Proof Round 2024-2025 Solutions

Problem 1. **[5]** Does there exist a prime p and distinct positive integers y_1, y_2, y_3 with $y_i < \frac{p}{3}$ for each $1 \leq i \leq 3$ and $y_1^3 \equiv y_2^3 \equiv y_3^3 \pmod{p}$?

Proposed by Samuel Goodman

Solution: Note that $y_1, y_2, y_3 \not\equiv 0 \pmod{p}$. So if $y_1^3 \equiv y_2^3 \equiv y_3^3 \pmod{p}$, then $\left(\frac{y_2}{y_1}\right)^3 \equiv \left(\frac{y_3}{y_1}\right)^3 \equiv 1 \pmod{p}$. Thus, $y_2 y_1^{-1}$ and $y_3 y_1^{-1}$ are distinct nonzero cube roots of 1 in $\pmod{p}$.
We claim that if $p \equiv 1 \pmod{3}$ then there are exactly three cube roots of 1 in $\pmod{p}$, and they are $1, \alpha, \alpha^2$ for some residue α, and if $p \not\equiv 1 \pmod{3}$ then the only cube root of 1 in $\pmod{p}$ is 1. This is because of primitive roots; if g is a primitive root $\pmod{p}$ and $p \neq 3$ then $g^{p-1} \equiv 1 \pmod{3}$, so if $p \equiv 1 \pmod{3}$ then the cube roots of 1 are $1, g^{\frac{p-1}{3}}, g^{2 \cdot \frac{p-1}{3}}$, and if $p \not\equiv 1 \pmod{3}$ then the only cube root of 1 in $\pmod{p}$ is 1.
Thus, assuming that $p \equiv 1 \pmod{3}$, we must have $\{y_2 y_1^{-1}, y_3 y_1^{-1}\} = \{\alpha, \alpha^2\}$. So,

$$y_1 + y_2 + y_3 = y_1(1 + \alpha + \alpha^2) = y_1\left(\frac{\alpha^3 - 1}{\alpha - 1}\right).$$

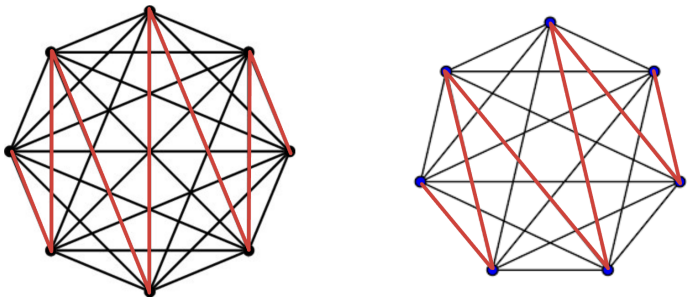
$\alpha \neq 1$ and $\alpha^3 = 1$ since α is a cube root of unity in $\pmod{p}$, so $y_1 + y_2 + y_3 \equiv 0 \pmod{p}$. If $0 < y_1, y_2, y_3 < \frac{p}{3}$, then $0 < y_1 + y_2 + y_3 < p$, so it is impossible for $y_1 + y_2 + y_3 \equiv 0 \pmod{p}$. Thus, the answer is no.

Problem 2. **[5]** The n vertices of a regular n-gon are drawn, and each of the $\binom{n}{2}$ edges between them is colored such that no two edges of the same color intersect at a point which is not a vertex of the n-gon. What is the minimum number of different colors that can be used to color all the edges?

Proposed by Vivian Loh

Solution: The answer is $\lceil \frac{n}{2} \rceil$. First we will show that we need $\geq \lceil \frac{n}{2} \rceil$ colors. For n even, consider the $\frac{n}{2}$ longest diagonals (that go through the center of the n-gon); all of these intersect each other so they must be different colors. For n odd, consider the n longest diagonals, which form a star. Let two of these diagonals be called "adjacent" if they are adjacent edges of the star, AKA they share a vertex of the n-gon. Then all non-adjacent pairs of diagonals among these n longest diagonals intersect each other, so if two of them are the same color then they must be adjacent. This implies that we need $\geq \lceil \frac{n}{2} \rceil$ colors.

Now for the construction; we will show that $\lceil \frac{n}{2} \rceil$ colors is enough. Consider the following zigzag sequences of $n-1$ edges, drawn in red, for the $n = 8$ and $n = 7$ cases.



For n even, we can overlay $\frac{n}{2}$ of them (the original, its rotation by $\frac{360}{n}^\circ$, its rotation by $2 \cdot \frac{360}{n}^\circ$, ..., its rotation by $(\frac{n}{2}-1)\frac{360}{n}^\circ$), and have each copy be a different color. For n odd, we can overlay $\frac{n-1}{2}$ of these zigzag paths (rotation by 0° through rotation by $\left(\frac{n-3}{2}\right)\frac{360}{n}^\circ$) in the same way as for the n even case, and then the last $\frac{n-1}{2}$ edges, which make up half of a "copy" themselves, will be colored with the $\left(\frac{n+1}{2}\right)$th color.

So, it is possible to use just $\lceil \frac{n}{2} \rceil$ colors, but we also must use at least this many, and so $\boxed{\lceil \frac{n}{2} \rceil}$ is the answer.

Problem 3. [10] Let p be a prime and S be the set of positive integers m such that the only factors of m which are congruent to $1 \pmod p$ are 1 and m. Suppose we have some $m \in S$ such that m has $p-1$ distinct prime factors. Show that $m = q_1 \cdots q_{p-1}$ for distinct primes $q_1, \cdots, q_{p-1}$ such that $q_1 \equiv \cdots \equiv q_{p-1} \mod p$.

Proposed by Samuel Goodman

Solution: Since m has $p-1$ distinct prime factors, $m = q_1^{e_1} q_2^{e_2} \cdots q_{p-1}^{e_{p-1}}$ for some exponents $e_1, e_2, \ldots, e_{p-1} \geq 1$. We claim that $e_1 = e_2 = \cdots = e_{p-1}$. Consider the sequence $1, q_1, \ldots, q_1^{e_1}, q_1^{e_1} q_2, \ldots, q_1^{e_1} q_2^{e_2}, \ldots, m$. Each term in this sequence is a multiple of all the terms before it, and there are exactly $1 + e_1 + e_2 + \cdots + e_{p-1}$ terms in this sequence. Consider the representation of each nonzero residue $\pmod p$ as a power of g, where g is a primitive root $\pmod g$. Then the nonzero residues are $g, g^2, \ldots, g^{p-1} = 1$ in some order. Since none of the terms of the sequence are $\equiv 0 \pmod p$, if two different terms of the sequence are congruent $\pmod p$, then their quotient is $\equiv 1 \pmod p$. Note that their quotient would be a factor of m. So, the only terms of the sequence which can be congruent $\pmod p$ are the first and last terms, which by Pigeonhole implies that the sequence has at most p terms total, or $e_1 = e_2 = \cdots = e^{p-1} = 1$.

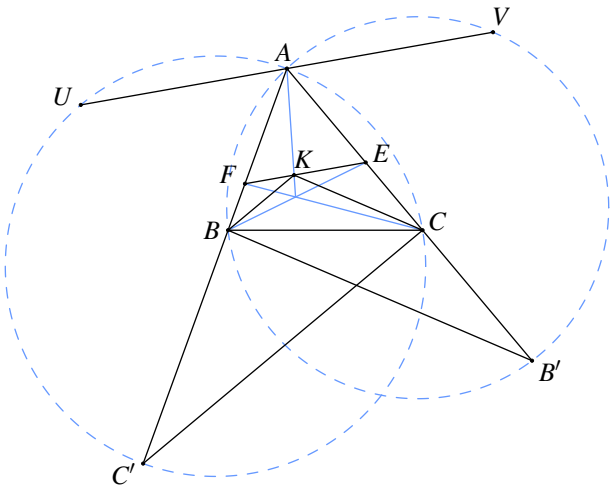
Now we will show that $q_1 \equiv q_2 \equiv \cdots \equiv q_{p-1} \pmod p$. For all $1 \leq i \leq p-1$, let $q_i = g^{a_i}$, where $1 \leq a_i \leq p-1$. Then $m = g^{a_1} g^{a_2} \cdots g^{a_{p-1}}$. Consider the sequence from before, which is now $1, q_1, q_1 q_2, \ldots, m$. We will now show that if the a_i's aren't all the same $\pmod{p-1}$, then we can find some subset of the a_i's that add to 0 $\pmod{p-1}$. If the a_i's are not all congruent $\pmod{p-1}$, then we can find two different ones. Without loss of generality, these correspond to a_1 and a_2. (We can just reorder the q_i's so that this is true.) By Pigeonhole, $1 \equiv m \equiv 1 \pmod p$ and the other $p-2$ terms in between cover each residue from g^1 through g^{p-2} once each. So, one of $\{a_1 + a_2, a_1 + a_2 + a_3, \ldots, a_1 + a_2 + \cdots + a_{p-2}\}$ must be $\equiv a_2 \pmod{p-1}$. Note that it cannot be a_1 or 0 or $a_1 + a_2 + \cdots + a_{p-1}$, since $a_2 \not\equiv 0 \pmod{p-1}$ (or else we would have $q_2 \equiv 1 \pmod p$). So, there is some $2 \leq x \leq p-2$ such that $a_1 + a_2 + \cdots + a_x \equiv a_2 \pmod{p-1}$. Now we can simply subtract a_2 from $a_1 + a_2 + \cdots + a_x$ to obtain $a_1 + a_3 + a_4 + \cdots + a_x \equiv 0 \pmod{p-1}$, and thus $q_1 q_3 q_4 \cdots q_x \equiv 1 \pmod p$. Thus, if the a_i's aren't all congruent $\pmod{p-1}$, (which is equivalent to the q_i's being congruent $\pmod p$), then m has a factor other than 1 and m which is $\equiv 1 \pmod p$, contradiction.

Clearly, it works if $m = q_1 q_2 \cdots q_{p-1}$ where $q_1 \equiv q_2 \equiv \cdots \equiv q_{p-1} \equiv g$ for some primitive root $g \pmod p$, because then the smallest power of g which is $\equiv 1 \pmod p$ is g^{p-1}, so the only factors of m which are 1 $\pmod p$ would be those with 0 or $p-1$ prime factors, which are precisely 1 and m.

Problem 4. **[10]** In triangle ABC, points E and F are chosen on sides AC and AB respectively such that $AE = AF$. Point K is on segment EF such that AK, BE, and CF intersect at a point, and points B' and C' are on lines AC and AB such that $BB' \parallel CK$ and $CC' \parallel BK$. Points U and V are on the line through A parallel to EF such that $UC = UC'$ and $VB = VB'$. Prove that $AU = AV$.

Proposed by Vivian Loh

Solution: We first claim that $UACC'$ and $VABB'$ are cyclic. This is true because the external bisector of $\angle BAC$ intersects (ACC') at the midpoint of major arc $\widehat{CAC'}$, which is U. Next, we claim that $\triangle UAC \sim \triangle BFK$. This is true because $\angle AUC = \angle AC'C = \angle FBK$, and $\angle UAC = \angle BFK$. So, $AU = BF \cdot \frac{AC}{FK}$, and similarly $AV = EC \cdot \frac{AB}{EK}$, so we just have to show that $BF \cdot \frac{AC}{FK} = EC \cdot \frac{AB}{EK}$. By Ceva on $\triangle ABC$ and then the Ratio Lemma on $\triangle AEF$ and $\triangle ABC$, $\frac{FK}{KE} = \frac{BF}{EC} \cdot \frac{AC}{AB}$, which finishes the problem.



Problem 5. [10] Let $\mathbb{Q}$ denote the set of rational numbers. Suppose $f : \mathbb{Q} \to \mathbb{Q}$ is a function that satisfies $0 < |f(x) - f(y)| \leqslant |x - y|$ for all $x \neq y \in \mathbb{Q}$. Must f be monotonic?

A function f is increasing if $f(x) < f(y)$ whenever $x < y$. A function f is monotonic if either f or $-f$ is increasing.

Proposed by Justin Lee

Solution: The answer is no. Consider the function

$$f(x) = \begin{cases} \frac{1}{2}\left(\frac{1}{1+x}\right)^2 & \text{if } x > 3-2\sqrt{2} \\ \frac{1}{4}\left(\frac{1}{1-x}\right)^2 & \text{if } x < 3-2\sqrt{2} \end{cases}$$

with its domain extended to all real numbers. Clearly, $f(x)$ is rational for any rational x. Now we shall show that for any real numbers x and y, we have $|f(x) - f(y)| \leqslant |x - y|$. We first show that this holds in the case where $y > x \geqslant 3 - 2\sqrt{2}$. Note that

$$f(x) - f(y) = \frac{1}{2}\left(\left(\frac{1}{1+x}\right)^2 - \left(\frac{1}{1+y}\right)^2\right) = \frac{1}{2}\left(\frac{1}{1+x} + \frac{1}{1+y}\right)\left(\frac{1}{1+x} - \frac{1}{1+y}\right)$$

Since $\frac{1}{1+y} < \frac{1}{1+x} \leqslant \frac{2+\sqrt{2}}{4}$, it follows that

$$f(x) - f(y) = \frac{1}{2}\left(\frac{1}{1+x} + \frac{1}{1+y}\right)\left(\frac{y-x}{(1+x)(1+y)}\right) \leqslant \left(\frac{2+\sqrt{2}}{4}\right)^3 (y-x) < y - x$$

Now we consider the case where $x < y \leqslant 3 - 2\sqrt{2}$. As before, note that

$$f(y) - f(x) = \frac{1}{4}\left(\left(\frac{1}{1-y}\right)^2 - \left(\frac{1}{1-x}\right)^2\right) = \frac{1}{4}\left(\frac{1}{1-x} + \frac{1}{1-y}\right)\left(\frac{1}{1-y} - \frac{1}{1-x}\right)$$

Since $\frac{1}{1-x} < \frac{1}{1-y} \leqslant \frac{1+\sqrt{2}}{2}$, it follows that

$$f(x) - f(y) = \frac{1}{4}\left(\frac{1}{1-x} + \frac{1}{1-y}\right)\left(\frac{y-x}{(1-x)(1-y)}\right) \leqslant \frac{1}{2} \cdot \left(\frac{1+\sqrt{2}}{2}\right)^3 (y-x) < y - x$$

In the case where $x \leqslant 3 - 2\sqrt{2} \leqslant y$, we have that

$$\begin{aligned} |f(x) - f(y)| &\leqslant |f(x) - f(3-2\sqrt{2})| + |f(3-2\sqrt{2}) - f(y)| \\ &\leqslant |(x - (3-2\sqrt{2}))| + |(3-2\sqrt{2} - y)| \\ &= |x - y| \end{aligned}$$

Lastly, it remains to show that for any rational numbers $r \neq s$, we have $f(r) \neq f(s)$. Indeed, $f(x)$ is increasing for $x < 3 - 2\sqrt{2}$ and decreasing for $x > 3 - 2\sqrt{2}$, so $f(r) \neq f(s)$ if both r and s are less than $3 - 2\sqrt{2}$, or both are greater than $3 - 2\sqrt{2}$. On the other hand, if WLOG $r < 3 - 2\sqrt{2} < s$, then

$$\frac{f(r)}{f(s)} = \frac{1}{2}\left(\frac{1+s}{1-r}\right)^2 \neq 1$$

since 2 is not the square of a rational number. This completes the proof.

Problem 6. **[15]** Let a, b, c, and d be positive integers such that

- $ab = c^2 + d$
- $2c \mid a - b$
- $cd < a - b$

Prove that d is a perfect square.

Proposed by Justin Lee

Solution: Let $a-b = 2ck$ and $a+b = 2x$. Then we have that $(a+b)^2 = (a-b)^2 + 4ab \implies x^2 = (ck)^2 + c^2 + d$, which we shall rearrange to $x^2 - (k^2+1)c^2 = d$. Fix the values of k and d. We have that $d < 2k$.

Claim. If (x,c) satisfies $x^2 - (k^2+1)c^2 = d$ then so does the pair $(|2k^2+1)x - 2k(k^2+1)c|, |(2k^2+1)c - 2kx|)$, and moreover, when $c \geqslant k$, this new pair is smaller than (x,c).

Proof. The first part is direct algebra. To show the second part, we shall show that $-c < (2k^2+1)c - 2kx < c$. The second inequality follows from $x = \sqrt{(k^2+1)c^2 + d} > kc$, and the first inequality holds because

$$\begin{aligned} &\left(1 + \tfrac{1}{k^2}\right) c^2 > k^2 \\ \implies &\left(\left(k + \tfrac{1}{k}\right) c\right)^2 > (k^2+1)c^2 + k^2 \\ \implies &\left(k + \tfrac{1}{k}\right) c > x \end{aligned}$$

as desired. □

Now notice that no solution (x,c) with $0 < c < k$ exists because $(kc)^2 < (k^2+1)c^2 + d < (kc+1)^2$. Therefore, in infinite descent, all solutions must be reduced to a solution $(x', 0)$, and it follows that d is a perfect square.

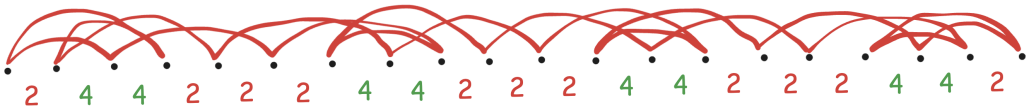
Problem 7. [20] Puddles the Frog has a row of $n \geq 2$ lilypads, labeled 1 through n, with 1 unit between consecutive lilypads. He is at lilypad 1, and wishes to visit lilypads 2 through n once each, before ending up back at lilypad 1. However, he may jump no more than 3 units at a time. Let $f(n)$ be the maximum total distance of Puddles's trip, starting from lilypad 1 and ending back at lilypad 1. Determine, with proof, the value of

$$\lim_{n\to\infty} \frac{f(n)}{n}.$$

Proposed by Vivian Loh

Solution: The answer is $\boxed{\frac{14}{5}}$. Consider each of the 2024 unit segments between consecutive lilypads. Each segment must be covered an even number of times and at least twice.

Here is a construction for $\approx \frac{2}{5}$ of the segments to be covered 4 times and the rest to be covered 2 times. It uses 20 lilypads, but can be extended to infinitely large numbers by inserting more sections of 5 unit segments (covered $4,4,2,2,2$ times) in the middle. The numbers underneath the unit segments are the number of times each segment is covered.



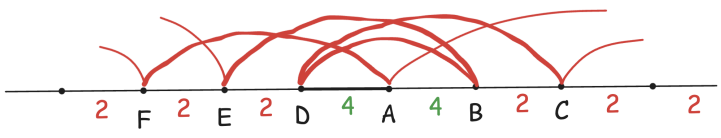
Claim 1: It is impossible for any segment to be covered more than 4 times.

Let F, E, D, A, B, C be 6 consecutive lilypads in that order. We will be analyzing the segment between A and D, which we will call AD. Because each jump is at most 3 units in length, each jump that goes over AD must be between one of $\{A,B,C\}$ and one of $\{D,E,F\}$. Since each node in this graph has degree 2, there are at most 6 such jumps, but F and C can each only be used once (because we can't repeat any one jump), so there are at most 5 jumps. Since each segment must be covered an even number of times, AD must be covered at most 4 times.

Claim 2: Each occurrence of 4 must either be surrounded by three 2's on either side, like 2 2 2 4 2 2 2, or adjacent to another 4 and together they are surrounded by three 2's on either side, like 2 2 2 4 2 2 2 (unless they get cut off by the row ending, in which case some of the 2's can get cut off).

Suppose AD is covered 4 times. The 4 jumps that cover AD must have one endpoint in $\{A,B,C\}$ and one endpoint in $\{D,E,F\}$. Thus, by pigeonhole, at least one of $\{A,B,C\}$ must be the endpoint of two jumps that cover AD. It cannot be C, so it must be either A or B or both. If it is both, then all 4 jumps that cover AD have A or B as their right endpoint, which is bad because it means Puddles does not visit C nor anything to the right of C. This is okay if and only if B is the very last lilypad (so lilypad C does not even exist). And we can see that in this case, AB is covered twice.

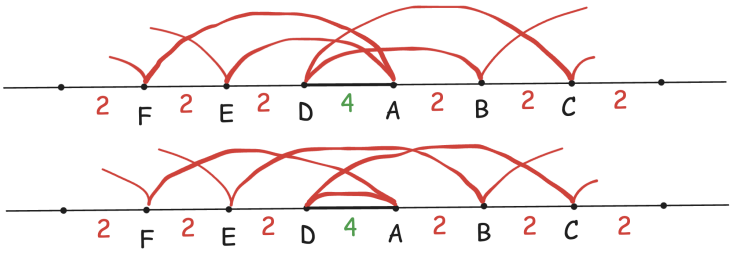
Normally, (if C exists), exactly one of $\{A,B\}$ would be the an endpoint of two jumps that cover AD. Let this vertex be called the "bounce vertex". Then we have two different cases: A is the "bounce vertex", or B is the "bounce vertex". Similarly, there is one "bounce vertex" on the left side, and it is either D or E. Through experimentation, we find that if A, B, C, D, E, F all exist, then if B is the "bounce vertex" on the right, D **must** be the "bounce vertex" on the left.



This causes AD to be covered 4 times, AB to be covered 4 times, and each of the three segments to the left of AD and each of the three segments to the right of AB to all be covered 2 times, since in order for a segment to be covered 4 times, it must have a "bounce vertex" among the 3 lilypads to its left, and a "bounce vertex" among the 3 lilypads to its right.

Similarly, if E is the "bounce vertex" on the left, then A must be the "bounce vertex" on the right, and the diagram looks like the flipped version of this.

The last case that we must consider is where A and D are the two "bounce vertices", and then through experimentation we have these two cases:



However, the first one is actually impossible because the path would be two disjoint loops in this case. In the second case, AD is covered 4 times and the three segments to the left of AD and the three segments to the right of AD each must be covered only twice.

Thus, Claim 2 is proven, and the construction at the beginning of the solution (which can be extended for larger numbers of lilypads) shows that it's possible for $\approx \frac{2}{5}$ of the segments to be covered 4 times, and the other $\approx \frac{3}{5}$ to be covered 2 times, yielding an answer of $\frac{4+4+2+2+2}{5} = \boxed{\frac{14}{5}}$.