PUTNAM PRACTICE SET 32: SOLUTIONS

PROF. DRAGOS GHIOCA

Problem 1. Let M be an even positive integer. Show that for each positive integer n, the number

$$M^{M^{M^n}} + M^{M^n} + M^n - 1$$

is a not prime.

Solution. We write each positive integer n as $2^j \cdot m$, where $j \geq 0$ and $m \geq 1$ are integers, with m odd. We will show that our number

$$N := M^{M^{M^n}} + M^{M^n} + M^n - 1$$

is divisible by $L := M^{2^j} + 1$. Since

$$L \geq M + 1 > 1 \text{ and } N > 1 + 1 + M^{2^j} - 1 = L,$$

this delivers our desired conclusion. Now, in order to show the desired divisibility, we note that

$$M^n \equiv M^{2^j \cdot m} \equiv (L-1)^m \equiv (-1)^m \equiv -1 \pmod{L}$$

because m is odd. Furthermore, for each positive integer k, we have:

$$M^{2^j \cdot k} \equiv (-1)^k \pmod{L}. \tag{1}$$

Now, because M is even (say $M = 2\ell$), we have that

$$M^n = (2\ell)^n = 2^n \cdot \ell^n = 2^j \cdot 2^{n-j} \cdot \ell^n$$

and $n - j > 0$ because $n = 2^j \cdot m \geq 2^j > j$ for each $j \geq 0$. So,

$$M^n = 2^j \cdot a,$$

for some even positive integer a. Similarly, because

$$M^{M^n} = 2^{M^n} \cdot \ell^{M^n} = 2^j \cdot 2^{M^n - j} \cdot \ell^{M^n}$$

and $M^n \geq 2^n > n > j$, we can also write

$$M^{M^n} = 2^j \cdot b,$$

for some even positive integer b. Therefore,

$$M^{M^n} \equiv M^{2^j a} \equiv (-1)^a \equiv 1 \pmod{L}$$

and similarly,

$$M^{M^{M^n}} \equiv M^{2^j b} \equiv (-1)^b \equiv 1 \pmod{L}.$$

In conclusion,

$$N \equiv 1 + 1 - 1 - 1 \equiv 0 \pmod{L},$$

as desired.

Problem 2. Let A, B and C be noncollinear points in the plane with integer coordinates such that also the three distances between the points (AB, BC and CA) are integer numbers. What is the smallest possible value for AB?

Solution. We claim that the smallest such distance AB is 3, which is achieved when $A = (0, 0)$, $B = (3, 0)$ and $C = (0, 4)$. In order to show that this is indeed the minimum possible distance, we have to exclude the possibilities 1 and 2 for the length of AB (since the points A, B and C are not collinear, then we can't have $A = B$ and so, we cannot have $|AB| = 0$).

Now, without loss of generality, we may assume $|AC| \geq |BC|$. Since ABC is a triangle, then the triangle inequality forces that

$$|AB| > |AC| - |BC|$$

and so, if $|AB| = 1$, we would actually need to have $|AC| = |BC|$. But since A, B and C have integer coordinates and furthermore, $|AB| = 1$, we must have that

$$A = (m, n) \text{ and } B = (m \pm 1, n)$$

or

$$A = (m, n) \text{ and } B = (m, n \pm 1).$$

In the first case, this means $C = (m \pm 1/2, k)$, while the second possibility yields $C = (k, n \pm 1/2)$; either way, this prevents C to have integer coordinates. Thus, we cannot have that $|AB| = 1$, which only leaves us with the possibility that $|AB| = 2$. This means that the points A and B have coordinates:

$$(m \pm 1, n) \text{ or } (m, n \pm 1).$$

Without loss of generality, we assume

$$A = (m - 1, n) \text{ and } B = (m + 1, n).$$

As before, we have the inequality

$$|AB| = 2 > |AC| - |BC|$$

This time noticing that for any point $C = (k, \ell)$, we have that

$$|AC|^2 = (m - 1 - k)^2 + (n - \ell)^2 \equiv (m + 1 - k)^2 + (n - \ell)^2 = |BC|^2 \pmod 2,$$

we have that $|AC|$ and $|BC|$ have the same parity, which means that if the difference between $|AC|$ and $|BC|$ is less than 2 in absolute value, then it means that $|AC| = |BC|$. So, this yields that $k = m$ and so, we would need that

$$1 + (n - \ell)^2 \text{ is a perfect square.}$$

However, this last condition is only met when $n = \ell$, which would then force the points A, B and C be collinear, contradiction. So, indeed, $|AB| = 3$ is the minimum possible distance, as claimed.

Problem 3. Find all pairs of polynomials $P(x)$ and $Q(x)$ with the property that

$$P(x)Q(x + 1) - P(x + 1)Q(x) = 1.$$

Solution. First we notice that our given polynomial identity yields that the polynomials $P(x)$ and $Q(x)$ are coprime.

Now, using the identity also in the case $x \mapsto x - 1$, i.e., subtracting

$$P(x)Q(x + 1) - P(x + 1)Q(x) = 1$$

from

$$P(x-1)Q(x) - P(x)Q(x-1) = 1$$

yields

$$(P(x-1) + P(x+1)) \cdot Q(x) = P(x) \cdot (Q(x-1) + Q(x+1)).$$

Because $\gcd(P(x), Q(x)) = 1$, then we conclude that $Q(x)$ must divide the polynomial $Q(x+1) + Q(x-1)$, i.e., there exists a polynomial $R(x)$ such that

$$Q(x+1) + Q(x-1) = R(x) \cdot Q(x).$$

On the other hand, because $\deg(Q(x+1) + Q(x-1)) = \deg(Q(x))$ and the leading coefficient of $Q(x+1)+Q(x-1)$ is twice the leading coefficient of $Q(x)$, we conclude that $R(x)$ is identically equal to 2. So, after a similar analysis for $P(x)$, we conclude that

$$P(x+1) + P(x-1) = 2P(x) \text{ and } Q(x+1) + Q(x-1) = 2Q(x). \tag{2}$$

Letting the polynomials $A(x) := P(x) - P(x-1)$ and $B(x) := Q(x) - Q(x-1)$, we see that our polynomial identities from (2) yields that

$$A(x+1) = A(x) \text{ and } B(x+1) = B(x) \text{ for all } x.$$

Because $A(x)$ and $B(x)$ are polynomials, we conclude that $A(x) := a$ and $B(x) := b$ are identically equal with the two constants a and b.

Now, for a polynomial $f(x)$, if $f(x+1) - f(x)$ is a constant, then this means that its derivative

$$f'(x+1) - f'(x) = 0 \text{ for all } x$$

and so, $f'(x)$ must itself be a constant, i.e., $f(x)$ is a linear polynomial. Therefore, both $P(x)$ and $Q(x)$ are linear polynomials, i.e. for some two other constants c and d, we have that

$$P(x) = ax + c \text{ and } Q(x) = bx + d.$$

But then our polynomial identity

$$P(x)Q(x+1) - P(x+1)Q(x) = 1$$

leads us to the relation:

$$bc - ad = 1.$$

In conclusion, the only solutions are any two linear polynomials $(P(x), Q(x)) = (ax + c, bx + d)$ for constants a, b, c, d satisfying $bc - ad = 1$.

Problem 4. Let $n \in \mathbb{N}$ and let $A \in M_{n,n}(\mathbb{R})$. For each $k \in \mathbb{N}$, we denote by $A^{[k]}$ the n-by-n matrix whose entries are the k-th powers of the corresponding entries in A. If

$$A^{[k]} = A^k \text{ for each } 1 \leq k \leq n+1,$$

then $A^{[k]} = A^k$ for all $k \geq 1$.

Solution. In terms of notation, for each polynomial $P(x) \in \mathbb{R}[x]$, we denote by $[P(x)]A$ the matrix whose entries are computed by applying the polynomial $P(x)$ to each corresponding entry from the matrix A. So, our hypothesis now reads $A^{[k]} = [x^k]A$ for each $k \geq 1$ and so,

$$[x^k]A = A^k \text{ for } 1 \leq k \leq n+1.$$

Now, we know there exists a monic polynomial $f(x) \in \mathbb{R}[x]$ of degree n (by Hamilton-Cayley's famous theorem) such that $f(A)$ is the zero matrix $O_{n,n}$; in particular, letting

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

(for some real numbers a_j), we also have (after multiplying $f(A)$ by A) that

$$A^{n+1} + a_{n-1}A^n + a_{n-2}A^{n-1} + \cdots + a_2 A^3 + a_1 A^2 + a_0 A = O_{n,n}.$$

Since $A^j = [x^j]A$ for $1 \leq j \leq n+1$, then the above matrix identity yields that

$$[x^{n+1}]A + a_{n-1}[x^n]A + a_{n-2}[x^{n-1}]A + \cdots + a_2[x^3]A + a_1[x^2]A + a_0[x]A = O_{n,n}.$$

Furthermore, because for each $j = 1, \ldots, n+1$ and each real constant c, we have

$$c[x^j]A = [cx^j]A$$

and also, for any two polynomials $g, h \in \mathbb{R}[x]$, we have

$$[g(x)]A + [h(x)]A = [g(x) + h(x)]A,$$

we conclude that

$$[xf(x)]A = O_{n,n}.$$

In particular, for each entry a_{ij} of A, we have that

$$a_{ij} f(a_{ij}) = 0,$$

which also means that for each $k \geq 2$, we have that

$$a_{ij}^k f(a_{ij}) = 0.$$

So, this means that also

$$[x^k f(x)]A = O_{n,n} \text{ for each } k \geq 2.$$

Now, we obtain the desired conclusion that

$$[x^m]A = A^m \text{ for each } m \geq 1$$

by induction on m. We already know this conclusion for $m = 1, \ldots, n+1$ and so, for the inductive hypothesis, we assume that

$$[x^k]A = A^k,\ [x^{k+1}]A = A^{k+1},\ \cdots, [x^{k+n}]A = A^{k+n}$$

for some integer $k \geq 1$ and next we show that also,

$$[x^{k+n+1}]A = A^{k+n+1}.$$

To see this, we use that

$$[x^{k+1} f(x)]A = O_{n,n},$$

which means that

(3)
$$[x^{n+k+1}]A + a_{n-1}[x^{k+n}]A + a_{n-2}[x^{k+n-1}]A + \cdots + a_2[x^{k+3}]A + a_1[x^{k+2}]A + a_0[x^{k+1}]A = O_{n,n}.$$

Now, we know (by the inductive hypothesis) that

$$[x^m]A = A^m \text{ for } m = k+1, \ldots, k+n \tag{4}$$

and we also know that since $A^{k+1}f(A) = O_{n,n}$, then

$$A^{n+k+1} + a_{n-1}A^{n+k} + a_{n-2}A^{n+k-1} + \cdots + a_2 A^{k+3} + a_1 A^{k+2} + a_0 A^{k+1} = O_{n,n}. \tag{5}$$

So, combining (3), (4) and (5) yields that we must also have that

$$[x^{n+k+1}]A = A^{n+k+1},$$

as desired. This concludes the proof for this problem.