, it is still true, but more complicated to show, that $f(x)$ still has at least one root on the unit circle. We will return to this in the section on complex numbers.

Example 13 Let

$$f(x) = x^6 - x^4 + 2x^3 - x^2 + 1.$$

(a) Prove that $f(x)$ has no positive real roots.

Solution: It is not at all clear how to start. It seems that we need to compare the size of powers of x. Recall that if $m \leqslant n$, then $x^n \leqslant x^m$ when $0 \leqslant x \leqslant 1$ and $x^m \leqslant x^n$ when $x \geqslant 1$.

Therefore, if $x \geqslant 1$, then $x^6 - x^4 \geqslant 0$ and $x^3 - x^2 \geqslant 0$, so $f(x) = (x^6 - x^4) + x^3 + (x^3 - x^2) + 1 > 0$ if $x \geqslant 1$.

What if $0 \leqslant x < 1$? Then $x^3 - x^4 \geqslant 0$ and $1 - x^2 \geqslant 0$, so $f(x) = x^6 + (-x^4 + x^3) + x^3 + (-x^2 + 1) > 0$ also in this case.

□

(b) Determine a nonzero polynomial $g(x)$ of minimum degree for which all the coefficients of $f(x)g(x)$ are non-negative rational numbers.

Solution: Let see if there is a polynomial of degree one for which all the coefficients of $f(x)g(x)$ are non-negative rational numbers. We can assume that this polynomial is of the

form $x + a$ with $a \in \mathbb{Q}$.

$$\begin{aligned}(x+a)f(x) &= x^7 - x^5 + 2x^4 - x^3 + x + ax^6 ax^4 + 2ax^3 ax^2 + a \\ &= x^7 + ax^6 x^5 + (2-a)x^4 + (2a-1)x^3 ax^2 + x + a\end{aligned}$$

Looking for instance at the coefficient of x^5, we can see that it is impossible for all the coefficients of this polynomial to be non-negative.

Let's try instead a polynomial of degree two, which we can assume is monic, so equal to $x^2 + ax + b$ for some $a, b, \in \mathbb{Q}$.

$$\begin{aligned}(x^2+ax+b)f(x) &= x^8 - x^6 + 2x^5 - x^4 + x^2 + ax^7 - ax^5 + 2ax^4 - ax^3 + ax \\ &\quad + bx^6 - bx^4 + 2bx^3 - bx^2 + b \\ &= x^8 + ax^7 + (b-1)x^6 + (2-a)x^5 + (2a-b-1)x^4 \\ &\quad + (2b-a)x^3 + (1-b)x^2 + ax + b\end{aligned}$$

In order for all the coefficients to be non-negative rational numbers, the following inequalities must hold:

$$b - 1 \geqslant 0,\ 2 - a \geqslant 0,\ 2a - b - 1 \geqslant 0,\ 2b - a \geqslant 0,\ 1 - b \geqslant 0,\ a \geqslant 0,\ b \geqslant 0$$

The inequalities $b - 1 \geqslant 0$ and $1 - b \geqslant 0$ can only hold when $b = 1$, in which case the other inequalities become

$$2 \geqslant a,\ 2a - 1 - 1 \geqslant 0,\ 2 - a \geqslant 0,\ a \geqslant 0.$$

These are satisfied when $1 \leqslant a \leqslant 2$.

In conclusion, $g(x)$ can be any quadratic polynomial $x^2 + ax + 1$ with $1 \leqslant a \leqslant 2$. For instance, if $a = 2$, then $g(x) = (x + 1)^2$. □

It can be proved, more generally, that for any polynomial $f(x)$ in $\mathbb{R}[x]$ there exists a polynomial $g(x)$ for which all the coefficients of $f(x)g(x)$ are non-negative if and only if $f(x)$ does not have a positive root.

Wednesday, September 30, 2020

Powers of $x + 1$ are palindromic:

$$(x+1)^n = \sum_{k=0}^{n} \binom{n}{k} x^k \text{ and } \binom{n}{k} = \binom{n}{n-k}.$$

It can be useful to know the values of $\binom{n}{k}$ when k and n are small, as the next example about palindromic polynomials shows.

Example 14 Solve the equation $z^8 + 4z^6 - 10z^4 + 4z^2 + 1 = 0$.

Solution: Since there are only even powers of z, let's set $x = z^2$, so the equation becomes

$$x^4 + 4x^3 - 10x^2 + 4x + 1 = 0 \tag{7}$$

and the solutions of the original equation are the square roots of the solutions of the latter equation.

This second equation should make you think of the binomial expansion of $(x+1)^4$, which is:

$$(x+1)^4 = x^4 + \binom{4}{3}x^3 + \binom{4}{2}x^2 + \binom{4}{1}x + 1 = x^4 + 4x^3 + 6x^2 + 4x + 1.$$

The only difference is the coefficient of x^2 and $-10x^2 = 6x^2 - 16x^2$, so we can rewrite equation (7) as

$$(x+1)^4 - 16x^2 = 0,$$

which is equivalent to

$$(x+1)^4 = 16x^2.$$

Taking square roots on both sides leads to the two equations

$$(x+1)^2 = 4x \text{ and } (x+1)^2 = -4x.$$

These are two quadratic equations which can be solved as usual:

$$(x+1)^2 = 4x \Leftrightarrow x^2 + 2x + 1 = 4x \Leftrightarrow x^2 - 2x + 1 = 0 \Leftrightarrow (x-1)^2 = 0 \Leftrightarrow x = 1$$

and

$$(x+1)^2 = -4x \Leftrightarrow x^2 + 2x + 1 = -4x \Leftrightarrow x^2 + 6x + 1 = 0 \Leftrightarrow x = \frac{-6 \pm \sqrt{6^2 - 4}}{2} = -3 \pm 2\sqrt{2}.$$

The solutions of the original equations are obtained by taking the square roots of the solutions of (7), so they are ± 1, $\pm(-3+2\sqrt{2})^{\frac{1}{2}}$ and $\pm(-3-2\sqrt{2})^{\frac{1}{2}}$. Notice that $-3+2\sqrt{2}$ and $-3-2\sqrt{2}$ are both < 0, so taking their square roots involves using complex numbers. This will be our next topic, so if you don't know or don't recall how you can take the square root of a complex numbers, don't worry, we'll review this in the next section. □

If you take a course like MATH 228 or MATH 326, you will learn that there are similarities between the ring of integers and the ring of polynomials with coefficients in $\mathbb{Q}, \mathbb{R}$ or $\mathbb{C}$. One common property is the possibility to do division with remainder: see Theorem 1.2. When $f(x) = g(x)q(x)$, that is, when the remainder is zero, we say that the polynomial $g(x)$ divides $f(x)$ or that $f(x)$ is a multiple of $g(x)$. A similar definition is applicable to polynomials in many variables: for instance, $g(x, y, z)$ divides $f(x, y, z)$ if there exists a polynomial $h(x, y, z)$ such that $f(x, y, z) = g(x, y, z)h(x, y, z)$, and we can also say, in this case, that $f(x, y, z)$ is a multiple of $g(x, y, z)$.

It is useful to know some polynomial identities about factorization of polynomials. For instance:

$$x^2-1=(x-1)(x+1),\ x^3-1=(x-1)(x^2+x+1),$$
$$x^n-1=(x-1)(x^{n-1}+x^{n-2}+x^{n-3}+\cdots+x^2+x+1),$$
$$\text{If } n \text{ is odd: } x^n+1=(x+1)(x^{n-1}-x^{n-2}+\cdots-x+1)$$

More generally, the following identities hold:

$$x^2-y^2=(x-y)(x+y),\ x^3-y^3=(x-y)(x^2+xy+y^2),$$
$$x^n-y^n=(x-y)(x^{n-1}+x^{n-2}y+\cdots+xy^{n-2}+y^{n-1})$$
$$\text{If } n \text{ is even, } n=2m\text{: } x^n-y^n=(x^{2m}-y^{2m})=(x^m-y^m)(x^m+y^m),$$
$$\text{If } n \text{ is odd: } x^n+y^n=(x^n-(-y)^n)=(x+y)(x^{n-1}-x^{n-2}y+\cdots-xy^{n-2}+y^{n-1})$$

Example 15 For which n does x^2+x+1 divide $x^{2n}+x^n+1$?

Solution: There is a solution that involves complex numbers, but let's keep it for later. Instead, let's start by recalling that

$$x^3-1=(x-1)(x^2+x+1).$$

This suggests that the answer may be related to the residue of n modulo 3. Let's consider three different cases: $n\equiv 0,1,2 \bmod 3$. Moreover, $x^3\equiv 1 \bmod x^2+x+1$.

Case 1: $n\equiv 0 \bmod 3$, $n=3m$.

$$\begin{aligned}x^{2n}+x^n+1=x^{6m}+x^{3m}+1&=(x^3)^{2m}+(x^3)^m+1\\&\equiv 1^{2m}+1^m+1\equiv 3 \bmod x^2+x+1.\end{aligned}$$

Therefore, in this case, x^2+x+1 does not divide $x^{2n}+x^n+1$.

Case 2: $n\equiv 1 \bmod 3$, $n=3m+1$.

$$\begin{aligned}x^{2n}+x^n+1=x^{6m+2}+x^{3m+1}+1&=(x^3)^{2m}\cdot x^2+(x^3)^m\cdot x+1\\&\equiv 1^{2m}\cdot x^2+1^m\cdot x+1\equiv 0 \bmod x^2+x+1.\end{aligned}$$

Therefore, in this case, x^2+x+1 divides $x^{2n}+x^n+1$.

Case 3: $n\equiv 2 \bmod 3$, $n=3m+2$.

$$\begin{aligned}x^{2n}+x^n+1=x^{6m+4}+x^{3m+2}+1&=(x^3)^{2m+1}\cdot x+(x^3)^m\cdot x^2+1\\&\equiv 1^{2m+1}\cdot x+1^m\cdot x^2+1\equiv 0 \bmod x^2+x+1.\end{aligned}$$

Therefore, in this case also, x^2+x+1 divides $x^{2n}+x^n+1$. □

Wednesday, October 7, 2020

Example 16. Find all positive integers n such that the polynomial $(x^4-1)^n+(x^2-x)^n$ is divisible by x^5-1 in $\mathbb{R}[x]$.

Solution:

$$\begin{aligned}(x^4-1)^n+(x^2-x)^n &= (x-1)^n(x^3+x^2+x+1)^n+(x-1)^n x^n\\ &= (x-1)^n((x^3+x^2+x+1)^n+x^n)\end{aligned}$$

and $x^5-1=(x-1)(x^4+x^3+x^2+x+1)$. $x-1$ always divides $(x-1)^n$. Therefore, the problem reduces to determining the positive integers n for which $(x^3+x^2+x+1)^n+x^n$ is divisible by $x^4+x^3+x^2+x+1$.

Set $f(x)=x^4+x^3+x^2+x+1$. Then

$$(x^3+x^2+x+1)^n+x^n=(f(x)-x^4)^n+x^n\equiv(-x^4)^n+x^n\equiv x^n((-x^3)^n+1) \bmod f(x).$$

$f(x)$ does not divide x^n, so we are left to determine for which n $f(x)$ divides $(-x^3)^n+1$, that is, for which n the polynomial $f(x)$ divides $(-1)^n x^{3n}+1$.

Recall that $(x-1)f(x)=x^5-1$, so $f(x)$ divides x^5-1. Moreover,

$$x^{5m}-1=(x^5)^m-1=(x^5-1)(x^{5(m-1)}+x^{5(m-2)}+\cdots+x^5+1),$$

so $f(x)$ divides x^{5m-1} for any integer $m\geqslant 1$. Using congruences, this means that

$$x^{5m}-1\equiv 0 \bmod f(x),\ \text{hence } x^{5m}\equiv 1 \bmod f(x).$$

This suggests that we should consider the residue of $3n$ modulo 5 and the parity of n.

Let us write $3n=5k+\ell$ with $0\leqslant\ell\leqslant 4$ and let's try to find the values of k and ℓ for which $f(x)$ divides $(-1)^n x^{3n}+1$.

$$(-1)^n x^{3n}+1\equiv(-1)^{3n}x^{5k+\ell}+1\equiv(-1)^{5k+\ell}x^\ell+1\equiv(-1)^{k+\ell}x^\ell+1 \bmod f(x).$$

If $\ell=1,2,3$, then $(-1)^{k+\ell}x^\ell+1$ is a polynomial of degree <3, hence is not divisible by $f(x)$ which is a polynomial of degree 4. If $\ell=4$, then $(-1)^{k+\ell}x^\ell+1=(-1)^k x^4+1$, which is also not divisible by $f(x)$.

Therefore, the only possibility is that $\ell=0$. In this case, $(-1)^{k+\ell}x^\ell+1=(-1)^k+1$ and this is divisible by $f(x)$ when k is odd so that $(-1)^k+1=0$.

In conclusion, $3n=5k$, hence $3n$ is an odd multiple of 5 and the same must be true of n. □

Example 17. Solve the system

$$x^5+y^5=33,\ \ x+y=3.$$

Solution: $x + y = 3$ and $3^5 = 243 \Longrightarrow$

$$243 = (x+y)^5 = x^5+5x^4y+10x^3y^2+10x^2y^3+5xy^4+y^5 = 33+5x^4y+10x^3y^2+10x^2y^3+5xy^4$$

where $(x + y)^5$ was expended as a sum of monomials using the Binomial Formula: see Theorem 1.1. Since $x^5 + y^5 = 33$,

$$243 - 33 = 5x^4y + 10x^3y^2 + 10x^2y^3 + 5xy^4 = 210$$

and, dividing by 5, we obtain

$$x^4y + 2x^3y^2 + 2x^2y^3 + xy^4 = 42.$$

$$\Longrightarrow xy(x^3 + 2x^2y + 2xy^2 + y^3) = 42$$

$$\Longrightarrow xy((x + y)^3 - x^2y - xy^2) = 42$$

since $(x + y)^3 = x^3 + 3x^2y + 3xy^2 + y^3$ by the Binomial Formula. Since $x + y = 3$,

$$xy(27 - x^2y - xy^2) = 42 \text{ and } xy(27 - xy(x + y)) = 42,$$

hence

$$xy(27 - 3xy) = 42.$$

This last equation can be rewritten as $3(xy)^2 - 27xy + 42 = 0$ and as $z^2 - 9z + 14 = 0$ where $z = xy$.

$z^2 - 9z + 14 = 0 \Longrightarrow (z - 2)(z - 7) = 0 \Longrightarrow z = 2$ or $z = 7 \Longrightarrow xy = 2$ or $xy = 7$.

If $x + y = 3$ and $xy = 2$, then $y = 3 - x$ and $x(3 - x) = 2$, so $x^2 - 3x + 2 = 0$ and $(x - 1)(x - 2) = 0$: therefore, either $x = 1, y = 2$ or $x = 2, y = 1$.

If $x + y = 3$ and $xy = 7$, then $y = 3 - x$ and $x(3 - x) = 7$, so $x^2 - 3x + 7 = 0$ and

$$x = \frac{3 \pm \sqrt{(-3)^2 - 4 \cdot 7}}{2} = \frac{3 \pm \sqrt{-19}}{2},$$

$$y = 3 - x = \frac{3 \mp \sqrt{-19}}{2}.$$

□

To end this first section about polynomials, let us now look at problems about polynomials that have appeared in past Putnam Math Competitions.

Example 18. [1971 Putnam, A–2] Determine all polynomials $P(x)$ such that $P(x^2 + 1) = (P(x))^2 + 1$ and $P(0) = 0$.

Solution: The only such polynomial is $P(x) = x$.

$P(0) = 0 \Longrightarrow P(1) = P(0^2 + 1) = P(0)^2 + 1 = 1 \Longrightarrow P(2) = P(1^2 + 1) = P(1)^2 + 1 = 2$. Define the sequence $\{a_n\}_{n=0}^{\infty}$ by $a_0 = 0$ and $a_{n+1} = a_n^2 + 1$ for $n \geqslant 0$. Then

$$P(a_{n+1}) = P(a_n^2 + 1) = P(a_n)^2 + 1.$$

If we know that $P(a_n) = a_n$, then it follows that

$$P(a_{n+1}) = P(a_n^2 + 1) = P(a_n)^2 + 1 = a_n^2 + 1 = a_{n+1}.$$

This means that, by induction, $P(a_n) = a_n$ for all $n \geqslant 0$. Therefore, the polynomials $P(x)$ and x take the same values on the infinite sequence $\{a_n\}_{n=0}^{\infty}$, hence they must be equal. $\square$

The end of the previous solution used the following fact about polynomials which is useful to know.

Lemma 1.9. *Suppose that $f(x)$ and $g(x)$ are two polynomials in $F[x]$, where $F = \mathbb{Q}, \mathbb{R}$ or $\mathbb{C}$. Suppose that $\deg(f(x)) \leqslant N$ and $\deg(g(x)) \leqslant N$ for some integer N. If $a_0, a_1, \ldots, a_N$ are $N + 1$ numbers in F such that $f(a_i) = g(a_i)$, then $f(x) = g(x)$.*

If $N = 1$, then this says that two polynomials of degree one which agree at two values of x must be equal: since the graphs of those polynomials are straight lines, this result corresponds to the fact that, given two points in the plane, there is a unique line passing through those two points. Since the graph of polynomials of degree two is a parabola, this lemma says that, given three points in the plane, there is a unique parabola passing through those points.

Wednesday, October 14, 2020

Example 19. [1999 Putnam, A–2] Let $p(x)$ be a polynomial that is nonnegative for all real x. Prove that, for some integer k, there are polynomials $f_1(x), \ldots, f_k(x)$ such that

$$p(x) = \sum_{j=1}^{k} (f_j(x))^2.$$

Solution: Without loss of generality, $p(x)$ can be assumed to be monic. Polynomials of odd degree take both positive and negative values, so the degree of $p(x)$ is even. The proof is by induction on the degree of $p(x)$.

If $\deg(p(x)) = 2$, then

$$p(x) = x^2 + ax + b = \left(x + \frac{a}{2}\right)^2 + b - \left(\frac{a}{2}\right)^2$$

and $b - \left(\frac{a}{2}\right)^2 \geqslant 0$ since $p\left(-\frac{a}{2}\right) \geqslant 0$ by assumption on $p(x)$. Another way to see that $b - \left(\frac{a}{2}\right)^2 \geqslant 0$ is that, since $p(x) \geqslant 0$ for all $x \in \mathbb{R}$, its discriminant, which is $a^2 - 4b$, is $\leqslant 0$. The inequality $a^2 - 4b \leqslant 0$ is equivalent to $b - \left(\frac{a}{2}\right)^2 \geqslant 0$.

The statement is thus true when $\deg(p(x)) = 2$ with $k = 2$, $f_1(x) = x + \frac{a}{2}$ and $f_2(x) = \left(b - \frac{a}{2}\right)^{\frac{1}{2}}$. (We can take the square root of $b - \frac{a}{2}$ since this number is $\geqslant 0$.)

By the Fundamental Theorem of Algebra, $p(x)$ is a product of irreducible factors of degree one or two in $\mathbb{R}[x]$. Suppose that $p(x) = p_1(x)p_2(x)$ and $p_2(x)$ is irreducible in $\mathbb{R}[x]$ of degree two. In particular, either $p_2(x) > 0$ for all $x \in \mathbb{R}$ or $p_2(x) < 0$ for all $x \in \mathbb{R}$. Without loss of generality, we can assume that $p_2(x) > 0$ for all $x \in \mathbb{R}$. Then $p_2(x) = g_1(x)^2 + g_2(x)^2$ as proved above. Moreover, $p_1(x) \geqslant 0$ for all $x \in \mathbb{R}$ so, by induction on the degree, $p_1(x) = \sum_{j=1}^{k} (f_j(x))^2$ for some polynomials $f_1(x), \ldots, f_k(x)$ in $\mathbb{R}[x]$. In follows that

$$p(x) = \left(\sum_{j=1}^{k} (f_j(x))^2\right) (g_1(x)^2 + g_2(x)^2) = \sum_{j=1}^{k} (f_j(x)g_1(x))^2 + \sum_{j=1}^{k} (f_j(x)g_2(x))^2.$$

This proves the result when $p(x) = p_1(x)p_2(x)$ and $p_2(x)$ is irreducible in $\mathbb{R}[x]$ of degree two.

If $p(x)$ does not have an irreducible factor of degree 2, then $p(x)$ is a product of polynomials of degree one:

$$p(x) = (x - a_1)^{e_1}(x - a_2)^{e_2} \cdots (x - a_m)^{e_m}.$$

Suppose that $e_i \geqslant 2$ for some i. Without loss of generality, let us assume that $i = 1$. Then $\frac{p(x)}{(x-a_1)^2}$ is a polynomial of degree $< \deg(p(x))$ which is non-negative. By induction on the degree, there are polynomials $f_1(x), \ldots, f_k(x)$ such that

$$\frac{p(x)}{(x - a_1)^2} = \sum_{j=1}^{k} (f_j(x))^2,$$

hence

$$p(x) = \sum_{j=1}^{k} ((x - a_1)f_j(x))^2.$$

Finally, observe that it is impossible to have that

$$p(x) = (x - a_1)(x - a_2) \cdots (x - a_m)$$

where all the roots $a_1, a_2, \ldots, a_m$ are distinct because, in this case, $p(x)$ does not have the same sign on the intervals $(a_i - \epsilon, a_i)$ and $(a_i, a_i + \epsilon)$ for some $\epsilon > 0$ small enough, so $p(x)$ is not always non-negative. □

Example 20. [2004 Putnam, B–1] Let $P(x) = c_n x^n + c_{n-1}x^{n-1} + \cdots + c_0$ be a polynomial with integer coefficients. Suppose that r is a rational number such that $P(r) = 0$. Show

that the n numbers

$$c_n r,\ c_n r^2 + c_{n-1} r,\ c_n r^3 + c_{n-1} r^2 + c_{n-2} r,$$
$$\ldots,\ c_n r^n + c_{n-1} r^{n-1} + \cdots + c_1 r$$

are integers.

Solution: We can assume that $r \neq 0$. Write r as $\frac{a}{b}$ with $a, b \in \mathbb{Z}\backslash\{0\}$ and $\gcd(a, b) = 1$.

$$\begin{aligned} P(r) = 0 &\Leftrightarrow c_n r^n + c_{n-1} r^{n-1} + \cdots + c_1 r + c_0 = 0 \\ &\Leftrightarrow c_n a^n + c_{n-1} a^{n-1} b + c_{n-2} a^{n-2} b^2 + \cdots + c_1 a b^{n-1} + c_0 b^n = 0. \end{aligned}$$

The last equality can be rewritten as

$$c_n a^n + c_{n-1} a^{n-1} b + c_{n-2} a^{n-2} b^2 + \cdots + c_{n-i} a^{n-i} b^i = -c_{n-i-1} a^{n-i-1} b^{i+1} - \cdots - c_1 a b^{n-1} - c_0 b^n$$

and as

$$\begin{aligned} &(c_n a^{i+1} + c_{n-1} a^i b + c_{n-2} a^{i-1} b^2 + \cdots + c_{n-i} a b^i) a^{n-i-1} \\ &\qquad = -b^{i+1}(c_{n-i-1} a^{n-i-1} + \cdots + c_1 a b^{n-i-2} + c_0 b^{n-i-1}). \end{aligned}$$

The right-hand side is divisible by b^{i+1}, hence so is the left-hand side. Since $\gcd(a, b) = 1$, b^{i+1} must divide

$$c_n a^{i+1} + c_{n-1} a^i b + c_{n-2} a^{i-1} b^2 + \cdots + c_{n-i} a b^i,$$

hence

$$c_n r^{i+1} + c_{n-1} r^i + c_{n-2} r^{i-1} + \cdots + c_{n-i} r$$

is an integer. □

Example 21. [1999 Putnam, B–2] Let $P(x)$ be a polynomial of degree n such that $P(x) = Q(x)P''(x)$, where $Q(x)$ is a quadratic polynomial and $P''(x)$ is the second derivative of $P(x)$. Show that if $P(x)$ has at least two distinct roots then it must have n distinct roots.

Solution: Suppose that $P(x)$ has a root a of multiplicity $m \geqslant 2$, so $P(x) = (x - a)^m R(x)$ with $R(a) \neq 0$. Then a is a root of $P''(x)$ of multiplicity $m - 2$ since

$$P''(x) = m(m-1)(x-a)^{m-2} R(x) + 2m(x-a) R'(x) + (x-a)^m R''(x).$$

(If $m - 2 = 0$, this means that a is actually not a root of $P''(x)$.)

It follows that $P''(x) = (x - a)^{m-2} S(x)$ for some polynomial $S(x)$ with $S(a) \neq 0$ and

$$P(x) = Q(x)P''(x) \Longrightarrow (x-a)^m R(x) = Q(x)(x-a)^{m-2} S(x) \Longrightarrow (x-a)^2 R(x) = Q(x)S(x).$$

This implies that $Q(x) = C(x - a)^2$ for some constant C since $Q(x)$ has degree two.

Without loss of generality, we can assume that $P(x)$ is monic, so the term of highest degree of $P(x)$ is x^n. Then the term of highest degree of $P''(x)$ is $n(n-1)x^{n-2}$. From $P(x) = Q(x)P''(x)$ and $Q(x) = C(x-a)^2$, comparing the coefficients of x^n on both sides shows that $1 = Cn(n-1)$, hence $C = \frac{1}{n(n-1)}$.

The following formula is useful to know. It is similar to the Binomial Formula (see Theorem 1.1) and is applicable to the derivative. It is a generalization of the product rule for the derivative and can be proved by induction: if $f(x)$ and $g(x)$ are two functions that can be differentiated m times, then the m^{th} derivative of $f(x)g(x)$ is

$$(f(x)g(x))^{(m)} = \sum_{k=0}^{m} \binom{m}{k} f^{(k)}(x)g^{(m-k)}(x).$$

Let us apply this formula to $P(x) = Q(x)P''(x)$ by taking the m^{th} derivative on both sides:

$$P^{(m)}(x) = Q(x)P^{(m+2)}(x) + mQ'(x)P^{(m+1)}(x) + \frac{m(m-1)}{2}Q''(x)P^{(m)}(x).$$

Since $Q(x) = \frac{1}{n(n-1)}(x-a)^2$, it follows that $Q''(x) = \frac{2}{n(n-1)}$ and the previous equality can be rewritten as

$$\left(1 - \frac{m(m-1)}{n(n-1)}\right) P^{(m)}(x) = \frac{1}{n(n-1)}(x-a)^2P^{(m+2)}(x) + \frac{2m}{n(n-1)}(x-a)P^{(m+1)}(x).$$

The right-hand side is divisible by $x-a$, hence so is the left-hand side. However, since a is a root of $P(x)$ of multiplicity m, $P^{(m)}(a) \neq 0$, so it follows that the left-hand side must be zero, hence

$$1 - \frac{m(m-1)}{n(n-1)} = 0.$$

This implies that $m(m-1) = n(n-1)$ and it follows that $m = n$ since

$$m(m-1) = n(n-1) \Leftrightarrow m^2 - n^2 - m + n = 0 \Leftrightarrow (m-n)(m+n-1) = 0.$$

Since $m, n > 0$, the last equality can hold only when $m = n$.

It has been proved that if $P(x)$ has a root of multiplicity $\geqslant 2$, then this root actually has multiplicity n and is thus the only root of $P(x)$. This means that if $P(x)$ has at least two distinct roots, then it must have n distinct roots. □

Wednesday, October 21, 2020

Example 22. [2005 Putnam, B–1] Find a nonzero polynomial $P(x, y)$ such that

$$P(\lfloor a \rfloor, \lfloor 2a \rfloor) = 0$$

for all real numbers a. (Note: $\lfloor \nu \rfloor$ is the greatest integer less than or equal to ν.)

Solution: Let $P(x,y) = P_1(x,y)P_2(x,y)$ where $P_1(x,y) = (2x-y)$ and $P_2(x,y) = (2x+1-y)$.

If $0 \leqslant a - \lfloor a \rfloor < \frac{1}{2}$, then $\lfloor 2a \rfloor = 2\lfloor a \rfloor$ and $P_1(\lfloor a \rfloor, \lfloor 2a \rfloor) = 0$.

If $\frac{1}{2} \leqslant a - \lfloor a \rfloor < 1$, then $\lfloor 2a \rfloor = 2\lfloor a \rfloor + 1$ and $P_2(\lfloor a \rfloor, \lfloor 2a \rfloor) = 0$.

Once you know the answer, you can check as above that it works, but this raises the question: how can one come up with $P_1(x,y)$ and $P_2(x,y)$ in the first place? One natural question is: does $\lfloor 2a \rfloor$ always equal $2\lfloor a \rfloor$? The answer is no, not always.

When working with the floor function $\lfloor\ \rfloor$, it is useful to write the number a as $a = \lfloor a \rfloor + \{a\}$ where $\{a\} \in [0,1)$. Then $2a = 2\lfloor a \rfloor + 2\{a\}$ and $0 \leqslant 2\{a\} < 2$, so $2\lfloor a \rfloor$ is not always equal to $\lfloor 2a \rfloor$: they are equal exactly when $0 \leqslant 2\{a\} < 1$, that is, when $0 \leqslant \{a\} < \frac{1}{2}$. In this case,

$$P_1(\lfloor a \rfloor, \lfloor 2a \rfloor) = P_1(\lfloor a \rfloor, 2\lfloor a \rfloor) = 0.$$

The other case to consider is thus when $\frac{1}{2} \leqslant \{a\} < 1$, so $1 \leqslant 2\{a\} < 2$. Then

$$2a = 2\lfloor a \rfloor + 2\{a\} = 2\lfloor a \rfloor + 1 + (2\{a\} - 1)$$

and $0 \leqslant 2\{a\} - 1 < 1$, so, in this case, $\lfloor 2a \rfloor = 2\lfloor a \rfloor + 1$. □

2 Complex numbers

The set of complex numbers will be denoted $\mathbb{C}$. It can be obtained by starting with $\mathbb{R}^2$:

$$\mathbb{R}^2 = \{(x,y) : x, y \in \mathbb{R}\}.$$

You know that $\mathbb{R}^2$ is a real vector space, so we have an addition and a scalar multiplication:

$$(x_1,y_1) + (x_2,y_2) = (x_1 + x_2, y_1 + y_2) \text{ and } r(x,y) = (rx, ry)$$

for any $x_1, y_1, x_2, y_2, r \in \mathbb{R}$. We will now introduce a new binary operation simply denoted $\cdot$ on $\mathbb{R}^2$:

$$(x_1,y_1) \cdot (x_2,y_2) = (x_1x_2 - y_1y_2, x_1y_2 + x_2y_1).$$

This formula looks complicated, but soon I will show you an easy way to remember it. The set of complex numbers $\mathbb{C}$ is equal to the set $\mathbb{R}^2$ endowed with the two operations of addition $+$ and multiplication $\cdot$.

$\mathbb{R}^2$ has a basis given by $e_1 = (1,0), e_2 = (0,1)$. Notice that

$$e_1 \cdot e_1 = (1,0) = e_1 \text{ and } e_2 \cdot e_2 = (-1,0) = -e_1.$$

Although it is common to use e_1, e_2 to denote the standard basis of $\mathbb{R}^2$, when one thinks of $\mathbb{R}^2$ as the set $\mathbb{C}$ of complex numbers, one uses instead the following notation:

$$(1,0) \rightsquigarrow 1 \text{ and } (0,1) \rightsquigarrow i.$$

$(x,y) = xe_1 + ye_2$, so any complex number is of the form $x + yi$ with $x, y \in \mathbb{R}$.

Using this notation, the multiplication is then given by

$$(x_1 + y_1 i) \cdot (x_2 + y_2 i) = x_1 x_2 - y_1 y_2 + (x_1 y_2 + y_1 x_2) i.$$

Moreover, $i \cdot i = -1$: this shows that i is a solution of the equation $x^2 = -1$. For this reason, i is often denoted $\sqrt{-1}$.

If we think of i as $\sqrt{-1}$, then the formula for multiplication in $\mathbb{C}$ becomes easier to remember:

$$\begin{aligned}(x_1 + y_1 i) \cdot (x_2 + y_2 i) &= (x_1 + y_1\sqrt{-1}) \cdot (x_2 + y_2\sqrt{-1}) \\ &= x_1 x_2 + y_1 y_2 \sqrt{-1}\sqrt{-1} + (x_1 y_2 + y_1 x_2)\sqrt{-1} \\ &= x_1 x_2 - y_1 y_2 + (x_1 y_2 + y_1 x_2)\sqrt{-1}.\end{aligned}$$

For instance,

$$5 - 8i + 9 + 2i = 14 - 6i \text{ and } (5 - 8i) \cdot (9 + 2i) = (45 + 16) + (10 - 72)i = 61 - 62i.$$

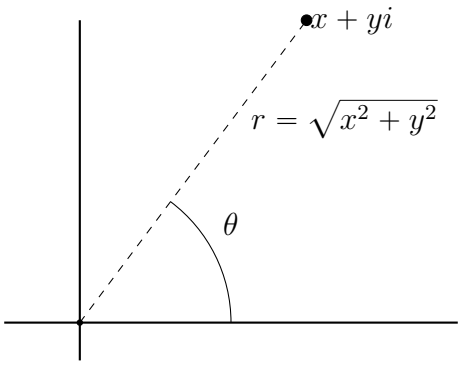
If $z = x + yi$, its complex conjugate, which is denoted $\bar{z}$, is equal to $x - yi$. The norm of z is $\sqrt{x^2 + y^2}$ and is equal to the distance between z and the origin 0 in $\mathbb{C}$. It is denoted $\| z \|$. Observe that

$$z\bar{z} = (x + yi)(x - yi) = x^2 - y^2(-1) = x^2 + y^2 = \| z \|^2,$$

so $z \cdot \frac{\bar{z}}{\|z\|^2} = 1$ if $z \neq 0$: this shows that, if $z \neq 0$, then $z^{-1} = \frac{\bar{z}}{\|z\|^2}$. In particular, if $\| z \| = 1$, which means that z is on the unit circle, then $z^{-1} = \bar{z}$.

One property of complex conjugation which is useful to know is $\overline{z_1 z_2} = \overline{z_1} \cdot \overline{z_2}$. It follows that $\| z_1 z_2 \| = \| z_1 \| \cdot \| z_2 \|$.

Complex numbers can be described using polar coordinates and this is sometimes very useful. If we think of the complex number $x + yi$ as the point (x, y) in $\mathbb{R}^2$, then its distance from the origin is $\sqrt{x^2 + y^2}$ and the line segment from the origin $(0, 0)$ to (x, y) forms an angle of θ with the positive x-axis, θ being measured counterclockwise.



Since $x = \cos(\theta)\sqrt{x^2 + y^2}$ and $y = \sin(\theta)\sqrt{x^2 + y^2}$, it follows that

$$z = x + yi = \sqrt{x^2 + y^2}(\cos(\theta) + i\sin(\theta)).$$

Moreover, $\theta = \arctan\left(\frac{y}{x}\right)$ if $x > 0$ (so that $\theta \in \left(-\frac{\pi}{2}, \frac{\pi}{2}\right)$).

There is an exponential function e^z for any complex number z and it is given by the power series

$$e^z = 1 + z + \frac{z^2}{2!} + \frac{z^3}{3!} + \cdots = \sum_{n=0}^{\infty} \frac{z^n}{n!}.$$

Euler's Formula says that

$$e^{i\theta} = \cos(\theta) + i\sin(\theta)$$

and the exponential function has the property $e^{z_1+z_2} = e^{z_1}e^{z_2}$. If (x, y) has polar coordinates r and θ, then $x + yi = re^{i\theta}$ (where $r = \sqrt{x^2 + y^2}$). In particular, if $x = -1$, $y = 0$ and $\theta = \pi$, then

$$e^{i\pi} = -1,$$

which is quite an amazing identity relating e, π and $\sqrt{-1}$.

Multiplication of complex numbers has a geometric interpretation: $e^{i\theta}z$ is the complex number obtained by rotating z by an angle of θ counter-clockwise around the origin. If $r > 1$, $re^{i\theta}z$ is the complex number obtained by rotating z by an angle of θ counter-clockwise around the origin and then stretching it by a factor of r. If $0 < r < 1$, $re^{i\theta}z$ is the complex number obtained by rotating z by an angle of θ counter-clockwise around the origin and then shrinking it by a factor of r.

Complex numbers can be used to solve a quadratic equation $ax^2 + bx + c = 0$ where $a, b, c \in \mathbb{C}$. If $a, b, c \in \mathbb{R}$ and the discriminant $b^2 - 4ac$ is < 0, then the roots are

$$\frac{-b \pm \sqrt{b^2 - 4ac}}{2a}$$

and $b^2 - 4ac = -d$ for some positive real number d. We then have

$$\pm\sqrt{b^2 - 4ac} = \pm\sqrt{-d} = \pm\sqrt{d}\sqrt{-1} = \pm\sqrt{d}i.$$

This raises the question: what if $b^2 - 4ac \notin \mathbb{R}$? How can we calculate the square roots $\pm\sqrt{b^2-4ac}$? The exponential function can be used to do just that. If $z = x + yi = re^{i\theta}$ where $r = \sqrt{x^2+y^2}$ and $\theta = \arctan\left(\frac{y}{x}\right)$ (if $x \neq 0$), then the square roots of z are $\pm\sqrt{r}e^{\frac{i\theta}{2}}$ since

$$\left(\pm\sqrt{r}e^{\frac{i\theta}{2}}\right)^2 = \sqrt{r}^2 e^{\frac{2i\theta}{2}} = re^{i\theta}$$

. (If $x = 0$, then $\theta = \frac{\pi}{2}$ or $\frac{3\pi}{2}$ depending on the sign of y.)

Here is a fact about complex roots of polynomials in $\mathbb{R}[x]$ which is useful to know.

Lemma 2.1. *Let $f(x) \in \mathbb{R}[x]$. If $z \in \mathbb{C}$ and $f(z) = 0$, then $f(\bar{z}) = 0$. In other words, if z is a root of $f(x)$, then $\bar{z}$ is also a root of $f(x)$.*

Let's now look at problems that can be solved with the help of complex numbers.

Example 1. Solve the equation $x^2 + 2x - 3i = 0$.

Solution: The standard formula $\frac{-b\pm\sqrt{b^2-4ac}}{2a}$ gives the roots

$$\frac{-2 \pm \sqrt{4-12i}}{2},$$

which equal $-1 \pm \sqrt{1-3i}$. This is a good enough answer, but it raises the question: what are the square roots of $1 - 3i$? Let's write this complex number in polar form: $1 - 3i = re^{i\theta}$ where

$$r = \| \, 1 - 3i \, \| = \sqrt{1 + (-3)^2} = \sqrt{10} \text{ and } \theta = \arctan(-3).$$

It's not possible to say more about the angle θ although an approximate value can be obtained using a calculator. Then

$$\sqrt{1-3i} = \sqrt{r}e^{\frac{i\theta}{2}}$$

is one square root of $1 - 3i$, the other one being $-\sqrt{r}e^{\frac{i\theta}{2}}$, which equals $\sqrt{r}e^{\frac{i\theta}{2}+\pi i}$. □

Example 2. Let m and n be two integers such that each can be expressed as the sum of two perfect squares. Prove that mn has this property as well. For instance $17 = 4^2 + 1^2$, $13 = 2^2 + 3^2$, and $17 \cdot 13 = 221 = 14^2 + 5^2$.

First solution: If $m = a^2 + b^2$ and $n = c^2 + d^2$, then $m = \| \, a + bi \, \|^2$ and $n = \| \, c + di \, \|^2$. Set $z_1 = a + bi$ and $z_2 = c + di$. Then

$$mn = \| \, z_1 \, \|^2 \| \, z_2 \, \|^2 = \| \, z_1 z_2 \, \|^2 = e^2 + f^2$$

where e and f are given by $z_1 z_2 = e + fi$. □

Second solution: Observe that we have the following factorization: $x^2+y^2 = (x-yi)(x+yi)$. If $m = a^2+b^2$ and $n = c^2+d^2$, then $m = (a-bi)(a+bi)$ and $n = (c-di)(c+di)$. Therefore,

$$\begin{aligned} mn &= (a-bi)(a+bi)(c-di)(c+di) = (a-bi)(c-di)(a+bi)(c+di) \\ &= (ac-bd-(ad+bc)i)(ac-bd+(ad+bc)i) = (ac-bd)^2+(ad+bc)^2. \end{aligned}$$

□

Example 3. If $a, b, n \in \mathbb{Z}_{>0}$, prove that there exist integers x and y such that

$$(a^2+b^2)^n = x^2+y^2.$$

Solution: Let $z = a+bi$. Then $a^2+b^2 = \| z \|^2$, so

$$(a^2+b^2)^n = (\| z \|^2)^n = \| z \|^{2n} = (\| z \|^n)^2 = (\| z^n \|)^2.$$

z^n is also a complex number, so $z^n = x+yi$ for some $x, y \in \mathbb{R}$ and actually $x, y \in \mathbb{Z}$ since $a, b \in \mathbb{Z}$. It follows that

$$(a^2+b^2)^n = (\| z^n \|)^2 = \| x+yi \|^2 = x^2+y^2.$$

□

Wednesday, October 28, 2020

Example 4. Express $\cos(3\theta)$ in terms of $\cos(\theta)$.

Solution: De Moivre's Theorem says that $e^{3i\theta} = \cos(3\theta) + i\sin(3\theta)$, so $\cos(3\theta) = \mathrm{Re}(e^{3i\theta})$. To compute the real part of $e^{3i\theta}$ in a different way, let's expand it:

$$\begin{aligned} e^{3i\theta} &= (e^{i\theta})^3 = (\cos(\theta)+i\sin(\theta))^3 \\ &= \cos^3(\theta) + 3\cos^2(\theta) i\sin(\theta) + 3\cos(\theta)(i\sin(\theta))^2 + (i\sin(\theta))^3 \\ &= \cos^3(\theta) + 3\cos^2(\theta) i\sin(\theta) - 3\cos(\theta)\sin^2(\theta) - i\sin(\theta)^3. \end{aligned}$$

The real part of the right-hand side is $\cos^3(\theta) - 3\cos(\theta)\sin^2(\theta)$, hence

$$\cos(3\theta) = \cos^3(\theta) - 3\cos(\theta)\sin^2(\theta).$$

We have to express $\cos(3\theta)$ in terms of $\cos(\theta)$ only. Substituting $\sin^2(\theta) = 1-\cos^2(\theta)$ into the previous equation, we finally arrive at

$$\cos(3\theta) = \cos^3(\theta) - 3\cos(\theta)(1-\cos^2(\theta)) = 4\cos^3(\theta) - 3\cos(\theta).$$

□

Example 5. Using that $e^{i\theta} - e^{-i\theta} = 2i\sin(\theta)$ and $e^{ik\theta} + e^{-ik\theta} = 2\cos(k\theta)$ for any $k \in \mathbb{Z}_{\geqslant 0}$, express $\sin^{2n}(\theta)$ as a linear combination of $\cos(k\theta)$ with $0 \leqslant k \leqslant 2n$.

Solution: Let's raise $e^{i\theta} - e^{-i\theta} = 2i\sin(\theta)$ to its $2n^{th}$-power:

$$(e^{i\theta} - e^{-i\theta})^{2n} = (2i\sin(\theta))^2 n = (-4)^n \sin^{2n}(\theta).$$

Let's apply the Binomial Theorem to expand the left-hand side:

$$\begin{aligned} e^{2ni\theta} - \binom{2n}{1} e^{(2n-1)i\theta} e^{-i\theta} + \binom{2n}{2} e^{(2n-2)i\theta} e^{-2i\theta} + \cdots \\ + \binom{2n}{2n-2} e^{2i\theta} e^{-(2n-2)i\theta} - \binom{2n}{2n-1} e^{i\theta} e^{-(2n-1)i\theta} + \binom{2n}{2n} e^{-2ni\theta} \\ = (-4)^n \sin^{2n}(\theta). \end{aligned}$$

The left-hand side can be rewritten as

$$\begin{aligned} (e^{2ni\theta} + e^{-2ni\theta}) - \binom{2n}{1}(e^{(2n-1)i\theta} e^{-i\theta} + e^{i\theta} e^{-(2n-1)i\theta}) + \binom{2n}{2}(e^{(2n-2)i\theta} e^{-2i\theta} + e^{2i\theta} e^{-(2n-2)i\theta}) \\ + \cdots + (-1)^n \binom{2n}{n}(e^{ni\theta} e^{-ni\theta}) = (-4)^n \sin^{2n}(\theta) \end{aligned}$$

and thus as

$$\begin{aligned} (e^{2ni\theta} + e^{-2ni\theta}) - \binom{2n}{1}(e^{(2n-2)i\theta} + e^{-(2n-2)i\theta}) + \binom{2n}{2}(e^{(2n-4)i\theta} + e^{-(2n-4)i\theta}) \\ + \cdots + (-1)^n \binom{2n}{n} = (-4)^n \sin^{2n}(\theta). \end{aligned}$$

Using $e^{ik\theta} + e^{-ik\theta} = 2\cos(k\theta)$, we finally obtain

$$\begin{aligned} 2\cos(2n\theta) - 2\binom{2n}{1}\cos((2n-2)\theta) + 2\binom{2n}{2}\cos((2n-4)\theta) \\ + \cdots + 2(-1)^{n-1}\binom{2n}{n-1}\cos(2\theta) + (-1)^n \binom{2n}{n} = (-4)^n \sin^{2n}(\theta). \end{aligned}$$

Dividing by $(-4)^n$ yields the desired linear combination. □

Example 6. Find a closed formula for the sum

$$\cos(\theta) + \cos(2\theta) + \cdots + \cos(n\theta).$$

Solution: Since $\cos(k\theta) = \mathrm{Re}(e^{ik\theta})$, we can write

$$\begin{aligned}\cos(\theta) + \cos(2\theta) + \cdots + \cos(n\theta) &= \mathrm{Re}\left(e^{i\theta} + e^{2i\theta} + \cdots + e^{ni\theta}\right) \\ &= \mathrm{Re}\left(e^{i\theta} + (e^{i\theta})^2 + \cdots + (e^{i\theta})^n\right) \\ &= \mathrm{Re}\left(\frac{e^{(n+1)\theta} - e^{i\theta}}{e^{i\theta} - 1}\right)\end{aligned}$$

Here, the following formula has been used with $t = e^{i\theta}$:

$$1 + t + t^2 + \cdots + t^n = \frac{t^{n+1} - 1}{t - 1}.$$

Actually, what we need is the formula for this sum except for the initial constant 1:

$$t + t^2 + \cdots + t^n = t(1 + t + \cdots + t^{n-1}) = t\left(\frac{t^n - 1}{t - 1}\right) = \frac{t^{n+1} - t}{t - 1}.$$

We are left to determine the real part of $\frac{e^{(n+1)\theta} - e^{i\theta}}{e^{i\theta} - 1}$, so we need to write this complex number in the form $x + yi$ with $x, y \in \mathbb{R}$. If we have a complex number of the form $\frac{w}{z}$ with $z \in \mathbb{C}, z \neq 0$, the standard way to do that is to multiply by $\frac{\bar{z}}{\bar{z}}$ since

$$\frac{w}{z}\frac{\bar{z}}{\bar{z}} = \frac{w\bar{z}}{z\bar{z}}$$

and the denominator $z\bar{z}$ is a real number:

$$\frac{e^{(n+1)\theta} - e^{i\theta}}{e^{i\theta} - 1} = \left(\frac{e^{(n+1)\theta} - e^{i\theta}}{e^{i\theta} - 1}\right)\left(\frac{e^{-i\theta} - 1}{e^{-i\theta} - 1}\right) = \frac{e^{ni\theta} - 1 - e^{(n+1)i\theta} + e^{i\theta}}{2 - e^{i\theta} - e^{-i\theta}}.$$

$2 - e^{i\theta} - e^{-i\theta}$ is indeed real and equal to $2 - 2\cos(\theta)$. The real part of the numerator is

$$\cos(n\theta) - 1 - \cos((n+1)\theta) + \cos(\theta).$$

Therefore, in conclusion, the real part of $\frac{e^{(n+1)\theta} - e^{i\theta}}{e^{i\theta} - 1}$ is equal to

$$\frac{\cos(n\theta) - 1 - \cos((n+1)\theta) + \cos(\theta)}{2 - 2\cos(\theta)}$$

and this is a closed formula for the sum $\cos(\theta) + \cos(2\theta) + \cdots + \cos(n\theta)$. □

Wednesday, November 4, 2020

Example 7. Suppose that $\theta \neq k\pi$ for any $k \in \mathbb{Z}$. Sum the infinite series

$$\cos(\theta) + \frac{1}{2}\cos(2\theta) + \frac{1}{3}\cos(3\theta) + \cdots$$

Solution: $\cos(k\theta) = \mathrm{Re}(e^{ki\theta})$, so we have to find the real part of

$$e^{i\theta} + \frac{e^{2i\theta}}{2} + \frac{e^{3i\theta}}{3} + \cdots,$$

which equals the real part of

$$e^{i\theta} + \frac{(e^{i\theta})^2}{2} + \frac{(e^{i\theta})^3}{3} + \cdots$$

This suggest considering the power series

$$x + \frac{x^2}{2} + \frac{x^3}{3} + \cdots$$

From calculus, recall that this equals $-\ln(1-x)$ when $|x| < 1$. This power series expansion is also valid for $-\ln(1-z)$ when $z \in \mathbb{C}$ and $\| z \| < 1$.

This brings the question: given $w \in \mathbb{C}^\times$, what is the real part of $\ln(w)$? If $w = re^{i\theta}$ with $r > 0$, then we can write $r = e^a$ for some $a \in \mathbb{R}$ and

$$w = e^a e^{i\theta} = e^{a+i\theta}.$$

This shows that

$$\ln(w) = a + i\theta \text{ and } \mathrm{Re}(\ln(w)) = \ln(r) = a.$$

In order to determine the real part of $-\ln(1-e^{i\theta})$, we have to determine the norm r of $1 - e^{i\theta}$:

$$\begin{aligned} r^2 &= \| 1 - e^{i\theta} \|^2 \\ &= \| 1 - \cos(\theta) + i\sin(\theta) \|^2 \\ &= (1-\cos(\theta))^2 + \sin(\theta)^2 \\ &= 1 - 2\cos(\theta) + \cos(\theta)^2 + \sin(\theta)^2 \\ &= 2 - 2\cos(\theta)) \end{aligned}$$

so $r = \sqrt{2(1-\cos(\theta))}$. Therefore,

$$-\mathrm{Re}(\ln(1-e^{i\theta})) = -\ln(r) = -\frac{1}{2}\ln(2-2\cos(\theta)).$$

□

The roots-of-unity are complex numbers that are useful to know. Given $n \in \mathbb{Z}_{\geqslant 1}$, the n^{th} roots-of-unity are the complex numbers $e^{\frac{2\pi k i}{n}}$ for $0 \leqslant k \leqslant n-1$, that is, they are

$$1,\ e^{\frac{2\pi}{n}i},\ e^{\frac{2\pi\cdot 2i}{n}},\ e^{\frac{2\pi\cdot 3i}{n}},\ \ldots,\ e^{\frac{2\pi(n-1)i}{n}}.$$

Observe that $e^{\frac{2\pi ki}{n}} = (e^{\frac{2\pi i}{n}})^k$ and all the roots-of-unity are located on the unit circle:

$$e^{\frac{2\pi ki}{n}} = \cos\left(\frac{2\pi ki}{n}\right) + i\sin\left(\frac{2\pi ki}{n}\right).$$

They form the vertices of a regular polygon with vertices on the unit circle. To simplify the notation, let us set

$$\zeta_k = e^{\frac{2\pi ki}{n}}, \text{ so } \zeta_k = \zeta_1^k.$$

Each root-of-unity ζ_k satisfies $\zeta_k^n = 1$, which explains their name. There is a smallest positive integer ℓ (that depends on k) such that $\zeta_k^\ell = 1$. For instance, if $n = 4$, then $\zeta_1 = i$ and $\ell = 4$, whereas $\zeta_2 = -1$ and $\ell = 2$. It can be shown that ℓ is a divisor of n. The roots-of-unity ζ_k such that $\zeta_k^i \neq 1$ for $1 \leqslant i \leqslant n-1$ are called the primitive n^{th} roots-of-unity. It can be proved that ζ_k is primitive if and only if $\gcd(k, n) = 1$. Any n^{th} root-of-unity ζ_k is a primitive ℓ^{th} root-of-unity for ℓ as defined above.

Some basic properties of the roots-of-unit are:

$$\zeta_{n-k} = \zeta_k^{-1} = \zeta_{-k} = \overline{\zeta_k}.$$

The n^{th} roots-of-unity are exactly the n roots of the polynomials $x^n - 1$, so

$$x^n - 1 = (x-1)(x-\zeta_1)(x-\zeta_2)\cdots(x-\zeta_{n-1}) = (x-1)(x-\zeta)(x-\zeta^2)\cdots(x-\zeta^{n-1})$$

where $\zeta = \zeta_1$. Since

$$x^n - 1 = (x-1)(x^{n-1} + x^{n-2} + \cdots + x^2 + x + 1),$$

it follows that all the roots-of-unity except 1 are roots of $x^{n-1} + x^{n-2} + \cdots + x^2 + x + 1$, so

$$x^{n-1} + x^{n-2} + \cdots + x^2 + x + 1 = (x-\zeta)(x-\zeta_2)\cdots(x-\zeta_{n-1}).$$

Moreover, this means that the roots-of-unity are algebraic integers. The primitive n^{th} roots-of-unity are the roots of a polynomial with integral coefficients of lower degree called the n^{th} cyclotomic polynomial $\Phi_n(x)$ and it can be seen that

$$x^n - 1 = \prod_{\ell \mid n} \Phi_\ell(x).$$

This last product is the factorization of $x^n - 1$ into a product of irreducible factors in $\mathbb{Q}[x]$.

Roots-of-unity can sometimes be used to solve certain problems in geometry about regular polygons.

Wednesday, November 18, 2020

Example 8. Let ζ be a primitive n^{th} root-of-unity. Show that

$$(1-\zeta)(1-\zeta^2)\cdots(1-\zeta^{n-1}) = n.$$

First solution: The polynomial $x^n - 1$ can be factored as

$$x^n - 1 = (x-1)(x^{n-1} + x^{n-2} + \cdots + x^2 + x + 1) = (x-1)(x-\zeta)(x-\zeta^2)\cdots(x-\zeta^{n-1}).$$

Dividing by $x - 1$ gives

$$(x^{n-1} + x^{n-2} + \cdots + x^2 + x + 1) = (x-\zeta)(x-\zeta^2)\cdots(x-\zeta^{n-1}).$$

Setting $x = 1$ in the previous identity yields

$$1 + 1 + \cdots + 1 + 1 + 1 = n = (1-\zeta)(1-\zeta^2)\cdots(1-\zeta^{n-1}).$$

□

Second solution (proposed by Justin Stevens): Set $\alpha_k = 1 - \zeta^k$. Then

$$(1-\alpha_k)^n = (\zeta^k)^n = (\zeta^n)^k = 1^k = 1,$$

so $(1-\alpha_k)^n - 1 = 0$ which means that ζ_k is a root of the polynomial $(1-x)^n - 1$ for $k = 1, 2, \ldots, n-1$. Let's denote this polynomial by $f(x)$.

$f(x)$ has degree n and α_k for $k = 1, 2, \ldots, n-1$ are $n-1$ distinct roots of $f(x)$. The other root of $f(x)$ is 0. $f(x)$ is not monic: its leading coefficient is $(-1)^n$. The constant term of $f(x)$ is 0 since 0 is a root.

The coefficient of x in $f(x)$ is $-\binom{n}{1}$ by the Binomial Theorem, so it equals $-n$. By Vieta's formulas, this coefficient is equal to the sum of all the products of $n-1$ roots, up to the sign $(-1)^n(-1)^{n-1}$. The sign $(-1)^{n-1}$ comes from the fact that we are considering $n-1$ roots of $f(x)$ and the sign $(-1)^n$ is the leading coefficient of $f(x)$. All those products are 0 except the product $\alpha_1\alpha_2\cdots\alpha_{n-1}$. Therefore,

$$(-1)^n(-1)^{n-1}\alpha_1\alpha_2\cdots\alpha_{n-1} = -n \text{ hence } \alpha_1\alpha_2\cdots\alpha_{n-1} = n.$$

□

Example 9. Show that

$$\sin\left(\frac{\pi}{n}\right)\sin\left(\frac{2\pi}{n}\right)\cdots\sin\left(\frac{(n-1)\pi}{n}\right) = \frac{n}{2^{n-1}}.$$

Solution: Recall that $\sin(\theta) = \frac{1}{2i}(e^{i\theta} - e^{-i\theta})$, which is a consequence of Euler's formula. Therefore,

$$\sin\left(\frac{k\pi i}{n}\right) = \frac{1}{2i}(e^{\frac{k\pi i}{n}} - e^{-\frac{k\pi i}{n}}) = \frac{1}{2i}(e^{\frac{2\pi i}{n}\cdot\frac{k}{2}} - e^{-\frac{2\pi i}{n}\cdot\frac{k}{2}}) = \frac{1}{2i}(\zeta^{\frac{k}{2}} - \zeta^{-\frac{k}{2}})$$

where ζ is the root-of-unity $e^{\frac{2\pi i}{n}}$.

The product

$$\sin\left(\frac{\pi}{n}\right)\sin\left(\frac{2\pi}{n}\right)\cdots\sin\left(\frac{(n-1)\pi}{n}\right)$$

is thus equal to

$$\left(\frac{1}{2i}\right)^{n-1}(\zeta^{-\frac{1}{2}}-\zeta^{\frac{1}{2}})(\zeta^{-\frac{2}{2}}-\zeta^{\frac{2}{2}})\cdots(\zeta^{-\frac{n-1}{2}}-\zeta^{\frac{n-1}{2}}).$$

Observe that

$$(\zeta^{\frac{k}{2}}-\zeta^{-\frac{k}{2}})=\zeta^{-\frac{k}{2}}(\zeta^k-1)=-\zeta^{-\frac{k}{2}}(1-\zeta^k).$$

Therefore, the product that we have to evaluate equals

$$\left(\frac{1}{2i}\right)^{n-1}(-1)^{n-1}\zeta^{-\frac{1}{2}}(1-\zeta)\zeta^{-\frac{2}{2}}(1-\zeta^2)\cdots\zeta^{-\frac{(n-1)}{2}}(1-\zeta^{n-1}),$$

which simplifies to

$$\frac{1}{2^{n-1}}i^{n-1}\zeta^{-\frac{(n-1)n}{4}}(1-\zeta)(1-\zeta^2)\cdots(1-\zeta^{n-1}).$$

Here, we used that

$$\frac{1}{2}+\frac{2}{2}+\frac{3}{2}+\cdots+\frac{n-1}{2}=\frac{1}{2}(1+2+3+\cdots+(n-1))=\frac{1}{2}\frac{(n-1)n}{2}=\frac{(n-1)n}{4}$$

and that

$$\zeta^{-\frac{1}{2}}\zeta^{-\frac{2}{2}}\zeta^{-\frac{3}{2}}\cdots\zeta^{-\frac{(n-1)}{2}}=\zeta^{-\frac{1}{2}-\frac{2}{2}-\frac{3}{2}-\cdots-\frac{(n-1)}{2}}.$$

Since $\zeta=e^{\frac{2\pi i}{n}}$,

$$\zeta^{-\frac{(n-1)n}{4}}=e^{-\frac{2\pi i}{n}\cdot\frac{(n-1)n}{4}}=e^{-\frac{\pi(n-1)i}{2}}=(-i)^{n-1}.$$

In the previous example, it was shown that

$$n=(1-\zeta)(1-\zeta^2)\cdots(1-\zeta^{n-1}).$$

Putting all this together shows that

$$\sin\left(\frac{\pi}{n}\right)\sin\left(\frac{2\pi}{n}\right)\cdots\sin\left(\frac{(n-1)\pi}{n}\right)$$

is equal to

$$\left(\frac{1}{2}\right)^{n-1}i^{n-1}(-i)^{n-1}n,$$

which simplifies to

$$\frac{n}{2^{n-1}}.$$

□

Example 10. Show that $\cos\left(\frac{2\pi}{5}\right) = \frac{-1+\sqrt{5}}{4}$.

Solution: Observe that $\cos\left(\frac{2\pi}{5}\right)$ is the real part of $e^{\frac{2\pi i}{5}}$, which is a primitive 5^{th} root-of-unity. Set $\zeta = e^{\frac{2\pi}{5}}$. Then $\zeta^5 - 1 = 0$ and thus

$$(\zeta - 1)(\zeta^4 + \zeta^3 + \zeta^2 + \zeta + 1) = 0.$$

Since $\zeta \neq 1$, it follows that

$$\zeta^4 + \zeta^3 + \zeta^2 + \zeta + 1 = 0.$$

ζ is thus a root of $x^4 + x^3 + x^2 + x + 1$. The solution to this problem resides in the fact that it is possible to express roots of this polynomials using radicals, but this is not obvious. The trick is to write it in a more symmetric way by dividing it by x^2 and rearranging the terms:

$$\begin{aligned} x^4 + x^3 + x^2 + x + 1 = 0 &\Longleftrightarrow \frac{1}{x^2}(x^4 + x^3 + x^2 + x + 1) = 0 \\ &\Longleftrightarrow x^2 + x + 1 + x^{-1} + x^{-2} = 0 \\ &\Longleftrightarrow \left(x + \frac{1}{x}\right)^2 + \left(x + \frac{1}{x}\right) - 1 = 0. \end{aligned}$$

This last equation is a quadratic equation in y if we set $y = x + \frac{1}{x}$. The solutions of $y^2 + y - 1 = 0$ are

$$\frac{-1 \pm \sqrt{5}}{2},$$

so

$$x + \frac{1}{x} = \frac{-1 \pm \sqrt{5}}{2}.$$

Multiplying by x, we obtain the equivalent quadratic equations (one when $\pm = +$ and one when $\pm = -$):

$$x^2 + \left(\frac{-1 \pm \sqrt{5}}{2}\right) x + 1 = 0.$$

The solutions of these last equations are

$$\frac{\frac{-1+\sqrt{5}}{2} \pm \sqrt{\left(\frac{-1+\sqrt{5}}{2}\right)^2 - 4}}{2} = \frac{-1 + \sqrt{5} \pm \sqrt{-2\sqrt{5} - 10}}{4}$$

and

$$\frac{\frac{-1-\sqrt{5}}{2} \pm \sqrt{\left(\frac{-1-\sqrt{5}}{2}\right)^2 - 4}}{2} = \frac{-1 - \sqrt{5} \pm \sqrt{2\sqrt{5} - 10}}{4}.$$

ζ must be one of these four numbers. Since $2\sqrt{5} - 10 < 0$, the real parts of these numbers are $\frac{-1+\sqrt{5}}{4}$ and $\frac{-1-\sqrt{5}}{4}$. The real part of ζ is > 0 since $0 < \frac{2\pi}{5} < \frac{\pi}{2}$, so

$$\cos\left(\frac{2\pi}{5}\right) = \mathrm{Re}(e^{\frac{2\pi i}{5}}) = \frac{-1 + \sqrt{5}}{4}.$$

□

Wednesday, November 25, 2020

Example 11: Prove that $\cos\left(\frac{\pi}{30}\right)$ is an irrational number.

Solution: One idea that is needed is that if r is a rational number, that is, if $r \in \mathbb{Q}$, and if $p(x) \in \mathbb{Q}[x]$, that is, if $p(x)$ is a polynomial with coefficients in $\mathbb{Q}$, then $p(r)$ is also a rational number since adding and multiplying fractions produces a fraction.

The other idea that is needed is one we have seen before in some specific cases, namely that $\cos(n\theta)$ (where $n \in \mathbb{N}$) is a polynomial in $\cos(\theta)$ with coefficients in $\mathbb{Z}$. Combining these two ideas, we see that if $\cos(\theta)$ is a rational number, then so is $\cos(n\theta)$. The contrapositive of this statement is that if $\cos(n\theta)$ is not rational, then $\cos(\theta)$ is also not a rational number.

We can thus use proof by contradiction if we can find an integer n for which $\cos\left(\frac{n\pi}{30}\right)$ is known to be irrational. If $n = 5$, then $\frac{n\pi}{30} = \frac{\pi}{6}$ and $\cos\left(\frac{\pi}{6}\right) = \frac{\sqrt{3}}{2}$, which is an irrational number.

For any angle θ, we have that $\cos(5\theta)$ is the real part of $e^{5i\theta}$ and

$$e^{5i\theta} = (e^{i\theta})^5 = (\cos(\theta) + i\sin(\theta))^5 = \sum_{k=0}^{5} \binom{5}{k} \cos(\theta)^k (i\sin(\theta))^{5-k}$$

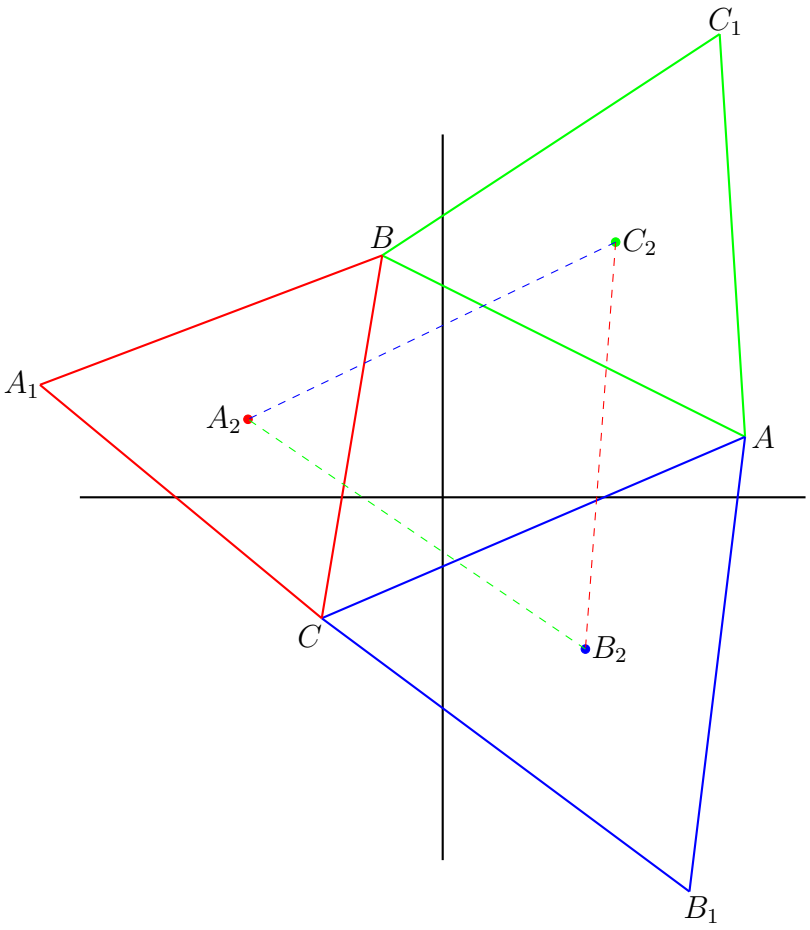
The terms in this sum which are real are those for which $5 - k$ is even, that is, when k is odd. Therefore,

$$\begin{aligned}
\cos(5\theta) &= \mathrm{Re}\left(e^{5i\theta}\right) \\
&= \binom{5}{4} \cos(\theta)(i\sin(\theta))^4 + \binom{5}{3} \cos(\theta)^3 (i\sin(\theta))^{5-3} + \binom{5}{5} \cos(\theta)^5 \\
&= 5\cos(\theta)(\sin(\theta)^2)^2 - 10\cos(\theta)^3 \sin(\theta)^2 + \cos(\theta)^5 \\
&= 5\cos(\theta)(1 - \cos(\theta)^2)^2 - 10\cos(\theta)^3(1 - \cos(\theta)^2) + \cos(\theta)^5 \\
&= 16\cos(\theta)^5 - 20\cos(\theta)^3 + 5\cos(\theta)
\end{aligned}$$

Setting $\theta = \frac{\pi}{30}$, we see that if $\cos\left(\frac{\pi}{30}\right)$ was rational, then $\cos\left(\frac{5\pi}{30}\right)$ would also be rational. However, as pointed above, since $\frac{5\pi}{30} = \frac{\pi}{6}$, $\cos\left(\frac{5\pi}{30}\right)$ is irrational. It follows that $\cos\left(\frac{\pi}{30}\right)$ must be irrational also. □

Example 12: Consider a triangle T with vertices A, B and C. and draw outwardly, on each of its three sides, an equilateral triangle. Call the new vertices A_1, B_1 and C_1 so that the three equilateral triangles are ΔA_1BC, ΔAB_1C and ΔABC_1. Let A_2 be the center of ΔA_1BC, let B_2 be the center of ΔAB_1C and similarly for C_2 and ΔABC_1. See the picture below.

Prove that the triangle $\Delta A_2B_2C_2$ is equilateral.



Solution: Let's view all those points as complex numbers in the plane. Since A_2, B_2 and C_2 are the centers of their respective triangles,

$$A_2 = \frac{A_1 + B + C}{3},\ B_2 = \frac{A + C + B_1}{3},\ C_2 = \frac{A + B + C_1}{3}.$$

Let $\zeta = e^{\frac{i\pi}{3}}$. Then multiplication by ζ rotates a complex number by an angle of $\frac{\pi}{3}$ counter-clockwise. Therefore, as can be seen on the diagram above,

$$A_1 = C + (B - C)\zeta,\ B_1 = A + (C - A)\zeta,\ \ C_1 = B + (A - B)\zeta.$$

From these equations, it follows that

$$\begin{aligned} A_2 - C_2 &= \frac{2C - A - B + \zeta(2B - A - C)}{3} \\ A_2 - B_2 &= \frac{C + B - 2A + \zeta(A + B - 2C)}{3} \\ B_2 - C_2 &= \frac{A + C - 2B + \zeta(B + C - 2A)}{3} \end{aligned}$$

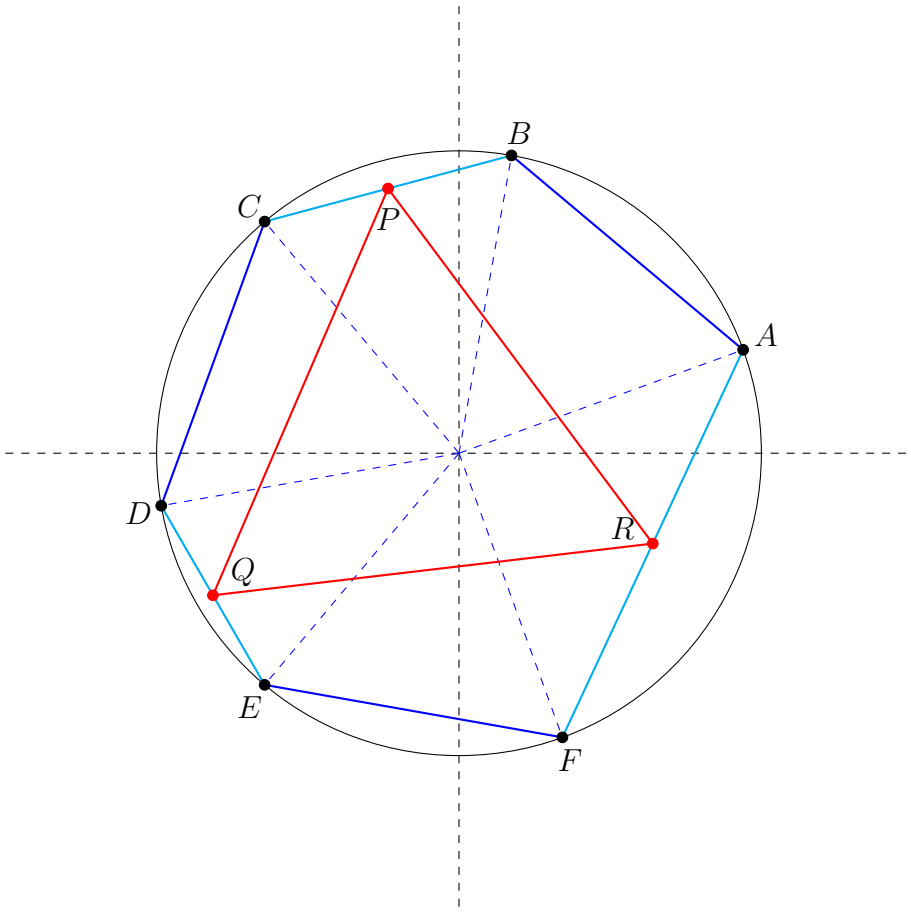
We will need to use that $\zeta^2 - \zeta + 1 = 0$. This follows from the fact that $\zeta^3 = e^{i\pi} = -$, so $\zeta^3 + 1 = 0$ and $(\zeta + 1)(\zeta^2 - \zeta + 1) = 0$: since $\zeta \neq -1$, $\zeta^2 - \zeta + 1 = 0$. Therefore,

$$\begin{aligned}(A_2 - C_2)\zeta &= \frac{(2C - A - B)\zeta}{3} + \frac{\zeta^2(2B - A - C)}{3} \\ &= \frac{(2C - A - B)\zeta}{3} + \frac{(\zeta - 1)(2B - A - C)}{3} \\ &= \frac{A + C - 2B}{3} + \frac{\zeta(B + C - 2A)}{3} \\ &= B_2 - C_2.\end{aligned}$$

This shows that the sides A_2C_2 is of the same length as B_2C_2 and the angle between them is $\frac{\pi}{3}$. □

Wednesday, December 2, 2020

Example 13. [1967 Putnam, B–1] Let $(ABCDEF)$ be a hexagon inscribed in a circle of radius r. Show that if $\overline{AB} = \overline{CD} = \overline{EF} = r$, then the midpoints of $\overline{BC}, \overline{DE}, \overline{FA}$ are the vertices of an equilateral triangle.



Solution: Let $\theta_A, \theta_B, \theta_C, \theta_D, \theta_E, \theta_F$ be the angles such that $A = e^{i\theta_A}$, $B = e^{i\theta_B}$, $C = e^{i\theta_C}$, $D = e^{i\theta_D}$, $E = e^{i\theta_E}$ and $F = e^{i\theta_F}$. Then

$$P = \frac{1}{2}(e^{i\theta_B} + e^{i\theta_C}),\ Q = \frac{1}{2}(e^{i\theta_D} + e^{i\theta_E}),\ R = \frac{1}{2}(e^{i\theta_F} + e^{i\theta_A})$$

and

$$\overline{QP} = P - Q = \frac{1}{2}(e^{i\theta_B} + e^{i\theta_C} - e^{i\theta_D} - e^{i\theta_E})$$
$$\overline{QR} = R - Q = \frac{1}{2}(e^{i\theta_F} + e^{i\theta_A} - e^{i\theta_D} - e^{i\theta_E})$$

The triangle ΔPQR is equilateral if we can show that $\overline{QP}$ is obtained by rotating $\overline{QR}$ by $\frac{\pi}{3}$, that is, if we can show that $\overline{QP} = e^{\frac{\pi i}{3}} \cdot \overline{QR}$.

$$\begin{aligned} e^{\frac{\pi i}{3}} \cdot \overline{QR} &= \frac{1}{2} e^{\frac{\pi i}{3}}(e^{i\theta_F} + e^{i\theta_A} - e^{i\theta_D} - e^{i\theta_E}) \\ &= \frac{1}{2}(e^{i\theta_F + \frac{\pi i}{3}} + e^{i\theta_A + \frac{\pi i}{3}} - e^{i\theta_D + \frac{\pi i}{3}} - e^{i\theta_E + \frac{\pi i}{3}}) \\ &= \frac{1}{2}(e^{i\theta_F + \frac{\pi i}{3}} + e^{i\theta_B} - e^{i\theta_D + \frac{\pi i}{3}} - e^{i\theta_F}) \end{aligned} \tag{8}$$

By assumption, ΔOCD is an equilateral triangle, so $\overline{DC}$ is obtained from $\overline{DO}$ by rotating it by $\frac{\pi}{3}$ around D, so

$$\overline{DC} = C - D = e^{\frac{\pi i}{3}} \cdot \overline{DO} = -e^{\frac{\pi i}{3}} e^{i\theta_D},$$

so

$$e^{i\theta_C} - e^{i\theta_D} = -e^{\frac{\pi i}{3} + i\theta_D}. \tag{9}$$

Similarly, since the triangle ΔOEF is equilateral, $\overline{FE}$ is obtained from $\overline{FO}$ by rotating it by $\frac{\pi}{3}$ around F, so

$$\overline{FE} = E - F = e^{\frac{\pi i}{3}} \cdot \overline{FO} = -e^{\frac{\pi i}{3}} e^{i\theta_F},$$

so

$$e^{i\theta_E} - e^{i\theta_F} = -e^{\frac{\pi i}{3} + i\theta_F}. \tag{10}$$

It follows from (8), (9) and (10) that

$$e^{\frac{\pi i}{3}} \cdot \overline{QR} = \frac{1}{2}(-e^{i\theta_E} + e^{i\theta_B} + e^{i\theta_C} - e^{i\theta_D}) = \overline{QP}.$$

This proves that $\overline{QP}$ is obtained by rotating $\overline{QR}$ by $\frac{\pi}{3}$, hence the triangle ΔPQR is equilateral. □

Example 14. [2015 Putnam, A–3] Compute

$$\log_2\left(\prod_{a=1}^{2015}\prod_{b=1}^{2015}(1+e^{2\pi iab/2015})\right)$$

Here i is the imaginary unit (that is, $i^2=-1$).

Solution: If ζ is a primitive n^{th} root-of-unity, then

$$x^{n-1}+x^{n-2}+\cdots+x^2+x+1=(x-\zeta)(x-\zeta^2)\cdots(x-\zeta^{n-1}).$$

If n is odd, setting $x=-1$ in the previous identity shows that

$$1=(1+\zeta)(1+\zeta^2)\cdots(1+\zeta^{n-1}). \tag{11}$$

If $\gcd(ab,2015)=1$, then $e^{2\pi iab/2015}$ is a primitive 2015^{th} root-of-unity. In particular, if $ab\equiv k \bmod 2015$ and $0\leqslant k\leqslant 2014$, then $e^{2\pi iab/2015}=e^{2\pi ik/2015}$ and

$$\prod_{l=1}^{2014}(1+e^{2\pi ikl/2015})=1 \text{ by (11)}.$$

If $\gcd(ab,2015)=1$, then $\gcd(a,2015)=1$ and $\gcd(b,2015)=1$. This suggests considering various cases depending on the value of $\gcd(a,2015)$.

Note that $2015=5\cdot 403=5\cdot 13\cdot 31$. In all the cases below, let $d=\gcd(a,2015)$, $e=\frac{2015}{d}$, $\widetilde{a}=\frac{a}{d}$ and set $\zeta=e^{2\pi ia/2015}=e^{2\pi\widetilde{a}i/e}$, so ζ is a primitive e^{th} root-of-unity and $\zeta^e=1$. It is primitive since $\gcd(\widetilde{a},e)=1$.

Given a positive integer n, let's denote by $\phi(n)$ the number of integers between 1 and n relatively prime to n. This is called Euler's totient function.

Case 1: $\gcd(a,2015)=1$

Then, using (11),

$$\prod_{b=1}^{2015}(1+e^{2\pi iab/2015})=\prod_{b=1}^{2015}(1+\zeta^b)=\left(\prod_{b=1}^{2014}(1+\zeta^b)\right)(1+\zeta^{2015})=1\cdot(1+1)=1\cdot 2=2.$$

Therefore,

$$\prod_{\substack{a=1\\ \gcd(a,2015)=1}}^{2015}\prod_{b=1}^{2015}(1+e^{2\pi iab/2015})=2^{\phi(2015)}$$

as each integer a such that $\gcd(a,2015)=1$ contributes a factor of 2 and there are $\phi(2015)$ such integers.

Case 2: $\gcd(a, 2015) = 2015$

In this case, $a = 2015$ and $1 + e^{2\pi iab/2015} = 1 + e^{2\pi ib} = 1 + 1 = 2$, so

$$\prod_{b=1}^{2015}(1 + e^{2\pi iab/2015}) = \prod_{b=1}^{2015}(1 + e^{2\pi ib}) = 2^{2015}.$$

Case 3: $\gcd(a, 2015) = 5$

Then $e = \frac{2015}{5} = 403$, ζ is a primitive 403^{th} root-of-unity and

$$\prod_{b=1}^{403}(1 + e^{2\pi iab/2015}) = \prod_{b=1}^{403}(1 + \zeta^b) = \left(\prod_{b=1}^{402}(1 + \zeta^b)\right)(1 + \zeta^{403}) = 1 \cdot (1 + 1) = 1 \cdot 2 = 2.$$

Similarly, since $\zeta^{403} = 1$,

$$\prod_{b=404}^{2\cdot 403}(1 + e^{2\pi iab/2015}) = \prod_{b=404}^{2\cdot 403}(1 + \zeta^b) = \prod_{b=1}^{403}(1 + \zeta^b) = 1 \cdot 2 = 2.$$

More generally, for any $k \in \mathbb{Z}_{\geqslant 0}$, since $\zeta^{403k} = 1$,

$$\prod_{b=k\cdot 403+1}^{(k+1)\cdot 403}(1 + e^{2\pi iab/2015}) = \prod_{b=k\cdot 403+1}^{(k+1)\cdot 403}(1 + \zeta^b) = \prod_{b=1}^{403}(1 + \zeta^b) = 2.$$

Therefore, since $2015 = 5 \cdot 403$,

$$\begin{aligned}
\prod_{b=1}^{2015}(1 + e^{2\pi iab/2015}) &= \prod_{b=1}^{2015}(1 + \zeta^b) \\
&= \left(\prod_{b=1}^{403}(1 + \zeta^b)\right)\left(\prod_{b=404}^{2\cdot 403}(1 + \zeta^b)\right)\left(\prod_{b=2\cdot 403+1}^{3\cdot 403}(1 + \zeta^b)\right) \\
&\quad \cdot \left(\prod_{b=3\cdot 403+1}^{4\cdot 403}(1 + \zeta^b)\right)\left(\prod_{b=4\cdot 403+1}^{5\cdot 403}(1 + \zeta^b)\right) \\
&= \left(\prod_{b=1}^{403}(1 + \zeta^b)\right)^5 \\
&= 2^5.
\end{aligned}$$

Furthermore,

$$\prod_{\substack{a=1 \\ \gcd(a,2015)=5}}^{2015}\prod_{b=1}^{2015}(1 + e^{2\pi iab/2015}) = 2^{5\cdot\phi(403)}.$$

The last equality follows from the fact that the number of integers a between 1 and 2015 such that $\gcd(a, 2015) = 5$ is $\phi\left(\frac{2015}{5}\right) = \phi(403)$ since a must be of the form $a = 5 \cdot \widetilde{a}$ with $\gcd(\widetilde{a}, 403) = 1$, $1 \leqslant \widetilde{a} \leqslant 403$, so there are $\phi(403)$ possibilities for $\widetilde{a}$.

Case 4,5,6,7,8: It would be possible to consider the five remaining cases separately, that is, when $d = 13, 31, 65, 155$ and $d = 403$. However, if we look at the solution when $d = 5$ above, we can see that the same solution works if 5 is replaced by any divisor of 2015. We can thus write the general solution for any value of d.

More generally, for any value of the greatest common divisor d,

$$\prod_{b=1}^{e}(1+e^{2\pi iab/2015}) = \prod_{b=1}^{e}(1+\zeta^b) = \left(\prod_{b=1}^{e-1}(1+\zeta^b)\right)(1+\zeta^e) = 1\cdot(1+1) = 1\cdot 2 = 2.$$

Furthermore, for any $k \geqslant 0$, since $\zeta^e = 1$,

$$\prod_{b=ke+1}^{(k+1)e}(1+e^{2\pi iab/2015}) = \prod_{b=ke+1}^{(k+1)e}(1+\zeta^b) = \prod_{b=1}^{e}(1+\zeta^b) = 2.$$

It follows that, since $2015 = d \cdot e$,

$$\begin{aligned}\prod_{b=1}^{2015}(1+e^{2\pi iab/2015}) = &\left(\prod_{b=1}^{e}(1+e^{2\pi iab/2015})\right)\left(\prod_{b=e+1}^{2e}(1+e^{2\pi iab/2015})\right)\cdots \\ &\cdots\left(\prod_{b=(d-1)e+1}^{2015}(1+e^{2\pi iab/2015})\right) \\ &= 2^d\end{aligned}$$

and

$$\prod_{\substack{a=1\\ \gcd(a,2015)=d}}^{2015}\prod_{b=1}^{2015}(1+e^{2\pi iab/2015}) = 2^{d\cdot\phi\left(\frac{2015}{d}\right)}. \tag{12}$$

The last equality follows from the fact that the number of integers a between 1 and 2015 such that $\gcd(a, 2015) = d$ is $\phi\left(\frac{2015}{d}\right)$, which equals $\phi(e)$, since $a = d \cdot \widetilde{a}$ and $\widetilde{a}$ could be any integer between 1 and e such that $\gcd(\widetilde{a}, e) = 1$.

It follows from (12) that

$$\prod_{a=1}^{2015}\prod_{b=1}^{2015}(1+e^{2\pi iab/2015}) = \prod_{d\,|\,2015}\prod_{\substack{a=1\\ \gcd(a,2015)=d}}^{2015}\prod_{b=1}^{2015}(1+e^{2\pi iab/2015}) = \prod_{d\,|\,2015}2^{d\cdot\phi\left(\frac{2015}{d}\right)}.$$

Taking $\log_2$, we see that the answer is

$$\sum_{d\,|\,2015} d\cdot\phi\left(\frac{2015}{d}\right).$$

It remains to calculate $\phi(e)$ for any divisor e of 2015. If e is prime, then $\phi(e) = e-1$. If $e = rs$ with r and s both primes, then $\phi(e) = rs-r-s+1$. In particular, $\phi(65) = 65-5-13+1 = 48$, $\phi(155) = 155-5-31+1 = 120$ and $\phi(403) = 403-31-13+1 = 360$. If $e = 2015$, then

$$\phi(2015) = 2015-403-155-65+5+13+31-1 = 1440.$$

In conclusion,

$$\begin{aligned}\sum_{d\,|\,2015} d \cdot \phi\left(\frac{2015}{d}\right) &= 2015\phi(1) + 403 \cdot \phi(5) + 155 \cdot \phi(13) + 65 \cdot \phi(31) \\ &\quad + 31 \cdot \phi(65) + 13 \cdot \phi(155) + 5 \cdot \phi(403) + 1 \cdot \phi(2015) \\ &= 2015 + 403 \cdot 4 + 155 \cdot 12 + 65 \cdot 30 + 31 \cdot 48 + 13 \cdot 120 + 5 \cdot 360 + 1440 \\ &= 13725.\end{aligned}$$

□