Solutions to the Problems on Polynomials

1: Let $p(x)$ be a polynomial over $\mathbf{Z}$ with at least four distinct integral roots. Show that there is no integer k such that $p(k)$ is prime.

Solution: Suppose that $p(a) = p(b) = p(c) = p(d) = 0$ where a, b, c and d are distinct integers. Then we have $p(x) = (x-a)(x-b)(x-c)(x-d)h(x)$ for some polynomial $h(x)$. Thus for all $k \in \mathbf{Z}$, $p(k)$ is a multiple of each of the four distinct integers $(k-a)$, $(k-b)$, $(k-c)$ and $(k-d)$. Either one of these four integers is equal to zero, or two of these four integers are not equal to 0 or ± 1. In either case, $p(k)$ is not prime.

2: Let $p(x)$ be a polynomial over $\mathbf{C}$. Show that $p(x)$ is even if and only if there exists a polynomial $q(x)$ over $\mathbf{C}$ such that $p(x) = q(x)q(-x)$.

Solution: Suppose that $p(x) = q(x)q(-x)$ for some polynomial q. Then we have $p(-x) = q(-x)q(x) = p(x)$, so p is even. Conversely, suppose that p is even. Let $p(x) = a_0 + a_1 x + \cdots + a_n x^n$ where $a_n \neq 0$. Since p is even we have $p(x) = p(-x)$ for all x, so $a_0 + a_1 x + a_2 x^2 + \cdots + a_n x^n = a_0 - a_1 x + a_2 x^2 - \cdots + (-1)^n a_n x^n$ for all x. Comparing coefficients, we see that $0 = a_1 = a_3 = a_5 = \cdots$, so we have

$$p(x) = a_0 + a_2 x^2 + a_4 x^4 + \cdots + a_{2k} x^{2k} = r(x^2),$$

where $r(u) = a_0 + a_2 u + a_4 u^2 + \cdots + a_{2k} u^k$. Say $r(u) = a_{2k}(u - r_1)(u - r_2)\cdots(u - r_k)$. Then we have

$$p(x) = r(x^2) = a_{2k}(x^2 - r_1)(x^2 - r_2)\cdots(x^2 - r_k) = (-1)^k a_{2k}(r_1 - x^2)(r_2 - x^2)\cdots(r_k - x^2)\,.$$

Choose $b_i \in \mathbf{C}$ so that ${b_0}^2 = (-1)^k a_{2k}$ and ${b_i}^2 = r_i$ for $i \geq 1$. Then

$$p(x) = {b_0}^2({b_1}^2 - x^2)({b_2}^2 - x^2)\cdots({b_k}^2 - x^2) = q(-x)q(x)\,,$$

where $q(x) = b_0(b_1 + x)(b_2 + x)\cdots(b_k + x)$.

3: Let $p(x)$ be a polynomial over $\mathbf{R}$ of odd degree. Show that $p(p(x))$ has at least as many real roots as $p(x)$.

Solution: Let $a_1, a_2, \cdots, a_n$ be the distinct real roots of $p(x)$. Note that since $p(x)$ has odd degree, it is onto, and so for each i, we can choose $x_i \in \mathbf{R}$ so that $p(x_i) = a_i$. Note that the numbers x_i are distinct (since $x_i = x_j \Longrightarrow a_i = p(x_i) = p(x_j) = a_j$) and we have $p\big(p(x_i)\big) = p(a_i) = 0$ for all i.

4: Let $p(x)$ be a monic polynomial over $\mathbf{Z}$ with the property that there exist positive integers k and l such that none of the integers $p(k+i)$ with $i = 1, 2, \cdots, l$ is divisible by l. Show that $p(x)$ has no rational roots.

Solution: Let a be a rational root of a monic polynomial p with integer coefficients, and let k and l be positive integers. Since p is monic, we have $a \in \mathbf{Z}$, so $p(x) = (x-a)q(x)$ for some monic polynomial $q(x)$ over $\mathbf{Z}$. For all i we have $p(k+i) = (k+i-a)q(a)$. Choose i with $1 \leq i \leq l$ so that $l \big| (k+i-a)$. Then we have $l \big| p(k+i)$.

5: Let $p(x) = \sum\limits_{k=0}^{2n} (-1)^k (2n+1-k)\, x^k$. Show that $p(x)$ has no real roots.

Solution: When $x \leq 0$, $p(x) = (2n+1) + (2n)|x| + (2n-1)|x|^2 + \cdots + 3|x|^{2n-2} + 2|x|^{2n-1} + |x|^{2n} \geq (2n+1) > 0$. Also, we have

$$\begin{aligned} p(x) &= (2n+1) - (2n)x + (2n-1)x^2 - \cdots + 3x^{2n-2} - 2x^{2n-1} + x^{2n} \text{ , and} \\ xp(x) &= (2n+1)x - (2n)x^2 + \cdots - 2x^{2n} + x^{2n+1} \text{ , so} \\ p(x)(1+x) &= (2n+1) + x - x^2 + x^3 - \cdots + x^{2n+1} = (2n+1) + \frac{x(x^{2n+1}+1)}{x+1} \,, \end{aligned}$$

so that when $x > 0$ we have $p(x) > 0$. Thus $p(x) > 0$ for all x.

Alternatively, once one writes down the cases $n = 1, 2, 3$, one can express $p(x)$ as a sum of squares:

$$p(x) = \sum_{i=1}^{n} i x^{2n-2i}(x-1)^2 + n + 1.$$

6: Let $p(x)$ be a polynomial with non-negative real coefficients. Show that $p(a^2)p(b^2) \geq p(ab)^2$ for all $a, b \in \mathbf{R}$.

Solution: Let $p(x) = \sum\limits_{i=0}^{n} c_i x^i$ with each $c_i \geq 0$. Let $u, v \in \mathbf{R}^{n+1}$ be the vectors with $u_i = \sqrt{c_i}\, a^i$ and

$v_i = \sqrt{c_i}\, b^i$ for $0 \le i \le n$. Then $|u|^2 = u \cdot u = \sum_{i=0}^{n} c_i a^{2i} = p(a^2)$, and $|v|^2 = v \cdot v = \sum_{i=1}^{n} c_i b^{2i} = p(b^2)$, and $u \cdot v = \sum_{i=0}^{n} c_i\, a^i b^i = p(ab)$. By the Cauchy-Schwarz Inequality, $p(ab)^2 = (u \cdot v)^2 \le |u|^2 |v|^2 = p(a^2)p(b^2)$.

Alternatively, we can prove this by induction on the degree of $p(x)$. Suppose the statement is true for any polynomial with degree less than $\deg p$. Without loss of generality, we assume $p(x)$ is monic and write $p(x) = x^n + q(x)$ with $\deg(q) < \deg(p)$. Then $q(a^2)q(b^2) \ge q(ab)^2$. Now

$$\begin{aligned}
p(a^2)p(b^2) - p(ab)^2 &= a^{2n}q(b^2) + b^{2n}q(a^2) - 2a^n b^n q(ab) + q(a^2)q(b^2) - q(ab)^2 \\
&\ge a^{2n}q(b^2) + b^{2n}q(a^2) - 2a^n b^n q(ab) \\
&\ge 2|a^n b^n|(\sqrt{q(a^2)q(b^2)} - q(ab)) \\
&\ge 0.
\end{aligned}$$

7: Let $p(x)$ be a polynomial over $\mathbf{Z}$ of degree at least 2. Show that there is a polynomial $q(x)$ over $\mathbf{Z}$ such that $p(q(x))$ is reducible over $\mathbf{Z}$.

Solution: For $g(x) = p(x) - p(a)$ we have $g(a) = 0$ and so $(x-a)\big|g(x)$. Say $g(x) = (x-a)h(x)$, that is $p(x) - p(a) = (x-a)h(x)$. Note that since $\deg(p) \geq 2$ we have $\deg(h) \geq 1$. It follows that for any polynomial $f(x)$ we have $p(x) - p\big(f(x)\big) = \big(x - f(x)\big)h(x)$. Take $f(x) = p(x) + x$ to get $p(x) - p\big(p(x)+x\big) = -p(x)h(x)$, so we have $p\big(p(x)+x\big) = p(x)\big(1 + h(x)\big)$. Thus we can take $q(x) = p(x) + x$.

8: Let a and b be distinct real numbers. Solve $(z-a)^4 + (z-b)^4 = (a-b)^4$ for $z \in \mathbf{C}$.

Solution: It is easy to see that a and b are solutions. We can then factor

$$(z-a)^4 + (z-b)^4 - (a-b)^4 = 2(z-a)(z-b)((z-b)^2 - (z-b)(a-b) + 2(a-b)^2).$$

Hence the other two solutions are

$$\frac{(a+b) \pm i\,(a-b)\sqrt{7}}{2}.$$

9: Let $a_1, a_2, \cdots, a_n$ be distinct integers. Show that $p(x) = \prod\limits_{i=1}^{n}(x - a_i) - 1$ is irreducible.

Solution: Suppose, for a contradiction, that $p(x)$ is reducible. Say $p(x) = f(x)g(x)$ where f and g are both of degree less than n. For each i we have $p(a_i) = -1$ so $f(a_i)g(a_i) = -1$, and so either $f(a_i) = 1$ and $g(a_i) = -1$ or $f(a_i) = -1$ and $g(a_i) = 1$. Thus for all i we have we have $f(a_i) + g(a_i) = 0$. Since $f + g$ is of degree less than n, and the a_i are distinct, we must have $f(x) + g(x) = 0$ for all x. Since $g(x) = -f(x)$, we have $p(x) = f(x)g(x) = -f(x)^2$. But the coefficient of x^n in $p(x)$ is equal to 1, and the coefficient of x^n in $-f(x)^2$ is equal to -1, so this is not possible.

10: Let $p_1(x) = x^2 - 2$ and for $k \geq 2$ let $p_k(x) = p_1(p_{k-1}(x))$. Show that the roots of $p_n(x) - x$ are real and distinct for all n.

Solution: Let $x(t) = 2\cos t$ for $0 \leq t \leq \pi$. We have $p_1(x(t)) = (2\cos t)^2 - 2 = 4\cos^2 t - 2 = 2\cos 2t$. Verify using mathematical induction that $p_n(x(t)) = 2\cos(2^n t)$ for all $n \geq 1$. For $0 \leq t \leq \pi$ we have

$$\begin{aligned} p_n(x(t)) = x(t) &\iff 2\cos(2^n t) = 2\cos t \iff \cos 2^n t = \cos t \\ &\iff 2^n t = \pm t + 2\pi\, k\ , \text{ for some } k \in \mathbf{Z} \\ &\iff t = \frac{2\pi k}{2^n \pm 1}\ , \text{ for some } k \in \{0, 1, 2, \cdots, 2^n - 1\}\,. \end{aligned}$$

Thus we have found 2^n distinct solutions $x(t)$ with $0 \leq t \leq \pi$, and since the polynomial $p_n(x) - x$ is of degree 2^n, these are all of the roots of $p_n(x) - x$.

11: Let $p(x) = \sum\limits_{i=0}^{n} a_i x^i$ with $a_0 = a_n = 1$ and $a_i > 0$ for all i. Show that if $p(x)$ has n distinct real roots then $p(2) \geq 3^n$.

Solution: Since every $a_i \geq 0$, all of the roots of $p(x)$ must be negative. Say the roots are $-r_1, -r_2, \cdots, -r_n$, so we have $p(x) = (x + r_1)(x + r_2)\cdots(x + r_n)$. Using the fact that $2 + r \geq 3r^{1/3}$ for all $r > 0$, and the fact that $r_1 r_2 \cdots r_n = p(0) = 1$, we have

$$p(2) = (2 + r_1)(2 + r_2)\cdots(2 + r_n) \geq \big(3{r_1}^{1/3}\big)\big(3{r_2}^{1/3}\big)\cdots\big(3{r_n}^{1/3}\big) = 3^n\big(r_1 r_2 \cdots r_n\big)^{1/3} = 3^n\,.$$

12: Let $p(x)$ be the polynomial of degree n such that that $p(k) = \frac{k}{k+1}$ for $k = 0, 1, \cdots, n$. Find $p(n+1)$.

Solution: Let $q(x) = (x+1)p(x) - x$. Then $\deg(q) = n+1$ and we have $q(k) = (k+1)\frac{k}{k+1} - k = 0$ for $0 \le k \le n$, and so $q(x) = c(x-0)(x-1)\cdots(x-n)$ for some constant c. Also, note that $q(-1) = -1$ so that $c(-1)(-2)\cdots(-1-n) = -1$, and so we have $c = \frac{(-1)^{n+1}}{(n+1)!}$. Thus $q(x) = \frac{(-1)^{n+1}}{(n+1)!}(x-0)(x-1)\cdots(x-n)$. In particular $q(n+1) = \frac{(-1)^{n+1}}{(n+1)!}(n+1)(n)\cdots(1) = (-1)^{n+1}$. Since $q(x) = (x+1)p(x) - x$, we have $p(x) = \frac{q(x)+x}{x+1}$, and in particular

$$p(n+1) = \frac{(-1)^{n+1} + (n+1)}{n+2} = \begin{cases} \dfrac{n}{n+2} & \text{if } n \text{ is even,} \\ 1 & \text{if } n \text{ is odd.} \end{cases}$$

13: Find all polynomials over $\mathbf{C}$ whose coefficients are all equal to ± 1 and whose roots are all real.

Solution: Let $p(x) = \sum\limits_{i=0}^{n} c_i x^i$ with each $c_i = \pm 1$, and suppose the roots of $p(x)$ are all real. Let the roots be $a_1, a_2, \cdots, a_n$, repeated if necessary according to multiplicity, so that $p(x) = c_n(x-a_1)(x-a_2)\cdots(x-a_n)$. By partially expanding this product, we see that $c_0 = (-1)^n c_n \prod\limits_{1\le i\le n} a_i$, and $c_{n-1} = -c_n \sum\limits_{1\le i\le n} a_i$, and $c_{n-2} = c_n \sum\limits_{1\le i<j\le n} a_i a_j$. From the formulas for c_{n-1} and c_{n-2} we have

$$\sum_{1\le i\le n} {a_i}^2 = \Big(\sum_{1\le i<j\le n} a_i\Big)^2 - 2\sum_{1\le i\le n} a_i a_j = \left(\tfrac{c_{n-1}}{c_n}\right)^2 - 2\left(\tfrac{c_{n-2}}{c_n}\right).$$

Since each $c_i = \pm 1$ this gives $\sum\limits_{1\le i\le n} {a_i}^2 = 1 \pm 2$, and since $\sum\limits_{1\le i\le n} {a_i}^2 \ge 0$ we must have $\sum\limits_{1\le i\le n} {a_i}^2 = 1 + 2 = 3$. By the Algebraic Geometric Mean Inequality, we have

$$1 = \sqrt[n]{1} = \sqrt[n]{{c_0}^2} = \sqrt[n]{\prod_{1\le i\le n} {a_i}^2} \le \frac{\sum\limits_{1\le i\le n} {a_i}^2}{n} = \frac{3}{n},$$

and so we must have $n \le 3$. When $n = 1$ we find that all 4 polynomials $p(x) = \pm x \pm 1$ have real roots. When $n = 2$ we find that of the 8 polynomials $\pm x^2 \pm x \pm 1$, only the 4 polynomials $p(x) = \pm(x^2 \pm x - 1)$ have real roots. When $n = 3$, we must have equality in the Algebraic Geometric Mean Inequality, and this occurs when ${a_1}^2 = {a_2}^2 = {a_3}^2 = 1$. Of the 8 polynomials $\pm(x-1)^3$, $\pm(x-1)^2(x+1)$, $\pm(x-1)(x+1)^2$ and $\pm(x+1)^3$, only the 4 polynomials $p(x) = \pm(x-1)^2(x+1)$, $\pm(x-1)(x+1)^2$ have all coefficients ± 1.

14: Find all polynomials $p(x)$ over $\mathbf{R}$ such that $p(x)p(x+1) = p(x^2+x+1)$.

Solution: Let $p(x)$ be a polynomial over $\mathbf{R}$ with $p(x)p(x+1) = p(x^2+x+1)$. If $p(x)$ is constant, say $p(x) = c$, then $c^2 = c$ so that $c = 0$ or 1. Suppose that $p(x)$ is not constant. By replacing x by $x-1$, we see that $p(x-1)p(x) = p\big((x-1)^2 + (x-1) + 1\big) = p(x^2 - x + 1)$. Let $a \in \mathbf{C}$ be a root of $p(x)$ of largest possible norm. Then we have $p(a^2+a+1) = p(a)p(a+1) = 0$ and we have $p(a^2-a+1) = p(a-1)p(a) = 0$. Note that for any $0 \ne u \in \mathbf{C}$, one of the two complex numbers $u \pm a$ has larger norm than a $\big($indeed, since $|u \pm a|^2 = |u|^2 \pm 2\,\mathrm{Re}(u\bar{a}) + |a|^2$, we see that if $\mathrm{Re}(u\bar{a}) \ge 0$ then $|u+a| > |a|$ and if $\mathrm{Re}(u\bar{a}) \le 0$ then $|u-a| > |a|\big)$. In particular, if $a \ne \pm i$ then $a^2+1 \ne 0$ and so one of $a^2 \pm a + 1$ has a larger norm than a, but since $a^2 \pm a + 1$ are both roots of $p(x)$, this would contradict our choice of a. Thus we must have $a = \pm i$. Say $p(x) = (x^2+1)^k q(x)$ where $q(\pm i) \ne 0$. Then since $(x^2+1)(x^2+2x+2) = (x^2+x+1)^2 + 1$ we have

$$q(x)q(x+1) = \frac{p(x)}{(x^2+1)^k} \cdot \frac{p(x+1)}{(x^2+2x+2)^k} = \frac{p(x^2+x+1)}{\big((x^2+x+1)^2+1\big)^k} = q(x^2+x+1)$$

and so $q(x)$ satisfies the same recursion as $p(x)$. As above, if $q(x)$ was not constant then its roots of largest norm would be $a = \pm i$, but we have $q(\pm i) \ne 0$ and so $q(x)$ must be constant, say $q(x) = c$. Also as above, we must have $q(x) = 0$ or $q(x) = 1$. But we cannot have $q(x) = 0$ since this would imply that $p(x) = (x^2+1)^k q(x) = 0$. Thus $q(x) = 1$ and $p(x) = (x^2+1)^k q(x) = (x^2+1)^k$.