Theorem 1. *If A and B are two polynomials then:*

(i) $\deg(A \pm B) \le \max(\deg A, \deg B)$, *with the equality if* $\deg A \ne \deg B$.

(ii) $\deg(A \cdot B) = \deg A + \deg B$. $\square$

The conventional equality $\deg 0 = -\infty$ actually arose from these properties of degrees, as else the equality (ii) would not be always true.

Unlike a sum, difference and product, a quotient of two polynomials is not necessarily a polynomial. Instead, like integers, they can be divided with a residue.

Theorem 2. *Given polynomials A and $B \ne 0$, there are unique polynomials Q (quotient) and R (residue) such that*

$$A = BQ + R \quad \textit{and} \quad \deg R < \deg B.$$

Proof. Let $A(x) = a_n x^n + \cdots + a_0$ and $B(x) = b_k x^k + \cdots + b_0$, where $a_n b_k \ne 0$. Assume k is fixed and use induction on n. For $n < k$ the statement is trivial. Suppose that $n = N \ge k$ and that the statement is true for $n < N$. Then $A_1(x) = A(x) - \frac{a_n}{b_k} x^{n-k} B(x)$ is a polynomial of degree less than n (for its coefficient at x^n iz zero); hence by the inductive assumption there are unique polynomials Q_1 and R such that $A_1 = BQ_1 + R$ and $\deg R$. But this also implies

$$A = BQ + R, \quad \text{where} \quad Q(x) = \frac{a_n}{b_k} x^{n-k} + Q_1(x)\,. \ \square$$

Example 2. *The quotient upon division of $A(x) = x^3 + x^2 - 1$ by $B(x) = x^2 - x - 3$ is $x+2$ with the residue $5x + 5$, as*

$$\frac{x^3 + x^2 - 1}{x^2 - x - 3} = x + 2 + \frac{5x + 5}{x^2 - x - 3}.$$

We say that polynomial A is *divisible* by polynomial B if the remainder R when A is divided by B equal to 0, i.e. if there is a polynomial Q such that $A = BQ$.

Theorem 3 (Bezout's theorem). *Polynomial $P(x)$ is divisible by binomial $x - a$ if and only if $P(a) = 0$.*

Proof. There exist a polynomial Q and a constant c such that $P(x) = (x - a)Q(x) + c$. Here $P(a) = c$, making the statement obvious. $\square$

Number a is a *zero (root)* of a given polynomial $P(x)$ if $P(a) = 0$, i.e. $(x - a) \mid P(x)$.

To determine a zero of a polynomial f means to solve the equation $f(x) = 0$. This is not always possible. For example, it is known that finding the exact values of zeros is impossible in general when f is of degree at least 5. Nevertheless, the zeros can always be computed with an arbitrary precision. Specifically, $f(a) < 0 < f(b)$ implies that f has a zero between a and b.

Example 3. *Polynomial $x^2 - 2x - 1$ has two real roots: $x_{1,2} = 1 \pm \sqrt{2}$.*

Polynomial $x^2 - 2x + 2$ has no real roots, but it has two complex roots: $x_{1,2} = 1 \pm i$.

Polynomial $x^5 - 5x + 1$ has a zero in the interval $[1.44, 1.441]$ which cannot be exactly computed.

More generally, the following simple statement holds.

Theorem 4. *If a polynomial P is divisible by a polynomial Q, then every zero of Q is also a zero of P.* $\square$

The converse does not hold. Although every zero of x^2 is a zero of x, x^2 does not divide x.

Problem 1. *For which n is the polynomial $x^n + x - 1$ divisible by a) $x^2 - x + 1$, b) $x^3 - x + 1$?*

Theorem 19 (Newton's interpolating polynomial). *For given numbers $y_0, \dots, y_n$ and distinct $x_0, \dots, x_n$ there is a unique polynomial $P(x)$ of n-th degree such that $P(x_i) = y_i$ for $i = 0, 1, \dots, n$. This polynomial is given by the formula*

$$P(x) = \sum_{i=0}^{n} y_i \prod_{j \neq i} \frac{(x - x_j)}{(x_i - x_j)}. \quad \Box$$

Example 6. *Find the cubic polynomial Q such that $Q(i) = 2^i$ for $i = 0, 1, 2, 3$.*

Solution. $Q(x) = \frac{(x-1)(x-2)(x-3)}{-6} + \frac{2x(x-2)(x-3)}{2} + \frac{4x(x-1)(x-3)}{-2} + \frac{8x(x-1)(x-2)}{6} = \frac{x^3+5x+6}{6}$. $\triangle$

In order to compute the value of a polynomial given in this way in some point, sometimes we do not need to determine its Newton's polynomial. In fact, Newton's polynomial has an unpleasant property of giving the answer in a complicated form.

Example 7. *If the polynomial P of n-th degree takes the value 1 in points $0, 2, 4, \dots, 2n$, compute $P(-1)$.*

Solution. $P(x)$ is of course identically equal to 1, so $P(-1) = 1$. But if we apply the Newton polynomial, here is what we get:

$$P(1) = \sum_{i=0}^{n} \prod_{j \neq i} \frac{1 - 2i}{(2j - 2i)} = \sum_{i=0}^{n} \prod_{j \neq i} \frac{-1 - 2j}{(2i - 2j)} = \frac{(2n+1)!!}{2^n} \sum_{i=1}^{n+1} \frac{(-1)^{n-i}}{(2i+1)i!(n-i)!}. \quad \triangle$$

Instead, it is often useful to consider the *finite difference* of polynomial P, defined by $P^{[1]}(x) = P(x+1) - P(x)$, which has the degree by 1 less than that of P. Further, we define the k-th finite difference, $P^{[k]} = (P^{[k-1]})^{[1]}$, which is of degree $n - k$ (where $\deg P = n$). A simple induction gives a general formula

$$P^{[k]} = \sum_{i=0}^{k} (-1)^{k-i} \binom{k}{i} P(x+i).$$

In particular, $P^{[n]}$ is constant and $P^{[n+1]} = 0$, which leads to

Theorem 20. $P(x+n+1) = \sum_{i=0}^{n} (-1)^{n-i} \binom{n+1}{i} P(x+i)$. $\Box$

Problem 15. *Polynomial P of degree n satisfies $P(i) = \binom{n+1}{i}^{-1}$ for $i = 0, 1, \dots, n$. Evaluate $P(n+1)$.*

Solution. We have

$$0 = \sum_{i=0}^{n+1} (-1)^i \binom{n+1}{i} P(i) = (-1)^{n+1} P(n+1) + \begin{cases} 1, & 2 \mid n; \\ 0, & 2 \nmid n. \end{cases}$$

It follows that $P(n+1) = \begin{cases} 1, & 2 \mid n; \\ 0, & 2 \nmid n. \end{cases}$ $\triangle$

Problem 16. *If $P(x)$ is a polynomial of an even degree n with $P(0) = 1$ and $P(i) = 2^{i-1}$ for $i = 1, \dots, n$, prove that $P(n+2) = 2P(n+1) - 1$.*

Solution. We observe that $P^{[1]}(0) = 0$ i $P^{[1]}(i) = 2^{i-1}$ for $i = 1, \dots, n-1$; furthermore, $P^{[2]}(0) = 1$ i $P^{[2]}(i) = 2^{i-1}$ for $i = 1, \dots, n-2$, etc. In general, it is easily seen that $P^{[k]}(i) = 2^{i-1}$ for $i = 1, \dots, n-k$, and $P^{[k]}(0)$ is 0 for k odd and 1 for k even. Now

$$P(n+1) = P(n) + P^{[1]}(n) = \dots = P(n) + P^{[1]}(n-1) + \dots + P^{[n]}(0) = \begin{cases} 2^n, & 2 \mid n; \\ 2^n - 1, & 2 \nmid n. \end{cases}$$

Similarly, $P(n+2) = 2^{2n+1} - 1$. $\triangle$

19. If P and Q are monic polynomials such that $P(P(x)) = Q(Q(x))$, prove that $P \equiv Q$.

20. Let m, n and a be natural numbers and $p < a - 1$ a prime number. Prove that the polynomial $f(x) = x^m(x-a)^n + p$ is irreducible.

21. Prove that the polynomial $F(x) = (x^2 + x)^{2^n} + 1$ is irreducible for all $n \in \mathbb{N}$.

22. A polynomial $P(x)$ has the property that for every $y \in \mathbb{Q}$ there exists $x \in \mathbb{Q}$ such that $P(x) = y$. Prove that P is a linear polynomial.

23. Let $P(x)$ be a monic polynomial of degree n whose zeros are $i-1, i-2, \dots, i-n$ (where $i^2 = -1$) and let $R(x)$ and $S(x)$ be the real polynomials such that $P(x) = R(x) + iS(x)$. Prove that the polynomial $R(x)$ has n real zeros.

24. Let a, b, c be natural numbers. Prove that if there exist coprime polynomials P, Q, R with complex coefficients such that
$$P^a + Q^b = R^c,$$
then $\frac{1}{a} + \frac{1}{b} + \frac{1}{c} > 1$.

    Corollary: The Last Fermat Theorem for polynomials.

25. Suppose that all zeros of a monic polynomial $P(x)$ with integer coefficients are of module 1. Prove that there are only finitely many such polynomials of any given degree; hence show that all its zeros are actually roots of unity, i.e. $P(x) \mid (x^n - 1)^k$ for some natural n, k.

9 Solutions

1. The polynomial $f(x) - 10x$ vanishes at points $x = 1, 2, 3$, so it is divisible by polynomial $(x-1)(x-2)(x-3)$. The monicity implies that $f(x) - 10x = (x-1)(x-2)(x-3)(x-c)$ for some c. Now
$$f(12) + f(-8) = 11 \cdot 10 \cdot 9 \cdot (12 - c) + 120 + (-9)(-10)(-11)(-8-c) - 80 = 19840.$$

2. Note that $Q(x^2) = \prod(x^2 - x_i^2) = \prod(x - x_i) \cdot \prod(x + x_i) = (-1)^n P(x)P(-x)$. We now have
$$b_1 + b_2 + \dots + b_n = Q(1) - 1 = (-1)^n P(1)P(-1) - 1 = (-1)^n(1 + B - A)(1 + B + A),$$
where $A = a_1 + a_3 + a_5 + \cdots$ and $B = a_2 + a_4 + \cdots$.

3. It follows from the conditions that $P(-\sin x) = P(\sin x)$, i.e. $P(-t) = P(t)$ for infinitely many t, so the polynomials $P(x)$ and $P(-x)$ coincide. Therefore, $P(x) = S(x^2)$ for some polynomial S. Now $S(\cos^2 x) = S(\sin^2 x)$ for all x, i.e. $S(1-t) = S(t)$ for infinitely many t, which implies $S(x) \equiv S(1-x)$. This is equivalent to $R(x - \frac{1}{2}) = R(\frac{1}{2} - x)$, i.e. $R(y) \equiv R(-y)$, where R is a polynomial such that $S(x) = R(x - \frac{1}{2})$. Now $R(x) = T(x^2)$ for some polynomial T, and therefore $P(x) = S(x^2) = R(x^2 - \frac{1}{2}) = T(x^4 - x^2 + \frac{1}{4}) = Q(x^4 - x^2)$ for some polynomial Q.

4. (a) Clearly, $T_0(x) = 1$ and $T_1(x) = x$ satisfy the requirements. For $n > 1$ we use induction on n. Since $\cos(n+1)x = 2\cos x \cos nx - \cos(n-1)x$, we can define $T_{n+1} = 2T_1T_n - T_{n-1}$. Since T_1T_n and T_{n-1} are of degrees $n+1$ and $n-1$ respectively, T_{n+1} is of degree $n+1$ and has the leading coefficient $2 \cdot 2^n = 2^{n+1}$. It also follows from the construction that all its coefficients are integers.

   (b) The relation follows from the identity $\cos(m+n)x + \cos(m-n)x = 2\cos mx \cos nx$.