# PUTNAM PRACTICE SET 28: SOLUTIONS

PROF. DRAGOS GHIOCA

*Problem 1.* What is the maximum number of points in the cartesian plane whose both coordinates are rational numbers, which lie on the same circle whose center is not a point whose both coordinates are rational numbers?

*Solution.* Let $(x_0, y_0)$ be the coordinates of the center of the circle and let $(x_i, y_i)$ for $i = 1, \dots, \ell$ be points with both coordinates rational numbers lying on our circle; our goal is to find the largest value for $\ell$. We know that $\ell = 2$ is possible since both $(-1, 0)$ and $(1, 0)$ lie on the same circle centered at the point $(0, \alpha)$ for *any* $\alpha \in \mathbb{R}$. We will show below that $\ell \geq 3$ is impossible.

So, assume $\ell \geq 3$; then we know that for each $i = 1, \dots, \ell$, we have that

$$(x_i - x_0)^2 + (y_i - y_0)^2 = (x_1 - x_0)^2 + (y_1 - y_0)^2.$$

This last equation simplifies to

$$x_i^2 + y_i^2 - x_1^2 - y_1^2 = 2(x_i - x_1) \cdot x_0 + 2(y_i - y_1) \cdot y_0. \tag{1}$$

We know that noth both $x_0$ and $y_0$ are rational numbers; without loss of generality, we may assume $y_0 \notin \mathbb{Q}$.

Since not all 3 points $(x_i, y_i)$ for $i = 1, 2, 3$ can lie on the same line, then we cannot have that $y_1 = y_2 = y_3$; so, without loss of generality, we assume $y_3 \neq y_1$. Using (1) for $i = 3$, we conclude that also $x_3 - x_1 \neq 0$ since otherwise we would derive a contradiction because the left hand side is given to be rational, while the right hand wouldn't be rational.

Now, similar to equation (1), we get

$$x_2^2 + y_2^2 - x_3^2 - y_3^2 = 2(x_2 - x_3) \cdot x_0 + 2(y_2 - y_3) \cdot y_0. \tag{2}$$

So, either $y_2 - y_3 \neq 0$ or $y_2 - y_1 \neq 0$; again, without loss of generality, we may assume $y_2 - y_1 \neq 0$. Therefore, arguing as before, we get $x_2 - x_1 \neq 0$; also, we have:

$$(x_2 - x_1) \cdot x_0 + (y_2 - y_1) \cdot y_0 \in \mathbb{Q} \text{ and } (x_3 - x_1) \cdot x_0 + (y_3 - y_1) \cdot y_0 \in \mathbb{Q}. \tag{3}$$

Now, if

$$\frac{y_2 - y_1}{x_2 - x_1} \neq \frac{y_3 - y_1}{x_3 - x_1}, \tag{4}$$

then (3) yields that $x_0, y_0 \in \mathbb{Q}$, which is a contradiction. So, we must have that

$$\frac{y_3 - y_1}{x_3 - x_1} = \frac{y_2 - y_1}{x_2 - x_1},$$

which means that the three points $(x_1, y_1)$, $(x_2, y_2)$ and $(x_3, y_3)$ are on the same line, contradicting that they are on the same circle. So, indeed we cannot have more than 2 points with rational coordinates on the same circle whose center doesn't have rational coordinates.

*Problem 2.* Let $F_0(x) = \log(x)$ and for each $n \ge 1$ and $x > 0$, we let

$$F_n(x) = \int_0^x F_{n-1}(t)\mathrm{dt}.$$

Compute

$$\lim_{n\to\infty} \frac{n! \cdot F_n(1)}{\ln(n)}.$$

*Solution.* We claim that for each $n \ge 1$, we have that

$$F_n(x) = \frac{x^n}{n!} \cdot \left(\log(x) - \sum_{k=1}^{n} \frac{1}{k}\right).$$

The statement is easily seen to be true when $n = 1$ since - integrating by parts - we obtain that $F_1(x) = x\log(x) - x$. (Here we also use implicitly the fact that

$$\lim_{x\to 0^+} x\log(x) = 0$$

and thus, more generally, for any positive integer $m$, we have that

$$\lim_{x\to 0^+} x^m \log(x) = 0.$$

The above limits are easily computed using L'Hôpital's Rule, for example.) Then, inductively, we see that if

$$F_n(x) = \frac{x^n}{n!} \cdot \left(\log(x) - \sum_{k=1}^{n} \frac{1}{k}\right),$$

then computing $F_{n+1}(x)$ (again using integration by parts and the above limit of $x^m \log(x)$ as $x \to 0^+$), we get

$$F_{n+1}(x) = \frac{x^{n+1}}{(n+1)!} \cdot \log(x) - \frac{x^{n+1}}{(n+1)! \cdot (n+1)} - \frac{x^{n+1}}{(n+1)!} \cdot \left(\sum_{k=1}^{n} \frac{1}{k}\right),$$

which delivers the desired formula for $F_{n+1}(x)$ inductively. Therefore

$$n! \cdot F_n(1) = -\sum_{k=1}^{n} \frac{1}{k}$$

and so, we are left to compute the limit

$$\lim_{n\to\infty} \frac{\sum_{k=1}^{n} \frac{1}{k}}{\log(n)}.$$

Now, using the fact that the function $x \mapsto \frac{1}{x}$ is decreasing for $x \ge 1$, we see that

$$\int_1^{n+1} \frac{1}{x}\mathrm{dx} < \sum_{k=1}^{n} \frac{1}{k} < 1 + \int_1^{n} \frac{1}{x}\mathrm{dx}$$

(after considering left, rspectively right Riemann sums for the integral of $1/x$). So, this means that

$$\log(n+1) < \sum_{k=1}^{n} \frac{1}{k} < 1 + \log(n)$$

and therefore, using the Squeeze Theorem, we conclude that

$$\lim_{n\to\infty} \frac{n! \cdot F_n(1)}{\log(n)} = -\lim_{n\to\infty} \frac{\sum_{k=1}^{n} \frac{1}{k}}{\log(n)} = -1.$$

*Problem 3.* Let $p$ be a prime number and let $f \in \mathbb{Z}[x]$. Assume that the integers $f(k)$ for $0 \le k \le p^2 - 1$ are all distinct modulo $p^2$. Then prove that for each $n \in \mathbb{N}$, the integers $f(k)$ for $0 \le k \le p^n - 1$ are distinct modulo $p^n$.

*Solution.* First of all, we know that if

$$x \equiv y \pmod{m} \text{ then } f(x) \equiv f(y) \pmod{m}$$

for any integers $x, y, m$. In particular, this means that

$$f(k + pj) \equiv f(k) \pmod{p} \text{ for each } k, j = 0, \dots, p-1.$$

On the other hand, a simple computation shows that

$$f(k + pj) \equiv f(k) + pjf'(k) \pmod{p^2} \text{ for } k, j = 0, \dots, p-1.$$

Since the numbers $f(k + pj)$ are distinct modulo $p^2$, then this means that actually $f'(k)$ is not divisible by $p$ (for each $k = 0, \dots, p-1$).

Now, we prove inductively on $n$ that the numbers $f(0), \dots, f(p^n - 1)$ are all distinct modulo $p^n$; the statement for $n = 1, 2$ is already the hypothesis in our problem. So, we assume that $f(0), \dots, f(p^n - 1)$ are distinct modulo $p^n$ (for some $n \ge 2$) and we prove that $f(0), \dots, f(p^{n+1} - 1)$ are distinct modulo $p^{n+1}$.

We have that for each $\ell \in \{0, \dots, p^n - 1\}$,

$$f'(\ell) \not\equiv 0 \pmod{p}$$

because each $f'(\ell)$ is congruent with some $f'(k)$ modulo $p$ where $\ell \equiv k \pmod{p}$ and we know that for $k \in \{0, \dots, p-1\}$, we have that

$$f'(k) \not\equiv 0 \pmod{p}.$$

Now, since each $f(\ell)$ are distinct modulo $p^n$ for $\ell = 0, \dots, p^n - 1$, in order to obtain the inductive conclusion, all we need to show is that for each $j \in \{0, \dots, p-1\}$, the numbers $f(\ell + jp^n)$ are distinct modulo $p^{n+1}$. But using the same computation as before (which is essentially a Taylor expansion around $x = \ell$, or alternatively obtained from expanding each monomial from $f(\ell + jp^n)$), we have that

$$f(\ell + jp^n) \equiv f(\ell) + jp^n f'(\ell) \pmod{p^{n+1}}.$$

Since $p$ doesn't divide $f'(\ell)$, then as we vary $j \in \{0, \dots, p-1\}$, we obtain distinct residue classes modulo $p^{n+1}$ for the numbers $f(\ell + jp^n)$, therefore showing that the integers $f(0), \dots, f(p^{n+1} - 1)$ are all distinct modulo $p^{n+1}$, as desired. Indeed, if $0 \le i_1 < i_2 \le p^{n+1} - 1$, then either

$$i_2 \not\equiv i_1 \pmod{p^n},$$

in which case by the inductive hypothesis, we have that

$$f(i_1) \not\equiv f(i_2) \pmod{p^n}$$

and therefore, also

$$f(i_2) \not\equiv f(i_1) \pmod{p^{n+1}},$$

or $i_2 = i_1 + p^n j$ for some $1 \le j \le p-1$ and then

$$f(i_2) \equiv f(i_1) + p^n j f'(i_1) \pmod{p^{n+1}}$$

and because $p$ doesn't divide $f'(i_1)$ (nor divides $j$), then

$$f(i_2) \not\equiv f(i_1) \pmod{p^{n+1}}.$$

*Problem 4.* Find all functions $f : \mathbb{R} \longrightarrow \mathbb{R}$ whose derivative is continuous with the property that for each rational number $\frac{a}{b}$, written in lowest terms (i.e., $a, b \in \mathbb{Z}$ with $b \in \mathbb{N}$ and $\gcd(a, b) = 1$), we have that also $f\left(\frac{a}{b}\right)$ is a rational number whose denominator, when we write $f(a/b)$ in lowest terms, is also equal to $b$.

*Solution.* Let $\frac{a}{b} \in \mathbb{Q}$ be a fraction in its lowest terms (so, $\gcd(a, b) = 1$). We consider the limit:

$$L := \lim_{n\to\infty} \frac{f\left(\frac{a}{b} + \frac{1}{bn}\right) - f\left(\frac{a}{b}\right)}{\frac{1}{bn}}.$$

Clearly, since $f$ is differentiable, then we have that $L = f'\left(\frac{a}{b}\right)$.

On the other hand, we claim that $L$ must be an integer; here's why. We have that

$$\frac{a}{b} + \frac{1}{bn} = \frac{an+1}{bn}$$

is a rational number whose denominator (in lowest terms) is a divisor of $bn$. Therefore, due to our hypothesis, we have that there exists some integer $k_n$ such that

$$f\left(\frac{a}{b} + \frac{1}{bn}\right) = \frac{k_n}{bn}.$$

On the other hand, we already know (again due to our hypothesis) that there exists an integer $\ell$ such that

$$f\left(\frac{a}{b}\right) = \frac{\ell}{b},$$

which means that

$$\frac{f\left(\frac{a}{b} + \frac{1}{bn}\right) - f\left(\frac{a}{b}\right)}{\frac{1}{bn}} = \frac{\frac{k_n}{bn} - \frac{\ell}{b}}{\frac{1}{bn}} = k_n - n\ell \in \mathbb{Z}.$$

So, $L$ is actually a limit of some integers; therefore, $L$ itself must be an integer (and actually, it means that for *all $n$ sufficiently large*, we have that $k_n - n\ell$ must be constant).

So, we have that for each rational number $q \in \mathbb{Q}$, $f'(q) \in \mathbb{Z}$. Now, since (by our hypothesis), $f'(x)$ is a continuous function, then this means that $f'(x)$ must be a constant function. Indeed, first of all, because each real number is the limit point of a sequence of rational numbers and $f'(q) \in \mathbb{Z}$ when $q \in \mathbb{Q}$, then this forces that for any $x_0 \in \mathbb{R}$,

$$f'(x_0) = \lim_{\substack{q\to x_0\\ q\in\mathbb{Q}}} f'(q) \in \mathbb{Z}.$$

So, $f' : \mathbb{R} \longrightarrow \mathbb{Z}$ is a continuous function, which in particular, it means that it must satisfy the Intermediate Value Theorem. However $f'(x)$ never takes values which are not integers; therefore, $f'(x)$ cannot take two distinct integer values $r < s$ (say) because then this would violate the Intermediate Value Theorem since $f'(x)$ would never take the value $r + \frac{1}{2}$. So, $f'(x)$ is constant (equal to some integer $c$), which means that

$$f(x) = cx + d \text{ for some given } c \in \mathbb{Z} \text{ and } d \in \mathbb{R}.$$

Now, since $f(q) \in \mathbb{Q}$ whenever $q \in \mathbb{Q}$, then this means that $d \in \mathbb{Q}$. Moreover, because $f(0) = d$, applying our hypothesis to the rational number $\frac{0}{1}$ yields that $d$ itself must be an integer number. We finally claim that $c$ must be either equal to 1 or to $-1$.

Now, first of all, $c$ cannot be equal to 0 because then $f(x) = d \in \mathbb{Z}$ and so, $f\left(\frac{1}{2}\right)$ would not be a fraction in its lowest terms with denominator equal to 2.

Second, if $|c| > 1$, then we consider

$$f\left(\frac{1}{2c}\right) = \frac{1}{2} + d$$

is a fraction in lowest terms with denominator equal to 2, thus contradicting our hypothesis (because it should have denominator equal to $|2c| > 2$). So, indeed, we need $|c| = 1$.

On the other hand, if $f(x) = x + d$ or $f(x) = -x + d$, then clearly, our hypothesis is verified and we are done.