Solutions to the 76th William Lowell Putnam Mathematical Competition
Saturday, December 5, 2015

Manjul Bhargava, Kiran Kedlaya, and Lenny Ng

A1 **First solution:** Without loss of generality, assume that A and B lie in the first quadrant with $A = (t_1, 1/t_1)$, $B = (t_2, 1/t_2)$, and $t_1 < t_2$. If $P = (t, 1/t)$ with $t_1 \leq t \leq t_2$, then the area of triangle APB is

$$\frac{1}{2}\begin{vmatrix} 1 & 1 & 1 \\ t_1 & t & t_2 \\ 1/t_1 & 1/t & 1/t_2 \end{vmatrix} = \frac{t_2 - t_1}{2t_1t_2}(t_1 + t_2 - t - t_1t_2/t).$$

When t_1, t_2 are fixed, this is maximized when $t + t_1t_2/t$ is minimized, which by AM-GM exactly holds when $t = \sqrt{t_1t_2}$.

The line AP is given by $y = \frac{t_1+t-x}{tt_1}$, and so the area of the region bounded by the hyperbola and AP is

$$\int_{t_1}^{t}\left(\frac{t_1 + t - x}{tt_1} - \frac{1}{x}\right)dx = \frac{t}{2t_1} - \frac{t_1}{2t} - \log\left(\frac{t}{t_1}\right),$$

which at $t = \sqrt{t_1t_2}$ is equal to $\frac{t_2-t_1}{2\sqrt{t_1t_2}} - \log(\sqrt{t_2/t_1})$. Similarly, the area of the region bounded by the hyperbola and PB is $\frac{t_2}{2t} - \frac{t}{2t_2} - \log\frac{t_2}{t}$, which at $t = \sqrt{t_1t_2}$ is also $\frac{t_2-t_1}{2\sqrt{t_1t_2}} - \log(\sqrt{t_2/t_1})$, as desired.

Second solution: For any $\lambda > 0$, the map $(x,y) \mapsto (\lambda x, \lambda^{-1}y)$ preserves both areas and the hyperbola $xy = 1$. We may thus rescale the picture so that A, B are symmetric across the line $y = x$, with A above the line. As P moves from A to B, the area of APB increases until P passes through the point $(1,1)$, then decreases. Consequently, $P = (1,1)$ achieves the maximum area, and the desired equality is obvious by symmetry. Alternatively, since the hyperbola is convex, the maximum is uniquely achieved at the point where the tangent line is parallel to AB, and by symmetry that point is P.

A2 **First solution:** One possible answer is 181. By induction, we have $a_n = ((2+\sqrt{3})^n + (2-\sqrt{3})^n)/2 = (\alpha^n + \beta^n)/2$ for all n, where $\alpha = 2+\sqrt{3}$ and $\beta = 2-\sqrt{3}$. Now note that if k is an odd positive integer and $a_n \neq 0$, then $\frac{a_{kn}}{a_n} = \frac{\alpha^{kn}+\beta^{kn}}{\alpha^n+\beta^n} = \alpha^{(k-1)n} - \alpha^{(k-2)n}\beta^n + \cdots - \alpha^n\beta^{(k-2)n} + \beta^{(k-1)n}$. This expression is both rational (because a_n and a_{kn} are integers) and of the form $a + b\sqrt{3}$ for some integers a, b by the expressions for α, β; it follows that it must be an integer, and so a_{kn} is divisible by a_n. Applying this to $n = 5$ and $k = 403$, we find that a_{2015} is divisible by $a_5 = 362$ and thus by 181.

Second solution: By rewriting the formula for a_n as $a_{n-2} = 4a_{n-1} - a_n$, we may extend the sequence backwards to define a_n for all integers n. Since $a_{-1} = 2$, we may see by induction that $a_{-n} = a_n$ for all n. For any integer m and any prime p dividing a_m, p also divides a_{-m}; on the other hand, p cannot divide a_{-m+1}, as otherwise p would also divide $a_{-m+2}, \dots, a_0 = 1$, a contradiction. We can thus find an integer k such that $a_{m+1} \equiv ka_{-m+1} \pmod{p}$; by induction on n, we see that $a_n \equiv ka_{n-2m} \pmod{p}$ for all n. In particular, if k is odd, then p also divides a_{km}; we thus conclude (again) that a_{2015} is divisible by $a_5 = 362$ and thus by 181.

Remark: Although it was not needed in the solution, we note in passing that if $a_n \equiv 0 \pmod{p}$, then $a_{2n+k} \equiv -a_k \pmod{p}$ for all k.

Remark: One can find other odd prime factors of a_{2015} in the same manner. For example, a_{2015} is divisible by each of the following quantities. (The prime factorizations were computed using the `Magma` computer algebra system.)

$$\begin{aligned}
a_{13} &= 2 \times 6811741 \\
a_{31} &= 2 \times 373 \times 360250962984637 \\
a_{5\cdot 13} &= 2 \times 181 \times 6811741 \\
&\quad \times 3045046274679316654761356161 \\
a_{5\cdot 31} &= 1215497709121 \times 28572709494917432101 \\
&\quad \times 13277360555506179816997827126375881581 \\
a_{13\cdot 31} &= 2 \times 373 \times 193441 \times 6811741 \times 360250962984637 \\
&\quad \times 16866100753000669 \\
&\quad \times 79988387992470656916594531961 \times p_{156}
\end{aligned}$$

where p_{156} is a prime of 156 decimal digits. Dividing a_{2015} by the product of the primes appearing in this list yields a number N of 824 decimal digits which is definitely not prime, because $2^N \not\equiv 2 \pmod{N}$, but whose prime factorization we have been unable to establish. Note that N is larger than a 2048-bit RSA modulus, so the difficulty of factoring it is not surprising.

One thing we can show is that each prime factor of N is congruent to 1 modulo $6 \times 2015 = 12090$, thanks to the following lemma.

Lemma. *Let n be an odd integer. Then any odd prime factor p of a_n which does not divide a_m for any divisor m of n is congruent to* 1 *modulo* $\operatorname{lcm}(6,n)$. *(By either solution of the original problem, p also does not divide a_m for any positive integer $m < n$.)*

Proof. We first check that $p \equiv 1 \pmod{3}$. In $\mathbb{F}_q = \mathbb{F}_p(\sqrt{3})$ we have $(\alpha/\beta)^n \equiv -1$. If $p \equiv 2 \pmod{3}$, then $q = p^2$ and α and β are conjugate in p; consequently, the equality $\alpha^n = -\beta^n$ in $\mathbb{F}_{q^2}$ means that $\alpha^n = c\sqrt{3}$, $\beta^n = -c\sqrt{3}$ for some $c \in \mathbb{F}_p$. But then $-3c^2 = \alpha^n\beta^n = 1$ in $\mathbb{F}_q$ and hence in $\mathbb{F}_p$, which contradicts $p \equiv 2 \pmod{3}$ by quadratic reciprocity.

By the previous paragraph, α and β may be identified with elements of $\mathbb{F}_p$, and we have $(\alpha/\beta)^n \equiv -1$, but the same does not hold with n replaced by any smaller value. Since $\mathbb{F}_p^\times$ is a cyclic group of order $p-1$, this forces $p \equiv 1 \pmod{n}$ as claimed. □

A3 The answer is 13725. We first claim that if n is odd, then $\prod_{b=1}^n (1+e^{2\pi iab/n}) = 2^{\gcd(a,n)}$. To see this, write $d = \gcd(a,n)$ and $a = da_1$, $n = dn_1$ with $\gcd(a_1,n_1) = 1$. Then $a_1, 2a_1, \dots, n_1a_1$ modulo n_1 is a permutation of $1, 2, \dots, n_1$ modulo n_1, and so $\omega^{a_1}, \omega^{2a_1}, \dots, \omega^{n_1a_1}$ is a permutation of $\omega, \omega^2, \dots, \omega^{n_1}$; it follows that for $\omega = e^{2\pi i/n_1}$,

$$\prod_{b=1}^{n_1}(1+e^{2\pi iab/n}) = \prod_{b=1}^{n_1}(1+e^{2\pi ia_1b/n_1}) = \prod_{b=1}^{n_1}(1+\omega^b).$$

Now since the roots of $z^{n_1}-1$ are $\omega, \omega^2, \dots, \omega^{n_1}$, it follows that $z^{n_1}-1 = \prod_{b=1}^{n_1}(z-\omega^b)$. Setting $z=-1$ and using the fact that n_1 is odd gives $\prod_{b=1}^{n_1}(1+\omega^b) = 2$.

Finally, $\prod_{b=1}^{n}(1+e^{2\pi iab/n}) = (\prod_{b=1}^{n_1}(1+e^{2\pi iab/n}))^d = 2^d$, and we have proven the claim.

From the claim, we find that

$$\begin{aligned}
&\log_2\left(\prod_{a=1}^{2015}\prod_{b=1}^{2015}(1+e^{2\pi iab/2015})\right) \\
&= \sum_{a=1}^{2015}\log_2\left(\prod_{b=1}^{2015}(1+e^{2\pi iab/2015})\right) \\
&= \sum_{a=1}^{2015}\gcd(a,2015).
\end{aligned}$$

Now for each divisor d of 2015, there are $\phi(2015/d)$ integers between 1 and 2015 inclusive whose gcd with 2015 is d. Thus

$$\sum_{a=1}^{2015}\gcd(a,2015) = \sum_{d|2015} d\cdot\phi(2015/d).$$

We factor $2015 = pqr$ with $p=5$, $q=13$, and $r=31$, and calculate

$$\begin{aligned}
&\sum_{d|pqr} d\cdot\phi(pqr/d) \\
&= 1\cdot(p-1)(q-1)(r-1) + p\cdot(q-1)(r-1) \\
&\quad + q\cdot(p-1)(r-1) + r\cdot(p-1)(q-1) + pq\cdot(r-1) \\
&\quad + pr\cdot(q-1) + qr\cdot(p-1) + pqr\cdot 1 \\
&= (2p-1)(2q-1)(2r-1).
\end{aligned}$$

When $(p,q,r) = (5,13,31)$, this is equal to 13725.

Remark: Noam Elkies suggests the following similar but shorter derivation of the equality $\prod_{b=1}^{n_1}(1+\omega^b) = 2$: write

$$\prod_{b=1}^{n_1-1}(1+\omega^b) = \frac{\prod_{b=1}^{n_1-1}(1-\omega^{2b})}{\prod_{b=1}^{n_1-1}(1-\omega^b)}$$

and note (as above) that $\omega^2, \omega^4, \dots, \omega^{2(n_1-1)}$ is a permutation of $\omega, \dots, \omega^{n_1-1}$, so the two products in the fraction are equal.

Remark: The function $f(n) = \sum_{d|n} d\cdot\phi(n/d)$ is multiplicative: for any two coprime positive integers m,n, we have $f(mn) = f(m)f(n)$. This follows from the fact that $f(n)$ is the convolution of the two multiplicative functions $n \mapsto n$ and $n \mapsto \phi(n)$; it can also be seen directly using the Chinese remainder theorem.

A4 The answer is $L = 4/7$. For $S \subset \mathbb{N}$, let $F(S) = \sum_{n\in S} 1/2^n$, so that $f(x) = F(S_x)$. Note that for $T = \{1,4,7,10,\dots\}$, we have $F(T) = 4/7$.

We first show by contradiction that for any $x \in [0,1)$, $f(x) \geq 4/7$. Since each term in the geometric series $\sum_n 1/2^n$ is equal to the sum of all subsequent terms, if S, S' are different subsets of $\mathbb{N}$ and the smallest positive integer in one of S, S' but not in the other is in S, then $F(S) \geq F(S')$. Assume $f(x) < 4/7$; then the smallest integer in one of S_x, T but not in the other is in T. Now $1 \in S_x$ for any $x \in [0,1)$, and we conclude that there are three consecutive integers $n, n+1, n+2$ that are not in S_x: that is, $\lfloor nx \rfloor$, $\lfloor (n+1)x \rfloor$, $\lfloor (n+2)x \rfloor$ are all odd. Since the difference between consecutive terms in nx, $(n+1)x$, $(n+2)x$ is $x < 1$, we conclude that $\lfloor nx \rfloor = \lfloor (n+1)x \rfloor = \lfloor (n+2)x \rfloor$ and so $x < 1/2$. But then $2 \in S_x$ and so $f(x) \geq 3/4$, contradicting our assumption.

It remains to show that $4/7$ is the greatest lower bound for $f(x)$, $x \in [0,1)$. For any n, choose $x = 2/3 - \varepsilon$ with $0 < \varepsilon < 1/(9n)$; then for $1 \leq k \leq n$, we have $0 < m\varepsilon < 1/3$ for $m \leq 3n$, and so

$$\begin{aligned}
\lfloor (3k-2)x \rfloor &= \lfloor (2k-2) + 2/3 - (3k-2)\varepsilon \rfloor = 2k-2 \\
\lfloor (3k-1)x \rfloor &= \lfloor (2k-1) + 1/3 - (3k-1)\varepsilon \rfloor = 2k-1 \\
\lfloor (3k)x \rfloor &= \lfloor (2k-1) + 1 - 3k\varepsilon \rfloor = 2k-1.
\end{aligned}$$

It follows that S_x is a subset of $S = \{1,4,7,\dots,3n-2,3n+1,3n+2,3n+3,\dots\}$, and so $f(x) = F(S_x) \leq f(S) = (1/2 + 1/2^4 + \cdots + 1/2^{3n+1}) + 1/2^{3n+1}$. This last expression tends to $4/7$ as $n \to \infty$, and so no number greater than $4/7$ can be a lower bound for $f(x)$ for all $x \in [0,1)$.

A5 **First solution:** By inclusion-exclusion, we have

$$\begin{aligned}
N_q &= \sum_{d|q} \mu(d) \left\lfloor \frac{\lfloor q/4 \rfloor}{d} \right\rfloor \\
&= \sum_{d|q} \mu(d) \left\lfloor \frac{q/d}{4} \right\rfloor \\
&\equiv \sum_{d|q \text{ squarefree}} \left\lfloor \frac{q/d}{4} \right\rfloor \pmod{2},
\end{aligned}$$

where μ is the Möbius function. Now

$$\left\lfloor \frac{q/d}{4} \right\rfloor \equiv \begin{cases} 0 \pmod{2} & \text{if } q/d \equiv 1,3 \pmod{8} \\ 1 \pmod{2} & \text{if } q/d \equiv 5,7 \pmod{8}. \end{cases}$$

So N_q is odd if and only if q has an odd number of squarefree factors d congruent to $5q$ or $7q$ (mod 8).

If q has a prime factor p congruent to 1 or 3 (mod 8), then the squarefree factors d of q occur in pairs c, pc, which are either both 1 or 3 (mod 8) or both 5 or 7 (mod 8). Hence q must have an even number of factors that are congruent to $5q$ or $7q$ (mod 8), and so N_q is even in this case.

If q has two prime factors p_1 and p_2, each congruent to either 5 or 7 (mod 8), then the squarefree factors d of q occur in quadruples $d, p_1 d, q_1 d, p_1 q_1 d$, which are then congruent respectively to some permutation of 1,3,5,7 (mod 8) (if p_1 and p_2 are distinct mod 8) or are congruent respectively to $d, p_1 d, p_1 d, d$ (mod 8). Either way, we see that exactly two of the four residues are congruent to $5q$ or $7q$ (mod 8). Thus again q must have an even number of factors that are $5q$ or $7q$ (mod 8), and so N_q is even in this case as well.

If $q = 1$, then $N_q = 0$ is even. The only case that remains is that $q = p^k$ is a positive power of a prime p congruent to 5 or 7 (mod 8). In this case, q has two squarefree factors, 1 and p, of which exactly one is congruent to $5q$ or $7q$ (mod 8). We conclude that N_q is odd in this case, as desired.

Second solution: Consider the set S of all integers in $\{1, \dots, q-1\}$ that are even and relatively prime to q. Then the product of all elements in S is

$$2^{\phi(q)/2} \prod_{\substack{1 \leq a \leq (q-1)/2 \\ (a,q)=1}} a.$$

On the other hand, we can rewrite the set of elements in $S \pmod q$ as a set T of residues in the interval $[-(q-1)/2, (q-1)/2]$. Then for each $1 \leq a \leq (q-1)/2$ with $(a,q) = 1$ contains exactly one element from $\{a, -a\}$: if $-2r = 2s$ for some $r, s \in \{1, \dots, (q-1)/2\}$, then $r \equiv -s \pmod q$, which is impossible given the ranges of r and s. Thus the product of all elements in T is

$$(-1)^n \prod_{\substack{1 \leq a \leq (q-1)/2 \\ (a,q)=1}} a,$$

where n denotes the number of elements of S greater than $(q-1)/2$. We conclude that $(-1)^n \equiv 2^{\phi(q)/2} \pmod q$.

However, note that the number of elements of S less than $(q-1)/2$ is N_q, by definition, so $\phi(q)/2 = N_q + n$; therefore, we obtain

$$(-1)^{N_q} \equiv (-1)^{\phi(q)/2} 2^{\phi(q)/2} = (-2)^{\phi(q)/2} \pmod q.$$

If $q = 1$, then N_q is even. If q has more than one prime factor, then the group $(\mathbb{Z}/q\mathbb{Z})^\times$ has exponent dividing $\phi(q)/2$, so $(-1)^{N_q} \equiv (-2)^{\phi(q)/2} \equiv 1 \pmod q$, and thus N_q must be even in this case as well. Finally, we assume that q is a prime power p^k with p odd and k positive. Since $(\mathbb{Z}/q\mathbb{Z})^\times$ is a cyclic group of order $\phi(q) = p^{k-1}(p-1)$, in which the only square roots of unity are ± 1, it follows that $(-2)^{\phi(q)/2} \equiv \pm 1 \pmod q$ in accordance with whether $(-2)^{(p-1)/2} \equiv \pm 1 \pmod p$, i.e., whether -2 is a quadratic residue or nonresidue. But recall that -2 is a quadratic residue modulo p if and only if $p \equiv 1, 3 \pmod 8$. Thus N_q is odd in this case if and only if $p \equiv 5$ or $7 \pmod 8$.

We conclude that for any odd integer $q \geq 1$, the quantity N_q is odd if and only if $q = p^k$ with k positive and p a prime that is 5 or 7 (mod 8).

Remark: The combination of the two solutions is close to one of Gauss's proofs of the law of quadratic reciprocity.

A6 **First solution:** (by Noam Elkies) Using row and column operations, we may construct invertible matrices U, V such that $U^{-1}MV$ is a block diagonal matrix of the form

$$\begin{pmatrix} I & 0 \\ 0 & 0 \end{pmatrix}.$$

Put $A' = U^{-1}AU, M' = U^{-1}MV, B' = V^{-1}BV$, $X' = V^{-1}XU$, so that $A'M' = M'B'$, $\det(A - MX) = \det(U^{-1}(A - MX)U) = \det(A' - M'X')$, and $\det(B - XM) = \det(V^{-1}(B - XM)V) = \det(B' - X'M')$. Form the corresponding block decompositions

$$A' = \begin{pmatrix} A_{11} & A_{12} \\ A_{21} & A_{22} \end{pmatrix}, B' = \begin{pmatrix} B_{11} & B_{12} \\ B_{21} & B_{22} \end{pmatrix}, X' = \begin{pmatrix} X_{11} & X_{12} \\ X_{21} & X_{22} \end{pmatrix}.$$

We then have

$$A'M' = \begin{pmatrix} A_{11} & 0 \\ A_{21} & 0 \end{pmatrix}, \qquad M'B' = \begin{pmatrix} B_{11} & B_{12} \\ 0 & 0 \end{pmatrix},$$

so we must have $A_{11} = B_{11}$ and $A_{21} = B_{12} = 0$; in particular, the characteristic polynomial of A is the product of the characteristic polynomials of A_{11} and A_{22}, and the characteristic polynomial of B is the product of the characteristic polynomials of B_{11} and B_{22}. Since $A_{11} = B_{11}$, it follows that A_{22} and B_{22} have the same characteristic polynomial. Since

$$X'M' = \begin{pmatrix} X_{11} & 0 \\ X_{21} & 0 \end{pmatrix}, \qquad M'X' = \begin{pmatrix} X_{11} & X_{12} \\ 0 & 0 \end{pmatrix},$$

we conclude that

$$\begin{aligned}
\det(A - MX) &= \det(A' - M'X') \\
&= \det \begin{pmatrix} A_{11} - X_{11} & A_{12} - X_{12} \\ 0 & A_{22} \end{pmatrix} \\
&= \det(A_{11} - X_{11}) \det(A_{22}) \\
&= \det(B_{11} - X_{11}) \det(B_{22}) \\
&= \det \begin{pmatrix} B_{11} - X_{11} & 0 \\ B_{21} - X_{21} & B_{22} \end{pmatrix} \\
&= \det(B' - X'M') \\
&= \det(B - XM),
\end{aligned}$$

as desired. (By similar arguments, $A-MX$ and $B-XM$ have the same characteristic polynomial.)

Second solution: We prove directly that $A-MX$ and $B-XM$ have the same characteristic polynomial, i.e., for any $t \in \mathbb{R}$, writing $A_t = A - tI$, $B_t = B - tI$, we have

$$\det(A_t - MX) = \det(B_t - XM).$$

For fixed A,B,M, the stated result is a polynomial identity in t and the entries of X. It thus suffices to check it assuming that A_t, B_t, X are all invertible. Since $AM = MB$, we also have $A_tM = MB_t$, so $A_tMB_t^{-1} = M$. Since $\det(A_t) = \det(B_t)$ by hypothesis,

$$\begin{aligned}
\det(A_t - MX) &= \det(A_t - A_tMB_t^{-1}X) \\
&= \det(A_t)\det(1 - MB_t^{-1}X) \\
&= \det(A_t)\det(X)\det(B_t)^{-1}\det(X^{-1}B_t - M) \\
&= \det(X)\det(X^{-1}B_t - M) \\
&= \det(B_t - XM).
\end{aligned}$$

Remark: One can also assert directly that $\det(1 - MB_t^{-1}X) = \det(1 - XMB_t^{-1})$ using the fact that for any square matrices U and V, UV and VU have the same characteristic polynomial; the latter is again proved by reducing to the case where one of the two matrices is invertible, in which case the two matrices are similar.

Third solution: (by Lev Borisov) We will check that for each positive integer k,

$$\operatorname{Trace}((A-MX)^k) = \operatorname{Trace}((B-XM)^k).$$

This will imply that $A-MX$ and $B-XM$ have the same characteristic polynomial, yielding the desired result.

We establish the claim by expanding both sides and comparing individual terms. By hypothesis, A^k and B^k have the same characteristic polynomial, so $\operatorname{Trace}(A^k) = \operatorname{Trace}(B^k)$. To compare the other terms, it suffices to check that for any sequence $i_1, i_2, \dots, i_m$ of nonnegative integers,

$$\begin{aligned}
&\operatorname{Trace}(A^{i_1}MXA^{i_2}MX\cdots A^{i_{m-1}}MXA^{i_m}) \\
&\quad = \operatorname{Trace}(B^{i_1}XMB^{i_2}XM\cdots B^{i_{m-1}}XMB^{i_m}).
\end{aligned}$$

To establish this equality, first apply the remark following the previous solution to write

$$\begin{aligned}
&\operatorname{Trace}(A^{i_1}MXA^{i_2}MX\cdots A^{i_{m-1}}MXA^{i_m}) \\
&\quad = \operatorname{Trace}(A^{i_m+i_1}MXA^{i_2}MX\cdots A^{i_{m-1}}MX).
\end{aligned}$$

Then apply the relation $AM = MB$ repeatedly to commute M past A, to obtain

$$\operatorname{Trace}(MB^{i_m+i_1}XMB^{i_2}XM\cdots XMB^{i_{m-1}}X).$$

Finally, apply the remark again to shift MB^{i_m} from the left end to the right end.

Remark: The conclusion holds with $\mathbb{R}$ replaced by an arbitrary field. In the second solution, one must reduce to the case of an infinite field, e.g., by replacing the original field with an algebraic closure. The third solution only applies to fields of characteristic 0 or positive characteristic greater than n.

Remark: It is tempting to try to reduce to the case where M is invertible, as in this case $A-MX$ and $B-XM$ are in fact similar. However, it is not clear how to make such an argument work.

B1 Let $g(x) = e^{x/2}f(x)$. Then g has at least 5 distinct real zeroes, and by repeated applications of Rolle's theorem, g', g'', g''' have at least $4,3,2$ distinct real zeroes, respectively. But

$$g'''(x) = \frac{1}{8}e^{x/2}(f(x) + 6f'(x) + 12f''(x) + 8f'''(x))$$

and $e^{x/2}$ is never zero, so we obtain the desired result.

B2 We will prove that 42015 is such a number in the sequence. Label the sequence of sums $s_0, s_1, \dots$, and let a_n, b_n, c_n be the summands of s_n in ascending order. We prove the following two statements for each nonnegative integer n:

(a)$_n$ The sequence

$$a_{3n}, b_{3n}, c_{3n}, a_{3n+1}, b_{3n+1}, c_{3n+1}, a_{3n+2}, b_{3n+2}, c_{3n+2}$$

is obtained from the sequence $10n+1, \dots, 10n+10$ by removing one of $10n+5, 10n+6, 10n+7$.

(b)$_n$ We have

$$\begin{aligned}
s_{3n} &= 30n+6, \\
s_{3n+1} &\in \{30n+15, 30n+16, 30n+17\}, \\
s_{3n+2} &= 30n+27.
\end{aligned}$$

These statements follow by induction from the following simple observations:

- by computing the table of values

n	a_n	b_n	c_n	s_n
0	1	2	3	6
1	4	5	7	16
2	8	9	10	27

  we see that (a)$_0$ holds;
- (a)$_n$ implies (b)$_n$;
- (a)$_n$ and (b)$_1$, …, (b)$_n$ together imply (a)$_{n+1}$.

To produce a value of n for which $s_n \equiv 2015 \pmod{10000}$, we take $n = 3m+1$ for some nonnegative integer m for which $s_{3m+1} = 30m+15$. We must also have $30m \equiv 2000 \pmod{10000}$, or equivalently $m \equiv 400 \pmod{1000}$. By taking $m = 1400$, we ensure that $m \equiv 2 \pmod 3$, so $s_m = 10m+7$; this ensures that s_n does indeed equal $30m+15 = 42015$, as desired.

Remark: With a bit more work, we can give a complete description of s_n, and in particular find the first term in the sequence whose decimal expansion ends in 2015. Define the function on nonnegative integers

$$f(n) = s_{3n+1} - (30n+16)$$

which takes values in $\{-1,0,1\}$; we then have

$$f(n) = \begin{cases} 0 & n \equiv 0 \pmod 3 \\ -f((n-1)/3) & n \equiv 1 \pmod 3 \\ -1 & n \equiv 2 \pmod 3. \end{cases}$$

Consequently, if we write n in base 3, then $f(n) = 0$ unless the expansion ends with 2 followed by a string of 1s of length $k \geq 0$, in which case $f(n) = (-1)^{k+1}$.

In this notation, we have $s_n \equiv 2015 \pmod{10000}$ if and only if $n = 3m+1$ for some nonnegative integer m for which $m \equiv 400 \pmod{1000}$ and $f(m) = -1$. Since $400 = 112211_{(3)}$, the first such term in the sequence is in fact $s_{1201} = 12015$.

B3 **First solution:** Any element of S can be written as $M = \alpha A + \beta B$, where $A = \left(\begin{smallmatrix} 1 & 1 \\ 1 & 1 \end{smallmatrix}\right)$, $B = \left(\begin{smallmatrix} -3 & -1 \\ 1 & 3 \end{smallmatrix}\right)$, and $\alpha, \beta \in \mathbb{R}$. Note that $A^2 = \left(\begin{smallmatrix} 4 & 4 \\ 4 & 4 \end{smallmatrix}\right)$ and $B^3 = \left(\begin{smallmatrix} -24 & -8 \\ 8 & 24 \end{smallmatrix}\right)$ are both in S, and so any matrix of the form αA or βB, $\alpha, \beta \in \mathbb{R}$, satisfies the given condition.

We claim that these are also the only matrices in S satisfying the given condition. Indeed, suppose $M = \alpha A + \beta B$ where $\alpha, \beta \neq 0$. Let $C = \left(\begin{smallmatrix} 1 & 1/\sqrt{2} \\ -1 & 1/\sqrt{2} \end{smallmatrix}\right)$ with inverse $C^{-1} = \left(\begin{smallmatrix} 1/2 & -1/2 \\ 1/\sqrt{2} & 1/\sqrt{2} \end{smallmatrix}\right)$. If we define $D = C^{-1}MC$, then $D = 2\alpha \left(\begin{smallmatrix} 0 & \gamma \\ \gamma & 1 \end{smallmatrix}\right)$ where $\gamma = -\frac{\beta\sqrt{2}}{\alpha}$. Now suppose that M^k is in S with $k \geq 2$. Since $\left(\begin{smallmatrix} 1 & -1 \end{smallmatrix}\right) A \left(\begin{smallmatrix} 1 \\ -1 \end{smallmatrix}\right) = \left(\begin{smallmatrix} 1 & -1 \end{smallmatrix}\right) B \left(\begin{smallmatrix} 1 \\ -1 \end{smallmatrix}\right) = 0$, we have $\left(\begin{smallmatrix} 1 & -1 \end{smallmatrix}\right) M^k \left(\begin{smallmatrix} 1 \\ -1 \end{smallmatrix}\right) = 0$, and so the upper left entry of $C^{-1}M^kC = D^k$ is 0. On the other hand, from the expression for D, an easy induction on k shows that $D^k = (2\alpha)^k \left(\begin{smallmatrix} \gamma^2 p_{k-1} & \gamma p_k \\ \gamma p_k & p_{k+1} \end{smallmatrix}\right)$, where p_k is defined inductively by $p_0 = 0$, $p_1 = 1$, $p_{k+2} = \gamma^2 p_k + p_{k+1}$. In particular, it follows from the inductive definition that $p_k > 0$ when $k \geq 1$, whence the upper left entry of D^k is nonzero when $k \geq 2$, a contradiction.

Remark: A variant of this solution can be obtained by diagonalizing the matrix M.

Second solution: If a,b,c,d are in arithmetic progression, then we may write

$$a = r-3s, b = r-s, c = r+s, d = r+3s$$

for some r,s. If $s = 0$, then clearly all powers of M are in S. Also, if $r = 0$, then one easily checks that M^3 is in S.

We now assume $rs \neq 0$, and show that in that case M cannot be in S. First, note that the characteristic polynomial of M is $x^2 - 2rx - 8s^2$, and since M is nonsingular (as $s \neq 0$), this is also the minimal polynomial of M by the Cayley-Hamilton theorem. By repeatedly using the relation $M^2 = 2rM + 8s^2I$, we see that for each positive integer, we have $M^k = t_kM + u_kI$ for unique real constants t_k, u_k (uniqueness follows from the independence of M and I). Since M is in S, we see that M^k lies in S only if $u_k = 0$.

On the other hand, we claim that if $k > 1$, then $rt_k > 0$ and $u_k > 0$ if k is even, and $t_k > 0$ and $ru_k > 0$ if k is odd (in particular, u_k can never be zero). The claim is true for $k = 2$ by the relation $M^2 = 2rM + 8s^2I$. Assuming the claim for k, and multiplying both sides of the relation $M^k = t_kM + u_kI$ by M, yields

$$M^{k+1} = t_k(2rM + 8s^2I) + u_kM = (2rt_k + u_k)M + 8s^2t_kI,$$

implying the claim for $k+1$.

Remark: (from `artofproblemsolving.com`, user `hoeij`) Once one has $u_k = 0$, one can also finish using the relation $M \cdot M^k = M^k \cdot M$.

B4 **First solution:** The answer is $17/21$. For fixed b,c, there is a triangle of side lengths a,b,c if and only if $|b-c| < a < b+c$. It follows that the desired sum is

$$S = \sum_{b,c} \frac{1}{3^b5^c} \left(\sum_{a=|b-c|+1}^{b+c-1} 2^a \right) = \sum_{b,c} \frac{2^{b+c} - 2^{|b-c|+1}}{3^b5^c}.$$

We write this as $S = S_1 + S_2$ where S_1 sums over positive integers b,c with $b \leq c$ and S_2 sums over $b > c$. Then

$$\begin{aligned} S_1 &= \sum_{b=1}^{\infty} \sum_{c=b}^{\infty} \frac{2^{b+c} - 2^{c-b+1}}{3^b5^c} \\ &= \sum_{b=1}^{\infty} \left(\left(\left(\frac{2}{3}\right)^b - \frac{2}{6^b} \right) \sum_{c=b}^{\infty} \left(\frac{2}{5}\right)^c \right) \\ &= \sum_{b=1}^{\infty} \left(\left(\frac{2}{3}\right)^b - \frac{2}{6^b} \right) \frac{5}{3} \left(\frac{2}{5}\right)^b \\ &= \sum_{b=1}^{\infty} \left(\frac{5}{3} \left(\frac{4}{15}\right)^b - \frac{10}{3} \left(\frac{1}{15}\right)^b \right) \\ &= \frac{85}{231}. \end{aligned}$$

Similarly,

$$
\begin{aligned}
S_2 &= \sum_{c=1}^{\infty}\sum_{b=c+1}^{\infty} \frac{2^{b+c}-2^{b-c+1}}{3^b 5^c} \\
&= \sum_{c=1}^{\infty} \left(\left(\left(\frac{2}{5}\right)^c - \frac{2}{10^c} \right) \sum_{b=c+1}^{\infty} \left(\frac{2}{3}\right)^b \right) \\
&= \sum_{c=1}^{\infty} \left(\left(\frac{2}{5}\right)^c - \frac{2}{10^c} \right) 3 \left(\frac{2}{3}\right)^{c+1} \\
&= \sum_{c=1}^{\infty} \left(2\left(\frac{4}{15}\right)^c - 4\left(\frac{1}{15}\right)^c \right) \\
&= \frac{34}{77}.
\end{aligned}
$$

We conclude that $S = S_1 + S_2 = \frac{17}{21}$.

Second solution: Recall that the real numbers a,b,c form the side lengths of a triangle if and only if

$$
s-a, s-b, s-c > 0 \qquad s = \frac{a+b+c}{2},
$$

and that if we put $x = 2(s-a), y = 2(s-b), z = 2(s-c)$,

$$
a = \frac{y+z}{2}, b = \frac{z+x}{2}, c = \frac{x+y}{2}.
$$

To generate all *integer* triples (a,b,c) which form the side lengths of a triangle, we must also assume that x,y,z are either all even or all odd. We may therefore write the original sum as

$$
\sum_{x,y,z>0 \text{ odd}} \frac{2^{(y+z)/2}}{3^{(z+x)/2}5^{(x+y)/2}} + \sum_{x,y,z>0 \text{ even}} \frac{2^{(y+z)/2}}{3^{(z+x)/2}5^{(x+y)/2}}.
$$

To unify the two sums, we substitute in the first case $x = 2u+1, y = 2v+1, z = 2w+1$ and in the second case $x = 2u+2, y = 2v+2, z = 2w+2$ to obtain

$$
\begin{aligned}
\sum_{(a,b,c)\in T} \frac{2^a}{3^b 5^c} &= \sum_{u,v,w=1}^{\infty} \frac{2^{v+w}}{3^{w+u}5^{u+v}} \left(1 + \frac{2^{-1}}{3^{-1}5^{-1}}\right) \\
&= \frac{17}{2} \sum_{u=1}^{\infty} \left(\frac{1}{15}\right)^u \sum_{v=1}^{\infty} \left(\frac{2}{5}\right)^v \sum_{w=1}^{\infty} \left(\frac{2}{3}\right)^w \\
&= \frac{17}{2} \frac{1/15}{1-1/15} \frac{2/5}{1-2/5} \frac{2/3}{1-2/3} \\
&= \frac{17}{21}.
\end{aligned}
$$

B5 The answer is 4.

We write the permutations π counted by P_n as sequences $\pi(1), \pi(2), \dots, \pi(n)$. Let U_n be the number of permutations counted by P_n that end with $n-1, n$; let V_n be the number ending in $n, n-1$; let W_n be the number starting with $n-1$ and ending in $n-2, n$; let T_n be the number ending in $n-2, n$ but not starting with $n-1$; and let S_n be the number which has $n-1, n$ consecutively in that order, but not at the beginning or end. It is clear that every permutation π counted by P_n either lies in exactly one of the sets counted by U_n, V_n, W_n, T_n, S_n, or is the reverse of such a permutation. Therefore

$$
P_n = 2(U_n + V_n + W_n + T_n + S_n).
$$

By examining how each of the elements in the sets counted by $U_{n+1}, V_{n+1}, W_{n+1}, T_{n+1}, S_{n+1}$ can be obtained from a (unique) element in one of the sets counted by U_n, V_n, W_n, T_n, S_n by suitably inserting the element $n+1$, we obtain the recurrence relations

$$
\begin{aligned}
U_{n+1} &= U_n + W_n + T_n, \\
V_{n+1} &= U_n, \\
W_{n+1} &= W_n, \\
T_{n+1} &= V_n, \\
S_{n+1} &= S_n + V_n.
\end{aligned}
$$

Also, it is clear that $W_n = 1$ for all n. Therefore,

$$
\begin{aligned}
P_{n+5} &= 2(U_{n+5} + V_{n+5} + W_{n+5} + T_{n+5} + S_{n+5}) \\
&= 2((U_{n+4} + W_{n+4} + T_{n+4}) + U_{n+4} \\
&\qquad + W_{n+4} + V_{n+4} + (S_{n+4} + V_{n+4})) \\
&= P_{n+4} + 2(U_{n+4} + W_{n+4} + V_{n+4}) \\
&= P_{n+4} + 2((U_{n+3} + W_{n+3} + T_{n+3}) + W_{n+3} + U_{n+3}) \\
&= P_{n+4} + P_{n+3} + 2(U_{n+3} - V_{n+3} + W_{n+3} - S_{n+3}) \\
&= P_{n+4} + P_{n+3} + 2((U_{n+2} + W_{n+2} + T_{n+2}) - U_{n+2} \\
&\qquad + W_{n+2} - (S_{n+2} - V_{n+2})) \\
&= P_{n+4} + P_{n+3} + 2(2W_{n+2} + T_{n+2} - S_{n+2} - V_{n+2}) \\
&= P_{n+4} + P_{n+3} + 2(2W_{n+1} + V_{n+1} \\
&\qquad - (S_{n+1} + V_{n+1}) - U_{n+1}) \\
&= P_{n+4} + P_{n+3} + 2(2W_n + U_n - (S_n + V_n) - U_n \\
&\qquad - (U_n + W_n + T_n)) \\
&= P_{n+4} + P_{n+3} - P_n + 4,
\end{aligned}
$$

as desired.

Remark: There are many possible variants of the above solution obtained by dividing the permutations up according to different features. For example, Karl Mahlburg suggests writing

$$
P_n = 2P'_n, \qquad P'_n = Q'_n + R'_n
$$

where P'_n counts those permutations counted by P_n for which 1 occurs before 2, and Q'_n counts those permutations counted by P'_n for which $\pi(1) = 1$. One then has the recursion

$$
Q'_n = Q'_{n-1} + Q'_{n-3} + 1
$$

corresponding to the cases where $\pi(1), \pi(2) = 1, 2$; where $\pi(1), \pi(2), \pi(3) = 1, 3, 2$; and the unique case $1, 3, 5, \dots, 6, 4, 2$. Meanwhile, one has

$$
R'_n = R'_{n-1} + Q'_{n-2}
$$

corresponding to the cases containing $3,1,2,4$ (where removing 1 and reversing gives a permutation counted by R'_{n-1}); and where 4 occurs before $3,1,2$ (where removing $1,2$ and reversing gives a permutation counted by Q'_{n-2}).

Remark: The permutations counted by P_n are known as *key permutations*, and have been studied by E.S. Page, Systematic generation of ordered sequences using recurrence relations, *The Computer Journal* **14** (1971), no. 2, 150–153. We have used the same notation for consistency with the literature. The sequence of the P_n also appears as entry A003274 in the On-line Encyclopedia of Integer Sequences (`http://oeis.org`).

B6 (from `artofproblemsolving.com`) We will prove that the sum converges to $\pi^2/16$. Note first that the sum does not converge absolutely, so we are not free to rearrange it arbitrarily. For that matter, the standard alternating sum test does not apply because the absolute values of the terms does not decrease to 0, so even the convergence of the sum must be established by hand.

Setting these issues aside momentarily, note that the elements of the set counted by $A(k)$ are those odd positive integers d for which $m = k/d$ is also an integer and $d < \sqrt{2dm}$; if we write $d = 2\ell - 1$, then the condition on m reduces to $m \geq \ell$. In other words, the original sum equals

$$S_1 := \sum_{k=1}^{\infty} \sum_{\substack{\ell \geq 1, m \geq \ell \\ k = m(2\ell-1)}} \frac{(-1)^{m-1}}{m(2\ell-1)},$$

and we would like to rearrange this to

$$S_2 := \sum_{\ell=1}^{\infty} \frac{1}{2\ell-1} \sum_{m=\ell}^{\infty} \frac{(-1)^{m-1}}{m},$$

in which both sums converge by the alternating sum test. In fact a bit more is true: we have

$$\left| \sum_{m=\ell}^{\infty} \frac{(-1)^{m-1}}{m} \right| < \frac{1}{\ell},$$

so the outer sum converges absolutely. In particular, S_2 is the limit of the truncated sums

$$S_{2,n} = \sum_{\ell(2\ell-1) \leq n} \frac{1}{2\ell-1} \sum_{m=\ell}^{\infty} \frac{(-1)^{m-1}}{m}.$$

To see that S_1 converges to the same value as S_2, write

$$S_{2,n} - \sum_{k=1}^{n} (-1)^{k-1} \frac{A(k)}{k} = \sum_{\ell(2\ell-1) \leq n} \frac{1}{2\ell-1} \sum_{m = \lfloor \frac{n}{2\ell-1} + 1 \rfloor}^{\infty} \frac{(-1)^{m-1}}{m}.$$

The expression on the right is bounded above in absolute value by the sum $\sum_{\ell(2\ell-1) \leq n} \frac{1}{n}$, in which the number of summands is at most $\sqrt{n}$ (since $\sqrt{n}(2\sqrt{n}-1) \geq n$), and so the total is bounded above by $1/\sqrt{n}$. Hence the difference converges to zero as $n \to \infty$; that is, S_1 converges and equals S_2.

We may thus focus hereafter on computing S_2. We begin by writing

$$S_2 = \sum_{\ell=1}^{\infty} \frac{1}{2\ell-1} \sum_{m=\ell}^{\infty} (-1)^{m-1} \int_0^1 t^{m-1}\,dt.$$

Our next step will be to interchange the inner sum and the integral, but again this requires some justification.

Lemma 1. *Let $f_0, f_1, \dots$ be a sequence of continuous functions on $[0,1]$ such that for each $x \in [0,1]$, we have*

$$f_0(x) \geq f_1(x) \geq \cdots \geq 0.$$

Then

$$\sum_{n=0}^{\infty} (-1)^n \int_0^1 f_n(t)\,dt = \int_0^1 \left(\sum_{n=0}^{\infty} (-1)^n f_n(t) \right) dt$$

provided that both sums converge.

Proof. Put $g_n(t) = f_{2n}(t) - f_{2n+1}(t) \geq 0$; we may then rewrite the desired equality as

$$\sum_{n=0}^{\infty} \int_0^1 g_n(t)\,dt = \int_0^1 \left(\sum_{n=0}^{\infty} g_n(t) \right) dt,$$

which is a case of the Lebesgue monotone convergence theorem. □

By Lemma 1, we have

$$\begin{aligned} S_2 &= \sum_{\ell=1}^{\infty} \frac{1}{2\ell-1} \int_0^1 \left(\sum_{m=\ell}^{\infty} (-1)^{m-1} t^{m-1} \right) dt \\ &= \sum_{\ell=1}^{\infty} \frac{1}{2\ell-1} \int_0^1 \frac{(-t)^{\ell-1}}{1+t}\,dt. \end{aligned}$$

Since the outer sum is absolutely convergent, we may freely interchange it with the integral:

$$\begin{aligned} S_2 &= \int_0^1 \left(\sum_{\ell=1}^{\infty} \frac{1}{2\ell-1} \frac{(-t)^{\ell-1}}{1+t} \right) dt \\ &= \int_0^1 \frac{1}{\sqrt{t}(1+t)} \left(\sum_{\ell=1}^{\infty} \frac{(-1)^{\ell-1} t^{\ell-1/2}}{2\ell-1} \right) dt \\ &= \int_0^1 \frac{1}{\sqrt{t}(1+t)} \arctan(\sqrt{t})\,dt \\ &= \int_0^1 \frac{2}{1+u^2} \arctan(u)\,du \qquad (u = \sqrt{t}) \\ &= \arctan(1)^2 - \arctan(0)^2 = \frac{\pi^2}{16}. \end{aligned}$$