PUTNAM PRACTICE SET 33: SOLUTIONS

PROF. DRAGOS GHIOCA

Problem 1. For which positive integers n is there an n-by-n matrix A with integer entries with the property that every dot product of a row with itself is even, while every dot product of two different rows is odd?

Solution. We show that for each odd $n \in \mathbb{N}$ there exists such a matrix A, while for even positive integers n there is no such n-by-n matrix.

First, we let J_n be the n-by-n matrix all of whose entries equal 1 and if n is odd, we let $A := J_n - I_n$ (where I_n is the identity n-by-n matrix). Then clearly, the dot product of any row with itself equals $n-1$, which is even, while for any two distinct rows, their dot product equals $n-2$, which is odd, as desired.

Now, if n is even and A were a matrix satisfying the conditions from our problem, then we let $\bar{A}$ its reduction modulo 2, i.e., we reduce modulo 2 each entry in A and so, $\bar{A} \in M_{n,n}(\mathbb{F}_2)$.

Letting $\bar{v} \in M_{n,1}(\mathbb{F}_2)$ be the vector all of whose entries equal 1, we see that $\bar{A} \cdot \bar{v} = \bar{O}_{n,1}$ (the zero vector with n entries) because our hypothesis yields that the sum of the entries in each row of A must be even; hence $\bar{A}$ is a singular matrix in $M_{n,n}(\mathbb{F}_2)$, i.e.,

$$\det(\bar{A}) = 0 \in \mathbb{F}_2. \tag{1}$$

On the other hand, our hypothesis regarding A yields that

$$\bar{A} \cdot \bar{A}^t = \bar{J}_n - \bar{I}_n, \tag{2}$$

where $\bar{I}_n$ and $\bar{J}_n$ are the identity n-by-n matrix, respectively the n-by-n matrix whose entries all equal 1, both matrices living in $M_{n,n}(\mathbb{F}_2)$. A simple computation (also employing that n is assumed to be even) yields that

$$(\bar{J}_n - \bar{I}_n)^2 = n\bar{J}_n - 2\bar{J}_n + \bar{I}_n = \bar{I}_n,$$

thus showing that $\bar{J}_n - \bar{I}_n$ is invertible in $M_{n,n}(\mathbb{F}_2)$ (when n is even). Therefore (2) yields that $\bar{A}$ must also be invertible in $M_{n,n}(\mathbb{F}_2)$, which contradicts (1). This contradiction shows that only when n is odd, we can construct such a matrix A, which concludes our proof.

Problem 2. Let $a, b \in \mathbb{N}$. Prove that for each $\epsilon > 0$, we can find positive integers m and n with the property that

$$0 < \left|a\sqrt{m} - b\sqrt{n}\right| < \epsilon.$$

Solution. Let $k \in \mathbb{N}$. We take $n = a^2k^2$ and $m = b^2k^2 + 1$. Then clearly, $a\sqrt{m} > abk = b\sqrt{n}$ and moreover,

$$a\sqrt{m} - b\sqrt{n} = \sqrt{a^2b^2k^2 + a^2} - \sqrt{a^2b^2k^2} = \frac{a^2}{\sqrt{a^2b^2k^2 + a^2} + \sqrt{a^2b^2k^2}} < \frac{a^2}{2abk} = \frac{a}{2bk}$$

and so, choosing $k > \frac{a}{2b\epsilon}$ delivers the desired conclusion.

Problem 3. Let $g : \mathbb{R} \longrightarrow \mathbb{R}$ be a continuous function with $g(0) \neq 0$. If $f : \mathbb{R} \longrightarrow \mathbb{R}$ is a function with the property that both functions

$$\frac{f}{g} \text{ and } f \cdot g$$

are differentiable at $x = 0$, then does this imply that also f must be differentiable at $x = 0$?

Solution. Yes, it does; here's why. First of all, we note that f is continuous at $x = 0$ because g is continuous at $x = 0$ and also f/g is continuous at $x = 0$, thus showing that their product $g \cdot (f/g) = f$ is continuous at $x = 0$.

Since $f \cdot g$ and f/g are both differentiable at $x = 0$, then their product f^2 must also be differentiable at $x = 0$. If $f(0) \neq 0$, then $\sqrt{f(x)}$ is differentiable at $x = 0$ (as a composition of two differentiable functions at that point) and so, we get that f or $-f$ is differentiable at $x = 0$ (depending on the sign of $f(0)$); either way, we get that f is differentiable at $x = 0$. **Note that by the continuity of f at $x = 0$, we knew that if $f(0) \neq 0$, then in a small neighborhod of $x = 0$, $f(x)$ is either positive or negative for all values of x in that small interval.**

So, we're left to analyzing the differentiablility of f at $x = 0$ assuming $f(0) = 0$, i.e., we need to prove that the following limit exists:

$$\lim_{x \to 0} \frac{f(x) - f(0)}{x - 0} = \lim_{x \to 0} \frac{f(x)}{x}.$$

However, we know that f/g is differentiable at $x = 0$ and since $f(0) = 0$ (and $g(0) \neq 0$), then we know that the following limit exists:

$$\lim_{x \to 0} \frac{\frac{f(x)}{g(x)} - \frac{f(0)}{g(0)}}{x - 0} = \lim_{x \to 0} \frac{\frac{f(x)}{g(x)}}{x} = \lim_{x \to 0} \frac{f(x)}{xg(x)}.$$

So, because $g(x)$ is continuous at $x = 0$, then indeed the following limit exists:

$$\lim_{x \to 0} \frac{f(x)}{xg(x)} \cdot \lim_{x \to 0} g(x) = \lim_{x \to 0} \frac{f(x)}{x},$$

as desired.

Problem 4. Let p be an odd prime number. Prove that there exist at least $\frac{p+1}{2}$ distinct integers $n \in \{0, 1, 2, \dots, p-1\}$ with the property that p doesn't divide the integer:

$$\sum_{k=0}^{p-1} k! \cdot n^k.$$

(As always, we use the convention that $0! = 1$.)

Solution. We are asked to show that the polynomial

$$f(x) = \sum_{k=0}^{p-1} k! \cdot x^k \in \mathbb{F}_p[x]$$

has at most $\frac{p-1}{2}$ distinct roots in $\mathbb{F}_p$. Clearly, $f(x)$ doesn't have the root $x = 0$; so, it suffices to show that it doesn't have more than $\frac{p-1}{2}$ distinct nonzero roots in $\mathbb{F}_p$.

Now, it suffices to prove that the polynomial

$$f_1(x) = \frac{f(x)}{(p-1)!} \in \mathbb{F}_p[x]$$

has at most $\frac{p-1}{2}$ distinct nonzero roots in $\mathbb{F}_p$. Now, due to Wilson's Theorem, we have that
$$(p-1)! \equiv -1 \pmod{p}$$
and then for each $k = 1, \dots, p-2$, we write
$$(p-1)! = k! \cdot (k+1) \cdot (k+2) \cdots (p-1)$$
and so, for $i = 1, \dots, p-k-1$, using that $k + i \equiv -(p-k-i) \pmod{p}$, we obtain that
$$(p-1)! \equiv k! \cdot (-1)^{p-k-1} \cdot (p-k-1)! \pmod{p}.$$
So, working in $\mathbb{F}_p[x]$, we have:
$$f_1(x) = \sum_{k=0}^{p-1} \frac{k! \cdot x^k}{(-1)^{p-k-1} \cdot k! \cdot (p-k-1)!} = \sum_{k=0}^{p-1} \frac{x^k}{(-1)^{p-k-1}(p-k-1)!}.$$

Claim 0.1. *Let $h \in \mathbb{F}_p[x]$ be a polynomial of degree $p-1$ for which $h(0) \neq 0$. Then the number of distinct roots of $h(x) = 0$ in $\mathbb{F}_p$ is the same as the number of roots in $\mathbb{F}_p$ of $\tilde{h}(x) := x^{p-1} \cdot h(1/x)$.*

Proof of Claim 0.1. Indeed, both $h(x)$ and $\tilde{h}(x)$ are polynomials of degree $p-1$; neither one of them has the root 0, and moreover, for each $\alpha \in \mathbb{F}_p^*$, we have that $h(\alpha) = 0$ if and only if $\tilde{h}(1/\alpha) = 0$. This concludes our proof of Claim 0.1. □

Using Claim 0.1, then it suffices to prove that $\tilde{f}_1(x) := x^{p-1} \cdot f_1(1/x) \in \mathbb{F}_p[x]$ has at most $\frac{p-1}{2}$ distinct nonzero roots in $\mathbb{F}_p$. We compute:
$$\tilde{f}_1(x) = \sum_{k=0}^{p-1} \frac{x^{p-k-1}}{(-1)^{p-k-1}(p-k-1)!}$$
and so, letting $g(x) := \tilde{f}_1(-x)$, it suffices to prove that $g(x)$ has at most $\frac{p-1}{2}$ distinct roots in $\mathbb{F}_p$. We have that
$$g(x) = \sum_{k=0}^{p-1} \frac{x^k}{k!} \in \mathbb{F}_p[x].$$
Because for each $\alpha \in \mathbb{F}_p$, we have that $\alpha^p - \alpha = 0$, then it suffices to show that the number of nonzero distinct roots in $\mathbb{F}_p$ of
$$g_1(x) = x^p - x + g(x) \in \mathbb{F}_p[x]$$
is at most $\frac{p-1}{2}$. Now, because $(x^p)' = 0$, we see that
$$g_1'(x) = -1 + g'(x) = -1 + \sum_{k=0}^{p-2} \frac{x^k}{k!} = -1 - \frac{x^{p-1}}{(p-1)!} + g(x) = -1 + x^{p-1} + g(x),$$
where in the last equality (in $\mathbb{F}_p[x]$), we used the fact that $(p-1)! = -1 \in \mathbb{F}_p$. So, for each nonzero root $\alpha \in \mathbb{F}_p$ of $g_1(x)$, since $\alpha^p = \alpha$ and $\alpha^{p-1} = 1$ in $\mathbb{F}_p$, we conclude that
$$g_1(\alpha) = g(\alpha) = g_1'(\alpha) = 0.$$
Therefore, each nonzero root in $\mathbb{F}_p$ of $g_1(x)$ has multiplicity at least equal to 2, thus proving that g_1 (and so, in turn, g and then also f) has at most $\frac{p-1}{2}$ distinct roots in $\mathbb{F}_p$, as desired.