

Solutions to the 78th William Lowell Putnam Mathematical Competition
Saturday, December 2, 2017

Kiran Kedlaya and Lenny Ng

A1 We claim that the positive integers not in S are 1 and all multiples of 5. If S consists of all other natural numbers, then S satisfies the given conditions: note that the only perfect squares not in S are 1 and numbers of the form $(5k)^2$ for some positive integer k , and it readily follows that both (b) and (c) hold.

Now suppose that T is another set of positive integers satisfying (a), (b), and (c). Note from (b) and (c) that if $n \in T$ then $n+5 \in T$, and so T satisfies the following property:

(d) if $n \in T$, then $n+5k \in T$ for all $k \geq 0$.

The following must then be in T , with implications labeled by conditions (b) through (d):

$$\begin{aligned} 2 &\stackrel{c}{\Rightarrow} 49 \stackrel{c}{\Rightarrow} 54^2 \stackrel{d}{\Rightarrow} 56^2 \stackrel{b}{\Rightarrow} 56 \stackrel{d}{\Rightarrow} 121 \stackrel{b}{\Rightarrow} 11 \\ 11 &\stackrel{d}{\Rightarrow} 16 \stackrel{b}{\Rightarrow} 4 \stackrel{d}{\Rightarrow} 9 \stackrel{b}{\Rightarrow} 3 \\ 16 &\stackrel{d}{\Rightarrow} 36 \stackrel{b}{\Rightarrow} 6 \end{aligned}$$

Since $2, 3, 4, 6 \in T$, by (d) $S \subseteq T$, and so S is smallest.

A2 **First solution.** Define $P_n(x)$ for $P_0(x) = 1$, $P_1(x) = x$, and $P_n(x) = xP_{n-1}(x) - P_{n-2}(x)$. We claim that $P_n(x) = Q_n(x)$ for all $n \geq 0$; since $P_n(x)$ clearly is a polynomial with integer coefficients for all n , this will imply the desired result.

Since $\{P_n\}$ and $\{Q_n\}$ are uniquely determined by their respective recurrence relations and the initial conditions P_0, P_1 or Q_0, Q_1 , it suffices to check that $\{P_n\}$ satisfies the same recurrence as Q : that is, $(P_{n-1}(x))^2 - P_n(x)P_{n-2}(x) = 1$ for all $n \geq 2$. Here is one proof of this: for $n \geq 1$, define the 2×2 matrices

$$M_n = \begin{pmatrix} P_{n-1}(x) & P_n(x) \\ P_{n-2}(x) & P_{n-1}(x) \end{pmatrix}, \quad T = \begin{pmatrix} x & -1 \\ 1 & 0 \end{pmatrix}$$

with $P_{-1}(x) = 0$ (this value being consistent with the recurrence). Then $\det(T) = 1$ and $TM_n = M_{n+1}$, so by induction on n we have

$$(P_{n-1}(x))^2 - P_n(x)P_{n-2}(x) = \det(M_n) = \det(M_1) = 1.$$

Remark: A similar argument shows that any second-order linear recurrent sequence also satisfies a quadratic second-order recurrence relation. A familiar example is the identity $F_{n-1}F_{n+1} - F_n^2 = (-1)^n$ for F_n the n -th Fibonacci number. More examples come from various classes of *orthogonal polynomials*, including the Chebyshev polynomials mentioned below.

Second solution. We establish directly that $Q_n(x) = xQ_{n-1}(x) - Q_{n-2}(x)$, which again suffices. From the equation

$$1 = Q_{n-1}(x)^2 - Q_n(x)Q_{n-2}(x) = Q_n(x)^2 - Q_{n+1}(x)Q_{n-1}(x)$$

we deduce that

$$Q_{n-1}(x)(Q_{n-1}(x) + Q_{n+1}(x)) = Q_n(x)(Q_n(x) + Q_{n-2}(x)).$$

Since $\deg(Q_n(x)) = n$ by an obvious induction, the polynomials $Q_n(x)$ are all nonzero. We may thus rewrite the previous equation as

$$\frac{Q_{n+1}(x) + Q_{n-1}(x)}{Q_n(x)} = \frac{Q_n(x) + Q_{n-2}(x)}{Q_{n-1}(x)},$$

meaning that the rational functions $\frac{Q_n(x) + Q_{n-2}(x)}{Q_{n-1}(x)}$ are all equal to a constant value. By taking $n = 2$ and computing from the definition that $Q_2(x) = x^2 - 1$, we find the constant value to be x ; this yields the desired recurrence.

Remark: By induction, one may also obtain the explicit formula

$$Q_n(x) = \sum_{k=0}^{\lfloor n/2 \rfloor} (-1)^k \binom{n-k}{k} x^{n-2k}.$$

Remark: In light of the explicit formula for $Q_n(x)$, Karl Mahlburg suggests the following bijective interpretation of the identity $Q_{n-1}(x)^2 - Q_n(x)Q_{n-2}(x) = 1$. Consider the set C_n of integer compositions of n with all parts 1 or 2; these are ordered tuples (c_1, \dots, c_k) such that $c_1 + \dots + c_k = n$ and $c_i \in \{1, 2\}$ for all i . For a given composition c , let $o(c)$ and $d(c)$ denote the number of 1's and 2's, respectively. Define the generating function

$$R_n(x) = \sum_{c \in C_n} x^{o(c)};$$

then $R_n(x) = \sum_j \binom{n-j}{j} x^{n-2j}$, so that $Q_n(x) = i^{-n/2} R_n(ix)$. (The polynomials $R_n(x)$ are sometimes called *Fibonacci polynomials*; they satisfy $R_n(1) = F_n$. This interpretation of F_n as the cardinality of C_n first arose in the study of Sanskrit prosody, specifically the analysis of a line of verse as a sequence of long and short syllables, at least 500 years prior to the work of Fibonacci.)

The original identity is equivalent to the identity

$$R_{n+1}(x)R_{n-1}(x) - R_n(x)^2 = (-1)^{n-1}.$$

This follows because if we identify the composition c with a tiling of a $1 \times n$ rectangle by 1×1 squares and 1×2 dominoes, it is *almost* a bijection to place two tilings of length n on top of each other, offset by one square, and hinge at the first possible point (which is the first square in either). This only fails when both tilings are all dominoes, which gives the term $(-1)^{n-1}$.

Remark: This problem appeared on the 2012 India National Math Olympiad; see <https://artofproblemsolving.com/community/c6h1219629>. Another problem based on the same idea is problem A2 from the 1993 Putnam.

A3 **First solution.** Extend the definition of I_n to $n = 0$, so that $I_0 = \int_a^b f(x) dx > 0$. Since $\int_a^b (f(x) - g(x)) dx = 0$, we have

$$\begin{aligned} I_1 - I_0 &= \int_a^b \frac{f(x)}{g(x)} (f(x) - g(x)) dx \\ &= \int_a^b \frac{(f(x) - g(x))^2}{g(x)} dx > 0, \end{aligned}$$

where the inequality follows from the fact that the integrand is a nonnegative continuous function on $[a, b]$ that is not identically 0. Now for $n \geq 0$, the Cauchy–Schwarz inequality gives

$$\begin{aligned} I_n I_{n+2} &= \left(\int_a^b \frac{(f(x))^{n+1}}{(g(x))^n} dx \right) \left(\int_a^b \frac{(f(x))^{n+3}}{(g(x))^{n+2}} dx \right) \\ &\leq \left(\int_a^b \frac{(f(x))^{n+2}}{(g(x))^{n+1}} dx \right)^2 = I_{n+1}^2. \end{aligned}$$

It follows that the sequence $\{I_{n+1}/I_n\}_{n=0}^\infty$ is nondecreasing. Since $I_1/I_0 > 1$, this implies that $I_{n+1} > I_n$ for all n ; also, $I_n/I_0 = \prod_{k=0}^{n-1} (I_{k+1}/I_k) \geq (I_1/I_0)^n$, and so $\lim_{n \rightarrow \infty} I_n = \infty$ since $I_1/I_0 > 1$ and $I_0 > 0$.

Remark: Noam Elkies suggests the following variant of the previous solution, which eliminates the need to separately check that $I_1 > I_0$. First, the proof that $I_n I_{n+2} \geq I_{n+1}^2$ applies also for $n = -1$ under the convention that $I_{-1} = \int_a^b g(x) dx$ (as in the fourth solution below). Second, this equality must be strict for each $n \geq -1$: otherwise, the equality condition in Cauchy–Schwarz would imply that $g(x) = cf(x)$ identically for some $c > 0$, and the equality $\int_a^b f(x) dx = \int_a^b g(x) dx$ would then force $c = 1$, contrary to assumption. Consequently, the sequence I_{n+1}/I_n is strictly increasing; since $I_0/I_{-1} = 1$, it follows that for $n \geq 0$, we again have $I_{n+1}/I_n \geq I_1/I_0 > 1$ and so on.

Second solution. (from Art of Problem Solving, user

MSTang) Since $\int_a^b (f(x) - g(x)) dx = 0$, we have

$$\begin{aligned} I_{n+1} - I_n &= \int_a^b \left(\frac{(f(x))^{n+2}}{(g(x))^{n+1}} - \frac{(f(x))^{n+1}}{(g(x))^n} \right) dx \\ &= \int_a^b \frac{(f(x))^{n+1}}{(g(x))^{n+1}} (f(x) - g(x)) dx \\ &= \int_a^b \left(\frac{(f(x))^{n+1}}{(g(x))^{n+1}} - 1 \right) (f(x) - g(x)) dx \\ &= \int_a^b \frac{(f(x) - g(x))^2 ((f(x))^n + \dots + g(x)^n)}{(g(x))^{n+1}} dx. \end{aligned}$$

The integrand is continuous, nonnegative, and not identically zero; hence $I_{n+1} - I_n > 0$.

To prove that $\lim_{n \rightarrow \infty} I_n = \infty$, note that we cannot have $f(x) \leq g(x)$ identically, as then the equality $\int_a^b f(x) dx = \int_a^b g(x) dx$ would imply $f(x) = g(x)$ identically. That is, there exists some $t \in [a, b]$ such that $f(t) > g(t)$. By continuity, there exist a quantity $c > 1$ and an interval $J = [t_0, t_1]$ in $[a, b]$ such that $f(x) \geq cg(x)$ for all $x \in J$. We then have

$$I_n \geq \int_{t_0}^{t_1} \frac{(f(x))^{n+1}}{(g(x))^n} dx \geq c^n \int_{t_0}^{t_1} f(x) dx;$$

since $f(x) > 0$ everywhere, we have $\int_{t_0}^{t_1} f(x) dx > 0$ and hence I_n is bounded below by a quantity which tends to ∞ .

Remark: One can also give a variation of the second half of the solution which shows directly that $I_{n+1} - I_n \geq c^n d$ for some $c > 1, d > 0$, thus proving both assertions at once.

Third solution. (from David Savitt, via Art of Problem Solving) Extend the definition of I_n to all *real* n , and note that

$$I_{-1} = \int_a^b g(x) dx = \int_a^b f(x) dx = I_0.$$

By writing

$$I_n = \int_a^b \exp((n+1) \log f(x) - n \log g(x)) dx,$$

we see that the integrand is a strictly convex function of n , as then is I_n . It follows that I_n is strictly increasing and unbounded for $n \geq 1$.

Fourth solution. (by David Rusin) Again, extend the definition of I_n to $n = -1$. Now note that for $n \geq 0$ and $x \in [a, b]$, we have

$$(f(x) - g(x)) \left(\left(\frac{f(x)}{g(x)} \right)^{n+1} - \left(\frac{f(x)}{g(x)} \right)^n \right) \geq 0$$

because both factors have the same sign (depending on the comparison between $f(x)$ and $g(x)$); moreover, equality only occurs when $f(x) = g(x)$. Since f and g are not identically equal, we deduce that

$$I_{n+1} - I_n > I_n - I_{n-1}$$

and so in particular

$$I_{n+1} - I_n \geq I_1 - I_0 > I_0 - I_{-1} = 0.$$

This proves both claims.

Remark: This problem appeared in 2005 on an undergraduate math olympiad in Brazil. See <https://artofproblemsolving.com/community/c7h57686p354392> for discussion.

A4 First solution. Let a_1, \dots, a_{2N} be the scores in non-decreasing order, and define the sums $s_i = \sum_{j=i+1}^{2N} a_j$ for $i = 0, \dots, 2N$. Then $s_0 \leq \dots \leq s_{2N}$ and $s_0 + s_{2N} = \sum_{j=1}^{2N} a_j = 7.4(2N)$, so $s_0 \leq 7.4N \leq s_{2N}$. Let i be the largest index for which $s_i \leq 7.4N$; note that we cannot have $i = 2N$, as otherwise $s_0 = s_{2N} = 7.4N$ and hence $a_1 = \dots = a_{2N} = 7.4$, contradiction. Then $7.4N - s_i < s_{i+1} - s_i = a_{i+N+1} - a_i$ and so

$$a_i < s_i + a_{i+N+1} - 7.4N \leq a_{i+N+1};$$

since all possible scores occur, this means that we can find N scores with sum $7.4N$ by taking a_i, \dots, a_{i+N+1} and omitting one occurrence of the value $s_i + a_{i+N+1} - 7.4N$.

Remark: David Savitt (via Art of Problem Solving) points out that a similar argument applies provided that there are an even number of students, the total score is even, and the achieved scores form a block of consecutive integers.

Second solution. We first claim that for any integer m with $15 \leq m \leq 40$, we can find five distinct elements of the set $\{1, 2, \dots, 10\}$ whose sum is m . Indeed, for $0 \leq k \leq 4$ and $1 \leq \ell \leq 6$, we have

$$\binom{k}{j=1} + (k + \ell) + \binom{10}{j=k+7} = 34 - 5k + \ell,$$

and for fixed k this takes all values from $35 - 5k$ to $40 - 5k$ inclusive; then as k ranges from 0 to 4, this takes all values from 15 to 40 inclusive.

Now suppose that the scores are a_1, \dots, a_{2N} , where we order the scores so that $a_k = k$ for $k \leq 10$ and the subsequence $a_{11}, a_{12}, \dots, a_{2N}$ is nondecreasing. For $1 \leq k \leq N - 4$, define $S_k = \sum_{j=k+10}^{2N} a_j$. Note that for each k , $S_{k+1} - S_k = a_{k+N+5} - a_{k+10}$ and so $0 \leq S_{k+1} - S_k \leq 10$. Thus S_1, \dots, S_{N-4} is a nondecreasing sequence of integers where each term is at most 10 more than the previous one. On the other hand, we have

$$\begin{aligned} S_1 + S_{N-4} &= \sum_{j=11}^{2N} a_j \\ &= (7.4)(2N) - \sum_{j=1}^{10} a_j \\ &= (7.4)(2N) - 55, \end{aligned}$$

whence $S_1 \leq 7.4N - 27.5 \leq S_{N-4}$. It follows that there is some k such that $S_k \in [7.4N - 40, 7.4N - 15]$, since this interval has length 25 and $7.4N - 27.5$ lies inside it.

For this value of k , note that both S_k and $7.4N$ are integers (the latter since the sum of all scores in the class is the integer $(7.4)(2N)$ and so N must be divisible by 5). Thus there is an integer m with $15 \leq m \leq 40$ for which $S_k = 7.4N - m$. By our first claim, we can choose five scores from a_1, \dots, a_{10} whose sum is m . When we add these to the sum of the $N - 5$ scores $a_{k+10}, \dots, a_{k+N+4}$, we get precisely $7.4N$. We have now found N scores whose sum is $7.4N$ and thus whose average is 7.4.

Third solution. It will suffice to show that given any partition of the students into two groups of N , if the sums are not equal we can bring them closer together by swapping one pair of students between the two groups. To state this symbolically, let S be the set of students and, for any subset T of S , let ΣT denote the sum of the scores of the students in T ; we then show that if $S = A \cup B$ is a partition into two N -element sets with $\Sigma A > \Sigma B$, then there exist students $a \in A, b \in B$ such that the sets

$$A' = A \setminus \{a\} \cup \{b\}, \quad B' = A \setminus \{b\} \cup \{a\}$$

satisfy

$$0 \leq \Sigma A' - \Sigma B' < \Sigma A - \Sigma B.$$

In fact, this argument will apply at the same level of generality as in the remark following the first solution.

To prove the claim, let a_1, \dots, a_n be the scores in A and let b_1, \dots, b_n be the scores in B (in any order). Since $\Sigma A - \Sigma B \equiv \Sigma S \pmod{2}$ and the latter is even, we must have $\Sigma A - \Sigma B \geq 2$. In particular, there must exist indices $i, j \in \{1, \dots, n\}$ such that $a_i > b_j$. Consequently, if we sort the sequence $a_1, \dots, a_n, b_1, \dots, b_n$ into nondecreasing order, it must be the case that some term b_j is followed by some term a_i . Moreover, since the achieved scores form a range of consecutive integers, we must in fact have $a_i = b_j + 1$. Consequently, if we take $a = a_i$, $b = b_j$, we then have $\Sigma A' - \Sigma B' = \Sigma A - \Sigma B - 2$, which proves the claim.

A5 First solution. Let a_n, b_n, c_n be the probabilities that players A, B, C , respectively, will win the game. We compute these by induction on n , starting with the values

$$a_1 = 1, \quad b_1 = 0, \quad c_1 = 0.$$

If player A draws card k , then the resulting game state is that of a deck of $k - 1$ cards with the players taking turns in the order B, C, A, B, \dots . In this state, the probabilities that players A, B, C will win are $c_{k-1}, a_{k-1}, b_{k-1}$ provided that we adopt the convention that

$$a_0 = 0, \quad b_0 = 0, \quad c_0 = 1.$$

We thus have

$$a_n = \frac{1}{n} \sum_{k=1}^n c_{k-1}, \quad b_n = \frac{1}{n} \sum_{k=1}^n a_{k-1}, \quad c_n = \frac{1}{n} \sum_{k=1}^n b_{k-1}.$$

Put

$$x_n = a_n - b_n, \quad y_n = b_n - c_n, \quad z_n = c_n - a_n;$$

we then have

$$\begin{aligned} x_{n+1} &= \frac{n}{n+1}x_n + \frac{1}{n+1}z_n, \\ y_{n+1} &= \frac{n}{n+1}y_n + \frac{1}{n+1}x_n, \\ z_{n+1} &= \frac{n}{n+1}z_n + \frac{1}{n+1}y_n. \end{aligned}$$

Note that if $a_{n+1} = b_{n+1} = c_{n+1} = 0$, then

$$x_n = -nz_n = n^2y_n = -n^3x_n = n^4z_n$$

and so $x_n = z_n = 0$, or in other words $a_n = b_n = c_n$. By induction on n , we deduce that a_n, b_n, c_n cannot all be equal. That is, the quantities x_n, y_n, z_n add up to zero and at most one of them vanishes; consequently, the quantity $r_n = \sqrt{x_n^2 + y_n^2 + z_n^2}$ is always positive and the quantities

$$x'_n = \frac{x_n}{r_n}, \quad y'_n = \frac{y_n}{r_n}, \quad z'_n = \frac{z_n}{r_n}$$

form the coordinates of a point P_n on a fixed circle C in \mathbb{R}^3 .

Let P'_n be the point (z_n, x_n, y_n) obtained from P_n by a clockwise rotation of angle $\frac{2\pi}{3}$. The point P_{n+1} then lies on the ray through the origin passing through the point dividing the chord from P_n to P'_n in the ratio 1 : n . The (clockwise) arc from P_n to P_{n+1} therefore has a measure of

$$\arctan \frac{\sqrt{3}}{2n-1} = \frac{\sqrt{3}}{2n-1} + O(n^{-3});$$

these measures form a null sequence whose sum diverges. It follows that any arc of C contains infinitely many of the P_n ; taking a suitably short arc around the point $(\frac{\sqrt{2}}{2}, 0, -\frac{\sqrt{2}}{2})$, we deduce that for infinitely many n , A has the highest winning probability, and similarly for B and C .

Remark: From the previous analysis, we also deduce that

$$\frac{r_{n+1}}{r_n} = \frac{\sqrt{n^2 - n + 1}}{n + 1} = 1 - \frac{3}{2(n+1)} + O(n^{-2}),$$

from which it follows that $r_n \sim cn^{-3/2}$ for some $c > 0$.

Second solution. (by Noam Elkies) In this approach, we instead compute the probability $p_n(m)$ that the game ends after exactly m turns (the winner being determined

by the residue of $m \bmod 3$). We use the convention that $p_0(0) = 1$, $p_0(m) = 0$ for $m > 0$. Define the generating function $P_n(X) = \sum_{m=0}^n p_n(m)x^m$. We will establish that

$$P_n(X) = \frac{X(X+1)\cdots(X+n-1)}{n!}$$

(which may be guessed by computing $p_n(m)$ for small n by hand). There are several ways to do this; for instance, this follows from the recursion

$$P_n(X) = \frac{1}{n}XP_{n-1}(X) + \frac{(n-1)}{n}P_{n-1}(X).$$

(In this recursion, the first term corresponds to conditional probabilities given that the first card drawn is n , and the second term corresponds to the remaining cases.)

Let ω be a primitive cube root of 1. With notation as in the first solution, we have

$$P_n(\omega) = a_n + b_n\omega + c_n\omega;$$

combining this with the explicit formula for $P_n(X)$ and the observation that

$$\arg(\omega + n) = \arctan \frac{\sqrt{3}}{2n-1}$$

recovers the geometric description of a_n, b_n, c_n given in the first solution (as well as the remark following the first solution).

Third solution. For this argument, we use the auxiliary quantities

$$a'_n = a_n - \frac{1}{3}, \quad b'_n = b_n - \frac{1}{3}, \quad c'_n = c_n - \frac{1}{3};$$

these satisfy the relations

$$a'_n = \frac{1}{n} \sum_{k=1}^n c'_{k-1}, \quad b'_n = \frac{1}{n} \sum_{k=1}^n a'_{k-1}, \quad c'_n = \frac{1}{n} \sum_{k=1}^n b'_{k-1}$$

as well as

$$\begin{aligned} a'_{n+1} &= a'_n + \frac{1}{n+1}(c'_n - a'_n) \\ b'_{n+1} &= b'_n + \frac{1}{n+1}(a'_n - b'_n) \\ c'_{n+1} &= c'_n + \frac{1}{n+1}(b'_n - c'_n). \end{aligned}$$

We now show that $\sum_{n=1}^{\infty} a'_n$ cannot diverge to $+\infty$ (and likewise for $\sum_{n=1}^{\infty} b'_n$ and $\sum_{n=1}^{\infty} c'_n$ by similar reasoning). Suppose the contrary; then there exists some $\varepsilon > 0$ and some $n_0 > 0$ such that $\sum_{k=1}^n a'_k \geq \varepsilon$ for all $n \geq n_0$. For $n > n_0$, we have $b'_n \geq \varepsilon$; this in turn implies that $\sum_{n=1}^{\infty} b'_n$ diverges to $+\infty$. Continuing around the circle, we deduce that for n sufficiently large, all three of a'_n, b'_n, c'_n are positive; but this contradicts the identity

$a'_n + b'_n + c'_n = 0$. We thus conclude that $\sum_{n=1}^{\infty} a'_n$ does not diverge to $+\infty$; in particular, $\liminf_{n \rightarrow \infty} a'_n \leq 0$.

By the same token, we may see that $\sum_{n=1}^{\infty} a'_n$ cannot converge to a positive limit L (and likewise for $\sum_{n=1}^{\infty} b'_n$ and $\sum_{n=1}^{\infty} c'_n$ by similar reasoning). Namely, this would imply that $b'_n \geq L/2$ for n sufficiently large, contradicting the previous argument.

By similar reasoning, $\sum_{n=1}^{\infty} a'_n$ cannot diverge to $-\infty$ or converge to a negative limit L (and likewise for $\sum_{n=1}^{\infty} b'_n$ and $\sum_{n=1}^{\infty} c'_n$ by similar reasoning).

We next establish that there are infinitely many n for which $a'_n > 0$ (and likewise for b'_n and c'_n by similar reasoning). Suppose to the contrary that for n sufficiently large, we have $a'_n \leq 0$. By the previous arguments, the sum $\sum_{n=1}^{\infty} a'_n$ cannot diverge to ∞ or converge to a nonzero limit; it must therefore converge to 0. In particular, for n sufficiently large, we have $b'_n = \sum_{k=1}^n a'_{k-1} \geq 0$. Iterating the construction, we see that for n sufficiently large, we must have $c'_n \leq 0$, $a'_n \geq 0$, $b'_n \leq 0$, and $c'_n \geq 0$. As a result, for n sufficiently large we must have $a'_n = b'_n = c'_n = 0$; but we may rule this out as in the original solution.

By similar reasoning, we may deduce that there are infinitely many n for which $a'_n < 0$ (and likewise for b'_n and c'_n by similar reasoning). We now continue using a suggestion of Jon Atkins. Define the values of the sequence x_n according to the relative comparison of a'_n, b'_n, c'_n (using the fact that these cannot all be equal):

$$\begin{aligned} x_n = 1 &: a'_n \leq b'_n < c'_n \\ x_n = 2 &: b'_n \leq c'_n < a'_n \\ x_n = 3 &: c'_n \leq a'_n < b'_n \\ x_n = 4 &: a'_n < c'_n \leq b'_n \\ x_n = 5 &: b'_n < a'_n \leq c'_n \\ x_n = 6 &: c'_n < b'_n \leq a'_n. \end{aligned}$$

We consider these values as *states* and say that there is a *transition* from state i to state j , and write $i \Rightarrow j$, if for every $n \geq 2$ with $x_n = i$ there exists $n' > n$ with $x_{n'} = j$. (In all cases when we use this notation, it will in fact be the case that the *first* value of $n' > n$ for which $x_{n'} \neq i$ satisfies $x_{n'} = j$, but this is not logically necessary for our final conclusion.)

Suppose that $x_n = 1$. By the earlier discussion, we must have $a'_{n'} > 0$ for some $n' > n$, and so we cannot have $x_{n'} = 1$ for all $n' > n$. On the other hand, as long as $x_n = 1$, we have

$$\begin{aligned} c'_{n+1} - b'_{n+1} &= c'_n - b'_n + \frac{1}{n+1}(2b'_n - a'_n - c'_n) \\ &= \frac{n-1}{n+1}(c'_n - b'_n) + \frac{1}{n+1}(c'_n - a'_n) > 0 \\ c'_{n+1} - a'_{n+1} &= c'_n - a'_n + \frac{1}{n+1}(a'_n + b'_n - 2c'_n) \\ &= \frac{n-1}{n+1}(c'_n - a'_n) + \frac{1}{n+1}(b'_n - a'_n) > 0. \end{aligned}$$

Consequently, for n' the smallest value for which $x_{n'} \neq x_n$, we must have $x_{n'} = 2$. By this and two similar arguments, we deduce that

$$1 \Rightarrow 5, \quad 2 \Rightarrow 6, \quad 3 \Rightarrow 4.$$

Suppose that $x_n = 4$. By the earlier discussion, we must have $a'_{n'} < 0$ for some $n' > n$, and so we cannot have $x_{n'} = 4$ for all $n' > n$. On the other hand, as long as $x_n = 4$, we have

$$\begin{aligned} b'_{n+1} - a'_{n+1} &= b'_n - a'_n + \frac{1}{n+1}(2a'_n - b'_n - c'_n) \\ &= \frac{n-1}{n+1}(b'_n - a'_n) + \frac{1}{n+1}(b'_n - c'_n) > 0 \\ c'_{n+1} - a'_{n+1} &= c'_n - a'_n + \frac{1}{n+1}(a'_n + b'_n - 2c'_n) \\ &= \frac{n-1}{n+1}(c'_n - a'_n) + \frac{1}{n+1}(b'_n - a'_n) > 0. \end{aligned}$$

Consequently, for n' the smallest value for which $x_{n'} \neq x_n$, we must have $x_{n'} = 1$. By this and two similar arguments, we deduce that

$$4 \Rightarrow 1, \quad 5 \Rightarrow 2, \quad 6 \Rightarrow 3.$$

Combining, we obtain

$$1 \Rightarrow 5 \Rightarrow 2 \Rightarrow 6 \Rightarrow 3 \Rightarrow 4 \Rightarrow 1$$

and hence the desired result.

A6 The number of such colorings is $2^{20}3^{10} = 61917364224$.

First solution: Identify the three colors red, white, and blue with (in some order) the elements of the field \mathbb{F}_3 of three elements (i.e., the ring of integers mod 3). The set of colorings may then be identified with the \mathbb{F}_3 -vector space \mathbb{F}_3^E generated by the set E of edges. Let F be the set of faces, and let \mathbb{F}_3^F be the \mathbb{F}_3 -vector space on the basis F ; we may then define a linear transformation $T: \mathbb{F}_3^E \rightarrow \mathbb{F}_3^F$ taking a coloring to the vector whose component corresponding to a given face equals the sum of the three edges of that face. The colorings we wish to count are the ones whose images under T consist of vectors with no zero components.

We now show that T is surjective. (There are many possible approaches to this step; for instance, see the following remark.) Let Γ be the dual graph of the icosahedron, that is, Γ has vertex set F and two elements of F are adjacent in Γ if they share an edge in the icosahedron. The graph Γ admits a hamiltonian path, that is, there exists an ordering f_1, \dots, f_{20} of the faces such that any two consecutive faces are adjacent in Γ . For example, such an ordering can be constructed with f_1, \dots, f_5 being the five faces sharing a vertex of the icosahedron and f_{16}, \dots, f_{20} being the five faces sharing the antipodal vertex.

For $i = 1, \dots, 19$, let e_i be the common edge of f_i and f_{i+1} ; these are obviously all distinct. By prescribing

components for e_1, \dots, e_{19} in turn and setting the others to zero, we can construct an element of \mathbb{F}_3^E whose image under T matches any given vector of \mathbb{F}_3^F in the components of f_1, \dots, f_{19} . The vectors in \mathbb{F}_3^F obtained in this way thus form a 19-dimensional subspace; this subspace may also be described as the vectors for which the components of f_1, \dots, f_{19} have the same sum as the components of f_2, \dots, f_{20} .

By performing a mirror reflection, we can construct a second hamiltonian path g_1, \dots, g_{20} with the property that

$$g_1 = f_1, g_2 = f_5, g_3 = f_4, g_4 = f_3, g_5 = f_2.$$

Repeating the previous construction, we obtain a *different* 19-dimensional subspace of \mathbb{F}_3^F which is contained in the image of T . This implies that T is surjective, as asserted earlier.

Since T is a surjective homomorphism from a 30-dimensional vector space to a 20-dimensional vector space, it has a 10-dimensional kernel. Each of the 2^{20} elements of \mathbb{F}_3^F with no zero components is then the image of exactly 3^{10} colorings of the desired form, yielding the result.

Remark: There are many ways to check that T is surjective. One of the simplest is the following (from Art of Problem Solving, user Ravi12346): form a vector in \mathbb{F}^E with components 2, 1, 2, 1, 2 at the five edges around some vertex and all other components 0. This maps to a vector in \mathbb{F}^F with only a single nonzero component; by symmetry, every standard basis vector of \mathbb{F}^F arises in this way.

Second solution: (from Bill Huang, via Art of Problem Solving user superpi83) Let v and w be two antipodal vertices of the icosahedron. Let S_v (resp. S_w) be the set of five edges incident to v (resp. w). Let T_v (resp. T_w) be the set of five edges of the pentagon formed by the opposite endpoints of the five edges in S_v (resp. S_w). Let U be the set of the ten remaining edges of the icosahedron.

Consider any one of the 3^{10} possible colorings of U . The edges of $T_v \cup U$ form the boundaries of five faces with no edges in common; thus each edge of T_v can be colored in one of two ways consistent with the given condition, and similarly for T_w . That is, there are $3^{10}2^{10}$ possible colorings of $T_v \cup T_w \cup U$ consistent with the given condition.

To complete the count, it suffices to check that there are exactly 2^5 ways to color S_v consistent with any given coloring of T_v . Using the linear-algebraic interpretation from the first solution, this follows by observing that (by the previous remark) the map from $\mathbb{F}_3^{S_v}$ to the \mathbb{F}_3 -vector space on the faces incident to v is surjective, and hence an isomorphism for dimensional reasons. A direct combinatorial proof is also possible.

B1 Recall that L_1 and L_2 intersect if and only if they are not parallel. In one direction, suppose that L_1 and L_2 intersect. Then for any P and λ , the dilation (homothety) of

the plane by a factor of λ with center P carries L_1 to another line parallel to L_1 and hence not parallel to L_2 . Let A_2 be the unique intersection of L_2 with the image of L_1 , and let A_1 be the point on L_1 whose image under the dilation is A_2 ; then $\overrightarrow{PA_2} = \lambda \overrightarrow{PA_1}$.

In the other direction, suppose that L_1 and L_2 are parallel. Let P be any point in the region between L_1 and L_2 and take $\lambda = 1$. Then for any point A_1 on L_1 and any point A_2 on L_2 , the vectors $\overrightarrow{PA_1}$ and $\overrightarrow{PA_2}$ have components perpendicular to L_1 pointing in opposite directions; in particular, the two vectors cannot be equal.

Reinterpretation: (by Karl Mahlburg) In terms of vectors, we may find vectors \vec{v}_1, \vec{v}_2 and scalars c_1, c_2 such that $L_i = \{\vec{x} \in \mathbb{R}^2 : \vec{v}_i \cdot \vec{x} = c_i\}$. The condition in the problem amounts to finding a vector \vec{w} and a scalar t such that $P + \vec{w} \in L_1, P + \lambda \vec{w} \in L_2$; this comes down to solving the linear system

$$\begin{aligned} \vec{v}_1 \cdot (P + \vec{w}) &= c_1 \\ \vec{v}_2 \cdot (P + \lambda \vec{w}) &= c_2 \end{aligned}$$

which is nondegenerate and solvable for all λ if and only if \vec{v}_1, \vec{v}_2 are linearly independent.

B2 We prove that the smallest value of a is 16.

Note that the expression for N can be rewritten as $k(2a + k - 1)/2$, so that $2N = k(2a + k - 1)$. In this expression, $k > 1$ by requirement; $k < 2a + k - 1$ because $a > 1$; and obviously k and $2a + k - 1$ have opposite parity. Conversely, for any factorization $2N = mn$ with $1 < m < n$ and m, n of opposite parity, we obtain an expression of N in the desired form by taking $k = m$, $a = (n + 1 - m)/2$.

We now note that 2017 is prime. (On the exam, solvers would have had to verify this by hand. Since $2017 < 45^2$, this can be done by trial division by the primes up to 43.) For $N = 2017(2a + 2016)$ not to have another expression of the specified form, it must be the case that $2a + 2016$ has no odd divisor greater than 1; that is, $2a + 2016$ must be a power of 2. This first occurs for $2a + 2016 = 2048$, yielding the claimed result.

Reinterpretation: (by Karl Mahlburg) To avoid N having another representation, for $k = 2, \dots, 2016$, we must have

$$N \not\equiv \begin{cases} k/2 & k \equiv 0 \pmod{2} \\ 0 & k \equiv 1 \pmod{2}. \end{cases}$$

Consequently, $N \not\equiv 0 \pmod{p}$ for any odd prime $p < 2017$ and $N \equiv 0 \pmod{1024}$. Since N must be divisible by 2017, this again yields the claimed value of a .

B3 Suppose by way of contradiction that $f(1/2)$ is rational. Then $\sum_{i=0}^{\infty} c_i 2^{-i}$ is the binary expansion of a rational number, and hence must be eventually periodic; that is, there exist some integers m, n such that $c_i = c_{m+i}$ for all

$i \geq n$. We may then write

$$f(x) = \sum_{i=0}^{n-1} c_i x^i + \frac{x^n}{1-x^m} \sum_{i=0}^{m-1} c_{n+i} x^i.$$

Evaluating at $x = 2/3$, we may equate $f(2/3) = 3/2$ with

$$\frac{1}{3^{n-1}} \sum_{i=0}^{n-1} c_i 2^i 3^{n-i} + \frac{2^n 3^m}{3^{n+m-1} (3^m - 2^m)} \sum_{i=0}^{m-1} c_{n+i} 2^i 3^{m-1-i};$$

since all terms on the right-hand side have odd denominator, the same must be true of the sum, a contradiction.

Remark: Greg Marks asks whether the assumption that $f(2/3) = 3/2$ further ensures that $f(1/2)$ is transcendental. We do not know of any existing results that would imply this. However, the following result follows from a theorem of T. Tanaka (Algebraic independence of the values of power series generated by linear recurrences, *Acta Arith.* **74** (1996), 177–190), building upon work of Mahler. Let $\{a_n\}_{n=0}^{\infty}$ be a linear recurrent sequence of positive integers with characteristic polynomial P . Suppose that $P(0), P(1), P(-1) \neq 0$ and that no two distinct roots of P have ratio which is a root of unity. Then for $f(x) = \sum_{n=0}^{\infty} x^{a_n}$, the values $f(1/2)$ and $f(2/3)$ are algebraically independent over \mathbb{Q} . (Note that for f as in the original problem, the condition on ratios of roots of P fails.)

B4 We prove that the sum equals $(\log 2)^2$; as usual, we write $\log x$ for the natural logarithm of x instead of $\ln x$. Note that of the two given expressions of the original sum, the first is absolutely convergent (the summands decay as $\log(x)/x^2$) but the second one is not; we must thus be slightly careful when rearranging terms.

First solution. Define $a_k = \frac{\log k}{k} - \frac{\log(k+1)}{k+1}$. The infinite sum $\sum_{k=1}^{\infty} a_k$ converges to 0 since $\sum_{k=1}^n a_k$ telescopes to $-\frac{\log(n+1)}{n+1}$ and this converges to 0 as $n \rightarrow \infty$. Note that $a_k > 0$ for $k \geq 3$ since $\frac{\log x}{x}$ is a decreasing function of x for $x > e$, and so the convergence of $\sum_{k=1}^{\infty} a_k$ is absolute.

Write S for the desired sum. Then since $3a_{4k+2} + 2a_{4k+3} + a_{4k+4} = (a_{4k+2} + a_{4k+4}) + 2(a_{4k+2} + a_{4k+3})$, we have

$$\begin{aligned} S &= \sum_{k=0}^{\infty} (3a_{4k+2} + 2a_{4k+3} + a_{4k+4}) \\ &= \sum_{k=1}^{\infty} a_{2k} + \sum_{k=0}^{\infty} 2(a_{4k+2} + a_{4k+3}), \end{aligned}$$

where we are allowed to rearrange the terms in the infinite sum since $\sum a_k$ converges absolutely. Now $2(a_{4k+2} + a_{4k+3}) = \frac{\log(4k+2)}{2k+1} - \frac{\log(4k+4)}{2k+2} = a_{2k+1} + (\log 2) \left(\frac{1}{2k+1} - \frac{1}{2k+2} \right)$, and summing over k gives

$$\begin{aligned} \sum_{k=0}^{\infty} 2(a_{4k+2} + a_{4k+3}) &= \sum_{k=0}^{\infty} a_{2k+1} + (\log 2) \sum_{k=1}^{\infty} \frac{(-1)^{k+1}}{k} \\ &= \sum_{k=0}^{\infty} a_{2k+1} + (\log 2)^2. \end{aligned}$$

Finally, we have

$$\begin{aligned} S &= \sum_{k=1}^{\infty} a_{2k} + \sum_{k=0}^{\infty} a_{2k+1} + (\log 2)^2 \\ &= \sum_{k=1}^{\infty} a_k + (\log 2)^2 = (\log 2)^2. \end{aligned}$$

Second solution. We start with the following observation: for any positive integer n ,

$$\left. \frac{d}{ds} n^{-s} \right|_{s=1} = -(\log n) n^{-s}.$$

(Throughout, we view s as a *real* parameter, but see the remark below.) For $s > 0$, consider the absolutely convergent series

$$L(s) = \sum_{k=0}^{\infty} (3(4k+2)^{-s} - (4k+3)^{-s} - (4k+4)^{-s} - (4k+5)^{-s});$$

in the same range we have

$$\begin{aligned} L'(s) &= \sum_{k=0}^{\infty} \left(3 \frac{\log(4k+2)}{(4k+2)^s} - \frac{\log(4k+3)}{(4k+3)^s} \right. \\ &\quad \left. + \frac{\log(4k+4)}{(4k+4)^s} - \frac{\log(4k+5)}{(4k+5)^s} \right), \end{aligned}$$

so we may interchange the summation with taking the limit at $s = 1$ to equate the original sum with $-L'(1)$.

To make further progress, we introduce the Riemann zeta function $\zeta(s) = \sum_{n=1}^{\infty} n^{-s}$, which converges absolutely for $s > 1$. In that region, we may freely rearrange sums to write

$$\begin{aligned} L(s) + \zeta(s) &= 1 + 4(2^{-s} + 6^{-s} + 10^{-s} + \dots) \\ &= 1 + 2^{2-s}(1 + 3^{-s} + 5^{-s} + \dots) \\ &= 1 + 2^{2-s}(\zeta(s) - 2^{-s} - 4^{-s} - \dots) \\ &= 1 + 2^{2-s}\zeta(s) - 2^{2-2s}\zeta(s). \end{aligned}$$

In other words, for $s > 1$, we have

$$L(s) = 1 + \zeta(s)(-1 + 2^{2-s} - 2^{2-2s}).$$

Now recall that $\zeta(s) - \frac{s}{s-1}$ extends to a C^{∞} function for $s > 0$, e.g., by applying Abel summation to obtain

$$\begin{aligned} \zeta(s) - \frac{s}{s-1} &= \sum_{n=1}^{\infty} n(n^{-s} - (n+1)^{-s}) - \frac{s}{s-1} \\ &= s \sum_{n=1}^{\infty} n \int_n^{n+1} x^{-s-1} dx - \frac{s}{s-1} \\ &= -s \int_1^{\infty} (x - [x]) x^{-s-1} dx. \end{aligned}$$

Also by writing $2^{2-s} = 2 \exp((1-s)\log 2)$ and $2^{2-2s} = \exp(2(1-s)\log 2)$, we may use the exponential series to compute the Taylor expansion of

$$f(s) = \frac{-1 + 2^{2-s} - 2^{2-2s}}{s-1}$$

at $s = 1$; we get

$$f(s) = -(\log 2)^2 (s-1)^2 + O((s-1)^3).$$

Consequently, if we rewrite the previous expression for $L(s)$ as

$$L(s) = 1 + (s-1)\zeta(s) \cdot \frac{-1 + 2^{2-s} - 2^{2-2s}}{s-1},$$

then we have an equality of C^∞ functions for $s > 1$, and hence (by continuity) an equality of Taylor series about $s = 1$. That is,

$$L(s) = 1 - (\log 2)^2 (s-1) + O((s-1)^2),$$

which yields the desired result.

Remark:

The use of series $\sum_{n=1}^{\infty} c_n n^{-s}$ as functions of a *real* parameter s dates back to Euler, who observed that the divergence of $\zeta(s)$ as $s \rightarrow 1$ gives a proof of the infinitude of primes distinct from Euclid's approach, and Dirichlet, who upgraded this idea to prove his theorem on the distribution of primes across arithmetic progressions. It was Riemann who introduced the idea of viewing these series as functions of a *complex* parameter, thus making it possible to use the tools of complex analysis (e.g., the residue theorem) and leading to the original proof of the prime number theorem by Hadamard and de la Vallée Poussin.

In the language of complex analysis, one may handle the convergence issues in the second solution in a different way: use the preceding calculation to establish the equality

$$L(s) = 1 + \zeta(s)(-1 + 2^{2-s} - 2^{2-2s})$$

for $\text{Real}(s) > 1$, then observe that both sides are holomorphic for $\text{Real}(s) > 0$ and so the equality extends to that larger domain.

B5 The desired integers are $(a, b, c) = (9, 8, 7)$.

Suppose we have a triangle $T = \triangle ABC$ with $BC = a$, $CA = b$, $AB = c$ and $a > b > c$. Say that a line is an *area equalizer* if it divides T into two regions of equal area. A line intersecting T must intersect two of the three sides of T . First consider a line intersecting the segments AB at X and BC at Y , and let $BX = x$, $BY = y$. This line is an area equalizer if and only if $xy \sin B = 2 \text{area}(\triangle XBY) = \text{area}(\triangle ABC) = \frac{1}{2}ac \sin B$, that is, $2xy = ac$. Since $x \leq c$ and $y \leq a$, the area equalizers correspond to values of x, y with $xy = ac/2$ and $x \in [c/2, c]$. Such an area equalizer is also an equalizer if and only if $p/2 = x + y$, where $p = a + b + c$ is the perimeter of T . If we write $f(x) = x + ac/(2x)$, then we want to solve $f(x) = p/2$ for $x \in [c/2, c]$. Now note that f is convex, $f(c/2) = a + c/2 > p/2$, and $f(c) = a/2 + c < p/2$; it follows that there is exactly one solution to $f(x) = p/2$ in $[c/2, c]$. Similarly, for

equalizers intersecting T on the sides AB and AC , we want to solve $g(x) = p/2$ where $g(x) = x + bc/(2x)$ and $x \in [c/2, c]$; since g is convex and $g(c/2) < p/2$, $g(c) < p/2$, there are no such solutions.

It follows that if T has exactly two equalizers, then it must have exactly one equalizer intersecting T on the sides AC and BC . Here we want to solve $h(x) = p/2$ where $h(x) = x + ab/(2x)$ and $x \in [a/2, a]$. Now h is convex and $h(a/2) > p/2$, $h(a) > p/2$; thus $h(x) = p/2$ has exactly one solution $x \in [a/2, a]$ if and only if there is $x_0 \in [a/2, a]$ with $h'(x_0) = 0$ and $h(x_0) = p/2$. The first condition implies $x_0 = \sqrt{ab/2}$, and then the second condition gives $8ab = p^2$. Note that $\sqrt{ab/2}$ is in $[a/2, a]$ since $a > b$ and $a < b + c < 2b$.

We conclude that T has two equalizers if and only if $8ab = (a + b + c)^2$. Note that $(a, b, c) = (9, 8, 7)$ works. We claim that this is the only possibility when $a > b > c$ are integers and $a \leq 9$. Indeed, the only integers (a, b) such that $2 \leq b < a \leq 9$ and $8ab$ is a perfect square are $(a, b) = (4, 2), (6, 3), (8, 4), (9, 2)$, and $(9, 8)$, and the first four possibilities do not produce triangles since they do not satisfy $a < 2b$. This gives the claimed result.

B6 **First solution.** The desired count is $\frac{2016!}{1953!} - 63! \cdot 2016$, which we compute using the principle of inclusion-exclusion. As in A2, we use the fact that 2017 is prime; this means that we can do linear algebra over the field \mathbb{F}_{2017} . In particular, every nonzero homogeneous linear equation in n variables over \mathbb{F}_{2017} has exactly 2017^{n-1} solutions.

For π a partition of $\{0, \dots, 63\}$, let $|\pi|$ denote the number of distinct parts of π . Let π_0 denote the partition of $\{0, \dots, 63\}$ into 64 singleton parts. Let π_1 denote the partition of $\{0, \dots, 63\}$ into one 64-element part. For π, σ two partitions of $\{0, \dots, 63\}$, write $\pi|\sigma$ if π is a refinement of σ (that is, every part in σ is a union of parts in π). By induction on $|\pi|$, we may construct a collection of integers μ_π , one for each π , with the properties that

$$\sum_{\pi|\sigma} \mu_\pi = \begin{cases} 1 & \sigma = \pi_0 \\ 0 & \sigma \neq \pi_0 \end{cases}.$$

Define the sequence c_0, \dots, c_{63} by setting $c_0 = 1$ and $c_i = i$ for $i > 1$. Let N_π be the number of ordered 64-tuples (x_0, \dots, x_{63}) of elements of \mathbb{F}_{2017} such that $x_i = x_j$ whenever i and j belong to the same part and $\sum_{i=0}^{63} c_i x_i$ is divisible by 2017. Then N_π equals $2017^{|\pi|-1}$ unless for each part S of π , the sum $\sum_{i \in S} c_i$ vanishes; in that case, N_π instead equals $2017^{|\pi|}$. Since c_0, \dots, c_{63} are positive integers which sum to $1 + \frac{63 \cdot 64}{2} = 2017$, the second outcome only occurs for $\pi = \pi_1$. By inclusion-exclusion, the desired count may be written as

$$\sum_{\pi} \mu_\pi N_\pi = 2016 \cdot \mu_{\pi_1} + \sum_{\pi} \mu_\pi 2017^{|\pi|-1}.$$

Similarly, the number of ordered 64-tuples with no repeated elements may be written as

$$64! \binom{2017}{64} = \sum_{\pi} \mu_{\pi} 2017^{|\pi|}.$$

The desired quantity may thus be written as $\frac{2016!}{1953!} + 2016\mu_{\pi_1}$.

It remains to compute μ_{π_1} . We adopt an approach suggested by David Savitt: apply inclusion-exclusion to count distinct 64-tuples in an *arbitrary* set A . As above, this yields

$$|A|(|A|-1)\cdots(|A|-63) = \sum_{\pi} \mu_{\pi} |A|^{|\pi|}.$$

Viewing both sides as polynomials in $|A|$ and comparing coefficients in degree 1 yields $\mu_{\pi} = -63!$ and thus the claimed answer.

Second solution. (from Art of Problem Solving, user ABCDE) We first prove an auxiliary result.

Lemma. Fix a prime p and define the function $f(k)$ on positive integers by the conditions

$$\begin{aligned} f(1, p) &= 0 \\ f(k, p) &= \frac{(p-1)!}{(p-k)!} - kf(k-1, p) \quad (k > 1). \end{aligned}$$

Then for any positive integers a_1, \dots, a_k with $a_1 + \dots + a_k < p$, there are exactly $f(p)$ solutions to the equation $a_1x_1 + \dots + a_kx_k = 0$ with $x_1, \dots, x_k \in \mathbb{F}_p$ nonzero and pairwise distinct.

Proof. We check the claim by induction, with the base case $k = 1$ being obvious. For the induction step, assume the claim for $k-1$. Let S be the set of k -tuples of distinct elements of \mathbb{F}_p ; it consists of $\frac{p!}{(p-k)!}$ elements. This set is stable under the action of $i \in \mathbb{F}_p$ by translation:

$$(x_1, \dots, x_k) \mapsto (x_1 + i, \dots, x_k + i).$$

Since $0 < a_1 \cdots + a_k < p$, exactly one element of each orbit gives a solution of $a_1x_1 + \dots + a_kx_k = 0$. Each of these solutions contributes to $f(k)$ except for those in which $x_i = 0$ for

some i . Since then $x_j \neq 0$ for all $j \neq i$, we may apply the induction hypothesis to see that there are $f(k-1, p)$ solutions that arise this way for a given i (and these do not overlap). This proves the claim. \square

To compute $f(k, p)$ explicitly, it is convenient to work with the auxiliary function

$$g(k, p) = \frac{pf(k, p)}{k!};$$

by the lemma, this satisfies $g(1, p) = 0$ and

$$\begin{aligned} g(k, p) &= \binom{p}{k} - g(k-1, p) \\ &= \binom{p-1}{k} + \binom{p-1}{k-1} - g(k-1, p) \quad (k > 1). \end{aligned}$$

By induction on k , we deduce that

$$\begin{aligned} g(k, p) - \binom{p-1}{k} &= (-1)^{k-1} \left(g(1, p) - \binom{p-1}{1} \right) \\ &= (-1)^k (p-1) \end{aligned}$$

and hence $g(k, p) = \binom{p-1}{k} + (-1)^k (p-1)$.

We now set $p = 2017$ and count the tuples in question. Define c_0, \dots, c_{63} as in the first solution. Since $c_0 + \dots + c_{63} = p$, the translation action of \mathbb{F}_p preserves the set of tuples; we may thus assume without loss of generality that $x_0 = 0$ and multiply the count by p at the end. That is, the desired answer is

$$\begin{aligned} 2017f(63, 2017) &= 63!g(63, 2017) \\ &= 63! \left(\binom{2016}{63} - 2016 \right) \end{aligned}$$

as claimed.