Solutions to the 73rd William Lowell Putnam Mathematical Competition
Saturday, December 1, 2012

Kiran Kedlaya and Lenny Ng

A–1 Without loss of generality, assume $d_1 \leq d_2 \leq \cdots \leq d_{12}$. If $d_{i+2}^2 < d_i^2 + d_{i+1}^2$ for some $i \leq 10$, then d_i, d_{i+1}, d_{i+2} are the side lengths of an acute triangle, since in this case $d_i^2 < d_{i+1}^2 + d_{i+2}^2$ and $d_{i+1}^2 < d_i^2 + d_{i+2}^2$ as well. Thus we may assume $d_{i+2}^2 \geq d_i^2 + d_{i+1}^2$ for all i. But then by induction, $d_i^2 \geq F_i d_1^2$ for all i, where F_i is the i-th Fibonacci number (with $F_1 = F_2 = 1$): $i = 1$ is clear, $i = 2$ follows from $d_2 \geq d_1$, and the induction step follows from the assumed inequality. Setting $i = 12$ now gives $d_{12}^2 \geq 144 d_1^2$, contradicting $d_1 > 1$ and $d_{12} < 12$.

Remark. A materially equivalent problem appeared on the 2012 USA Mathematical Olympiad and USA Junior Mathematical Olympiad.

A–2 Write d for $a * c = b * c \in S$. For some $e \in S$, $d * e = a$, and thus for $f = c * e$, $a * f = a * c * e = d * e = a$ and $b * f = b * c * e = d * e = a$. Let $g \in S$ satisfy $g * a = b$; then $b = g * a = g * (a * f) = (g * a) * f = b * f = a$, as desired.

Remark. With slightly more work, one can show that S forms an abelian group with the operation $*$.

A–3 We will prove that $f(x) = \sqrt{1-x^2}$ for all $x \in [-1,1]$. Define $g : (-1,1) \to \mathbb{R}$ by $g(x) = f(x)/\sqrt{1-x^2}$. Plugging $f(x) = g(x)\sqrt{1-x^2}$ into equation (i) and simplifying yields

$$g(x) = g\left(\frac{x^2}{2-x^2}\right) \qquad (1)$$

for all $x \in (-1,1)$. Now fix $x \in (-1,1)$ and define a sequence $\{a_n\}_{n=1}^\infty$ by $a_1 = x$ and $a_{n+1} = \frac{a_n^2}{2-a_n^2}$. Then $a_n \in (-1,1)$ and thus $|a_{n+1}| \leq |a_n|^2$ for all n. It follows that $\{|a_n|\}$ is a decreasing sequence with $|a_n| \leq |x|^n$ for all n, and so $\lim_{n\to\infty} a_n = 0$. Since $g(a_n) = g(x)$ for all n by (1) and g is continuous at 0, we conclude that $g(x) = g(0) = f(0) = 1$. This holds for all $x \in (-1,1)$ and thus for $x = \pm 1$ as well by continuity. The result follows.

Remark. As pointed out by Noam Elkies, condition (iii) is unnecessary. However, one can use it to derive a slightly different solution by running the recursion in the opposite direction.

A–4 We begin with an easy lemma.

Lemma. *Let S be a finite set of integers with the following property: for all $a,b,c \in S$ with $a \leq b \leq c$, we also have $a + c - b \in S$. Then S is an arithmetic progression.*

Proof. We may assume $\#S \geq 3$, as otherwise S is trivially an arithmetic progression. Let a_1, a_2 be the smallest and second-smallest elements of S, respectively, and put $d = a_2 - a_1$. Let m be the smallest integer such that $a_1 + md \notin S$. Suppose that there exists an integer n contained in S but not in $\{a_1, a_1 + d, \dots, a_1 + (m-1)d\}$, and choose the least such n. By the hypothesis applied with $(a,b,c) = (a_1, a_2, n)$, we see that $n - d$ also has the property, a contradiction. □

We now return to the original problem. By dividing B, q, r by $\gcd(q,r)$ if necessary, we may reduce to the case where $\gcd(q,r) = 1$. We may assume $\#S \geq 3$, as otherwise S is trivially an arithmetic progression. Let a_1, a_2, a_3 be any three distinct elements of S, labeled so that $a_1 < a_2 < a_3$, and write $ra_i = b_i + m_i q$ with $b_i, m_i \in \mathbb{Z}$ and $b_i \in B$. Note that b_1, b_2, b_3 must also be distinct, so the differences $b_2 - b_1, b_3 - b_1, b_3 - b_2$ are all nonzero; consequently, two of them have the same sign. If $b_i - b_j$ and $b_k - b_l$ have the same sign, then we must have

$$(a_i - a_j)(b_k - b_l) = (b_i - b_j)(a_k - a_l)$$

because both sides are of the same sign, of absolute value less than q, and congruent to each other modulo q. In other words, the points $(a_1,b_1), (a_2,b_2), (a_3,b_3)$ in $\mathbb{R}^2$ are collinear. It follows that $a_4 = a_1 + a_3 - a_2$ also belongs to S (by taking $b_4 = b_1 + b_3 - b_2$), so S satisfies the conditions of the lemma. It is therefore an arithmetic progression.

Reinterpretations. One can also interpret this argument geometrically using cross products (suggested by Noam Elkies), or directly in terms of congruences (suggested by Karl Mahlburg).

Remark. The problem phrasing is somewhat confusing: to say that "S is the intersection of [the interval] A with an arithmetic progression" is the same thing as saying that "S is the empty set or an arithmetic progression" unless it is implied that arithmetic progressions are necessarily infinite. Under that interpretation, however, the problem becomes false; for instance, for

$$q = 5, r = 1, A = [1,3], B = [0,2],$$

we have

$$T = \{\cdots, 0, 1, 2, 5, 6, 7, \dots\}, S = \{1, 2\}.$$

A–5 The pairs (p,n) with the specified property are those pairs with $n = 1$, together with the single pair $(2,2)$. We first check that these do work. For $n = 1$, it is clear that taking $v = (1)$ and $M = (0)$ has the desired effect.

For $(p,n)=(2,2)$, we take $v=\begin{pmatrix}0 & 1\end{pmatrix}$ and $M=\begin{pmatrix}1 & 1\\ 0 & 1\end{pmatrix}$ and then observe that

$$G^{(k)}(0)=\begin{pmatrix}0\\0\end{pmatrix},\begin{pmatrix}0\\1\end{pmatrix},\begin{pmatrix}1\\0\end{pmatrix},\begin{pmatrix}1\\1\end{pmatrix},\; k=0,1,2,3.$$

We next check that no other pairs work, keeping in mind that the desired condition means that G acts on $\mathbb{F}_p^n$ as a cyclic permutation. Assume by way of contradiction that (p,n) has the desired property but does not appear in our list. In particular, we have $n\geq 2$.

Let I be the $n\times n$ identity matrix over $\mathbb{F}_p$. Decompose $\mathbb{F}_p^n$ as a direct sum of two subspaces V,W such that $M-I$ is nilpotent on V and invertible on W. Suppose that $W\neq 0$. Split v as v_1+v_2 with $v_1\in V$, $v_2\in W$. Since $M-I$ is invertible on W, there exists a unique $w\in W$ such that $(M-I)w=-v_2$. Then $G^{(k)}(w)-w\in V$ for all nonnegative integers k. Let k be the least positive integer such that $G^{(k)}(w)=w$; then k is at most the cardinality of V, which is strictly less than p^n because $W\neq 0$. This gives a contradiction and thus forces $W=0$.

In other words, the matrix $N=M-I$ is nilpotent; consequently, $N^n=0$. For any positive integer k, we have

$$\begin{aligned}G^{(k)}(0)&=v+Mv+\cdots+M^{k-1}v\\&=\sum_{j=0}^{k-1}\sum_{i=0}^{n-1}\binom{j}{i}N^iv\\&=\sum_{i=0}^{n-1}\binom{k}{i+1}N^iv.\end{aligned}$$

If $n\geq 2$ and $(p,n)\neq(2,2)$, then $p^{n-1}>n$ and so $G^k(0)=0$ for $k=p^{n-1}$ (because all of the binomial coefficients are divisible by p). This contradiction completes the proof.

A–6 **First solution.** Yes, $f(x,y)$ must be identically 0. We proceed using a series of lemmas.

Lemma 1. *Let R be a rectangular region of area 1 with corners A,B,C,D labeled in counterclockwise order. Then $f(A)+f(C)=f(B)+f(D)$.*

Proof. We may choose coordinates so that for some $c>0$,

$$A=(0,0),B=(c,0),C=(c,1/c),D=(0,1/c).$$

Define the functions

$$\begin{aligned}g(x,y)&=\int_x^{x+c}f(t,y)\,dt\\h(x,y)&=\int_0^y g(x,u)\,du.\end{aligned}$$

For any $x,y\in\mathbb{R}$,

$$h(x,y+1/c)-h(x,y)=\int_x^{x+c}\int_y^{y+1/c}f(t,u)\,dt\,du=0$$

by hypothesis, so $h(x,y+1/c)=h(x,y)$. By the fundamental theorem of calculus, we may differentiate both sides of this identity with respect to y to deduce that $g(x,y+1/c)=g(x,y)$. Differentiating this new identity with respect to x yields the desired equality. □

Lemma 2. *Let C be a circle whose diameter d is at least $\sqrt{2}$, and let AB and $A'B'$ be two diameters of C. Then $f(A)+f(B)=f(A')+f(B')$.*

Proof. By continuity, it suffices to check the case where $\alpha=\arcsin\frac{2}{d^2}$ is an irrational multiple of 2π. Let β be the radian measure of the counterclockwise arc from A to A'. By Lemma 1, the claim holds when $\beta=\alpha$. By induction, the claim also holds when $\beta\equiv n\alpha \pmod{2\pi}$ for any positive integer n. Since α is an irrational multiple of 2π, the positive multiples of α fill out a dense subset of the real numbers modulo 2π, so by continuity the claim holds for all β. □

Lemma 3. *Let R be a rectangular region of arbitrary (positive) area with corners A,B,C,D labeled in counterclockwise order. Then $f(A)+f(C)=f(B)+f(D)$.*

Proof. Let EF be a segment such that $AEFD$ and $BEFC$ are rectangles whose diagonals have length at least $\sqrt{2}$. By Lemma 2,

$$\begin{aligned}f(A)+f(F)&=f(D)+f(E)\\f(C)+f(E)&=f(B)+f(F),\end{aligned}$$

yielding the claim. □

Lemma 4. *The restriction of f to any straight line is constant.*

Proof. We may choose coordinates so that the line in question is the x-axis. Define the function $g(y)$ by

$$g(y)=f(0,y)-f(0,0).$$

By Lemma 3, for all $x\in\mathbb{R}$,

$$f(x,y)=f(x,0)+g(y).$$

For any $c>0$, by the original hypothesis we have

$$\begin{aligned}0&=\int_x^{x+c}\int_y^{y+1/c}f(u,v)\,du\,dv\\&=\int_x^{x+c}\int_y^{y+1/c}(f(u,0)+g(v))\,du\,dv\\&=\frac{1}{c}\int_x^{x+c}f(u,0)\,du+c\int_y^{y+1/c}g(v)\,dv.\end{aligned}$$

In particular, the function $F(x)=\int_x^{x+c}f(u,0)\,du$ is constant. By the fundamental theorem of calculus, we may differentiate to conclude that $f(x+c,0)=f(x,0)$ for all $x\in\mathbb{R}$. Since c was also arbitrary, we deduce the claim. □

To complete the proof, note that since any two points in $\mathbb{R}^2$ are joined by a straight line, Lemma 4 implies that f is constant. This constant equals the integral of f over any rectangular region of area 1, and hence must be 0 as desired.

Second solution (by Eric Larson, communicated by Noam Elkies). In this solution, we fix coordinates and assume only that the double integral vanishes on each rectangular region of area 1 with sides parallel to the coordinate axes, and still conclude that f must be identically 0.

Lemma. *Let R be a rectangular region of area 1 with sides parallel to the coordinate axes. Then the averages of f over any two adjacent sides of R are equal.*

Proof. Without loss of generality, we may take R to have corners $(0,0),(c,0),(c,1/c),(0,1/c)$ and consider the two sides adjacent to $(c,1/c)$. Differentiate the equality

$$0=\int_x^{x+c}\int_y^{y+1/c} f(u,v)\,du\,dv$$

with respect to c to obtain

$$0=\int_y^{y+1/c} f(x+c,v)\,dv-\frac{1}{c^2}\int_x^{x+c} f(u,y+1/c)\,du.$$

Rearranging yields

$$c\int_y^{y+1/c} f(x+c,v)\,dv=\frac{1}{c}\int_x^{x+c} f(u,y+1/c)\,du,$$

which asserts the desired result. □

Returning to the original problem, given any $c>0$, we can tile the plane with rectangles of area 1 whose vertices lie in the lattice $\{(mc,n/c): m,n\in\mathbb{Z}\}$. By repeated application of the lemma, we deduce that for any positive integer n,

$$\int_0^c f(u,0)\,du=\int_{nc}^{(n+1)c} f(u,0)\,du.$$

Replacing c with c/n, we obtain

$$\int_0^{c/n} f(u,0)\,du=\int_c^{c+1/n} f(u,0)\,du.$$

Fixing c and taking the limit as $n\to\infty$ yields $f(0,0)=f(c,0)$. By similar reasoning, f is constant on any horizontal line and on any vertical line, and as in the first solution the constant value is forced to equal 0.

Third solution. (by Sergei Artamoshin) We retain the weaker hypothesis of the second solution. Assume by way of contradiction that f is not identically zero.

We first exhibit a vertical segment PQ with $f(P)>0$ and $f(Q)<0$. It cannot be the case that $f(P)\leq 0$ for all P, as otherwise the vanishing of the zero over any rectangle would force f to vanish identically. By continuity, there must exist an open disc U such that $f(P)>0$ for all $P\in U$. Choose a rectangle R of area 1 with sides parallel to the coordinate axes with one horizontal edge contained in U. Since the integral of f over R is zero, there must exist a point $Q\in R$ such that $f(Q)<0$. Take P to be the vertical projection of Q onto the edge of R contained in U.

By translating coordinates, we may assume that $P=(0,0)$ and $Q=(0,a)$ for some $a>0$. For s sufficiently small, f is positive on the square of side length $2s$ centered at P, which we call S, and negative on the square of side length $2s$ centered at Q, which we call S'. Since the ratio $2s/(1-4s^2)$ tends to 0 as s does, we can choose s so that $2s/(1-4s^2)=a/n$ for some positive integer n.

For $i\in\mathbb{Z}$, let A_i be the rectangle

$$\Big\{(x,y): s\leq x\leq s+\frac{1-4s^2}{2s},\quad -s+i\frac{2s}{1-4s^2}\leq y\leq s+i\frac{2s}{1-4s^2}\Big\}$$

and let B_i be the rectangle

$$\Big\{(x,y): s\leq x\leq s+\frac{1-4s^2}{2s},\quad s+i\frac{2s}{1-4s^2}\leq y\leq -s+(i+1)\frac{2s}{1-4s^2}\Big\}.$$

Then for all $i\in\mathbb{Z}$,

$$S\cup A_0, A_n\cup S', A_i\cup B_i, B_i\cup A_{i+1}$$

are all rectangles of area 1 with sides parallel to the coordinate axes, so the integral over f over each of these rectangles is zero. Since the integral over S is positive, the integral over A_0 must be negative; by induction, for all $i\in\mathbb{Z}$ the integral over A_i is negative and the integral over B_i is positive. But this forces the integral over S' to be positive whereas f is negative everywhere on S', a contradiction.

B–1 Each of the following functions belongs to S for the reasons indicated.

$f(x),g(x)$	given
$\ln(x+1)$	(i)
$\ln(f(x)+1),\ln(g(x)+1)$	(ii) plus two previous lines
$\ln(f(x)+1)+\ln(g(x)+1)$	(ii)
e^x-1	(i)
$(f(x)+1)(g(x)+1)-1$	(ii) plus two previous lines
$f(x)g(x)+f(x)+g(x)$	previous line
$f(x)+g(x)$	(ii) plus first line
$f(x)g(x)$	(iii) plus two previous lines

B–2 Fix a face F of the polyhedron with area A. Suppose F is completely covered by balls of radii $r_1,\dots,r_n$ whose volumes sum to V. Then on one hand,

$$\sum_{i=1}^{n} \frac{4}{3}\pi r_i^3 = V.$$

On the other hand, the intersection of a ball of radius r with the plane containing F is a disc of radius at most r, which covers a piece of F of area at most πr^2; therefore

$$\sum_{i=1}^{n} \pi r_i^2 \geq A.$$

By writing n as $\sum_{i=1}^{n} 1$ and applying Hölder's inequality, we obtain

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

Consequently, any value of $c(P)$ less than $\frac{16}{9}\pi^2 A^3$ works.

B–3 The answer is yes. We first note that for any collection of m days with $1 \leq m \leq 2n-1$, there are at least m distinct teams that won a game on at least one of those days. If not, then any of the teams that lost games on all of those days must in particular have lost to m other teams, a contradiction.

If we now construct a bipartite graph whose vertices are the $2n$ teams and the $2n-1$ days, with an edge linking a day to a team if that team won their game on that day, then any collection of m days is connected to a total of at least m teams. It follows from Hall's Marriage Theorem that one can match the $2n-1$ days with $2n-1$ distinct teams that won on their respective days, as desired.

B–4 **First solution.** We will show that the answer is yes. First note that for all $x > -1$, $e^x \geq 1+x$ and thus

$$x \geq \log(1+x). \qquad (2)$$

We next claim that $a_n > \log(n+1)$ (and in particular that $a_n - \log n > 0$) for all n, by induction on n. For $n = 0$ this follows from $a_0 = 1$. Now suppose that $a_n > \log(n+1)$, and define $f(x) = x + e^{-x}$, which is an increasing function in $x > 0$; then

$$\begin{aligned} a_{n+1} &= f(a_n) > f(\log(n+1)) \\ &= \log(n+1) + 1/(n+1) \geq \log(n+2), \end{aligned}$$

where the last inequality is (2) with $x = 1/(n+1)$. This completes the induction step.

It follows that $a_n - \log n$ is a decreasing function in n: we have

$$\begin{aligned} &(a_{n+1} - \log(n+1)) - (a_n - \log n) \\ &= e^{-a_n} + \log(n/(n+1)) \\ &< 1/(n+1) + \log(n/(n+1)) \leq 0, \end{aligned}$$

where the final inequality is (2) with $x = -1/(n+1)$. Thus $\{a_n - \log n\}_{n=0}^{\infty}$ is a decreasing sequence of positive numbers, and so it has a limit as $n \to \infty$.

Second solution. Put $b_n = e^{a_n}$, so that $b_{n+1} = b_n e^{1/b_n}$. In terms of the b_n, the problem is to prove that b_n/n has a limit as $n \to \infty$; we will show that the limit is in fact equal to 1.

Expanding e^{1/b_n} as a Taylor series in $1/b_n$, we have

$$b_{n+1} = b_n + 1 + R_n$$

where $0 \leq R_n \leq c/b_n$ for some absolute constant $c > 0$. By writing

$$b_n = n + e + \sum_{i=0}^{n-1} R_i,$$

we see first that $b_n \geq n + e$. We then see that

$$\begin{aligned} 0 &\leq \frac{b_n}{n} - 1 \\ &\leq \frac{e}{n} + \sum_{i=0}^{n-1} \frac{R_i}{n} \\ &\leq \frac{e}{n} + \sum_{i=0}^{n-1} \frac{c}{nb_i} \\ &\leq \frac{e}{n} + \sum_{i=0}^{n-1} \frac{c}{n(i+e)} \\ &\leq \frac{e}{n} + \frac{c\log n}{n}. \end{aligned}$$

It follows that $b_n/n \to 1$ as $n \to \infty$.

Remark. This problem is an example of the general principle that one can often predict the asymptotic behavior of a recursive sequence by studying solutions of a sufficiently similar-looking differential equation. In this case, we start with the equation $a_{n+1} - a_n = e^{-a_n}$, then replace a_n with a function $y(x)$ and replace the difference $a_{n+1} - a_n$ with the derivative $y'(x)$ to obtain the differential equation $y' = e^{-y}$, which indeed has the solution $y = \log x$.

B–5 Define the function

$$f(x) = \sup_{s\in\mathbb{R}} \{x \log g_1(s) + \log g_2(s)\}.$$

As a function of x, f is the supremum of a collection of affine functions, so it is convex. The function $e^{f(x)}$ is then also convex, as may be checked directly from the definition: for $x_1, x_2 \in \mathbb{R}$ and $t \in [0,1]$, by the weighted AM-GM inequality

$$\begin{aligned} te^{f(x_1)} + (1-t)e^{f(x_2)} &\geq e^{tf(x_1)+(1-t)f(x_2)} \\ &\geq e^{f(tx_1+(1-t)x_2)}. \end{aligned}$$

For each $t \in \mathbb{R}$, draw a supporting line to the graph of $e^{f(x)}$ at $x = t$; it has the form $y = xh_1(t) + h_2(t)$ for some $h_1(t), h_2(t) \in \mathbb{R}$. For all x, we then have

$$\sup_{s\in\mathbb{R}}\{g_1(s)^x g_2(s)\} \geq xh_1(t) + h_2(t)$$

with equality for $x = t$. This proves the desired equality (including the fact that the maximum on the right side is achieved).

Remark. This problem demonstrates an example of *duality* for convex functions.

B–6 **First solution.** Since fixed points do not affect the signature of a permutation, we may ignore the residue class of 0 and consider π as a permutation on the nonzero residue classes modulo p. These form a cyclic group of order $p-1$, so the signature of π is also the signature of multiplication by 3 as a permutation σ of the residue classes modulo $p-1$. If we identify these classes with the integers $0, \dots, p-2$, then the signature equals the parity of the number of *inversions*: these are the pairs (i, j) with $0 \leq i < j \leq p-2$ for which $\sigma(i) > \sigma(j)$. We may write

$$\sigma(i) = 3i - (p-1)\left\lfloor \frac{3i}{p-1} \right\rfloor$$

from which we see that (i, j) cannot be an inversion unless $\lfloor \frac{3j}{p-1} \rfloor > \lfloor \frac{3i}{p-1} \rfloor$. In particular, we only obtain inversions when $i < 2(p-1)/3$.

If $i < (p-1)/3$, the elements j of $\{0, \dots, p-2\}$ for which (i, j) is an inversion correspond to the elements of $\{0, \dots, 3i\}$ which are not multiples of 3, which are $2i$ in number. This contributes a total of $0 + 2 + \cdots + 2(p-2)/3 = (p-2)(p+1)/9$ inversions.

If $(p-1)/3 < i < 2(p-1)/3$, the elements j of $\{0, \dots, p-2\}$ for which (i, j) is an inversion correspond to the elements of $\{0, \dots, 3i-p+1\}$ congruent to 1 modulo 3, which are $(3i-p+2)/3 = i - (p-2)/3$ in number. This contributes a total of $1 + \cdots + (p-2)/3 = (p-2)(p+1)/18$ inversions.

Summing up, the total number of inversions is $(p-2)(p+1)/6$, which is even if and only if $p \equiv 3 \pmod 4$. This proves the claim.

Second solution (by Noam Elkies). Recall that the sign of π (which is $+1$ if π is even and -1 if π is odd) can be computed as

$$\prod_{0\leq x<y<p} \frac{\pi(x) - \pi(y)}{x - y}$$

(because composing π with a transposition changes the sign of the product). Reducing modulo p, we get a congruence with

$$\prod_{0\leq x<y<p} \frac{x^3 - y^3}{x - y} = \prod_{0\leq x<y<p} (x^2 + xy + y^2).$$

It thus suffices to count the number of times each possible value of $x^2 + xy + y^2$ occurs. Each nonzero value c modulo p occurs $p+1$ times as $x^2 + xy + y^2$ with $0 \leq x, y < p$ and hence $(p + \chi(c/3))/2$ times with $0 \leq x < y < p$, where χ denotes the quadratic character modulo p. Since $p \equiv 2 \pmod 3$, by the law of quadratic reciprocity we have $\chi(-3) = +1$, so $\chi(c/3) = \chi(-c)$. It thus remains to evaluate the product $\prod_{c=1}^{p-1} c^{(p+\chi(-c))/2}$ modulo p.

If $p \equiv 3 \pmod 4$, this is easy: each factor is a quadratic residue (this is clear if c is a residue, and otherwise $\chi(-c) = +1$ so $p + \chi(-c)$ is divisible by 4) and -1 is not, so we must get $+1$ modulo p.

If $p \equiv 1 \pmod 4$, we must do more work: we choose a primitive root g modulo p and rewrite the product as

$$\prod_{i=0}^{p-2} g^{i(p+(-1)^i)/2}.$$

The sum of the exponents, split into sums over i odd and i even, gives

$$\sum_{j=0}^{(p-3)/2} \left(j(p+1) + \frac{(2j+1)(p-1)}{2} \right)$$

which simplifies to

$$\frac{(p-3)(p-1)(p+1)}{8} + \frac{(p-1)^3}{8} = \frac{p-1}{2}\left(\frac{p^2-1}{2} - p\right).$$

Hence the product we are trying to evaluate is congruent to $g^{(p-1)/2} \equiv -1$ modulo p.

Third solution (by Mark van Hoeij). We compute the parity of π as the parity of the number of cycles of even length in the cycle decomposition of π. For x a nonzero residue class modulo p of multiplicative order d, the elements of the orbit of x under π also have order d (because d divides $p-1$ and hence is coprime to 3). Since the group of nonzero residue classes modulo p is cyclic of order $p-1$, the elements of order d fall into $\varphi(d)/f(d)$ orbits under π, where φ is the Euler phi function and $f(d)$ is the multiplicative order of 3 modulo d. The parity of π is then the parity of the sum of $\varphi(d)/f(d)$ over all divisors d of $p-1$ for which $f(d)$ is even.

If d is odd, then $\varphi(d)/f(d) = \varphi(2d)/f(2d)$, so the summands corresponding to d and $2d$ coincide. It thus suffices to consider those d divisible by 4. If $p \equiv 3 \pmod 4$, then there are no such summands, so the sum is trivially even.

If $p \equiv 1 \pmod 4$, then $d = 4$ contributes a summand of $\varphi(4)/f(4) = 2/2 = 1$. For each d which is a larger multiple of 4, the group $(\mathbb{Z}/d\mathbb{Z})^*$ is isomorphic to the product of $\mathbb{Z}/2\mathbb{Z}$ with another group of even order, so the maximal power of 2 dividing $f(d)$ is strictly smaller than the maximal power of 2 dividing d. Hence $\varphi(d)/f(d)$ is even, and so the overall sum is odd.

Remark. Note that the second proof uses quadratic reciprocity, whereas the first and third proofs are similar to several classical proofs of quadratic reciprocity. Abhinav Kumar notes that the problem itself is a special case of the Duke-Hopkins quadratic reciprocity law for abelian groups (Quadratic reciprocity in a finite group, *Amer. Math. Monthly* **112** (2005), 251–256; see also `http://math.uga.edu/~pete/morequadrec.pdf`).