Polynomial Equations

Dušan Djukić

Contents

1 Introduction

The title refers to determining polynomials in one or more variables (e.g. with real or complex coefficients) which satisfy some given relation(s).

The following example illustrates some basic methods:

1. Determine the polynomials P for which $16P(x^2) = P(2x)^2$.

- *First method: evaluating at certain points and reducing degree.*

  Plugging $x = 0$ in the given relation yields $16P(0) = P(0)^2$, i.e. $P(0) = 0$ or 16.

  (i) Suppose that $P(0) = 0$. Then $P(x) = xQ(x)$ for some polynomial Q and $16x^2Q(x^2) = 4x^2Q(2x)^2$, which reduces to $4Q(x^2) = Q(2x)^2$. Now setting $4Q(x) = R(x)$ gives us $16R(x^2) = R(2x)^2$. Hence, $P(x) = \frac{1}{4}xR(x)$, with R satifying the same relation as P.

  (ii) Suppose that $P(0) = 16$. Putting $P(x) = xQ(x) + 16$ in the given relation we obtain $4xQ(x^2) = xQ(2x)^2 + 16Q(2x)$; hence $Q(0) = 0$, i.e. $Q(x) = xQ_1(x)$ for some polynomial Q_1. Furthermore, $x^2Q_1(x^2) = x^2Q_1(2x)^2 + 8Q_1(2x)$, implying that $Q_1(0) = 0$, so Q_1 too is divisible by x. Thus $Q(x) = x^2Q_1(x)$. Now suppose that x^n is the highest degree of x dividing Q, and $Q(x) = x^nR(x)$, where $R(0) \neq 0$. Then R satisfies $4x^{n+1}R(x^2) = 2^{2n}x^{n+1}R(2x)^2 + 2^{n+4}R(2x)$, which implies that $R(0) = 0$, a contradiction. It follows that $Q \equiv 0$ and $P(x) \equiv 16$.

  We conclude that $P(x) = 16\left(\frac{1}{4}x\right)^n$ for some $n \in \mathbb{N}_0$.

- *Second method: investigating coefficients.*

  We start by proving the following lemma (to be used frequently):

  Lemma 1. *If $P(x)^2$ is a polynomial in x^2, then so is either $P(x)$ or $P(x)/x$.*

  Proof. Let $P(x) = a_nx^n + a_{n-1}x^{n-1} + \cdots + a_0$, $a_n \neq 0$. The coefficient at x^{2n-1} is $2a_na_{n-1}$, from which we get $a_{n-1} = 0$. Now the coefficient at x^{2n-3} equals $2a_na_{n-3}$; hence $a_{n-3} = 0$, and so on. Continuing in this manner we conclude that $a_{n-2k-1} = 0$ for $k = 0, 1, 2, \dots$, i.e. $P(x) = a_nx^n + a_{n-2}x^{n-2} + a_{n-4}x^{n-4} + \cdots$. △

  Since $P(x)^2 = 16P(x^2/4)$ is a polynomial in x^2, we have $P(x) = Q(x^2)$ or $P(x) = xQ(x^2)$. In the former case we get $16Q(x^4) = Q(4x^2)^2$ and therefore $16Q(x^2) = Q(4x)^2$; in the latter case we similarly get $4Q(x^2) = Q(4x)^2$. In either case, $Q(x) = R(x^2)$ or $Q(x) = xR(x^2)$ for some polynomial R, so $P(x) = x^i R(x^4)$ for some $i \in \{0,1,2,3\}$. Proceeding in this way we find that $P(x) = x^i S(x^{2^k})$ for each $k \in \mathbb{N}$ and some $i \in \{0,1,\dots,2^k\}$. Now it is enough to take k with $2^k > \deg P$ and to conclude that S must be constant. Thus $P(x) = cx^i$ for some $c \in \mathbb{R}$. A simple verification gives us the general solution $P(x) = 16\left(\frac{1}{4}x\right)^n$ for $n \in \mathbb{N}_0$.

Investigating zeroes of the unknown polynomial is also counted under the first method.

A majority of problems of this type can be solved by one of the above two methods (although some cannot, making math more interesting!).

2 Problems with Solutions

1. Find all polynomials P such that $P(x)^2 + P(\frac{1}{x})^2 = P(x^2)P(\frac{1}{x^2})$.

   Solution. By the introducing lemma there exists a polynomial Q such that $P(x) = Q(x^2)$ or $P(x) = xQ(x^2)$. In the former case $Q(x^2)^2 + Q(\frac{1}{x^2}) = Q(x^4)Q(\frac{1}{x^4})$ and therefore $Q(x)^2 + Q(\frac{1}{x}) = Q(x^2)Q(\frac{1}{x^2})$ (which is precisely the relation fulfilled by P), whereas in the latter case (similarly) $xQ(x)^2 + \frac{1}{x}Q(\frac{1}{x})^2 = Q(x^2)Q(\frac{1}{x^2})$ which is impossible for the left and right hand side have odd and even degrees, respectively. We conclude that $P(x) = Q(x^2)$, where Q is also a solution of the considered polynomial equation. Considering the solution of the least degree we find that P must be constant.

2. Do there exist non-linear polynomials P and Q such that $P(Q(x)) = (x-1)(x-2)\cdots(x-15)$?

   Solution. Suppose there exist such polynomials. Then $\deg P \cdot \deg Q = 15$, so $\deg P = k \in \{3,5\}$. Putting $P(x) = c(x-a_1)\cdots(x-a_k)$ we get $c(Q(x)-a_1)\cdots(Q(x)-a_k) = (x-1)(x-2)\cdots(x-15)$. Thus the roots of polynomial $Q(x)-a_i$ are distinct and comprise the set $\{1,2,\dots,15\}$. All these polynomials mutually differ at the last coefficient only. Now, investigating parity of the remaining (three or five) coefficients we conclude that each of them has the equally many odd roots. This is impossible, since the total number of odd roots is 8, not divisible by 3 or 5.

3. Determine all polynomials P for which $P(x)^2 - 2 = 2P(2x^2-1)$.

   Solution. Denote $P(1) = a$. We have $a^2 - 2a - 2 = 0$. Substituting $P(x) = (x-1)P_1(x) + a$ in the initial relation and simplifying yields $(x-1)P_1(x)^2 + 2aP_1(x) = 4(x+1)P_1(2x^2-1)$. For $x = 1$ we have $2aP_1(1) = 8P_1(1)$, which (since $a \neq 4$) gives us $P_1(1) = 0$, i.e. $P_1(x) = (x-1)P_2(x)$, so $P(x) = (x-1)^2P_2(x) + a$. Suppose that $P(x) = (x-1)^nQ(x) + a$, where $Q(1) \neq 0$. Substituting in the initial relation and simplifying yields $(x-1)^nQ(x)^2 + 2aQ(x) = 2(2x+2)^nQ(2x^2-1)$, giving us $Q(1) = 0$, a contradiction. It follows that $P(x) = a$.

4. Determine all polynomials P for which $P(x)^2 - 1 = 4P(x^2-4x+1)$.

   Solution. Suppose that P is not constant. Fixing $\deg P = n$ and comparing coefficients of both sides we deduce that the coefficients of polynomial P must be rational. On the other hand, setting $x = a$ with $a = a^2 - 4a + 1$, that is, $a = \frac{5\pm\sqrt{21}}{2}$, we obtain $P(a) = b$, where $b^2 - 4b - 1 = 0$, i.e. $b = 2 \pm \sqrt{5}$. However, this is impossible because $P(a)$ must be of the form $p + q\sqrt{21}$ for some rational p,q for the coefficients of P are rational. It follows that $P(x)$ is constant.

5. For which real values of a does there exist a rational function $f(x)$ that satisfies $f(x^2) = f(x)^2 - a$?

   Solution. Write f as $f = P/Q$ with P and Q coprime polynomials and Q monic. By comparing leading coefficients we obtain that P too is monic. The condition of the problem became $P(x^2)/Q(x^2) = P(x)^2/Q(x)^2 - a$. Since $P(x^2)$ and $Q(x^2)$ are coprime (if, to the contrary, they had a zero in common, then so do P and Q), it follows that $Q(x^2) = Q(x)^2$. Therefore $Q(x) = x^n$ for some $n \in \mathbb{N}$. Now we have $P(x^2) = P(x)^2 - ax^{2n}$.

Let $P(x) = a_0 + a_1x + \cdots + a_{m-1}x^{m-1} + x^m$. Comparing coefficients of $P(x)^2$ and $P(x^2)$ gives us $a_{n-1} = \cdots = a_{2m-n+1} = 0$, $a_{2m-n} = a/2$, $a_1 = \cdots = a_{m-1} = 0$ and $a_0 = 1$. This is only possible if $a = 2$ and $2m - n = 0$, or $a = 0$.

6. Find all polynomials P satisfying $P(x^2+1) = P(x)^2 + 1$ for all x.

Solution. By the introducing lemma, there is a polynomial Q such that $P(x) = Q(x^2+1)$ or $P(x) = xQ(x^2+1)$. Then $Q((x^2+1)^2+1) = Q(x^2+1)^2 - 1$ or $(x^2+1)Q((x^2+1)^2+1) = x^2Q(x^2+1)^2 + 1$, respectively. Substituting $x^2+1 = y$ yields $Q(y^2+1) = Q(y)^2 + 1$ and $yQ(y^2+1) = (y-1)Q(y)^2 + 1$, respectively.

Suppose that $yQ(y^2+1) = (y-1)Q(y)^2 + 1$. Setting $y = 1$ we obtain that $Q(2) = 1$. Note that, if $a \neq 0$ and $Q(a) = 1$, then also $aQ(a^2+1) = (a-1)+1$ and hence $Q(a^2+1) = 1$. We thus obtain an infinite sequence of points at which Q takes value 1, namely the sequence given by $a_0 = 2$ and $a_{n+1} = a_n^2 + 1$. Therefore $Q \equiv 1$.

It follows that if $Q \not\equiv 1$, then $P(x) = Q(x^2+1)$. Now we can easily list all solutions: these are the polynomials of the form $T(T(\cdots(T(x))\cdots))$, where $T(x) = x^2 + 1$.

7. If a polynomial P with real coefficients satisfies for all x

$$P(\cos x) = P(\sin x),$$

prove that there exists a polynomial Q such that for all x, $P(x) = Q(x^4 - x^2)$.

Solution. It follows from the condition of the problem that $P(-\sin x) = P(\sin x)$, so $P(-t) = P(t)$ for infinitely many t; hence 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, so $S(1-t) = S(t)$ for infinitely many t, which gives us $S(x) \equiv S(1-x)$. This is equivalent to $R(x - \frac{1}{2}) = R(\frac{1}{2} - x)$, i.e. $R(y) \equiv R(-y)$, where R is the polynomial such that $S(x) = R(x - \frac{1}{2})$. Now $R(x) = T(x^2)$ for some polynomial T, and finally, $P(x) = S(x^2) = R(x^2 - \frac{1}{2}) = T(x^4 - x^2 + \frac{1}{4}) = Q(x^4 - x^2)$ for some polynomial Q.

8. Find all quadruples of polynomials (P_1, P_2, P_3, P_4) such that, whenever natural numbers x, y, z, t satisfy $xy - zt = 1$, it holds that $P_1(x)P_2(y) - P_3(z)P_4(t) = 1$.

Solution. Clearly $P_1(x)P_2(y) = P_2(x)P_1(y)$ for all natural numbers x and y. This implies that $P_2(x)/P_1(x)$ does not depend on x. Hence $P_2 = cP_1$ for some constant c. Analogously, $P_4 = dP_3$ for some constant d. Now we have $cP_1(x)P_1(y) - dP_3(z)P_3(t) = 1$ for all natural x, y, z, t with $xy - zt = 1$. Moreover, we see that $P_1(x)P_1(y)$ depends only on xy, i.e. $f(x) = P_1(x)P_1(n/x)$ is the same for all positive divisors x of natural number n. Since $f(x)$ is a rational function and the number of divisors x of n can be arbitrarily large, it follows that f is constant in x, i.e. a polynomial in n. It is easily verified that this is possible only when $P_1(x) = x^n$ for some n. Similarly, $P_3(x) = x^m$ for some m and $c(xy)^n - d(zt)^m = 1$. Therefore $m = n$ and $c = d = 1$, and finally $m = n = 1$. So, $P_1(x) = P_2(x) = P_3(x) = P_4(x) = x$.

9. Find all polynomials $P(x)$ with real coefficients that satisfy the equality

$$P(a-b) + P(b-c) + P(c-a) = 2P(a+b+c)$$

for all triples a, b, c of real numbers such that $ab + bc + ca = 0$. *(IMO 2004.2)*

Solution. Let $P(x) = a_0 + a_1x + \cdots + a_nx^n$. For every $x \in \mathbb{R}$ the triple $(a, b, c) = (6x, 3x, -2x)$ satisfies the condition $ab + bc + ca = 0$. Then the condition on P gives us $P(3x) + P(5x) + P(-8x) = 2P(7x)$ for all x, implying that for all $i = 0, 1, 2, \ldots, n$ the following equality holds:

$$\left(3^i + 5^i + (-8)^i - 2 \cdot 7^i\right) a_i = 0.$$

Suppose that $a_i \neq 0$. Then $K(i) = 3^i + 5^i + (-8)^i - 2 \cdot 7^i = 0$. But $K(i)$ is negative for i odd and positive for $i = 0$ or $i \geq 6$ even. Only for $i = 2$ and $i = 4$ do we have $K(i) = 0$. It follows that $P(x) = a_2x^2 + a_4x^4$ for some real numbers a_2, a_4. It is easily verified that all such $P(x)$ satisfy the required condition.

10. (a) If a real polynomial $P(x)$ satisfies $P(x) \geq 0$ for all x, show that there exist real polynomials $A(x)$ and $B(x)$ such that $P(x) = A(x)^2 + B(x)^2$.

(b) If a real polynomial $P(x)$ satisfies $P(x) \geq 0$ for all $x \geq 0$, show that there exist real polynomials $A(x)$ and $B(x)$ such that $P(x) = A(x)^2 + xB(x)^2$.

Solution. Polynomial $P(x)$ can be written in the form

$$P(x) = (x - a_1)^{\alpha_1} \cdots (x - a_k)^{\alpha_k} \cdot (x^2 - b_1x + c_1) \cdots (x^2 - b_mx + c_m), \qquad (*)$$

where a_i, b_j, c_j are real numbers such that a_i are distinct and the polynomials $x^2 - b_ix + c_i$ have no real roots.

It follows from the condition $P(x) \geq 0$ for all x that all the α_i are even, and from the condition $P(x) \geq 0$ for all $x \geq 0$ that $(\forall i)$ either α_i is even or $a_i < 0$. This ensures that each linear or quadratic factor in $(*)$ can be written in the required form $A^2 + B^2$ and/or $A^2 + xB^2$. The well-known formula $(a^2 + \gamma b^2)(c^2 + \gamma d^2) = (ac + \gamma bd)^2 + \gamma(ad - bc)^2$ now gives a required representation for their product $P(x)$.

11. Prove that if the polynomials P and Q have a real root each and

$$P(1 + x + Q(x)^2) = Q(1 + x + P(x)^2),$$

then $P \equiv Q$.

Solution. Note that there exists $x = a$ for which $P(a)^2 = Q(a)^2$. This follows from the fact that, if p and q are the respective real roots of P and Q, then $P(p)^2 - Q(p)^2 \leq 0 \leq P(q)^2 - Q(q)^2$, and moreover $P^2 - Q^2$ is continuous. Now $P(b) = Q(b)$ for $b = 1 + a + P(a)^2$. Taking a to be the largest real number for which $P(a) = Q(a)$ leads to an immediate contradiction.

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

Solution. Suppose that $R = P - Q \neq 0$ and that $0 < k \leq n - 1$ is the degree of $R(x)$. Then

$$P(P(x)) - Q(Q(x)) = [Q(P(x)) - Q(Q(x))] + R(P(x)).$$

Putting $Q(x) = x^n + \cdots + a_1x + a_0$ we have $Q(P(x)) - Q(Q(x)) = [P(x)^n - Q(x)^n] + \cdots + a_1[P(x) - Q(x)]$, where all summands but the first have a degree at most $n^2 - n$, while the first summand equals $R(x) \cdot \left(P(x)^{n-1} + P(x)^{n-2}Q(x) + \cdots + Q(x)^{n-1}\right)$ and therefore has the degree $n^2 - n + k$ with the leading coefficient n. Hence the degree of $Q(P(x)) - Q(Q(x))$ is $n^2 - n + k$. The degree of $R(P(x))$ is equal to $kn < n^2 - n + k$, from what we conclude that the degree of the difference $P(P(x)) - Q(Q(x))$ is $n^2 - n + k$, a contradiction.

In the remaining case when $R \equiv c$ is constant, the condition $P(P(x)) = Q(Q(x))$ gives us $Q(Q(x) + c) = Q(Q(x)) - c$, so the equality $Q(y + c) = Q(y) - c$ holds for infinitely many y, implying $Q(y + c) \equiv Q(y) - c$. But this is only possible for $c = 0$.

13. Assume that there exist complex polynomials P, Q, R such that

$$P^a + Q^b = R^c,$$

where a, b, c are natural numbers. Show that $\frac{1}{a} + \frac{1}{b} + \frac{1}{c} > 1$.

Solution. We use the following auxilliary statement.

Lemma 2. *If A, B and C are pairwise coprime polynomials with $A+B=C$, then the degree of each of them is less than the number of different zeroes of the polynomial ABC.*

Proof. Let

$$A(x)=\prod_{i=1}^{k}(x-p_i)^{a_i},\quad B(x)=\prod_{i=1}^{l}(x-q_i)^{b_i},\quad C(x)=\prod_{i=1}^{m}(x-r_i)^{c_i}.$$

Writing the condition $A+B=C$ as $A(x)C(x)^{-1}+B(x)C(x)^{-1}=1$ and differentiating it with respect to x gives us

$$A(x)C(x)^{-1}\left(\sum_{i=1}^{k}\frac{a_i}{x-p_i}-\sum_{i=1}^{m}\frac{c_i}{x-r_i}\right)=-B(x)C(x)^{-1}\left(\sum_{i=1}^{l}\frac{b_i}{x-q_i}-\sum_{i=1}^{m}\frac{c_i}{x-r_i}\right),$$

from which we see that $A(x)/B(x)$ can be written as a quotient of two polynomials od degrees not exceeding $k+l+m-1$. Our statement now follows from the fact that A and B are coprime. Apply this statement on polynomials P^a, Q^b, R^c. Each of their degrees $a\deg P$, $b\deg Q$, $c\deg R$ is less than $\deg P+\deg Q+\deg R$ and hence $\frac{1}{a}>\frac{\deg P}{\deg P+\deg Q+\deg R}$, etc. Summing up yields the desired inequality.

Corollary. "The Last Fermat's theorem" for polynomials.

14. The lateral surface of a cylinder is divided by $n-1$ planes parallel to the base and m meridians into mn cells ($n\geq 1, m\geq 3$). Two cells are called neighbors if they have a common side. Prove that it is possible to write real numbers in the cells, not all zero, so that the number in each cell equals the sum of the numbers in the neighboring cells, if and only if there exist k,l with $n+1\nmid k$ such that $\cos\dfrac{2l\pi}{m}+\cos\dfrac{k\pi}{n+1}=\dfrac{1}{2}$.

Solution. Denote by a_{ij} the number in the intersection of i-th parallel and j-th meridian. We assign to the i-th parallel the polynomial $p_i(x)=a_{i1}+a_{i2}x+\cdots+a_{im}x^{m-1}$ and define $p_0(x)=p_{n+1}(x)=0$. The property that each number equals the sum of its neighbors can be written as $p_i(x)=p_{i-1}(x)+p_{i+1}(x)+(x^{m-1}+x)p_i(x)$ modulo x^m-1, i.e.

$$p_{i+1}(x)=(1-x-x^{m-1})p_i(x)-p_{i-1}(x)\pmod{x^m-1}.$$

This sequence of polynomials is entirely determined by term $p_1(x)$. The numbers a_{ij} can be written in the required way if and only if a polynomial $p_1(x)\neq 0$ of degree less than m can be chosen so that $p_{n+1}(x)=0$.

Consider the sequence of polynomials $r_i(x)$ given by $r_0=0$, $r_1=1$ and $r_{i+1}=(1-x-x^{m-1})r_i-r_{i-1}$. Clearly, $p_{n+1}(x)\equiv r_{n+1}(x)p_1(x)\pmod{x^m-1}$. Polynomial $p_1\neq 0$ of degree $<m$ for which $p_{n+1}=0$ exists if and only if $r_{n+1}(x)$ and x^m-1 are not coprime, i.e. if and only if there exists ε such that $\varepsilon^m=1$ and $r_{n+1}(\varepsilon)=0$. Now consider the sequence (x_i) given by $x_0=0$, $x_1=1$ and $x_{i+1}=(1-\varepsilon-\varepsilon^{m-1})x_i-x_{i-1}$. Let us write $c=1-\varepsilon-\varepsilon^{m-1}$ and denote by u_1,u_2 the zeroes of polynomial x^2-cx+1. The general term of the above recurrent sequence is $x_i=\dfrac{u_1^i-u_2^i}{u_1-u_2}$ if $u_1\neq u_2$ and $x_i=iu_1^i$ if $u_1=u_2$. The latter case is clearly impossible. In the former case ($u_1\neq u_2$) equality $x_{n+1}=0$ is equivalent to $u_1^{n+1}=u_2^{n+1}$ and hence to $\omega^{n+1}=1$, where $u_1=u_2\omega$, which holds if and only if $(\exists u_2)\ u_2^2\omega=1$ and $u_2(1+\omega)=c$. Therefore $(1+\omega)^2=c^2\omega$, so

$$2+\omega+\overline{\omega}=(1-\varepsilon-\overline{\varepsilon})^2.$$

Now if $\omega=\cos\frac{2k\pi}{n+1}+i\sin\frac{2k\pi}{n+1}$ and $\varepsilon=\cos\frac{2l\pi}{m}+i\sin\frac{2l\pi}{m}$, the above equality becomes the desired one.