2008 BLUE MOP, POLYNOMIALS-I

ALİ GÜREL

(1) (Germany-97) Define the functions

$$\begin{aligned} f(x) &= x^5 + 5x^4 + 5x^3 + 5x^2 + 1, \\ g(x) &= x^5 + 5x^4 + 3x^3 - 5x^2 - 1. \end{aligned}$$

Find all prime numbers p for which there exists a natural number $0 \le x < p$, such that both $f(x)$ and $g(x)$ are divisible by p. Also find all such x.

(2) Prove that a polynomial of degree n that takes integer values at $n+1$ consecutive integers is an integer polynomial, i.e. it takes integer values at all integers.

(3) Suppose that a natural number m and a real polynomial $P(x)$ with degree n and leading coefficient a_n is given such that $P(x)$ is an integer divisible by m whenever x is an integer. Prove that $n!a_n$ is divisible by m.

(4) If $a_1, ..., a_n$ are integers, prove that the polynomial

$$P(x) = (x - a_1)(x - a_2)...(x - a_n) - 1$$

is irreducible.

(5) Let m, n and a be natural numbers and $p < a - 1$ a prime number. Prove that the polynomial

$$P(x) = x^m (x - a)^n + p$$

is irreducible.

(6) Suppose that all zeros of a monic polynomial $P(x)$ with integer coefficients have norm 1. Prove that all the roots are roots of unity.

(7) (Romania-97) Let $P(x)$ and $Q(x)$ be monic irreducible polynomials over the rational numbers. Suppose that P and Q have respective roots α and β such that $\alpha + \beta$ is rational. Prove that the polynomial $P(x)^2 - Q(x)^2$ has a rational root.

(8) (Romania-97) Let $n \ge 2$ be an integer and

$$P(x) = x^n + a_{n-1}x^{n-1} + ... + a_1 x + 1$$

be a polynomial with positive integer coefficients satisfying $a_k = a_{n-k}$ for $k = 1, 2, ..., n-1$. Prove that there exists infinitely many pairs x, y of positive integers such that $x|P(y)$ and $y|P(x)$.

Problem 1, Solution by Sergei Bernstein:

$$p|f(x) \text{ and } p|g(x) \Rightarrow p|f(x)+g(x) = 2x^5 + 10x^4 + 8x^3.$$

Since $x = 0$ doesn't work, $0 < x < p$ and p doesn't divide x. So $p|2x^3+10x^2+8x = 2x(x+4)(x+1)$. On the other hand, $p|f(x) - g(x) = 2x^3 + 10x^2 + 2$. Combining these, we get

$$p|(2x^3 + 10x^2 + 8x) - (2x^3 + 10x^2 + 2) = 8x - 2.$$

From before, we know that $p|2$ or $p|x+4$ or $p|x+1$. It is easily checked that $p \neq 2$. Using Euclidean algorithm, we get $p|17$ or $p|5$, so the only possible answers are $(x, p) = (13, 17)$ and $(4, 5)$. Finally, plugging these in show that they both work $\Box$

Problem 2, Solution by Taylor and Toan Phan: We proceed by using induction on the degree of P. If the degree is 0, the result is clear. Let's assume the result for polynomials with degree at most k and let P have degree $k+1$. Then, observe that $Q(x) = P(x+1) - P(x)$ takes integer values at k consecutive integers and has degree less than k, hence by our induction hypothesis Q takes integer values at all the integers. So does P $\Box$

Problem 3, Solution by Justin Brereton: For any number x, consider the finite differences of $P(x), P(x+1), ..., P(n+x)$. We know that the k-th order of finite differences is a degree $n-k$ polynomial. Furthermore,

$$P(x) = a_n x^n + a_{n-1}x^{n-1} + ... + a_0 \Rightarrow P(x+1) - P(x) = na_n x^{n-1} + ...$$

We need only consider the leading coefficient which is clearly $n(n-1)(n-2)...(n-k+1)a_n$ for the k-th order, therefore the constant term of the n-th order finite difference is $n!a_n$. Since all the values of $P(x)$ are divisible by m, clearly any combination of their sums and differences is too, so $m|n!a_n$ $\Box$

Problem 4, Solution by John Berman: Write $P(x) = Q(x)R(x)$ with $0 < deg(Q), deg(R) < n$ for the sake of contradiction. Then $Q(a_i)R(a_i) = -1$ implies $Q(a_i) = \pm 1$ and $R(a_i) = \mp 1$ for all $1 \leq i \leq n$, and in particular $R(x) = -Q(x)$ for n values of x: $\{a_1, a_2, ..., a_n\}$. Since $deg(Q+R) < n$, this means that $Q = -R$. But then the leading term of $P(x) = Q(x)R(x)$ would be negative. We deduce that P is irreducible, indeed $\Box$

Problem 5, Solution by Nicholas Triantafillou: Suppose P is reducible and let $P(x) = x^m(a-a)^n + p = Q(x)R(x)$. $Q(0)R(0) = Q(a)R(a) = p$. Without loss of generality, let $Q(0) = \pm 1$. Now, $a|Q(a) - Q(0)$ and $p < a-1$ so we cannot have $Q(a) = \pm p$. Hence $Q(a) = \pm 1$, as well. Let $\alpha_1, ..., \alpha_k$ be the roots of Q. Then $\alpha_1 ... \alpha_k = \pm 1$ and $(a - \alpha_1)...(a - \alpha_k) = \pm 1$. Also $|\alpha_j^m(\alpha_j - a)^n| = p$. Multiplying this from $j = 1$ through $j = k$ we get $1 = p^k$, which is a contradiction unless $degQ = 0$. We conclude that P is irreducible, as desired $\Box$

Problem 6, Solution by David B. Rush: Let $\{\lambda_1, ..., \lambda_n\}$ be the roots of a polynomial with integer coefficients. Then observe that the polynomial with roots $\{\lambda_1^m, ..., \lambda_n^m\}$, call it $P_m(x)$, have integer coefficients for all positive integers m which can be proved by induction on m using Vieta's relations. Note that $|\lambda_j^m| = 1$ for all j so the norm of the coefficient of x^k in $P_m(x)$ is at most $\binom{n}{k}$. Hence the set

$$P = \{P_m(x) \,|\, m \in \mathbb{Z}^+\}$$

is finite. Thus λ_j^m for $m = 1, 2, ...$ take only finitely many values and we deduce that λ_j is a root of unity for all j $\square$

Problem 7, Solution by Sergei Bernstein: Let $R(x) := Q(\alpha + \beta - x)$. Note that $R(x)$ is monic-irreducible and that it has α as a root. P and R are both divisible by the minimal polynomial with α as a root but they are irreducible so $P(x) = \pm R(x)$. Finally, observe that

$$P^2\left(\frac{\alpha+\beta}{2}\right) = R^2\left(\frac{\alpha+\beta}{2}\right) = Q^2\left(\frac{\alpha+\beta}{2}\right)$$

with $\frac{\alpha+\beta}{2}$ being the desired rational number $\square$

Problem 8, Solution by Zhifan Zang: A trivial example is $(x, y) = (1, 1)$. We will show that if a pair (x, y) satisfies the conditions with $x \leq y$, then so does the pair $(y, \frac{P(y)}{x})$ where $y \leq \frac{P(y)}{x}$. To do this, we need to show that $y|P\left(\frac{P(y)}{x}\right)$. Now, $P(y) \equiv 1 \pmod{y}$ and observe that since $a_k = a_{n-k}$, $P(x) = x^n P\left(\frac{1}{x}\right)$. So

$$P\left(\frac{P(y)}{x}\right) = \left(\frac{P(y)}{x}\right)^n P\left(\frac{x}{P(y)}\right) \equiv \frac{1}{x^n} P\left(\frac{x}{1}\right) \equiv 0 \pmod{y}$$

Finally, $P(y) > y^2 > xy$ so $\frac{P(y)}{x} > y$ $\square$