Putnam 2022 Solutions

Session A

A1. Determine all ordered pairs of real numbers (a, b) such that the line y = ax + b intersects the curve $y = \ln(1 + x^2)$ in exactly one point.

Answer. We have these three families of solutions:

$$\begin{cases} b = 0 & a = 0 \\ \forall b & |a| \ge 1 \\ b < \ln(\frac{2(1+\sqrt{1-a^2})}{a^2}) - (1+\sqrt{1-a^2}) \text{ or } b > \ln(\frac{2(1-\sqrt{1-a^2})}{a^2}) - (1-\sqrt{1-a^2}) & 0 < |a| < 1 \end{cases}$$
(1)

Solution. For each $a \in \mathbb{R}$, define the function $f_a(x) = \ln(1+x^2) - ax$. Then we have (a,b) a suitable pair if and only if $f_a(x) = b$ has a unique solution. Since $f_a(x) = f_{-a}(-x)$ for all $a, x \in \mathbb{R}$, it suffices to consider $a \ge 0$.

For a = 0, we have $f_a(x) = f_a(-x)$, and for all $x \neq 0$, $f_a(x) > 0 = f_a(0)$. Thus b = 0 is the only solution here. For all a > 0, we see that

$$\lim_{x \to -\infty} f_a(x) = +\infty \qquad \qquad \lim_{x \to +\infty} f_a(x) = -\infty$$
 (2)

The first is because $f_a(x) \ge -ax$ for all x and $-ax \to \infty$ as $-\infty$; the second is because asymptotically, as $x \to +\infty$ we have $\ln(1+x^2) = o(x)$ (i.e. grows slower than x). It therefore follows that f_a is surjective for all a > 0 (given that f_a is also continuous).

Next, notice that (henceforth derivatives are w.r.t. x)

$$f_a'(x) = \frac{2x}{1+x^2} - a \tag{3}$$

and we see that $1+x^2-|2x|=(|x|-1)^2\leq 1$. Therefore $|\frac{2x}{1+x^2}|\leq 1$. This means that if $a\geq 1$, $f_a'(x)\leq 0$ with the only equality at a=1,x=1. It then follows that f_a is decreasing when $a\geq 1$, and therefore injective. Combined with the surjectivity of f_a we have $f_a(x)=b$ has a unique solution for all real b.

Finally, consider 0 < a < 1. Denote:

$$a_1 = \frac{1 - \sqrt{1 - a^2}}{a}$$
 $a_2 = \frac{1 + \sqrt{1 - a^2}}{a}$

These are the roots of $f'_a(x) = 0$, and $f'_a(x) > 0$ for $x \in (a_1, a_2)$ and < 0 for $x < a_1$ or $x > a_2$. Therefore, f_a is increasing in $x \in (a_1, a_2)$ and decreasing otherwise. Since f_a is surjective and continuous, and $f_a(a_1) > f_a(a_2)$, it follows that for each b there's a solution $f_a(x) = b$ with $x \notin [a_1, a_2]$. On the other hand, if $b \notin [f_a(a_2), f_a(a_1)]$, then it has solution in either $x < a_1$ or $x > a_2$ but not both. Therefore b is suitable if and only if $b \notin [f_a(a_2), f_a(a_1)]$. Now,

$$f_a(a_1) = \ln(\frac{2(1-\sqrt{1-a^2})}{a^2}) - (1-\sqrt{1-a^2}) \qquad f_a(a_2) = \ln(\frac{2(1+\sqrt{1-a^2})}{a^2}) - (1+\sqrt{1-a^2})$$
(4)

The conclusion follows. For a < 0 the answer is the same (by changing a to -a).

A2. Let n be an integer with $n \ge 2$. Over all real polynomials p(x) of degree n, what is the largest possible number of negative coefficients of $p(x)^2$?

Answer. 2n-2.

Solution. The construction is given as the following:

$$p(x) = x^{n} + 1 - \epsilon(x + x^{2} + \dots + x^{n-1})$$
(5)

where $0 < \epsilon < \frac{1}{2n}$. If $p(x)^2 = \sum a_i x^i$ for $i = 0, \dots, 2n$ then for $i = 1, \dots, n-1$:

$$a_k = \begin{cases} (k-1)\epsilon^2 - 2\epsilon & 1 \le k \le n-1\\ (2n-1-k)\epsilon^2 - 2\epsilon & n+1 \le k \le 2n-1 \end{cases}$$
 (6)

With $0 < \epsilon < \frac{1}{2n}$ we have $(k-1)\epsilon < 2$ for all $k \le n-1$ and $(2n-1-k)\epsilon < 2$ for all $k \ge n+1$. Thus $a_k < 0$ for all $k = 1, \dots, n-1, n+1, \dots, 2n-1$.

To show that 2n-2 cannot be improved, let p(x) be arbitrary and set a_0, \dots, a_{2n} to be the coefficient of $1, \dots, x^{2n}$ in $p(x)^2$. We have $a_0, a_{2n} \geq 0$ so it remains to show that $a_k \geq 0$ for one other index. Let b_0, \dots, b_n to be the coefficient of $1, \dots, x^n$ in p(x). Then either b_0 and b_n have the same sign (assume that 0 is on the positive side here) or b_1 is of the same sign as exactly one of b_0, b_n . In any case there exists i such that $i \neq 0$ and $b_0b_i \geq 0$, or $i \neq n$ and $b_nb_i \geq 0$.

Now suppose we have the former case, and let k > 0 to be the minimal index such that $b_0b_k \ge 0$. Then $a_k = \sum_{i+j=k} b_ib_j$. Since $b_0b_k \ge 0$, and by the minimality of k, $b_ib_j \ge 0$ for all 0 < i, j < k, $a_k \ge 0$, as claimed (notice that $1 \le k \le n$).

A3. Let p be a prime number greater than 5. Let f(p) denote the number of infinite sequences a_1, a_2, a_3, \ldots such that $a_n \in \{1, 2, \ldots, p-1\}$ and $a_n a_{n+2} \equiv 1 + a_{n+1} \pmod{p}$ for all $n \geq 1$. Prove that f(p) is congruent to 0 or 2 (mod 5).

Solution. We'll use the fact that a valid sequence is uniquely determined by (a_1, a_2) , i.e. it suffices to count the number of suitable (a_1, a_2) . First, we see that the sequence is periodic. In fact, we see that 5 is a period via the following construction on a_1, a_2, \cdots :

$$a_1, a_2, \frac{a_2+1}{a_1}, \frac{a_1+a_2+1}{a_1a_2}, \frac{a_1+1}{a_2}, a_1, a_2, \cdots$$

Since 5 is a prime, the minimal period is either 1 or 5.

Now to count the number of such sequences, we note that $a_i = a_j$ and $a_{i+1} = a_{j+1}$ implies that $a_{i+k} = a_{j+k}$ for all $k \ge -\min(i,j)+1$, so the 5 pairs $(a_1,a_2),(a_2,a_3),(a_3,a_4),(a_4,a_5),(a_5,a_1)$ are either all distinct or all equal. Formally, we may define equivalence relation \sim such that $(a,b) \sim (c,d)$ if and only if there exists a sequence (a_1,a_2,\cdots) such that $(a,b) = (a_i,a_{i+1})$ and $(c,d) = (a_j,a_{j+1})$. (The identity and symmetry condition of \sim is clear; for transitivity, if a_1,\cdots and b_1,\cdots are such that $a_i=b_j$ and $a_{i+1}=b_{j+1}$ for some $i \ne j$ then if k=j-i>0 we have $a_{i'}=b_{i'+k}$, i.e. a cyclic shift). Each class has size either 5 or 1, so to verify the conclusion, it suffices to count the number of classes with size 1, that is, the number of x's such that there's a sequence with $x=a_1=a_2=a_3=\cdots$. This is the same as saying that $x^2=x+1 \pmod p$, or $x^2-x=1 \pmod p$. Now for each x,y we have

$$(x^2 - x) - (y^2 - y) = (x - y)(x + y - 1)$$

so $x^2 - x \equiv y^2 - y$ iff x = y or $x + y \equiv 1$. Thus if there's one solution x satisfying $x^2 - x \equiv 1$, we also have $(1 - x)^2 - (1 - x) \equiv 1$. If $x \equiv 1 - x$, then we have $x \equiv \frac{p+1}{2}$ which means $x^2 - x \equiv -\frac{1}{4}$ (multiplicate inverse allowed here since p is odd). But $-\frac{1}{4} \equiv 1$ happens only when p = 5, so in fact $x \not\equiv 1 - x \pmod{p}$. This shows that the number of such x's is either 0 or 2, and so $f(p) \equiv 0$ or 2 (mod 5).

Remark. In fact, such a sequence is valid if and only if $a_1, a_2 \in \{1, \dots, p-1\}$ and $a_1 + a_2 \not\equiv -1 \pmod{p}$. This gives $(p-2)(p-3) \pmod{5}$, which is always congruent to 0 or 2 mod 5.

A4. Suppose that X_1, X_2, \ldots are real numbers between 0 and 1 that are chosen independently and uniformly at random. Let

$$S = \sum_{i=1}^{k} \frac{X_i}{2^i}$$

where k is the least positive integer such that $X_k < X_{k+1}$, or $k = \infty$ if there is no such integer. Find the expected value of S.

Answer. $2e^{1/2} - 3$.

Solution. By the definition of k, we have $X_1 \ge X_2 \ge \cdots X_k < X_{k+1}$. We may therefore write S into the following form:

$$S = \sum_{i=1}^{k} \frac{X_i}{2^i}$$

$$= \sum_{i=1}^{\infty} \frac{X_i}{2^i} \cdot \mathbb{1}\{i \le k\}$$

$$= \sum_{i=1}^{\infty} \frac{X_i}{2^i} \cdot \mathbb{1}\{X_1 \le X_2 \le \dots \le X_i\}$$

$$(7)$$

Therefore, by the linearity of expectation, we have

$$\mathbb{E}[S] = \mathbb{E}\left[\sum_{i=1}^{\infty} \frac{X_i}{2^i} \cdot \mathbb{1}\{X_1 \le X_2 \le \dots \le X_i\}\right] = \sum_{i=1}^{\infty} \frac{1}{2^i} \mathbb{E}[X_i \cdot \mathbb{1}\{X_1 \le X_2 \le \dots \le X_i\}] \quad (8)$$

Let's now establish the following:

Lemma 1. For all $x \in [0,1]$ we have

$$\mathbb{P}[X_1 \ge \dots \ge X_k \ge x] = \frac{(1-x)^k}{k!} \tag{9}$$

Proof. We show two ways to establish this.

First principle solution: the LHS probability can be written as the following integration:

$$\int_{X_{1}=x}^{1} \int_{X_{2}=x}^{X_{1}} \cdots \int_{X_{k}=x}^{X_{k-1}} 1 dX_{k} \cdots X_{1}$$

$$\int_{X_{1}=x}^{1} \int_{X_{2}=x}^{X_{1}} \cdots \int_{X_{k-1}=x}^{X_{k-2}} (X_{k-1} - x) dX_{k-1} \cdots X_{1}$$

$$\int_{X_{1}=x}^{1} \int_{X_{2}=x}^{X_{1}} \cdots \int_{X_{k-2}=x}^{X_{k-3}} \frac{(X_{k-2} - x)^{2}}{2} dX_{k-2} \cdots X_{1}$$

$$\vdots$$

$$\int_{X_{1}=x}^{1} \int_{X_{2}=x}^{X_{1}} \cdots \int_{X_{k-\ell}=x}^{X_{k-\ell-1}} \frac{(X_{k-\ell} - x)^{\ell}}{\ell!} dX_{k-\ell} \cdots X_{1}$$

$$\vdots$$

$$\int_{X_{1}=x}^{1} \frac{(X_{1} - x)^{k-1}}{(k-1)!} dX_{1}$$

$$= \frac{(1-x)^{k}}{k!}$$
(10)

Solution via symmetry: we write the probability into the following:

$$\mathbb{P}[X_1 \ge \dots \ge X_k \ge x] = \mathbb{P}[X_i \ge x, \forall i = 1, \dots, k] \mathbb{P}[X_1 \ge \dots \ge X_k \mid X_i \ge x, \forall i = 1, \dots, k]$$
(11)

We have $\mathbb{P}[X_i \geq x, \forall i = 1, \dots, k] = (1-x)^k$. For the second probability, we consider all the k! permutations σ of $1, \dots, k$. All the k! combinations $(X_{\sigma(1)}, \dots, X_{\sigma(k)})$ have the same probability density; consider the case where X_1, \dots, X_k pairwise distinct, we have exactly one σ that has $X_{\sigma(1)} \geq \dots \geq X_{\sigma(k)}$. Since we have X_1, \dots, X_k pairwise distinct almost surely (i.e. probability 1), we have $\mathbb{P}[X_1 \geq \dots \geq X_k \mid X_i \geq x, \forall i = 1, \dots, k] = \frac{1}{k!}$ by the symmetry argument (i.e. the unique σ among k! permutations). Thus multiplying the two gives $\frac{(1-x)^k}{k!}$.

Thus now we have, for each $i \geq 1$,

$$\mathbb{E}[X_i \cdot \mathbb{1}\{X_1 \le X_2 \le \dots \le X_i\}] = \mathbb{E}[X_i \cdot \frac{(1 - X_i)^{i-1}}{(i-1)!}]$$

$$= \int_0^1 \frac{x(1-x)^{i-1}}{(i-1)!}$$

$$= \int_0^1 \frac{(1-x)^{i-1} - (1-x)^i}{(i-1)!}$$

$$= \frac{1}{(i-1)!} (\frac{1}{i} - \frac{1}{i+1})$$

$$= \frac{1}{(i+1)!}$$
(12)

And therefore,

$$\mathbb{E}[S] = \sum_{i=1}^{\infty} \frac{1}{2^{i}(i+1)!}$$

$$= 2 \sum_{i=2}^{\infty} \frac{1}{2^{i}i!}$$

$$= 2(\sum_{i=0}^{\infty} \frac{1}{2^{i}i!} - \frac{1}{2^{0}0!} - \frac{1}{2^{1}1!})$$
(13)

$$=2e^{1/2}-3\tag{15}$$

Section B

B1. Suppose that $P(x) = a_1x + a_2x^2 + \ldots + a_nx^n$ is a polynomial with integer coefficients, with a_1 odd. Suppose that $e^{P(x)} = b_0 + b_1x + b_2x^2 + \ldots$ for all x. Prove that b_k is nonzero for all $k \ge 0$.

Solution. We first note that $b_0 = 1$ and $b_1 = a_1 \neq 0$. For $k \geq 2$ we can show that:

$$b_k = \sum_{m=1}^k \sum_{(c_1, \dots, c_m): c_1 + \dots + c_m = k} \frac{a_{c_1} a_{c_2} \cdots a_{c_m}}{m!} = \frac{1}{k!} \sum_{m=1}^k \sum_{(c_1, \dots, c_m): c_1 + \dots + c_m = k} \frac{k!}{m!} a_{c_1} a_{c_2} \cdots a_{c_m}$$

$$\tag{16}$$

where $a_i = 0$ for all i > n. Using the fact that k(k-1) is even for all k, we have $\frac{k!}{m!}$ an even integer for all $m \le k-2$. Therefore,

$$k!b_{k} = \sum_{m=1}^{k} \sum_{(c_{1}, \cdots, c_{m}): c_{1} + \cdots + c_{m} = k} \frac{k!}{m!} a_{c_{1}} a_{c_{2}} \cdots a_{c_{m}}$$

$$\equiv k(k-1)a_{1}^{k-2} a_{2} + a_{1}^{k}$$

$$\equiv a_{1}^{k} \not\equiv 0 \pmod{2}$$
(17)

B2. Let \times represent the cross product in \mathbb{R}^3 . For what positive integers n does there exist a set $S \subset \mathbb{R}^3$ with exactly n elements such that

$$S = \{v \times w : v, w \in S\}?$$

Answer. n = 1, 7.

Solution. For n = 1 we have $S = \{(0,0,0)\}$; for n = 7 we have

$$S = \{(0,0,0), \pm(1,0,0), \pm(0,1,0), \pm(0,0,1)\}$$

We now show that these are the only examples, via the following lemma:

Lemma 2. All nonzero vectors are unit vectors and are either perpendicular or parallel to each other.

Proof. By the finiteness of S, we may consider v to be the longest vector in S. Suppose |v| > 1. Let $v = s \times t$, $s, t \in S$, then $1 < |v| = |s| \cdot |t| \cdot |\sin(s, t)| \le |s| \cdot |t|$ so either |s| > 1 or |t| > 1. In addition, both s, t are perpendicular to t. Now, if |s| > 1 then $w = s \times v \in S$ and $|w| = |s| \cdot |v| > |v|$, contradicting the maximality of |v|.

Now consider u to be the shortest nonzero vector in S. Suppose |u| < 1. Let $u = s \times t$, $s, t \in S$ for some s, t. Let $r = u \times s$. Then u, s, r are mutually perpendicular to each other and are nonzero. In addition, $|s| \le 1$ so $|r| \le |u|$. Since $|r \times u| = |r| \cdot |u| = |u|^2 < |u|$ and $r \times u \ne 0$, this contradicts the minimality of |u| among the nonzero vectors.

Finally, now that all nonzero vectors are unit, let $s, t \in S$ with |s| = |t| = 1. Then $|s \times t|$ is either 0 or 1, showing that s and t are either parallel or perpendicular to each other. \square

Now if S is nonempty, then $v \in S$ means $0 = v \times v \in S$. In addition, $v \times w = -w \times v$, and therefore $s \in S \to -S \in S$. If n > 1, then we can pick $s \in S$ that's nonzero, and therefore $s = t \times u$ for some $t, u \in S$. From our lemma, s, t, u are all unit and are mutually perpendicular to each other. We also have $-s, -t, -u \in S$ since S is closed under negation. Together with $0 \in S$ we have $|S| \ge 7$. Since a 3D space cannot admit more than 3 mutually perpendicular vectors (up to scalar constants), these 7 vectors are all the elements in S.

B3. Assign to each positive real number a color, either red or blue. Let D be the set of all distances d > 0 such that there are two points of the same color at distance d apart. Recolor the positive reals so that the numbers in D are red and the numbers not in D are blue. If we iterate the recoloring process, will we always end up with all the numbers red after a finite number of steps?

Answer. Yes. In fact, we show that all numbers will be red after 2 iterations.

Solution. Consider all numbers not in D (for the first iteration), and partition them into classes of rational ratio, i.e. each class has the form $E_v \subseteq \mathbb{Q}_v \triangleq \{vq : q \in \mathbb{Q}^+\}$. Consider one such class E_v and let $Q_v = \{q \in \mathbb{Q}, qv \in E_v\}$. For each rational number q > 0, we define the function ν_2 such that, if $q \in \mathbb{N}$, then $\nu_2(q) = \max\{k : 2^k \mid q\}$ (i.e. the highest exponent of 2 dividing q), and if $q = \frac{r}{s}$ with $r, s \in \mathbb{N}$ then $\nu_2(q) = \nu_2(r) = \nu_2(s)$. Here comes our key claim:

Lemma 3. All the rationals in Q_v has the same ν_2 . That is, there exists a constant $c \triangleq c(v)$ such that $\forall q \in Q_v : \nu_2(q) = c$.

Proof. Consider q_1 and $q_2 \in Q_v$, and choose any point a on the first iteration. We see that by the definition of D and that $q_1v, q_2v \notin D$, $a, a+q_1v, a+2q_1v, a+3q_1v, \cdots$ must be in alternating colour, so a and $a+nq_1v$ are of the same colour if and only if n is even. Similarly, a and $a+nq_2v$ are of the same colour if and only if n is even. Now consider integers r_1, t_2 such that $q_1r_1 = q_2r_2$, and such that $\gcd(r_1, r_2) = 1$. Since $r_1q_1v = r_2q_2v$, r_1, r_2 must have the same parity, i.e. both odd. Thus $\nu_2(q_1) = \nu_2(q_2)$ must hold here. \square

Now consider what happens after the first iteration. On second iteration, we see that we have a constant (integer) c(v) such that if $\nu_2(q) \neq c(v)$ then qv is painted red. Consider, now, any rational number r. Let $s = 2^{\min(c(v),\nu_2(r))-1}$, then with $\nu_2(s) < \nu_2(r)$ we have $\nu_2(s) = \nu_2(s+r) < c(v)$, which means that both sv and rv are painted red here. It then follows that rv will be painted red in the next round. Considering all such $r \in \mathbb{Q}^+$ and all such classes Q_v we have all points painted red after this iteration.

B4. Find all integers n with $n \ge 4$ for which there exists a sequence of distinct real numbers x_1, \ldots, x_n such that each of the sets

$$\{x_1, x_2, x_3\}, \{x_2, x_3, x_4\}, \dots, \{x_{n-2}, x_{n-1}, x_n\}, \{x_{n-1}, x_n, x_1\}, \text{ and } \{x_n, x_1, x_2\}$$

forms a 3-term arithmetic progression when arranged in increasing order.

Answer. All n such that $n \geq 9$ and $3 \mid n$.

Solution. We first determine one such construction. Let $k \geq 2$ and n = 3(k + 1), and consider the following n numbers:

$$0, 4, 8, \dots, 4k, 4k - 2, 4k - 1, 4k - 3, 4k - 5, \dots, 1, 2$$

The odd numbers are $1, \dots, 4k-1$, the even numbers are $0, \dots, 4k$, and 2 and 4k-2 (which are distinct since $k \geq 2$). Also the first k+1 numbers and the sequence of odd numbers define chains of arithmetic progression, so it remains to check the following:

$$(4k-4,4k,4k-2),(4k,4k-2,4k-1),(4k-2,4k-1,4k-3),(3,1,2),(1,2,0),(2,0,4)$$

which, when sorted within each triples, becomes

$$(4k-4,4k-2,4k),(4k-2,4k-1,4k),(4k-3,4k-2,4k-1),(1,2,3),(0,1,2),(0,2,4)$$

and therefore valid.

To show necessity, we first show that $3 \mid n$. Denote $d_i = x_{i+1} - x_i$ (indices taken modulo n), then we have the following properties on d_i :

- $\sum_{i=1}^{n} = 0$ (consistency);
- $d_{i+1} \in \{d_i, -\frac{d_i}{2}, -2d_i\}$ (arithmetic progression);
- For any i < j and $(i, j) \neq (1, n)$ we have $d_i + \cdots + d_j \neq 0$ (all x_i 's distinct).

By scaling, we may assume that $\min_{i=1,\dots,n} |d_i| = 1$, and by flipping signs we may also assume that there exists an i such that $d_i = 1$. Since $1 = (-2)^0, -2 = (-2)^1$ and $-\frac{1}{2} = (-2)^{-1}$, for each i there exists a k_i such that $d_i = (-2)^{k_i}$, and with $\min d_i = 1$ we have $\min k_i = 0$. In addition, $|k_{i+1} - k_i| \le 1$. Since $-2 \equiv 1 \pmod{3}$, $d_i \equiv 1 \pmod{3}$ and therefore

$$0 = \sum_{i=1}^{n} d_i \equiv \sum_{i=1}^{n} 1 = n \pmod{3}$$
 (18)

i.e. 3 | n.

It now remains to show that we do not have an example for n=6. First, since d_i are integers and $(-2)^k$ is even for $k \geq 1$, there's at least two numbers d_i that's equal to 1. Next, we cannot have all $d_i=1$ since the sum has to be 0. Considering a block B of consecutive 1's among the d_i 's; adjacent to the block has to be -2 (since min $|d_i|=1$). If B has length ≥ 2 then we have a consecutive chain of -2, 1, 1 which sums to 0, so $x_i=x_{i+3}$ for some i, which is a contradiction. It follows that we must have the two $d_i=1$'s having spaced either 2 or 3 apart (on the circle of 6 d_i 's). Considering that the $d_i=1$ must be neighboured by -2's, we have one of the following two scenarios:

$$(-2,1,-2,-2,1,-2) (19)$$

$$(1, -2, 1, -2, a, -2) \tag{20}$$

(21)

The first one is impossible since the sum is -6; the second one has sum -2 + a, which follows that a = 2. But this contradicts that $a = (-2)^k$ for some $k \in \mathbb{Z}_{\geq 0}$.