Putnam 2002

A1. Let k be a fixed positive integer. The n-th derivative of $\frac{1}{x^k-1}$ has the form $\frac{P_n(x)}{(x^k-1)^{n+1}}$ where $P_n(x)$ is a polynomial. Find $P_n(1)$.

Solution. We have

$$\begin{aligned}
\frac{P_{n+1}(x)}{(x^k-1)^{n+2}} &= \frac{d^{n+1}}{dx^{n+1}}\left(\frac{1}{x^k-1}\right) = \frac{d}{dx}\left(\frac{P_n(x)}{(x^k-1)^{n+1}}\right) \\
&= \frac{\left(x^k-1\right)^{n+1} P_n'(x) - P_n(x)(n+1)\left(x^k-1\right)^n kx^{k-1}}{(x^k-1)^{2n+2}} \\
&= \frac{\left(x^k-1\right) P_n'(x) - P_n(x)(n+1)kx^{k-1}}{(x^k-1)^{n+2}}.
\end{aligned}$$

Thus,

$$\begin{aligned}
P_{n+1}(x) &= \left(x^k-1\right) P_n'(x) - P_n(x)(n+1)kx^{k-1}, \text{ and} \\
P_{n+1}(1) &= -P_n(1)(n+1)k = P_{n-1}(1)\,n(n+1)k^2 \\
&= (-1)^{i+1} P_{n-i}(1)(n+1)n\cdots(n-i+1)k^{i+1} \\
&= (-1)^{n+1} P_0(1)(n+1)n\cdots 1k^{n+1} \\
&= (-1)^{n+1}(n+1)!k^{n+1}
\end{aligned}$$

Hence, $P_n(1) = (-1)^n n!k^n$.

A2. Given any five points on a sphere, show that some four of them must lie on a closed hemisphere.

Solution. Let the points be $x_1, \cdots, x_5$ and denote the sphere by S. Let P be the plane containing x_4, x_5 and the origin. Let H_1 and H_2 be the closed half-spaces with boundary P. If at least two of x_1, x_2 and x_3 (say x_1 and x_2) are in H_1, then x_1, x_2, x_4 and x_5 are four points in the closed hemisphere $H_1 \cap S$. If only one (say x_1) of x_1, x_2 and x_3 are in H_1, then x_2, x_3, x_4, x_5 are in $H_1 \cap S$. If none of x_1, x_2 and x_3 are in H_1, then all five of $x_1, \cdots, x_5$ are in $H_2 \cap S$. In any case, at least four points are in a closed hemisphere.

A3. Let $n \geq 2$ be an integer and T_n be the number of non-empty subsets S of $\{1, 2, 3, \ldots, n\}$ with the property that the average of the elements of S is an integer. Prove that $T_n - n$ is always even.

Solution. Suppose that S is a subset with the property that the average, say $A(S)$, of the elements of S is an integer. If $A(S) \notin S$, then $A(S \cup \{A(S)\}) = A(S)$, since

$$\frac{a_1+\cdots+a_k}{k} = A(S) \Rightarrow \frac{a_1+\cdots+a_k+A(S)}{k+1} = \frac{A(S)k+A(S)}{k+1} = A(S).$$

If $A(S) \in S$, then $S - \{A(S)\}$ is a set with $A(S - \{A(S)\}) = A(S)$, provided $S \neq \{A(S)\}$. Thus, as long as S has at least two elements and $A(S)$ is an integer, there is another subset, say

$$\overline{S} := \begin{cases} S \cup \{A(S)\} & \text{if } A(S) \notin S \\ S - \{A(S)\} & \text{if } A(S) \in S \end{cases}$$

with $A(\overline{S}) = A(S)$. Thus, the subsets S with $A(S)$ an integer ≥ 2 come in pairs $\{S, \overline{S}\}$. Since there are n singleton subsets $\{1\}, \{2\}, \cdots, \{n\}$ (with integral averages), we have that

$$\begin{aligned} & \#\{S \subset \{1, \ldots, n\} : A(S) \text{ is integral}\} - n \\ = \; & \#\{S \subset \{1, \ldots, n\} : A(S) \text{ is integral and } \#S \geq 2\} \end{aligned}$$

is even.

A4. In Determinant Tic-Tac-Toe, Player 1 enters a 1 in an empty 3×3 matrix. Player 0 counters with a 0 in a vacant position, and play continues in turn until the 3×3 matrix is completed with five 1's and four 0's. Player 0 wins if the determinant is 0 and player 1 wins otherwise. Assuming both players pursue optimal strategies, who will win and how?

Solution. By definition

$$\det \begin{bmatrix} a_{11} & a_{12} & a_{13} \\ a_{21} & a_{22} & a_{23} \\ a_{31} & a_{32} & a_{33} \end{bmatrix} = \begin{array}{c} a_{11}a_{22}a_{33} + a_{13}a_{21}a_{32} + a_{12}a_{23}a_{31} \\ -a_{12}a_{21}a_{33} - a_{11}a_{23}a_{32} - a_{13}a_{22}a_{31} \end{array}$$

Note that the terms are products the three rows and three columns of the "related" matrix

$$\begin{bmatrix} a_{11} & a_{22} & a_{33} \\ a_{32} & a_{13} & a_{21} \\ a_{23} & a_{31} & a_{12} \end{bmatrix}.$$

Thus, Player 0 will win if he just prevents a Player 1 win in ordinary Tic-Tac-Toe when he translates the selections to the "related" matrix and back again. It is well-known that Player 1 cannot force a win in ordinary Tic-Tac-Toe. Thus, Player 0 can always prevent a win by Player 1 in Determinant Tic-Tac-Toe. However, there is always a winner in Determinant Tic-Tac-Toe. Thus Player 0 can always win.

A5. Define a sequence by $a_0 = 1$, together with the rules $a_{2n+1} = a_n$ and $a_{2n+2} = a_n + a_{n+1}$ for each integer $n \geq 0$. Prove that every positive rational number appears in the set

$$\left\{ \frac{a_{n-1}}{a_n} : n \geq 1 \right\} = \left\{ \frac{1}{1}, \frac{1}{2}, \frac{2}{1}, \frac{1}{3}, \frac{3}{2}, \ldots \right\}.$$

Solution. We need to show that for relatively prime positive integers p and q, there is m such that $a_{m-1} = p$, $a_m = q$. We use induction on $p+q$. For $p+q = 1$, $m = 0$ works. Suppose first that $q > p$. Since $\frac{a_{2n+1}}{a_{2n+2}} = \frac{a_n}{a_n + a_{n+1}} < 1$ and $\frac{a_{2n+2}}{a_{2n+1}} > 1$ and $\frac{a_{m-1}}{a_m} = \frac{p}{q} < 1$, we search among even m for a solution of $a_{m-1} = p$, $a_m = q$. Then $m = 2n+2$ and $m-1 = 2n+1$ for some n. We want

$$\begin{aligned} p &= a_{m-1} = a_{2n+1} = a_n \\ q &= a_m = a_{2n+2} = a_n + a_{n+1} \end{aligned}$$

Solving these for a_n and a_{n+1} gives $a_n = p$ and $a_{n+1} = q-p$. Note that $p+q-p = q < p+q$, and so we can find n with $a_n = p$ and $a_{n+1} = q-p$ (> 0) by the induction assumption. Now assume that $q < p$, and look for solutions of $a_{m-1} = p$, $a_m = q$ among odd values of m, say $m = 2n+1$ and $m-1 = 2n = 2(n-1)+2$. We want

$$\begin{aligned} p &= a_{m-1} = a_{2(n-1)+2} = a_{n-1} + a_n \\ q &= a_m = a_{2n+1} = a_n, \end{aligned}$$

or $a_n = q$ and $a_{n-1} = p-q$ (> 0). But we can find such n by induction, since $q + (p-q) = p < p+q$.

A6. Fix an integer $b \geq 2$. Let $f(1) = 1$, $f(2) = 2$, and for each $n \geq 3$, define $f(n) = nf(d)$, where d is the number of base-b digits of n. For which values of b does

$$\sum_{n=1}^{\infty} \frac{1}{f(n)}$$

converge?

Solution. We have $f(n) = nf(d)$ for $b^{d-1} \leq n \leq b^d - 1$ for $n \geq 3$. If $n = 1$, then $d = 1$ and we have $f(n) = nf(d)$ for $n = 1$ (i.e., $f(1) = 1f(1) = 1$). If $n = 2$ and $b \geq 3$, then $d = 1$ and we have $f(n) = nf(d)$ for $n = 2$ (i.e., $f(2) = 2f(1) = 2$). Thus, if $b \geq 3$, then $f(n) = nf(d)$ holds for $b^{d-1} \leq n \leq b^d - 1$ for all $n \geq 1$. We assume first that $b \geq 3$ and consider $b = 2$ later. Then we have

$$\sum_{n=1}^{\infty} \frac{1}{f(n)} = \sum_{d=1}^{\infty} \frac{1}{f(d)} \sum_{n=b^{d-1}}^{b^d - 1} \frac{1}{n}.$$

Note that

$$\sum_{n=b^{d-1}}^{b^d-1} \frac{1}{n} \geq \int_{b^{d-1}}^{b^d} \frac{1}{x} dx = \ln b^d - \ln b^{d-1} = \ln b.$$

Thus,

$$\sum_{n=1}^{\infty} \frac{1}{f(n)} \geq \sum_{d=1}^{\infty} \frac{1}{f(d)} \ln b$$

which is a contradiction if $\sum_{n=1}^{\infty} \frac{1}{f(n)} < \infty$ and $\ln b > 1$. Thus, $\sum_{n=1}^{\infty} \frac{1}{f(n)} = \infty$ if $b \geq 3$. Now suppose $b = 2$. We have $f(n) = nf(d)$ for $2^{d-1} \leq n \leq 2^d - 1$ for all $n \geq 3$, where d is the number of base-2 digits of n. Now,

$$\sum_{n=3}^{\infty} \frac{1}{f(n)} = \sum_{d=2}^{\infty} \frac{1}{f(d)} \sum_{n=2^{d-1}}^{2^d-1} \frac{1}{n}$$

We have

$$\begin{aligned}\sum_{n=2^{d-1}}^{2^d-1}\frac{1}{n} &= \frac{1}{2^{d-1}}-\frac{1}{2^d}+\sum_{n=2^{d-1}+1}^{2^d}\frac{1}{n}\le\frac{1}{2^{d-1}}-\frac{1}{2^d}+\int_{2^{d-1}}^{2^d}\frac{1}{x}dx\\ &= \frac{1}{2^{d-1}}-\frac{1}{2^d}+\ln 2=\frac{1}{2^d}+\ln 2.\end{aligned}$$

Thus,

$$\begin{aligned}\sum_{n=3}^{2^D-1}\frac{1}{f(n)} &= \sum_{d=2}^{D}\frac{1}{f(d)}\sum_{n=2^{d-1}}^{2^d-1}\frac{1}{n}\le\sum_{d=2}^{D}\frac{1}{f(d)}\left(\frac{1}{2^d}+\ln 2\right)\\ &= \frac{1}{f(2)}\left(\frac{1}{2^2}+\ln 2\right)+\sum_{d=3}^{D}\frac{1}{f(d)}\left(\frac{1}{2^d}+\ln 2\right)\\ &= \frac{1}{2}\left(\frac{1}{2^2}+\ln 2\right)+\sum_{d=3}^{D}\frac{1}{f(d)}\left(\frac{1}{2^d}+\ln 2\right)\end{aligned}$$

Note that for $d\ge 3$,

$$\frac{1}{2^d}+\ln 2\le r:=\frac{1}{2^3}+\ln 2=.818\ldots<1.$$

With $a:=\frac{1}{2}\left(\frac{1}{2^2}+\ln 2\right)=.471$, we get

$$\sum_{n=3}^{2^D-1}\frac{1}{f(n)}\le a+r\sum_{d=3}^{D}\frac{1}{f(d)}$$

Now if $\sum_{d=3}^{D}\frac{1}{f(d)}=S<\infty$, then

$$S\le a+rS\Rightarrow S(1-r)\le a\Rightarrow S\le\frac{a}{1-r}=\frac{\frac{1}{2}\left(\frac{1}{2^2}+\ln 2\right)}{1-\left(\frac{1}{2^3}+\ln 2\right)}=2.59....$$

Let's try to prove $\sum_{n=3}^{2^D-1}\frac{1}{f(n)}\le\frac{a}{1-r}$ by induction. For $D=2$,

$$\sum_{n=3}^{2^D-1}\frac{1}{f(n)}=\frac{1}{f(3)}=\frac{1}{6}\le\frac{a}{1-r}$$

By induction, for $D\ge 3$

$$\begin{aligned}\sum_{n=3}^{2^D-1}\frac{1}{f(n)} &\le a+r\sum_{d=3}^{D}\frac{1}{f(d)}\le a+r\sum_{d=3}^{2^{D-1}-1}\frac{1}{f(d)}\le a+r\frac{a}{1-r}\\ &= \frac{a(1-r)}{1-r}+r\frac{a}{1-r}=\frac{a}{1-r}.\end{aligned}$$

Thus,

$$\sum_{n=3}^{\infty} \frac{1}{f(n)} \leq \frac{a}{1-r} < \infty.$$

Hence, we have convergence for $b = 2$.

B1. Shanille O'Keal shoots free throws on a basketball court. She hits the first and misses the second, and thereafter the probability that she hits the next shot is equal to the proportion of shots she has hit so far. What is the probability she hits exactly 50 of her first 100 shots?

Solution. Let $P(k,n)$ be the probability that she has exactly k hits in n shots. We have

$$P(k,n) = P(k-1,n-1)\frac{k-1}{n-1} + P(k,n-1)\left(1 - \frac{k}{n-1}\right)$$

Now

$$\begin{aligned}
P(k,3) &= P(k-1,2)\frac{k-1}{2} + P(k,2)\left(1-\frac{k}{2}\right) \\
P(1,3) &= P(0,2)\,0 + P(1,2)\frac{1}{2} = \frac{1}{2} \\
P(2,3) &= P(1,2)\frac{1}{2} + P(2,2)\,0 = \frac{1}{2}
\end{aligned}$$

$$\begin{aligned}
P(1,4) &= P(0,3)\frac{0}{3} + P(1,3)\left(1-\frac{1}{3}\right) = \frac{1}{2}\frac{2}{3} = \frac{1}{3} \\
P(2,4) &= P(1,3)\frac{1}{3} + P(2,3)\left(1-\frac{2}{3}\right) = \frac{1}{2}\frac{1}{3} + \frac{1}{2}\frac{1}{3} = \frac{1}{3} \\
P(3,4) &= P(2,3)\frac{2}{3} + P(3,3)\,0 = \frac{1}{2}\frac{2}{3} = \frac{1}{3}
\end{aligned}$$

On the evidence thus far, we try to prove

$$P(k,n) = \frac{1}{n-1} \text{ for } 1 < k < n$$

Assuming this, we try to prove $P(k,n+1) = \frac{1}{n}$: If $1 < k < n$, then

$$\begin{aligned}
P(k,n+1) &= P(k-1,n)\frac{k-1}{n} + P(k,n)\left(1-\frac{k}{n}\right) \\
&= \frac{1}{n-1}\frac{k-1}{n} + \frac{1}{n-1}\left(1-\frac{k}{n}\right) \\
&= \frac{1}{n(n-1)}(k-1+n-k) = \frac{1}{n}.
\end{aligned}$$

If $k = n < n + 1$, we have

$$\begin{aligned} P(n, n+1) &= P(n-1, n)\frac{n-1}{n} + P(n,n)\left(1 - \frac{k}{n}\right) \\ &= \frac{1}{n-1}\frac{n-1}{n} = \frac{1}{n}. \end{aligned}$$

Thus we are done by induction.

B2. Consider a polyhedron with at least five faces such that exactly three edges emerge from each of its vertices. Two players play the following game:

Each player, in turn, signs his or her name on a previously unsigned face. The winner is the player who first succeeds in signing three faces that share a common vertex.

Show that the player who signs first will always win by playing as well as possible.

Solution. If there is a face F_0 with 4 edges with at least four adjacent faces, say $F_1, F_2, F_3, F_4, \ldots$ (in order), then the first player (say #1) signs F_0. Regardless of where player #2 signs, player #1 signs a face adjacent to F_0, say F_3, where F_1 was possibly signed by player #2. If player #2 then signs F_2, then player #1 wins by signing F_4; otherwise player #1 signs F_2 and wins. Thus, it remains to show that a face F_0 with four edges exists. By Euler's formula, $F - E + V = 2 - 2g \leq 2$. Since each vertex has 3 edges and each edge shared by two vertices, we have $E = 3V/2$. If all faces have just 3 edges, then counting edges again, we have $3F = 2E$ or $3F/2 = E = 3V/2$ and so $F = V$. Thus,

$$\begin{aligned} V/2 &= V - 3V/2 + V = F - E + V \overset{\text{Euler}}{=} 2 - 2g \leq 2 \\ &\Rightarrow V \leq 4 \Rightarrow F \leq 4, \end{aligned}$$

but we are given $F \geq 5$. Thus, some face must have more than 3 edges.

B3. Show that, for all integers $n > 1$,

$$\frac{1}{2ne} < \frac{1}{e} - \left(1 - \frac{1}{n}\right)^n < \frac{1}{ne}.$$

Solution. The following are equivalent:

$$\begin{aligned} \frac{1}{2ne} - \frac{1}{e} &< -\left(1 - \frac{1}{n}\right)^n < \frac{1}{ne} - \frac{1}{e} \\ \frac{1}{e} - \frac{1}{2ne} &> \left(1 - \frac{1}{n}\right)^n > \frac{1}{e} - \frac{1}{ne} \\ 1 - \frac{1}{n} &< e\left(1 - \frac{1}{n}\right)^n < 1 - \frac{1}{2n} \\ \ln\left(1 - \frac{1}{n}\right) &< 1 + n\ln\left(1 - \frac{1}{n}\right) < \ln\left(1 - \frac{1}{2n}\right) \end{aligned}$$

Note that

$$-\ln(1-x) = \int \frac{1}{1-x}dx = \int \sum_{k=0}^{\infty} x^k dx = \sum_{k=0}^{\infty} \frac{x^{k+1}}{k+1} = \sum_{k=1}^{\infty} \frac{x^k}{k}.$$

Thus, we multiply the last sequence of inequalities through by -1, and obtain the equivalent sequences

$$\begin{aligned}
-\ln\left(1-\frac{1}{n}\right) &> -1 - n\ln\left(1-\frac{1}{n}\right) > -\ln\left(1-\frac{1}{2n}\right) \\
\sum_{k=1}^{\infty} \frac{\left(\frac{1}{n}\right)^k}{k} &> -1 + n\sum_{k=1}^{\infty} \frac{\left(\frac{1}{n}\right)^k}{k} > \sum_{k=1}^{\infty} \frac{\left(\frac{1}{2n}\right)^k}{k} \\
\sum_{k=1}^{\infty} \frac{1}{kn^k} &> \sum_{k=2}^{\infty} \frac{\left(\frac{1}{n}\right)^{k-1}}{k} > \sum_{k=1}^{\infty} \frac{1}{k2^kn^k} \\
\sum_{k=1}^{\infty} \frac{1}{kn^k} &> \sum_{k=1}^{\infty} \frac{1}{n^k(k+1)} > \sum_{k=1}^{\infty} \frac{1}{k2^kn^k},
\end{aligned}$$

which holds since the inequalities hold term-by-term. Note that $k \le k+1 \le k2^k$, strict for $k > 1$.

B4. An integer n, unknown to you, has been randomly chosen in the interval $[1, 2002]$ with uniform probability. Your objective is to select n in an **odd** number of guesses. After each incorrect guess, you are informed whether n is higher or lower, and you **must** guess an integer on your next turn among the numbers that are still feasibly correct. Show that you have a strategy so that the chance of winning is greater than $2/3$.

Solution.

1. If we just guess 1,2,3,... in order, the chance of guessing the correct number n in an odd number of guesses is $1/2$.

2. If we guess 1,3,5,..., and n is odd, then n is guessed on an odd guess if $n \equiv 1$ mod 4. If n is even, then n must be guessed after guessing the odd number $n+1$ and this happens on an even guess if $n \equiv 2$ mod 4. Thus again, the probability of guessing n in an odd number of guesses is $1/2$.

3. Suppose that we try a mixture of consecutive and skipping, say 1,2,4,5,7,8,10... . If $n \equiv 1 \bmod 3$, then n is guessed on an odd guess. If $n \equiv 2 \bmod 3$, then n is guessed on an even number of guesses. If $n \equiv 0 \bmod 3$, then after an odd number of guesses it is revealed that the guess is too high and then you must correctly guess the previous number on your next (even) guess. Thus the probability of guessing n in an odd number of guesses is $1/3$.

4. Suppose that we try the other mixture of consecutive and skipping, say 1,3,4,6,7,9,10,.... If $n \equiv 0 \bmod 3$, then n is guessed on an even guess. If $n \equiv 1 \bmod 3$, then n is guessed on an odd guess. If $n \equiv 2 \bmod 3$, then it is revealed on an even guess that the number is lower, and on the next guess (odd) you are forced to guess n. Thus, the number of guesses is odd if $n \equiv 1 \bmod 3$ or $n \equiv 2 \bmod 3$ with probability $2/3$. However, $2002 \equiv 1 \bmod 3$ and so there is

one more number with residue 1 than of residue 2 or 0. The number of integers with residue 1 or 2 is 1335 and $1335/2002 = .666\,833\cdots > 2/3$.

B5. A palindrome in base b is a positive integer whose base-b digits read the same backwards and forwards; for example, 2002 is a 4-digit palindrome in base 10. Note that 200 is not a palindrome in base 10, but it is the 3-digit palindrome 242 in base 9, and 404 in base 7. Prove that there is an integer which is a 3-digit palindrome in base b for at least 2002 different values of b.

Solution. If we solve

$$cb^2 + db + c = N$$

for b, we get

$$b = \frac{1}{2c}\left(-d + \sqrt{d^2 - 4c\,(c - N)}\right)$$

Note that if $d = 2c$, then this simplifies:

$$b = \frac{1}{2c}\left(-2c + \sqrt{(2c)^2 - 4c\,(c - N)}\right) = \frac{-c + \sqrt{cN}}{c} = \sqrt{\frac{N}{c}} - 1$$

Let's take N to be a square, say M^2, and $c = a^2$ where a divides M. Then

$$b = \sqrt{\frac{N}{c}} - 1 = \frac{M}{a} - 1$$

is an integer. In order to produce 2002 values for b, we need 2002 values for a which divide M. This is certainly the case for $M = 2002!$, since we can then choose $a = 1, 2, \ldots, 2002$. However, we need to check that the digits c and d (i.e., a^2 and $2a^2$) are less than $b = \frac{M}{a} - 1$. In other words, we need

$$\begin{aligned} 2a^2 &\leq \frac{2002!}{a} - 1, \text{ but this is the case since} \\ 2a^2 &\leq 2\,(2002)^2 \leq \frac{2002!}{2002} - 1 \leq \frac{2002!}{a} - 1 \end{aligned}$$

In summary,

$$(2002!)^2 = a^2b^2 + 2a^2b + a^2$$

for the 2002 values $b = \frac{2002!}{a} - 1$ obtained by letting $a = 1, \ldots, 2002$.

B6. Let p be a prime number. Prove that the determinant of the matrix

$$\begin{pmatrix} x & y & z \\ x^p & y^p & z^p \\ x^{p^2} & y^{p^2} & z^{p^2} \end{pmatrix}$$

is congruent modulo p to a product of polynomials of the form $ax + by + cz$, where a, b, c are integers. (We say two integer polynomials are congruent modulo p if corresponding coefficients are congruent modulo p.)

Solution. Let a, b, c be any integers. Note that

$$\begin{pmatrix} x & y & z \\ x^p & y^p & z^p \\ x^{p^2} & y^{p^2} & z^{p^2} \end{pmatrix} \begin{pmatrix} a \\ b \\ c \end{pmatrix} = \begin{pmatrix} ax+by+cz \\ ax^p+by^p+cz^p \\ ax^{p^2}+by^{p^2}+cz^{p^2} \end{pmatrix}$$

$$\equiv \begin{pmatrix} ax+by+cz \\ a^px^p+b^py^p+c^pz^p \\ a^{p^2}x^{p^2}+b^{p^2}y^{p^2}+c^{p^2}z^{p^2} \end{pmatrix} \equiv \begin{pmatrix} ax+by+cz \\ (ax+by+cz)^p \\ (ax+by+cz)^{p^2} \end{pmatrix} \bmod p$$

Here we have used the facts that $a^p \equiv a \bmod p$ (Euler's Theorem), and that the cross terms of $(ax+by+cz)^p$ and $(ax+by+cz)^{p^2}$ are 0 $\bmod p$. If $D(x,y,z) \neq 0$, Cramer's rule says that the solution (a,b,c) of this system obeys

$$a = \frac{1}{D(x,y,z)} \det \begin{pmatrix} ax+by+cz & y & z \\ (ax+by+cz)^p & y^p & z^p \\ (ax+by+cz)^{p^2} & y^{p^2} & z^{p^2} \end{pmatrix}$$

with similar formulas for b and c. Even if $D(x,y,z)=0$, we still have

$$aD(x,y,z) = \det \begin{pmatrix} ax+by+cz & y & z \\ (ax+by+cz)^p & y^p & z^p \\ (ax+by+cz)^{p^2} & y^{p^2} & z^{p^2} \end{pmatrix}$$

and similar equations hold for b and c. Since the right sides have a factor of $ax+by+cz$, the left sides $aD(x,y,z), bD(x,y,z), cD(x,y,z)$ also have this factor. Thus, $D(x,y,z)$ has a factor of $ax+by+cz$, provided $(a,b,c) \neq (0,0,0)$. If $a \neq 0$, then $ax+by+cz = a(x + a^{-1}by + a^{-1}cz)$. If $a=0$ and $b \neq 0$, $ax+by+cz = b(y+b^{-1}cz)$ and if $a=0$ and $b=0$ and $c \neq 0$, then $ax+by+cz = cz$. Thus, for some polynomial $q(x,y,z)$,

$$D(x,y,z) = q(x,y,z) \cdot z \prod_{k=0}^{p-1} (y+kz) \prod_{m,n=0}^{p-1} (x+my+nz)$$

However,

$$\deg \left(z \prod_{k=0}^{p-1} (y+kz) \prod_{m,n=0}^{p-1} (x+my+nz) \right) = 1+p+p^2 = \deg D(x,y,z)$$

Thus, $q(x,y,z)$ is constant, which must be -1 by comparing the coefficients of $zy^px^{p^2}$ on each side.