Putnam 2012

A1 Let $d_1, d_2, \ldots, d_{12}$ be real numbers in the open interval $(1, 12)$. Show that there exist distinct indices i, j, k such that d_i, d_j, d_k are the side lengths of an acute triangle.

Solution. We sort the numbers into $d_1 \leq d_2 \leq \cdots \leq d_{12}$. Suppose otherwise, then $d_i^2 + d_{i+1}^2 \leq d_{i+2}^2$. From $d_1, d_2 > 1$ we have $d_3 > \sqrt{2}$, $d_4 > \sqrt{3}$, $d_5 > \sqrt{5}$, $d_6 > \sqrt{8}$, $d_7 > \sqrt{13}$, $d_8 > \sqrt{21}$, $d_9 > \sqrt{34}$, $d_{10} > \sqrt{55}$, $d_{11} > \sqrt{89}$, $d_{12} > \sqrt{144} = 12$, contradiction.

A2 Let $*$ be a commutative and associative binary operation on a set S. Assume that for every x and y in S, there exists z in S such that $x * z = y$. (This z may depend on x and y.) Show that if a, b, c are in S and $a * c = b * c$, then $a = b$.

Solution. Now we suppose that $a * c = b * c$. Let x be the element satisfying $a * x = b$, y be the element satisfying $a * y = a$, then we have

$$(x * a) * c = (a * x) * c = b * c = a * c = (a * y) * c = (y * a) * c$$

and by the commutativity and associativity of $*$ we can arrange this into $x * (a * c) = y * (a * c)$. Now let d be the element such that $(a * c) * d = a$ we have $b = x * a = x * (a * c) * d = y * (a * c) * d = y * a = a$, as desired.

A3 Let $f : [-1, 1] \to \mathbb{R}$ be a continuous function such that

(i) $f(x) = \frac{2-x^2}{2} f\left(\frac{x^2}{2-x^2}\right)$ for every x in $[-1, 1]$,

(ii) $f(0) = 1$, and

(iii) $\lim_{x \to 1^-} \frac{f(x)}{\sqrt{1-x}}$ exists and is finite.

Prove that f is unique, and express $f(x)$ in closed form.

Answer. The function $f(x) = \sqrt{1 - x^2}$ is the unique solution.

Solution. We will skip the verification on the fact that this f works (with the third limit equals to $\sqrt{1+x}$), and jump straight into the fact that there's no other f that fits this criterion.

First, notice from the first condition that $f(x) = \frac{2-x^2}{2} f\left(\frac{x^2}{2-x^2}\right) = f(x) = \frac{2-(-x)^2}{2} f\left(\frac{(-x)^2}{2-(-x)^2}\right) = f(-x)$ so it suffices to consider those functions in the range $[0, 1]$. We first define a polynomial $P_n(x)$ in the following fashion: $P_0(x) = x$ and for each n, $P_{n+1}(x) = 2P_n^2(x) - 1$ (basically $P_n(\cos x) = \cos(2^n x)$). We have the following observations:

- If $x > 1$, then $\lim_{n\to\infty} P_n(x) = \infty$. To see why, for each $x > 1$ we have $2x^2 - 1 = x^2 + (x^2 - 1) > x^2$ so $P_1(x) > P_0(x)^2 = x^2$ and we can inductively show that $P_n(x) > x^{2^n}$. Since $\lim_{n\to\infty} x^{2^n} = \infty$ for each $x > 1$, the conclucion follows.
- Now for each $x > 1$ we have $f(\frac{1}{P_n(x)}) = \frac{2P_n(x)^2-1}{2P_n(x)^2} f(\frac{1}{2P_n(x)^2-1}) = \frac{P_{n+1}(x)}{2P_n(x)^2} f(\frac{1}{P_{n+1}(x)})$. Inductively we get the following telescoping sum:

$$f\left(\frac{1}{x}\right) = f\left(\frac{1}{P_0(x)}\right) = \frac{P_1(x)}{2P_0(x)^2} f\left(\frac{1}{P_1(x)}\right) = \frac{P_2(x)}{2^2 P_0(x)^2 P_1(x)} f\left(\frac{1}{P_2(x)}\right)$$

which leads to the ultimate $\frac{P_n(x)}{2^n P_0(x) \prod_{k=1}^{n-1} P_k(x)} f\left(\frac{1}{P_n(x)}\right)$. We also recall that as $x > 1$, $\lim_{n\to\infty} P_n(x) = \infty$ so $f\left(\frac{1}{P_n(x)}\right) \to f(0) = 1$ since f is continuous. Thus, $f\left(\frac{1}{x}\right) = \lim_{n\to\infty} \frac{P_n(x)}{2^n P_0(x) \prod_{k=1}^{n-1} P_k(x)}$.

- The identity that $2^n \cos(x)\cos(2x)\cos(4x)\cdots\cos(2^{n-1}(x))$ can be telescoped in the following manner: multiplying by $\sin(x)$ we have $2^n \sin(x)\cos(x)\cos(2x)\cos(4x)\cdots\cos(2^{n-1}(x)) = 2^{n-1}\sin(2x)\cos(2x)\cos(4x)\cdots\cos(2^{n-1}(x)) = \cdots = \sin(2^n x)$ since $2\sin x\cos x = \sin(2x)$ so $2^n\cos(x)\cos(2x)\cos(4x)\cdots\cos(2^{n-1}(x)) = \frac{\sin 2^n x}{\sin x}$. Unfortunately, we are dealing with $P_n(x)$ where each value is greater than 1, and is therefore less helpful. We nevertheless notice that the realization $\sin 2x = 2\cos x \sin x$ comes from the fact that $\sqrt{1-\cos^2 2x} = 2\cos x\sqrt{1-\cos^2 x}$, i.e. for each $0 \le x < 1$ we have $\sqrt{1-P_1(x)^2} = 2x\sqrt{1-x^2}$, or more generally, $\sqrt{1-P_{n+1}(x)^2} = 2P_n(x)\sqrt{1-P_n(x)^2}$. Multiplying $\sqrt{-1}$ into both sides (bad writing, only for iidea illustration purpose) we get $\sqrt{P_{n+1}(x)^2-1} = 2P_n(x)\sqrt{P_n(x)^2-1}$, which will help in the case $x > 1$.Thus we have the following telescoping sum for the following:

$$\begin{aligned}
2^n\sqrt{x^2-1}\prod_{k=1}^{n-1} P_k(x) &= 2^n\sqrt{P_0(x)^2-1}P_0(x)P_1(x)\cdots P_{n-1}(x)\\
&= 2^{n-1}\sqrt{P_1(x)^2-1}P_1(x)\cdots P_{n-1}(x)\\
&= 2^{n-2}\sqrt{P_2(x)^2-1}P_2(x)\cdots P_{n-1}(x)\\
&= \cdots\\
&= 2\sqrt{P_{n-1}(x)^2-1}P_{n-1}(x)\\
&= \sqrt{P_n(x)^2-1}
\end{aligned}$$

This means we actually have

$$f\left(\frac{1}{x}\right) = \lim_{n\to\infty}\frac{P_n(x)}{2^n x\prod_{k=1}^{n-1}P_k(x)} = \lim_{n\to\infty}\frac{P_n(x)\sqrt{x^2-1}}{2^n x\sqrt{x^2-1}\prod_{k=1}^{n-1}P_k(x)} = \lim_{n\to\infty}\frac{P_n(x)\sqrt{x^2-1}}{x\sqrt{P_n(x)^2-1}}$$

and since $P_n(x)\to\infty$, we have $\frac{P_n(x)}{\sqrt{P_n(x)^2-1}}\to 1$, so $f\left(\frac{1}{x}\right) = \dfrac{\sqrt{x^2-1}}{x} = \sqrt{1-\frac{1}{x^2}}$. Thus $f(x) = \sqrt{1-x^2}$, as desired.

A5 Let $\mathbb{F}_p$ denote the field of integers modulo a prime p, and let n be a positive integer. Let v be a fixed vector in $\mathbb{F}_p^n$, let M be an $n\times n$ matrix with entries in $\mathbb{F}_p$, and define $G:\mathbb{F}_p^n\to\mathbb{F}_p^n$ by $G(x) = v + Mx$. Let $G^{(k)}$ denote the k-fold composition of G with itself, that is, $G^{(1)}(x) = G(x)$ and $G^{(k+1)}(x) = G(G^{(k)}(x))$. Determine all pairs p, n for which there exist v and M such that the p^n vectors $G^{(k)}(0)$, $k = 1, 2, \ldots, p^n$ are distinct.

Answer. All $n = 1$ with any prime p, together with $n = 2, p = 2$.

Solution. For $n = 1$, taking $M = v = \begin{pmatrix}1\end{pmatrix}$ gives us the desired solution since $G^{(k)}(0) = \begin{pmatrix}k\end{pmatrix}$. For $n = 2$ and $p = 2$, take $M = \begin{pmatrix}1 & 1\\ 0 & 1\end{pmatrix}$ and $v = \begin{pmatrix}0\\1\end{pmatrix}$ gives us $G^{(1)}(0) = \begin{pmatrix}0\\1\end{pmatrix}$, $G^{(2)}(0) = \begin{pmatrix}1\\0\end{pmatrix}$, $G^{(3)}(0) = \begin{pmatrix}1\\1\end{pmatrix}$, $G^{(4)}(0) = \begin{pmatrix}0\\0\end{pmatrix}$, establishing the claim.

To show that these are the only pairs, we first expand $G^{(k)}(0)$ in the 'brute-force' manner, meaning that $G^{(k)}(0) = (1 + M + M^2 + \cdots + M^{k-1})v$. By Cayley-Hamilton theorem, if $P(x)$ is the characteristic polynomial of M, then P has degree n and $P(M) = 0$. Hence it suffices to consider the remainder of $1 + M + M^2 + \cdots + M^{k-1}$ when divided by $P(x)$. Now, denote the remainder of $1 + M + M^2 + \cdots + M^{k-1}$ as $a_0 + a_1M + \cdots + a_{n-1}M^{n-1}$. By our assumption, each of the p^n vectors are distinct, so this polynomial remainder must also be distinct as k varies across $1, 2, \cdots, p^n$. Denoting $Q_k(x)$ as the remainder of $1+x+\cdots+x^{k-1}(x)$. Then we have $Q_k(x) \equiv 1 + xQ_{k-1}(x) \pmod{P(x)}$ for all $k \ge 1$, with $Q_0(x) = 0$. It then follows that $Q_k(x)$ are all distinct for $k = 1, 2, \cdots, p^n$ and since there

are exactly p^n elements in the set $\{\sum_{j=0}^{n-1} a_j x^j, a_j \in \mathbb{F}_p\}$, each element in the set occurs exactly once in $Q_1, Q_2, \cdots, Q_{p^n}$ and since $Q_k = 1 + xQ_{k-1}$, $Q_1, Q_2, \cdots, Q_{p^n}$ form a cycle, and considering $Q_0 = 0$ we have $Q_{p^n} = 0$ too.

The relation $Q_{p^n} = 0$ implies that $P(x)|1 + x + \cdots x^{k-1}$ if and only if $p^n|k$. We first claim that $1 + x + \cdots x^{p^n-1} = (x-1)^{p^n-1}$. Indeed, the coefficient of x^k in this polynomial is

$$(-1)^k \binom{p^n - 1}{k} = (-1)^k \prod_{j=1}^{k} \left(\frac{p^n - j}{j}\right) = (-1)^k \prod_{j=1}^{k} \left(\frac{p^n}{j} - 1\right)$$

since j is not divisible by p^n, $\frac{p^n-j}{j}$ can be treated as an integer modulo p. In fact, $\frac{p^n}{j}$ is 0 modulo p since j is not divisible by n, so $\left(\frac{p^n}{j} - 1\right) \equiv -1 \pmod{p}$. This means that

$$(-1)^k \prod_{j=1}^{k} \left(\frac{p^n}{j} - 1\right) \equiv (-1)^k \prod_{j=1}^{k} (-1) = (-1)^{2k} = 1$$

and therefore $(x-1)^{p^n-1} = 1 + x + \cdots + x^{p^n-1}$ when considering elements in $\mathbb{F}_p[x]$, as desired. This means that Q_{p^n-1} has 1 as root, repeated $p^n - 1$ times, and so the only possible $P(x)$ (which must have degree n) is $(x-1)^n$. Nevertheless, our computation above also suggests that $1 + x + \cdots + x^{p^k-1} = (x-1)^{p^k-1}$ for all $k \geq 1$, too, so $P(x)|Q_{p^k-1}$ whenever $p^k - 1 \geq n$. This should not happen for $k < n$; otherwise $Q_{p^k-1} = 0$ for all such k and we have $G^{(p^k)}(0) = 0$. Therefore we need to have $p^{n-1} - 1 < n$, or $p^{n-1} \leq n$. This holds whenever $n = 1$, and when $n = 2$ we need $p \leq 2$, i.e. $p = 2$. For $n \geq 3$, we have $2^{n-1} > n$ (can be proven by induction) so no prime can satisfy this. This completes the proof, QED.

B1 Let S be a class of functions from $[0, \infty)$ to $[0, \infty)$ that satisfies:

(i) The functions $f_1(x) = e^x - 1$ and $f_2(x) = \ln(x+1)$ are in S;

(ii) If $f(x)$ and $g(x)$ are in S, the functions $f(x) + g(x)$ and $f(g(x))$ are in S;

(iii) If $f(x)$ and $g(x)$ are in S and $f(x) \geq g(x)$ for all $x \geq 0$, then the function $f(x) - g(x)$ is in S.

Prove that if $f(x)$ and $g(x)$ are in S, then the function $f(x)g(x)$ is also in S.

Solution. Now suppose that $f(x) \in S$ and $g(x) \in S$, we have $f_2(f(x)) = \ln(f(x)+1) \in S$ and $f_2(g(x)) = \ln(g(x)+1) \in S$. By (ii), we can add them up and obtain $\ln(f(x)+1)\ln(g(x)+1) = \ln((f(x)+1)(g(x)+1)) \in S$ and by (i) and (ii) again, $f_1(\ln((f(x)+1)(g(x)+1))) = e^{\ln((f(x)+1)(g(x)+1))} - 1 = (f(x)+1)(g(x)+1) - 1 = f(x)g(x) + f(x) + g(x) \in S$. By (ii) we have $f(x) + g(x) \in S$ and since $f(x), g(x)$ are both nonnegatively valued, $f(x)g(x) \geq 0$ and so $f(x)g(x) = (f(x)g(x) + f(x) + g(x)) - (f(x) + g(x)) \in S$.

B2 Let P be a given (non-degenerate) polyhedron. Prove that there is a constant $c(P) > 0$ with the following property: If a collection of n balls whose volumes sum to V contains the entire surface of P, then $n > c(P)/V^2$.

Solution. The power-mean inequality says that, if $r_1, r_2, \cdots, r_n$ are the radii of the given circles, then considering the quadratic mean and cubic mean gives

$$\sqrt[3]{\frac{\sum_{i=1}^{n} r_i^3}{n}} \geq \sqrt{\frac{\sum_{i=1}^{n} r_i^2}{n}}$$

Raising each part to the sixth power gives $\left(\frac{\sum_{i=1}^{n} r_i^3}{n}\right)^2 \geq \left(\frac{\sum_{i=1}^{n} r_i^2}{n}\right)^3$, which means $n(\sum_{i=1}^{n} r_i^3)^2 \geq (\sum_{i=1}^{n} r_i^2)^3 \cdots (*)$.

Having established (*), denote A as the surface area of our polyhedron, k as the number of faces of the polyhedron, and A_i as the total surface area covered by the spheres. Since the spheres jointly cover the polyhedron, we must have $\sum_{i=1}^{n} A_i \geq A$. On the other hand, since the i-th sphere has radius r_i, for each face of the polyhedron, the coverage of that sphere with this surface is at most πr_i^2 (since each face is part of some plane in the space, and the interesection of a plane and a sphere of radius r, if they do intersect, is a circle, and has area at most πr^2.) This gives $A_i \leq k r_i$, considering all faces. Thus we have the following:

$$A \leq \sum_{i=1}^{n} A_i \leq k\pi \sum_{i=1}^{n} r_i^2, \qquad \sum_{i=1}^{n} r_i^2 \geq \left(\frac{A}{k\pi}\right)$$

The total volume V is given by $\frac{4}{3}\pi \sum_{i=1}^{n} r_i^3$, so we have the following:

$$nV^2 = n\left(\frac{4}{3}\pi \sum_{i=1}^{n} r_i^3\right)^2 \geq \left(\frac{4}{3}\pi\right)^2 \left(\sum_{i=1}^{n} r_i^2\right)^3 \geq \frac{16}{9}\pi^2 \left(\frac{A}{k\pi}\right)^3 = \frac{16}{9} \cdot \frac{A^3}{k^3\pi}$$

The rightmost quantity above is positive since P is not degenerate, and so we can take $c(P)$ to be any constant in the interval $\left(\frac{16}{9} \cdot \frac{A^3}{k^3\pi}\right)$.

B3 A round-robin tournament among $2n$ teams lasted for $2n-1$ days, as follows. On each day, every team played one game against another team, with one team winning and one team losing in each of the n games. Over the course of the tournament, each team played every other team exactly once. Can one necessarily choose one winning team from each day without choosing any team more than once?

Answer. Yes.

Solution. We will proceeed by inducting on n. The case where $n = 1$ is trivial since we simply choose the winning team on the only match. Now suppose that for some $n \geq 2$, for any $k < n$ and any round-robin tournament of $2k$ teams of $2k-1$ days, we can always choose a unique winning team each day. We proceed with the following cases:

(a) Suppose that there is a $k \in [1, 2n-1]$ and a subset of k teams such that, the number of days in which at least one of the k teams win the game in that day is ℓ and $\ell < k$. If $k = 1$ then this team (namely T) loses in all the $2n-1$ days, so we can choose the team that beats T in each day, and these $2n-1$ teams selected are different. Otherwise, each of the matches between the k teams have exactly 1 winner, so they must happen within the ℓ days. Considering the matches between Team i and team j for $j \in [1,k]\backslash\{i\}$, which must happen on $k-1$ different days, we know that $\ell = k-1$. By considering the matches between the k teams, there are $\binom{k}{2} \div (k-1) = \frac{k}{2}$ matches in each of the $k-1$ days, hence k must be even. By induction hypothesis, since $k < 2n-1$, we can choose a winner in each of the $k-1$ days such that the $k-1$ winners chosen are all distinct, and are part of the k teams we mentioned before. In the rest of the $2n-k$ teams, fix one of the teams from the k teams (say, Team 1) which loses in all $2n-k$ matches. We then pick the player who beats Team 1 every day in the $2n-k$ days. Each of the $2n-k$ teams are different, and are also different from the $k-1$ teams we picked in the initial $k-1$ days. This concludes the inductive proof for this part.

(b) Now suppose that for each $k < 2n$ and for each subset of k teams, the number of days in which at east one of the k teams win the game in that day is at least k. Pick $2n-1$ teams from the $2n$ teams arbitrarily. Now consider the bipartite graph consisting the said $2n-1$ teams and $2n-1$ days, with two vertices being connected by an edge if and only if the team wins on the day. By assumption, any k teams are paired jointly to at least k days. By Hall's lemma, there exists a matching between the players and the days. This also finishes the inductive proof.

B4 Suppose that $a_0 = 1$ and that $a_{n+1} = a_n + e^{-a_n}$ for $n = 0, 1, 2, \ldots$. Does $a_n - \log n$ have a finite limit as $n \to \infty$? (Here $\log n = \log_e n = \ln n$.)

Answer. Yes, and the limit is in fact 0.

Solution. First we notice it's obvious that the sequence $\{a_n\}$ is increasing since $a_{n+1} > a_n$ for each n. We also note that, the function $x + e^{-x}$ has derivative $1 - e^{-x}$ and therefore has staionary point at $x = 0$. For $x > 0$ this derivative is positive, hence $x + e^{-x}$ is increasing when $x > 0$. Suppose that the limit doesn't exist. That is, either there exists $m > 0$ such that $a_n - \log n \geq m$ for infinitely many n or there exists $m < 0$ such that $a_n - \log n \leq m$ for infinitely many n. We will deal with each case separately.

In the first case, we show that if n is any number such that $a_{n_0} - \log n_0 \geq m$, then there must exists $n_1 > n$ with $a_{n_1} - \log n_1 < m$. Suppose otherwise, then $a_n - \log n \geq m$ for all $n \geq n_0$. For all such n we have

$$\begin{aligned} a_{n+1} - \log(n+1) &= (a_n - \log n) + e^{-a_n} - \log\left(\frac{n+1}{n}\right) \\ &\leq (a_n - \log n) + e^{-(m+\log n)} - \log\left(\frac{n+1}{n}\right) \\ &= (a_n - \log n) + e^{-m} \cdot \frac{1}{n} - \log\left(1 + \frac{1}{n}\right) \end{aligned}$$

and on the other hand we have, for all $x \in (-1, 1)$, the Taylor expansion of $\log(1+x)$ as $\sum_{j=1}^{\infty} (-1)^{j-1} \frac{x^j}{j}$. In terms of Taylor approximation (into finite terms) this translates into $(1 + h(x))x$ with $h(x) \to 0$ as $x \to 0$. Thus, $a_{n+1} - \log(n+1) = (a_n - \log n) + \frac{1}{n}(e^{-m} - 1 - h(\frac{1}{n}))$. Given that $e^{-m} < 1$ and that $h(\frac{1}{n}) \to 0$ as $n \to \infty$, for sufficiently large n we have $e^{-m} - 1 - h(\frac{1}{n}) < \frac{e^{-m}-1}{2}$. If n_0 is such that all $n \geq n_0$ has such property, we have $(a_{n+1} - \log(n+1)) - (a_n - \log n) \leq \frac{1}{n} \cdot \frac{e^{-m}-1}{2}$ and therefore

$$(a_{n+k} - \log(n+k)) - (a_n - \log n) \leq \frac{e^{-m} - 1}{2} \sum_{i=0}^{k-1} \frac{1}{n+i}$$

but then the series $\{\frac{1}{n}\}$ diverges so as $k \to \infty$, $(a_{n+k} - \log(n+k)) - (a_n - \log n) \to -\infty$, which is a contradiction. Thus for all n with $a_n - \log n \geq m$ there is an $n_1 > n$ with $a_{n_1} - \log n_1 < m$.

Now with the claim above established, suppose, still, there are infinitely many n such that $a_n - \log n \geq m$. For each such n, let $b(n)$ be any integer greater than n with $a_{(b(n))} - \log b(n) < m$. Notice also from earlier that $x + e^{-x}$ is increasing with $x > 0$, and therefore

$$\begin{aligned} a_{b(n)+1} - \log(b(n)+1) = &= a_{(b(n))} - \log b(n) + e^{a_{b(n)}} - \log(1 + \frac{1}{b(n)}) \\ &\leq m + e^{-m - \log b(n)} - \log(1 + \frac{1}{b(n)}) \\ &= m + e^{-m} \cdot \frac{1}{b(n)} - \log(1 + \frac{1}{b(n)}) \\ &= m + \frac{1}{b(n)}(e^{-m} - 1 - h(1/b(n))) \end{aligned}$$

with h being the function introduced above. Using the assumption that there are infinitely many n with such property, we can find n such that $e^{-m} - 1 - h(1/n) < 0$ as $e^{-m} < 1$ and $h(1/n) \to 0$. Therefore, $b(n)$ must also follow such property (as $b(n) > n$), and therefore $m + \frac{1}{b(n)}(e^{-m} - 1 - h(1/b(n))) < m$. This means for n sufficiently large, once

$a_{b(n)} - \log(b(n)) < m$ we have $a_{b(n)+1} - \log(b(n)+1) < m$, and this trend stays forever, contradicting our assumption.

The opposite case is the similar except flipping sign. Now that $m < 0$, we have $e^{-m} > 1$ and the assumption that $a_n - \log n \le m$ for all $n \ge n_0$ leads to the case $a_{n+1} - \log(n+1) \ge (a_n - \log n) + e^{-m} \cdot \frac{1}{n} - \log\left(1 + \frac{1}{n}\right) = (a_n - \log n) + \frac{1}{n}(e^{-m} - 1 - h(1/n))$ but then $h(1/n) \to 0$, and $\{\frac{1}{n}\}$ diverges which will lead $a_n - \log n \to +\infty$, a contradiction. Thus for each n with $a_n - \log n \le m$ there's $b(n)$ with $a_{b(n)} - \log b(n) > m$, which also means (by the increasing property of $x + e^{-x}$) $a_{b(n)+1} - \log(b(n)+1) \ge m + \frac{1}{b(n)}(e^{-m} - 1 - h(1/b(n)))$ and for n sufficiently large, $e^{-m} - 1 - h(1/b(n)) > 0$. Q.E.D.

B6 Let p be an odd prime number such that $p \equiv 2 \pmod 3$. Define a permutation π of the residue classes modulo p by $\pi(x) \equiv x^3 \pmod p$. Show that π is an even permutation if and only if $p \equiv 3 \pmod 4$.

Solution. Since $\pi(0) = 0$ (identity), removal of 0 from our consideration does not affect the parity of π. Hence we consider the numbers $1, 2, \cdots, p-1$, which are all invertible elements in $\mathbb{Z}_p$. We shall first say that π is indeed a permutation since 3 is relatively prime to $p - 1 = \Phi(p)$. Now for each number x we consider the permutation orbit formed by x, and the length of the orbit ℓ is the smallest positive integer such that $\pi^\ell x = x$. On the other hand $\pi^k(x) = x^{3^k}$ as defined (taking modulo p), so ℓ is the minimal positive k satisfying $x^{3^k} = x$. Dividing by x (allowed since x is invertible in $\mathbb{Z}_p$) yields $x^{3^k - 1} \equiv 1 \pmod p$ so we have ℓ as the smallest k with $\mathrm{ord}_p(x) | 3^k - 1$, which means ℓ is the order of 3 modulo $\mathrm{ord}_p(x)$.

Now that $\Phi(p) = p-1$, consider the primitive root g and $\{1, 2, \cdots, p-1\} = \{1, g, g^2, \cdots, g^{p-2}\}$. The order of g^k is the minimal ℓ such that $p - 1 | k\ell$, which is $\frac{p-1}{\gcd(p-1,k)}$. Therefore for each divisor x of $p - 1$ the number of elements with order x is $\phi(x)$. As discussed above, for each number y with order x modulo p, the length of orbit of y is $\mathrm{ord}_x(3)$, which means that the number of different orbits containing all numbers of order x is $\frac{\phi(x)}{\mathrm{ord}_x(3)}$, and here comes the total number of orbits arising fro π:

$$\sum_{x | p-1} \frac{\phi(x)}{\mathrm{ord}_x(3)}$$

The next task is to determine the parity of this number, which we will do this by grouping all the divisors of $p - 1$ based on the largest odd factor of x. To be precise, if q is the largest exponent of 2 dividing $p - 1$ then for each off factor y of $p - 1$ we consider the sum $\sum_{j=0}^{q} \frac{\phi(2^j y)}{\mathrm{ord}_{2^j y}(3)}$. Assuming $y \ne 1$, since y is odd (relatively prime to 2^j), $\phi(2^j y) = \phi(2^j)\phi(y) = 2^{j-1}\phi(y)$ and $\mathrm{ord}_{2^j y}(3) = \mathrm{lcm}(\mathrm{ord}_{2^j}(3), \mathrm{ord}_y(3))$ (all assuming $j \ge 1$). Knowing that $q \ge 1$, $\mathrm{lcm}(\mathrm{ord}_{2^j}(3), \mathrm{ord}_y(3)) | \mathrm{ord}_{2^j}(3)\mathrm{ord}_y(3)$, and $\mathrm{ord}_y(3) | \phi(y)$, $\mathrm{ord}_{2^j}(3) | \phi(2^j)$, we have the following observation: if $\frac{\phi(y)}{\mathrm{ord}_y(3)}$ is even, then for all $j \ge 1$ we have

$$\frac{\phi(2^j)\phi(y)}{\mathrm{ord}_{2^j}(3)\mathrm{ord}_y(3)} \Big| \frac{\phi(2^j)\phi(y)}{\mathrm{lcm}(\mathrm{ord}_{2^j}(3), \mathrm{ord}_y(3))} = \frac{\phi(2^j y)}{\mathrm{ord}_{2^j y}(3)}$$

and since $\frac{\phi(2^j)}{\mathrm{ord}_{2^j}(3)}$ is an integer, the expression above is even. Otherwise, $\frac{\phi(y)}{\mathrm{ord}_y(3)}$ is odd. We first notice that $2^1 || 3 - 1$, $2^3 || 3^2 - 1$ and if $2^k | 3^\ell - 1$ then $2^{k+1} | 2(3^{2\ell} - 1) | (3^\ell - 1)(3^\ell + 1)$ so we have, for $j \ge 2$, $\mathrm{ord}_{2^j}(3) \le 2^{j-2}$. This means that $2 | \frac{\phi(2^j)}{\mathrm{ord}_{2^j}(3)}$. This leaves us with $j = 0$ and $j = 1$, and we assumed that for $j = 0$ the fraction is odd. For $j = 1$ we have $\phi(2y) = \phi(y)$ and $\mathrm{ord}_{2y}(3) = \mathrm{ord}_y(3)$ since for $k \ge 1$, $y | 3^k - 1$ implies $2y | 3^k - 1$. Hence the fraction is also odd when $j = 1$. So this gives an even sum in total, considering y fixed and $j = 0, 1, \cdots, q$.

It remains to consider the case $y = 1$, which gives us the following sum:

$$\sum_{j=0}^{q} \frac{\phi(2^q)}{\mathrm{ord}_{2^j}(3)}$$

Now this sum is 1 when $j = 0, 1, 2$ and 2 otherwise, so if $q \geq 2$ this sum is odd and if $q = 1$ this sum is even. The first case corresponds to the case where $4|p-1$, and since we have an odd number of orbits, π is odd. The second case corresponds to the case where $4 \nmid p-1$ and since we have a n even number of orbits, π is even.