

# Shortlisted Problems

21<sup>st</sup> ELMO

Pittsburgh, PA, 2019

## Note of Confidentiality

The shortlisted problems should be kept strictly confidential until disclosed publicly by the committee on the ELMO.

## Contributing Students

The Problem Selection Committee for ELMO 2019 thanks the following proposers for contributing **88 problems** to this year's Competition:

Alex Xu, Andrew Gu, Ankit Bisain, Brandon Wang, Carl Schildkraut, Colin Tang, Daniel Hu, Daniel Zhu, Eric Gan, Ethan Joo, Evan Chen, Holden Mui, Jeffrey Kwan, Jirayus Jinapong, Kai Xiao, Kevin Ren, Luke Robitaille, Max Jiang, Michael Diao, Michael Ren, Mihir Singhal, Milan Haiman, Sean Li, Steven Liu, Swapnil Garg, Tristan Shin, Vincent Huang, Yunseo Choi, Zack Chroman

## Problem Selection Committee

The Problem Selection Committee for ELMO 2019 consisted of:

- Adam Ardeishar
- Carl Schildkraut
- Colin Tang
- Kevin Liu
- Krit Boonsiriseth
- Vincent Huang

## Contents

<b>1</b>	<b>Problems</b>	<b>4</b>
1.1	Problem A1 . . . . .	4
1.2	Problem A2 . . . . .	4
1.3	Problem A3 . . . . .	4
1.4	Problem A4 . . . . .	4
1.5	Problem A5 . . . . .	4
1.6	Problem C1 . . . . .	5
1.7	Problem C2 . . . . .	5
1.8	Problem C3 . . . . .	5
1.9	Problem C4 . . . . .	5
1.10	Problem C5 . . . . .	6
1.11	Problem G1 . . . . .	6
1.12	Problem G2 . . . . .	6
1.13	Problem G3 . . . . .	6
1.14	Problem G4 . . . . .	6
1.15	Problem G5 . . . . .	6
1.16	Problem G6 . . . . .	7
1.17	Problem N1 . . . . .	7
1.18	Problem N2 . . . . .	7
1.19	Problem N3 . . . . .	7
1.20	Problem N4 . . . . .	7
1.21	Problem N5 . . . . .	7
<b>2</b>	<b>Solutions</b>	<b>8</b>
2.1	Solution A1 . . . . .	8
2.2	Solution A2 . . . . .	9
2.3	Solution A3 . . . . .	10
2.4	Solution A4 . . . . .	11
2.5	Solution A5 . . . . .	13
2.6	Solution C1 . . . . .	15
2.7	Solution C2 . . . . .	16
2.8	Solution C3 . . . . .	17
2.9	Solution C4 . . . . .	19
2.10	Solution C5 . . . . .	21
2.11	Solution G1 . . . . .	24
2.12	Solution G2 . . . . .	26
2.13	Solution G3 . . . . .	28
2.14	Solution G4 . . . . .	29
2.15	Solution G5 . . . . .	30
2.16	Solution G6 . . . . .	32
2.17	Solution N1 . . . . .	33
2.18	Solution N2 . . . . .	34
2.19	Solution N3 . . . . .	35
2.20	Solution N4 . . . . .	36
2.21	Solution N5 . . . . .	37

# Problems

**A1.** Let  $a, b, c$  be positive reals such that  $\frac{1}{a} + \frac{1}{b} + \frac{1}{c} = 1$ . Show that

$$a^a bc + b^b ca + c^c ab \geq 27(ab + bc + ca).$$

*(Milan Haiman)*

**A2.** Find all functions  $f: \mathbb{Z} \rightarrow \mathbb{Z}$  with the property that for any surjective function  $g: \mathbb{Z} \rightarrow \mathbb{Z}$ , the function  $f + g$  is also surjective.

*(Sean Li)*

**A3.** Let  $n \geq 3$  be a fixed positive integer. Evan has a convex  $n$ -gon in the plane and wishes to construct the centroid of its vertices. He has no standard ruler or compass, but he does have a device with which he can dissect the segment between two given points into  $m$  equal parts. For which  $m$  can Evan necessarily accomplish his task?

*(Holden Mui and Carl Schildkraut)*

**A4.** Find all nondecreasing functions  $f: \mathbb{R} \rightarrow \mathbb{R}$  such that for all real numbers  $x, y$ ,

$$f(f(x)) + f(y) = f(x + f(y)) + 1.$$

*(Carl Schildkraut)*

**A5.** Define the set of functional expressions to be the smallest set of expressions so that the following properties hold:

- Any variable  $x_i$ , or any fixed real number, is a functional expression.
- Given any functional expression  $V$ , the expression  $f(V)$  is a functional expression, and given any two functional expressions  $V, W$ , the expressions  $V + W$  and  $V \cdot W$  are functional expressions.

A functional equation is an equation of the form  $V = 0$  for any functional expression  $V$ ; a function *satisfies* it if that equation holds for all choices of each  $x_i$  in the real numbers.

(For example, the equation  $f(x_1) + f(x_2) + (-1)(x_1 + x_2) = 0$  is a functional equation satisfied by only the identity function, while the equation  $f(x_1) + f(x_2) + (-1)f(x_1 + x_2) = 0$  is a functional equation satisfied by infinitely many functions. The equation  $f(\frac{1}{1+x_1^2}) = 0$  is not a functional equation at all.)

Does there exist a functional equation satisfied by a exactly one function  $f$ , and the function  $f$  satisfies  $f(\mathbb{R}) = \mathbb{Z}$ ?

*(Carl Schildkraut)*

**C1.** Let  $n \geq 3$  be fixed positive integer. Elmo is playing a game with his clone. Initially,  $n \geq 3$  points are given on a circle. On a player's turn, that player must draw a triangle using three unused points as vertices, without creating any crossing edges. The first player who cannot move loses. If Elmo's clone goes first and players alternate turns, which player wins for each  $n$ ?

*(Milan Haiman)*

**C2.** Adithya and Bill are playing a game on a connected graph with  $n > 2$  vertices and  $m$  edges. First, Adithya labels two of the vertices  $A$  and  $B$ , so that  $A$  and  $B$  are distinct and non-adjacent, and announces his choice to Bill. Then Adithya starts on vertex  $A$  and Bill starts on  $B$ .

Now the game proceeds in a series of rounds in which both players move simultaneously. In each round, Bill must move to an adjacent vertex, while Adithya may either move to an adjacent vertex or stay at his current vertex. Adithya loses if he is ever on the same vertex as Bill, and wins if he reaches  $B$  alone. Adithya cannot see where Bill is, but Bill can see where Adithya is.

Given that Adithya has a winning strategy, what is the maximum possible value of  $m$ , in terms of  $n$ ?

*(Steven Liu)*

**C3.** In the game of Ring Mafia, there are 2019 counters arranged in a circle, 673 of these which are mafia, and the remaining 1346 which are town. Two players, Tony and Madeline, take turns with Tony going first. Tony does not know which counters are mafia but Madeline does.

On Tony's turn, he selects any subset of the counters (possibly the empty set) and removes all counters in that set. On Madeline's turn, she selects a town counter which is adjacent to a mafia counter and removes it. (Whenever counters are removed, the remaining counters are brought closer together without changing their order so that they still form a circle.) The game ends when either all mafia counters have been removed, or all town counters have been removed.

Is there a strategy for Tony that guarantees, no matter where the mafia counters are placed and what Madeline does, that at least one town counter remains at the end of the game?

*(Andrew Gu)*

**C4.** Let  $n \geq 3$  be a positive integer. In a game,  $n$  players sit in a circle in that order. Initially, a deck of  $3n$  cards labeled  $\{1, \dots, 3n\}$  is shuffled and distributed among the players so that every player holds 3 cards in their hand. Then, every hour, each player simultaneously gives the smallest card in their hand to their left neighbor, and the largest card in their hand to their right neighbor. (Thus after each exchange, each player still has exactly 3 cards.)

Prove that each player's hand after the first  $n - 1$  exchanges is their same as their hand after the first  $2n - 1$  exchanges.

*(Carl Schildkraut and Colin Tang)*

**C5.** Given a permutation of  $1, 2, 3, \dots, n$ , with consecutive elements  $a, b, c$  (in that order), we may perform either of the moves:

- If  $a$  is the median of  $a, b$ , and  $c$ , we may replace  $a, b, c$  with  $b, c, a$  (in that order).
- If  $c$  is the median of  $a, b$ , and  $c$ , we may replace  $a, b, c$  with  $c, a, b$  (in that order).

What is the least number of sets in a partition of all  $n!$  permutations, such that any two permutations in the same set are obtainable from each other by a sequence of moves?

*(Milan Haiman)*

**G1.** Let  $ABC$  be an acute triangle with orthocenter  $H$  and circumcircle  $\Gamma$ . Let  $BH$  intersect  $AC$  at  $E$ , and let  $CH$  intersect  $AB$  at  $F$ . Let  $AH$  intersect  $\Gamma$  again at  $P \neq A$ . Let  $PE$  intersect  $\Gamma$  again at  $Q \neq P$ . Prove that  $BQ$  bisects segment  $\overline{EF}$ .

*(Luke Robitaille)*

**G2.** Snorlax is given three pairwise non-parallel lines  $\ell_1, \ell_2, \ell_3$  and a circle  $\omega$  in the plane. In addition to a normal straightedge, Snorlax has a special straightedge which takes a line  $\ell$  and a point  $P$  and constructs a new line  $\ell'$  passing through  $P$  parallel to  $\ell$ . Determine if it is always possible for Snorlax to construct a triangle  $XYZ$  such that the sides of  $\triangle XYZ$  are parallel to  $\ell_1, \ell_2, \ell_3$  in some order, and  $X, Y, Z$  each lie on  $\omega$ .

*(Vincent Huang)*

**G3.** Let  $\triangle ABC$  be an acute triangle with incenter  $I$  and circumcenter  $O$ . The incircle touches sides  $BC, CA$ , and  $AB$  at  $D, E$ , and  $F$  respectively, and  $A'$  is the reflection of  $A$  over  $O$ . The circumcircles of  $ABC$  and  $A'EF$  meet at  $G$ , and the circumcircles of  $AMG$  and  $A'EF$  meet at a point  $H \neq G$ , where  $M$  is the midpoint of  $EF$ . Prove that if  $GH$  and  $EF$  meet at  $T$ , then  $DT \perp EF$ .

*(Ankit Bisain)*

**G4.** Let triangle  $ABC$  have altitudes  $\overline{BE}$  and  $\overline{CF}$  which meet at  $H$ . The reflection of  $A$  over  $BC$  is  $A'$ . The circumcircles of  $\triangle AA'E$  and  $\triangle AA'F$  meet the circumcircle of  $\triangle ABC$  at  $P \neq A$  and  $Q \neq A$  respectively. Lines  $BC$  and  $PQ$  meet at  $R$ . Prove that  $\overline{EF} \parallel \overline{HR}$ .

*(Daniel Hu)*

**G5.** Given a triangle  $ABC$  for which  $\angle BAC \neq 90^\circ$ , let  $B_1, C_1$  be variable points on  $AB, AC$ , respectively. Let  $B_2, C_2$  be the points on line  $BC$  such that a spiral similarity centered at  $A$  maps  $B_1C_1$  to  $C_2B_2$ . Denote the circumcircle of  $AB_1C_1$  by  $\omega$ . Show that if  $B_1B_2$  and  $C_1C_2$  concur on  $\omega$  at a point distinct from  $B_1$  and  $C_1$ , then  $\omega$  passes through a fixed point other than  $A$ .

*(Maxwell Jiang)*

**G6.** Let  $ABC$  be an acute scalene triangle and let  $P$  be a point in the plane. For any point  $Q \neq A, B, C$ , define  $T_A$  to be the unique point such that  $\triangle T_A B P \sim \triangle T_A Q C$  and  $\triangle T_A B P, \triangle T_A Q C$  are oriented in the same direction (clockwise or counterclockwise). Similarly define  $T_B, T_C$ .

- Find all  $P$  such that there exists a point  $Q$  with  $T_A, T_B, T_C$  all lying on the circumcircle of  $\triangle ABC$ . Call such a pair  $(P, Q)$  a *tasty pair* with respect to  $\triangle ABC$ .
- Keeping the notations from (a), determine if there exists a tasty pair which is also tasty with respect to  $\triangle T_A T_B T_C$ .

(Vincent Huang)

**N1.** Let  $P$  be a polynomial with integer coefficients so that  $P(0) = 1$ . Let  $x_0 = 0$ , and let  $x_{i+1} = P(x_i)$  for all  $i \geq 0$ . Show that there are infinitely many positive integers  $n$  so that  $\gcd(x_n, n + 2019) = 1$ .

(Carl Schildkraut and Milan Haiman)

**N2.** Let  $f: \mathbb{Z}_{>0} \rightarrow \mathbb{Z}_{>0}$  be a function. Prove that the following two conditions are equivalent:

- $f(m) + n$  divides  $f(n) + m$  for all positive integers  $m \leq n$ ;
- $f(m) + n$  divides  $f(n) + m$  for all positive integers  $m \geq n$ .

(Carl Schildkraut)

**N3.** Let  $S$  be a nonempty set of integers so that, for any (not necessarily distinct) integers  $a$  and  $b$  in  $S$ ,  $ab + 1$  is also in  $S$ . Show that there are finitely many (possibly zero) primes which do not divide any element of  $S$ .

(Carl Schildkraut)

**N4.** A positive integer  $b \geq 2$  and a sequence  $a_0, a_1, a_2, \dots$  of base- $b$  digits  $0 \leq a_i < b$  is given. It is known that  $a_0 \neq 0$  and the sequence  $\{a_i\}$  is eventually periodic but has infinitely many nonzero terms. Let  $S$  be the set of positive integers  $n$  so that the base- $b$  number  $(a_0 a_1 \dots a_n)_b$  is divisible by  $n$ . Given that  $S$  is infinite, show that there are infinitely many primes dividing at least one element of  $S$ .

(Carl Schildkraut and Holden Mui)

**N5.** Let  $m$  be a fixed even positive integer. Find all positive integers  $n$  for which there exists a bijection  $f$  from  $\{1, \dots, n\}$  to itself such that for all  $x, y \in \{1, \dots, n\}$  with  $mx - y$  divisible by  $n$ , we also have

$$(n + 1) \mid f(x)^m - f(y).$$

(Milan Haiman and Carl Schildkraut)

# Solutions

**A1.** Let  $a, b, c$  be positive reals such that  $\frac{1}{a} + \frac{1}{b} + \frac{1}{c} = 1$ . Show that

$$a^a bc + b^b ca + c^c ab \geq 27(ab + bc + ca).$$

(Milan Haiman)

We present two solutions.

**First solution by Jensen (Ankan Bhattacharya)** Applying the change of variable  $(x, y, z) = (\frac{1}{a}, \frac{1}{b}, \frac{1}{c})$ , we wish to prove that

$$x^{1-1/x} + y^{1-1/y} + z^{1-1/z} \geq 27$$

whenever  $x, y, z > 0$  and  $x + y + z = 1$ .

We will prove that  $f(x) = x^{1-1/x}$  is convex on  $\mathbb{R}_{>0}$ , which will establish the result. A calculation shows that

$$\begin{aligned} f'(x) &= x^{-1/x} (x^{-1} \log x + 1 - x^{-1}) \\ f''(x) &= x^{-1/x} (x^{-3} (\log x - 1)^2 + x^{-2}) \end{aligned}$$

which is positive.

**Second solution (Jirayus Jinapong)** Dividing both sides by  $abc$ , we wish to show  $a^{a-1} + b^{b-1} + c^{c-1} \geq 27$ . In fact, we prove the following stronger claim.

**Claim** — We have  $a^{a-1} b^{b-1} c^{c-1} \geq 729$ .

*Proof.* Note that  $a, b, c > 1$ . By weighted AM-GM, we have

$$\frac{2}{a+b+c-3} = \sum_{\text{cyc}} \frac{a-1}{a+b+c-3} \cdot \frac{1}{a} \geq \prod_{\text{cyc}} \left( \frac{1}{a} \right)^{\frac{a-1}{a+b+c-3}}$$

Therefore, we have

$$a^{a-1} b^{b-1} c^{c-1} \geq \left( \frac{a+b+c+3}{2} \right)^{a+b+c-3}.$$

Since the given implies  $a+b+c \geq \frac{9}{1/a+1/b+1/c} = 9$ , we get the result.  $\square$



**A2.** Find all functions  $f: \mathbb{Z} \rightarrow \mathbb{Z}$  with the property that for any surjective function  $g: \mathbb{Z} \rightarrow \mathbb{Z}$ , the function  $f + g$  is also surjective.

(Sean Li)

Constant functions  $f$  work, so we prove that when  $f$  is nonconstant it is possible to find surjective  $g$  such that  $f + g$  is never equal to zero.

Note that the problem remains the same if we replace the domains by a countable set  $S = \{s_0, s_1, \dots\}$  with the order of the elements being irrelevant. So we will do so to ease notation.

We consider two cases.

- First, suppose that  $f$  has the form

$$\begin{aligned} f(s_0) &= t_0 \\ f(s_1) &= t_1 \\ &\vdots \\ f(s_n) &= t_n \\ f(s_{n+1}) &= c \\ f(s_{n+2}) &= c \\ f(s_{n+3}) &= c \\ &\vdots \end{aligned}$$

where none of the  $t_i$ 's equals zero. In other words,  $f$  is equal to some constant  $c$  for cofinitely many values. Since  $f$  is nonconstant,  $n > 0$ .

Then it suffices to define  $g$  by letting  $g(s_0) = -c$ , and then picking  $g(s_1), g(s_2), \dots, g(s_n)$  to be large positive integers exceeding  $\max |t_i|$ , and then picking  $g(s_{n+1}), \dots$  to be the remaining unchosen integers in some order.

- Otherwise, we claim the following algorithm works: we define  $g(s_n)$  inductively by letting it equal the smallest integer (in absolute value, say) which has not yet been chosen, and is also not equal to  $-f(s_n)$ .

The resulting function  $f + g$  avoids zero by definition; we just need it to be surjective, and this is true because for any constant  $c$ , there are infinitely many  $n$  for which  $f(s_n) \neq -c$ ; so  $c$  will get chosen by the  $(2c + 1)$ st such  $n$ .

**A3.** Let  $n \geq 3$  be a fixed positive integer. Evan has a convex  $n$ -gon in the plane and wishes to construct the centroid of its vertices. He has no standard ruler or compass, but he does have a device with which he can dissect the segment between two given points into  $m$  equal parts. For which  $m$  can Evan necessarily accomplish his task?

(Holden Mui and Carl Schildkraut)

The following solution was given by Ankan Bhattacharya. We ignore the hypothesis that the  $n$  vertices are convex. The given task is easily seen to be equivalent to the following one:

Evan writes the  $n$  vectors  $(n, 0, 0, \dots)$ ,  $(0, n, 0, \dots)$ ,  $\dots$ ,  $(0, 0, \dots, n)$  on a board. For any two vectors  $\mathbf{a}$  and  $\mathbf{b}$  on the board, Evan may write the vector  $\frac{k}{m}\mathbf{a} + \frac{\ell}{m}\mathbf{b}$  for any nonnegative integers  $k, \ell$  summing to  $m$ . The goal is to write  $(1, \dots, 1)$ .

We claim that the answer is that Evan can succeed if and only if  $m$  is divisible by 2 and every prime dividing  $n$ .

**Proof of necessity:** It is clear that  $m$  must be divisible by every prime factor  $p$  of  $n$ , since otherwise entries on the board will always be zero modulo  $p$ .

Now suppose  $n$  is odd; we show  $2 \mid m$  nonetheless. The initial given vectors are permutations of

$$(1, \underbrace{0, \dots, 0}_{n-1}) \pmod{2}.$$

The desired vector then is  $(1, \dots, 1) \pmod{2}$ . However, it is easy to see that no new vectors (modulo 2) can be added. Hence if  $n$  is odd then  $2 \mid m$  as well.

**Proof of sufficiency:** It is enough to prove that if  $n = 2p$  with  $p$  an odd prime, then  $m = 2p$  is valid.

We say a *achievable multiset*  $S$  is one for which the elements are positive integers with sum  $2p$  and Evan can achieve the vector whose nonzero entries coincide with that multiset. We start with  $S = \{1, p-1, 1, p-1\}$  as an achievable multiset. Thereafter, note that the following operations preserve achievability:

- (a) replace an even  $k$  with two copies of  $\frac{k}{2}$ ,
- (b) replace two different numbers  $k$  and  $\ell$  of the same parity with two copies of  $\frac{k+\ell}{2}$ ,

Note that every move decreases the sum of the squares (say), so consider an achievable multiset  $S$  at a situation when no more moves are possible. It must be constant then (as all numbers are odd and equal). Moreover all the entries are less than  $p$ . So we must have  $S = \{1, 1, \dots, 1\}$  as needed.

**A4.** Find all nondecreasing functions  $f: \mathbb{R} \rightarrow \mathbb{R}$  such that for all real numbers  $x, y$ ,

$$f(f(x)) + f(y) = f(x + f(y)) + 1.$$

(Carl Schildkraut)

Here is Ankan Bhattacharya's solution.

**Part I: answers.** For each positive integer  $n$  and real  $0 \leq \alpha < 1$ , the functions

$$f_{n,\alpha}^-(x) = \frac{1}{n} \lfloor nx + \alpha \rfloor + 1 \quad \text{and} \quad f_{n,\alpha}^+(x) = \frac{1}{n} \lceil nx - \alpha \rceil + 1,$$

along with  $f_0(x) = 1$  and  $f_\infty(x) = x + 1$ , are solutions (and they are all). The verification that they are valid solutions is left to the curious reader.

**Part II: substitution.** For the converse direction, it will be more helpful to work with the function  $g(x) = f(x) - 1$ , which is also nondecreasing.

**Lemma**

We have  $g(0) = 0$ ,  $g(x + 1) = g(x) + g(1)$ , and

$$Q(x, y) : g(x + g(y)) = g(x) + g(y).$$

*Proof.* The original functional equation reads

$$P(x, y) : g(g(x) + 1) + g(y) = g(x + g(y) + 1).$$

- First of all,  $P(0, 0)$  gives  $g(0) = 0$ .
- Next,

$$\begin{aligned} P(x, 0) &\implies g(g(x) + 1) = g(x + 1), \\ P(0, y) &\implies g(1) + g(y) = g(g(y) + 1), \end{aligned}$$

and in particular  $g(x + 1) = g(x) + g(1)$ . As a corollary,  $g$  is idempotent:  $g(g(x)) = g(x)$ .

This simplifies  $P(x, y)$  to the last part  $Q(x, y)$  of the claim. □

**Part III: analysis.** We are done playing around with expressions and are ready to do more serious analysis on  $g$ . If  $g(1) = 0$  then clearly  $g(n) = 0$  for every integer  $n$  so  $g$  is zero. Hence suppose  $g(1) > 0$ .

**Claim** — If  $g$  is not the identity function, then  $g(1) = 1$ .

*Proof.* Write  $g(1) = c$ . Now note  $g(n) = cn$  for any positive integer  $n$ , and also  $g(cn) = cn$  and  $g(c(n \pm 1)) = c(n \pm 1)$ . Hence  $c(n \pm 1)$  never belong to the interval from  $n$  to  $cn$ , which forces  $c = 1$  upon taking  $n \rightarrow \infty$ . □

We now denote by  $S = g(\mathbb{R})$  the image of  $g$ .

**Claim** —  $S$  is closed under subtraction.

*Proof.* Note  $Q(x - g(y), y)$  gives  $g(x) - g(y) = g(x - g(y))$ . □

Thus we have two cases.

- If  $S$  is dense, then by  $Q(0, y)$  the set of fixed points of  $g$  is dense, so  $g$  is identity.
- If  $S$  is not dense, then  $S$  (being closed under subtraction) must be of the form  $\frac{1}{n}\mathbb{Z}$  for some positive integer  $n$ . As  $g$  must be non-decreasing, it follows that  $g^{-1}(0)$  is a half-open interval of length  $\frac{1}{n}$  containing 0, and the desired characterization follows.

**A5.** Define the set of functional expressions to be the smallest set of expressions so that the following properties hold:

- Any variable  $x_i$ , or any fixed real number, is a functional expression.
- Given any functional expression  $V$ , the expression  $f(V)$  is a functional expression, and given any two functional expressions  $V, W$ , the expressions  $V + W$  and  $V \cdot W$  are functional expressions.

A functional equation is an equation of the form  $V = 0$  for any functional expression  $V$ ; a function *satisfies* it if that equation holds for all choices of each  $x_i$  in the real numbers.

(For example, the equation  $f(x_1) + f(x_2) + (-1)(x_1 + x_2) = 0$  is a functional equation satisfied by only the identity function, while the equation  $f(x_1) + f(x_2) + (-1)f(x_1 + x_2) = 0$  is a functional equation satisfied by infinitely many functions. The equation  $f(\frac{1}{1+x_1^2}) = 0$  is not a functional equation at all.)

Does there exist a functional equation satisfied by a exactly one function  $f$ , and the function  $f$  satisfies  $f(\mathbb{R}) = \mathbb{Z}$ ?

(Carl Schildkraut)

Yes, such a functional equation does exist. Here is Ankan Bhattacharya's construction (one of many).

We consider the following sequence.

**Claim** — The sequence

$$a_n = \begin{cases} 0 & n < 0, \\ m & n = 2m - 2, m \in \mathbb{Z}_{>0}, \\ -m & n = 2m - 1, m \in \mathbb{Z}_{>0}, \end{cases}$$

is the unique  $\mathbb{Z}$ -indexed satisfying the five properties

- $a_n = 0$  for  $n < 0$ ,
- $a_0 \in \{0, 1\}$ ,
- $a_{n+2} - 2a_n + a_{n-2} = 0$  for  $n \geq 0$ ,
- $a_n - a_{n-2} \in \{\pm 1\}$  for  $n \geq 0$ ,
- $a_n + a_{n+1} \in \{0, 1\}$  for  $n \geq 0$ .

*Proof.* Suppose  $a_0 = 0$ . Then  $a_2 = 2a_0 - a_{-2} = 0$ , but  $a_2 - a_0 \notin \{-1, 1\}$ , contradiction. Thus  $a_0 = 1$ . Now  $a_{-2} = 0$  and  $a_0 = 1$ , so by an easy induction  $\boxed{a_{2n-2} = n}$  for every nonnegative integer  $n$ . Now note  $a_{2n-2} = n$ ,  $a_{2n} = n + 1$ , and  $a_{2n-2} + a_{2n-1}$  and  $a_{2n-1} + a_{2n}$  are both in  $\{0, 1\}$  for every  $n \geq 0$ , so  $\boxed{a_{2n-1} = -n}$  for every  $n \geq 0$ . The end.  $\square$

Now we are ready to solve the problem. We claim that

$$\begin{aligned}
0 &= f(-x_1^2 - (x_1x_2 - 1)^2)^2 \\
&+ \left[ \left( f(-x_1^2 - (x_1x_2 - 1)^2 + 1) - \frac{1}{2} \right)^2 - \frac{1}{4} \right]^2 \\
&+ [f(x_1^2 + 2) - 2f(x_1^2) + f(x_1^2 - 2)]^2 \\
&+ \left[ (f(x_1^2) - f(x_1^2 - 2))^2 - 1 \right]^2 \\
&+ \left[ (f(x_1^2) + f(x_1^2 + 1) - \frac{1}{2})^2 - \frac{1}{4} \right]^2
\end{aligned}$$

works. Unraveling the equation, we obtain the equivalent condition set

- $f(s) = 0$  for  $s < 0$ ,
- $f(s) \in \{0, 1\}$  for  $s < 1$ ,
- $f(s + 2) - 2f(s) + f(s - 2) = 0$  for  $s \geq 0$ ,
- $f(s) - f(s - 2) \in \{\pm 1\}$  for  $s \geq 0$ ,
- $f(s) + f(s + 1) \in \{0, 1\}$  for  $s \geq 0$ .

This is equivalent to the sequence  $\{f(n + \alpha)\}_{n \in \mathbb{Z}}$  satisfying the hypothesis of the claim for any  $0 \leq \alpha < 1$ . This solves the problem.

**Remark.** It's interesting how annoying the constraint about not allowing division is. With division permitted, the much simpler construction

$$0 = [f((1 + x^2)^{-1}) - 1]^2 + [f(y + 1) - f(y) - 1]^2$$

works nicely: the first term requires that  $f(t) = 1$  for  $0 < t \leq 1$  and the second one means  $f(t + 1) = f(t) + 1$  for all  $t$ , ergo  $f$  is the ceiling function.

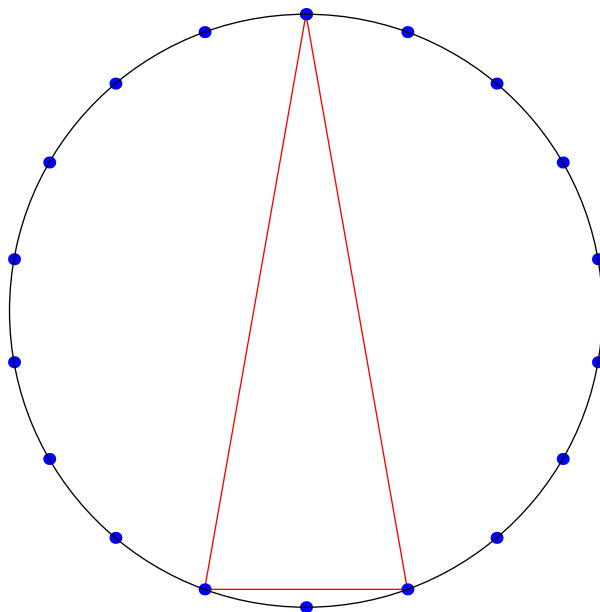
**C1.** Let  $n \geq 3$  be fixed positive integer. Elmo is playing a game with his clone. Initially,  $n \geq 3$  points are given on a circle. On a player's turn, that player must draw a triangle using three unused points as vertices, without creating any crossing edges. The first player who cannot move loses. If Elmo's clone goes first and players alternate turns, which player wins for each  $n$ ?

*(Milan Haiman)*

---

The first player (Elmo's clone) always wins. Indeed it obviously wins for  $n \leq 5$ .

For  $n \geq 6$ , the strategy is to start by picking an isosceles triangle whose base cuts off either 0 or 1 points (according to whether  $n$  is odd or even, respectively).



Then do strategy stealing: each time the second player moves, the first player copies it.

**C2.** Adithya and Bill are playing a game on a connected graph with  $n > 2$  vertices and  $m$  edges. First, Adithya labels two of the vertices  $A$  and  $B$ , so that  $A$  and  $B$  are distinct and non-adjacent, and announces his choice to Bill. Then Adithya starts on vertex  $A$  and Bill starts on  $B$ .

Now the game proceeds in a series of rounds in which both players move simultaneously. In each round, Bill must move to an adjacent vertex, while Adithya may either move to an adjacent vertex or stay at his current vertex. Adithya loses if he is ever on the same vertex as Bill, and wins if he reaches  $B$  alone. Adithya cannot see where Bill is, but Bill can see where Adithya is.

Given that Adithya has a winning strategy, what is the maximum possible value of  $m$ , in terms of  $n$ ?

(Steven Liu)

The answer is  $m = \binom{n-1}{2} + 1$ . Here is the solution by Milan Haiman.

**Construction:** suppose  $G$  consists of an  $(n-1)$ -clique, two of the vertices which are labeled  $C$  and  $A$ , with one extra leaf attached to  $C$ , which we label  $B$ . Then, Adithya wins by starting at  $A$  and following the sequence  $A \rightarrow A \rightarrow C \rightarrow B$ .

**Bound:** The main lemma is the following.

**Claim** — If  $B$  is part of any triangle, then Adithya can't guarantee victory.

*Proof.* Bill can move among those three vertices and arrive back at  $B$  after  $k$  moves, for any  $k \geq 2$ . Moreover Adithya takes at least two moves to reach  $B$ .  $\square$

So if Adithya is to win, we must have

$$m \leq \left( \binom{n-1}{2} - \binom{d}{2} \right) + d$$

where  $d$  is the degree of  $B$ , and this implies the result.



**C3.** In the game of Ring Mafia, there are 2019 counters arranged in a circle, 673 of these which are mafia, and the remaining 1346 which are town. Two players, Tony and Madeline, take turns with Tony going first. Tony does not know which counters are mafia but Madeline does.

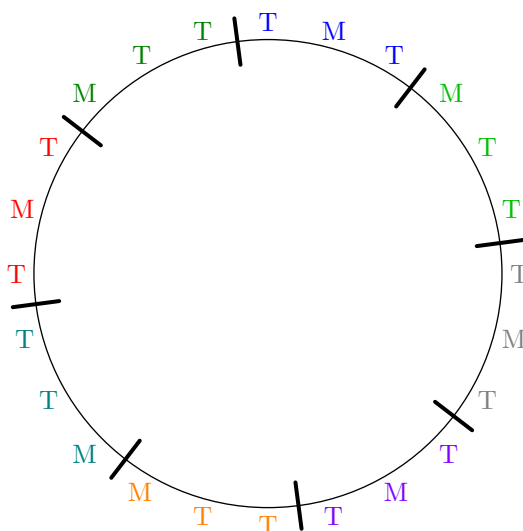
On Tony's turn, he selects any subset of the counters (possibly the empty set) and removes all counters in that set. On Madeline's turn, she selects a town counter which is adjacent to a mafia counter and removes it. (Whenever counters are removed, the remaining counters are brought closer together without changing their order so that they still form a circle.) The game ends when either all mafia counters have been removed, or all town counters have been removed.

Is there a strategy for Tony that guarantees, no matter where the mafia counters are placed and what Madeline does, that at least one town counter remains at the end of the game?

(Andrew Gu)

The answer is no. The following solution is due to Carl Schildkraut.

In fact, suppose we group the counters into 2019 blocks initially into 673 consecutive groups of 3 and it is declared publicly that there is exactly one Mafia token in each block.



**Claim —** At every step of the game, in every block with at least one token remaining, any token in that block could be Mafia. In other words, Tony cannot gain any information about any of the counters in a given block.

*Proof.* This is clearly true after any of Tony's moves, since within each block Tony has no information.

So we just have to verify it for Madeline. If the game is still ongoing, then there is some block with at least two tokens remaining. So:

- If there are only two tokens left, then they play symmetric roles; Madeline removes either one.
- If all three tokens remain, then since either the leftmost or rightmost counter could be Mafia, Madeline simply removes the middle counter.

This completes the proof. □

Therefore, it is impossible for Tony to guarantee that at least one town counter remains and no Mafia tokens remain, since any nonempty block could contain a Mafia token.

**C4.** Let  $n \geq 3$  be a positive integer. In a game,  $n$  players sit in a circle in that order. Initially, a deck of  $3n$  cards labeled  $\{1, \dots, 3n\}$  is shuffled and distributed among the players so that every player holds 3 cards in their hand. Then, every hour, each player simultaneously gives the smallest card in their hand to their left neighbor, and the largest card in their hand to their right neighbor. (Thus after each exchange, each player still has exactly 3 cards.)

Prove that each player's hand after the first  $n - 1$  exchanges is their same as their hand after the first  $2n - 1$  exchanges.

(Carl Schildkraut and Colin Tang)

For now, we focus only on the behavior of the cards in  $\{1, \dots, n\}$  and instead consider a modified game in which each player

- keeps their minimum card,
- passes their median card one right,
- passes their maximum card two right.

This is the same game up to rotating the names of players.

**Claim (Trail of tokens)** — For each  $1 \leq r \leq n$ , the card  $r$  stops moving after at most  $r - 1$  moves.

*Proof.* The trick is to treat the cards  $\{1, \dots, r\}$  as *indistinguishable*: we call such cards *blue tokens*. We show all tokens stop moving after at most  $r - 1$  time. The main trick is the following:

Whenever a player receives a token for the first time, (possibly before any moves, possibly more than one at once), we have them choose one of their tokens to turn grey, and have it never move afterwards.

Assume some token is still blue after  $h$  hours. If it moved from player 0 to player  $d$ , say (players numbered in order), then players 0, 1,  $\dots$ ,  $d$ , each have a grey token. Thus  $d + 1 \leq r - 1$ , but the token advanced at least one player per hour, hence  $d \geq h$ , so  $h \leq r - 2$ .

In other words, by time  $r - 1$  all tokens are grey. □

**Remark.** A similar proof shows that the card  $r$  travels a total distance at most  $r - 1$  too, by doing the same proof but without changing colors of tokens: if a token covers a total distance  $d$ , then players 0, 1,  $\dots$ ,  $d - 1$  all have a token.

The condition that a player holds at most three tokens at once is not used at any point.

**Back to main problem:** Return to the original exchange rules. By the main claim, after  $n - 1$  hours all the cards  $\{1, \dots, n\}$  are always passed left; in particular, they are in different hands, rotating. A similar claim holds for the large cards  $\{2n + 1, \dots, 3n\}$ . Thus the cards  $\{n + 1, \dots, 2n\}$  are standing still. This implies the problem.

**Remark.** Despite how tempting it is to apply induction on  $r$  to try and prove the main claim, it seems that using indistinguishable tokens makes things much simpler. Part of the reason is because the same cards can meet twice: suppose some adjacent players have the

hands

$\{1, 3, 6\}$      $\{7, 8, 9\}$      $\{4, 9001, 9002\}$      $\{5, 9003, 9004\}$     ...

Note the cards 8 and 9 meet again just a few hours later.

**C5.** Given a permutation of  $1, 2, 3, \dots, n$ , with consecutive elements  $a, b, c$  (in that order), we may perform either of the moves:

- If  $a$  is the median of  $a, b$ , and  $c$ , we may replace  $a, b, c$  with  $b, c, a$  (in that order).
- If  $c$  is the median of  $a, b$ , and  $c$ , we may replace  $a, b, c$  with  $c, a, b$  (in that order).

What is the least number of sets in a partition of all  $n!$  permutations, such that any two permutations in the same set are obtainable from each other by a sequence of moves?

(Milan Haiman)

The number of equivalence classes turns out to be

$$n^2 - 3n + 4 = 2 \left[ \binom{n-1}{2} + 1 \right].$$

First we show that at least  $2\binom{n-1}{2} + 2$  sets are required.

Define the *disorder* of a permutation to be the number of pairs  $(i, j)$  such that  $1 \leq i < j \leq n$  but  $i$  occurs after  $j$  in the permutation. We will also refer to these pairs as pairs that are out of order. We will refer to other such pairs with  $i$  occurring before  $j$  as in order.

Note that disorder is invariant under moves, as the only pairs whose relative orders change are the ones involved in the move. We can easily check that the number of pairs out of order does not change.

Consider the pair  $(1, n)$ . Notice that a move cannot change the relative order of this pair, as neither 1 nor  $n$  can be the median of three elements of a permutation of  $1, 2, 3, \dots, n$ .

**Lemma 1**

There exists a permutation of  $1, 2, 3, \dots, n$  with disorder  $d$ , if  $0 \leq d \leq \binom{n}{2}$ .

*Proof.* Start with the identity permutation  $1, 2, 3, \dots, n$ , which has disorder 0. Now repeatedly swap two adjacent elements that are in order. We may do this until all adjacent elements are out of order, which occurs only with the reverse permutation  $n, \dots, 3, 2, 1$ . Notice that each swap increases the disorder by exactly 1, and that this process takes us from disorder 0 to disorder  $\binom{n}{2}$ . Thus disorder  $d$  must have been attained after exactly  $d$  moves.  $\square$

Consider  $\binom{n-1}{2} + 1$  permutations of  $2, 3, 4, \dots, n$ , with one of each disorder from 0 to  $\binom{n-1}{2}$ , by Lemma 1. Putting the element 1 at the beginning of each of these permutations gives  $\binom{n-1}{2} + 1$  permutations of  $1, 2, 3, \dots, n$  with distinct disorders. Now consider the reverses of each of these permutations. They will all have the pair  $(1, n)$  out of order, and thus cannot be obtained from the original permutations by moves. Furthermore they all have distinct disorders, from  $\binom{n}{2} - \binom{n-1}{2} = n - 1$  to  $\binom{n}{2} - 0 = \binom{n}{2}$ . Thus these  $2\binom{n-1}{2} + 2$  permutations all cannot be obtained from each other by moves. This proves the lower bound.

Now we show that  $2\binom{n-1}{2} + 2$  sets are attainable. We will categorize permutations into sets by their disorder and whether the pair  $(1, n)$  is in order or not. Note that if  $(1, n)$  is in order we must have a disorder of at most  $\binom{n-1}{2}$ , since at most one of the pairs

$(1, k)$  and  $(k, n)$  can be out of order for each  $1 < k < n$ . Similarly if  $(1, n)$  is out of order we must have a disorder of at least  $n - 1$ . Thus we are using only  $2\binom{n-1}{2} + 2$  sets. It remains to show that any two permutations in the same set are obtainable from each other by a sequence of moves.

**Lemma 2**

Given a permutation of  $1, 2, 3, \dots, n$  we can perform a sequence of moves to obtain a permutation with  $n$  either at the beginning or the end.

*Proof.* If  $n$  is at the beginning or end of the permutation we are done. Otherwise suppose that  $k$  and  $l$  are the two elements adjacent to  $n$ , in some order. Without loss of generality,  $k < l < n$ . Then  $l$  is the median of the three elements  $k, l$ , and  $n$ . So we may perform a move on these three elements (as  $n$ , not  $l$ , is the middle term).

We will repeat this process. As we do so, consider the ordered pair  $(x, y)$ , where  $x$  is the minimum of the elements adjacent to  $n$ , and  $y$  is the number of elements on the other side of  $n$  from  $x$ . Note that if  $y$  ever reaches 0 then we are done.

We claim that this ordered pair is lexicographically monotonically decreasing. Suppose that this ordered pair is  $(x_0, y_0)$  before a move (as described above) and  $(x_1, y_1)$  after. Notice that the move will keep  $x_0$  adjacent to  $n$ . Thus if  $x_1 \neq x_0$  then  $x_1 = \min(x_0, x_1) < x_0$ . Now if  $x_1 = x_0$  then one number has moved from the other side of  $n$  from  $x$  to the same side of  $n$  as  $x$ . In this case  $y_1 = y_0 - 1 < y_0$ . This proves our claim. Now note that, by the claim, we must eventually obtain an ordered pair  $(x, y)$  with  $y = 0$ , as desired.  $\square$

Now we will show by induction on  $n$  that given two permutations  $\sigma$  and  $\pi$  of  $1, 2, 3, \dots, n$  with the same disorder and with  $(1, n)$  in the same relative order,  $\sigma$  and  $\pi$  are obtainable from each other by a sequence of moves.

It is easy to check values of  $n \leq 4$ .

WLOG assume that both  $\sigma$  and  $\pi$  have  $(1, n)$  in order. By Lemma 2 we can perform a sequence of moves to obtain  $n$  at the end of both permutations (it cannot be at the beginning since that would put  $(1, n)$  out of order). Now no pairs with  $n$  are out of order in either permutation. Thus looking at only the first  $n - 1$  terms of the permutations we see that they still have the same disorder. Then if the pair  $(1, n - 1)$  has the same relative order in both permutations we are done by induction.

Now suppose  $(1, n - 1)$  does not have the same relative order in both permutations. Consider the disorder  $d$  of both permutations. On one hand, since we have  $(1, n - 1)$  in order  $d \leq \binom{n-1}{2} - (n - 1)$ . Similarly, since we have  $(1, n - 1)$  out of order,  $d \geq n - 1$ .

Note that we can choose a permutation of  $1, 2, 3, \dots, n - 1$  with the last three terms being  $x, 1, n - 1$  and having disorder  $d$ , such that  $x \neq n - 2$ . Similarly, we can choose a permutation with the last two terms being  $n - 1, 1$  and having disorder  $d$ . By induction, we can perform a sequence of moves on the first  $n - 1$  terms (leaving  $n$  in place) of  $\sigma$  and  $\pi$  to obtain two permutations of the form  $\dots, x, 1, n - 1, n$  and  $\dots, n - 1, 1, n$ . It is sufficient to show that we can also perform a sequence of moves to obtain the latter from the former. We perform the following moves:

$$\dots, x, 1, n - 1, n \rightarrow \dots, 1, n - 1, x, n \rightarrow \dots, 1, x, n, n - 1$$

Now by Lemma 2 on the first  $n - 2$  terms we may perform a sequence of moves to move 1 to the beginning or to the end of the first  $n - 2$  terms. Since  $x \neq n - 2$ , 1 must be at the end of the first  $n - 2$  terms, otherwise the relative order of  $(1, n - 2)$  would change. Thus we now have a permutation of the form  $\dots, 1, n, n - 1$  from which we

obtain a permutation of the form  $\dots, n-1, 1, n$ . Then applying induction again we obtain specifically the desired permutation of the form  $\dots, n-1, 1, n$ .

**Remark.** We can also prove [Lemma 2](#) quite easily with induction. However the proof given more explicitly shows the actual moves we make. That is, we “attach”  $n$  to a “small” element and slide it around with that element until it hits an even “smaller” element repeatedly.

**Remark.** Result is known: <https://arxiv.org/pdf/0706.2996.pdf>.

**G1.** Let  $ABC$  be an acute triangle with orthocenter  $H$  and circumcircle  $\Gamma$ . Let  $BH$  intersect  $AC$  at  $E$ , and let  $CH$  intersect  $AB$  at  $F$ . Let  $AH$  intersect  $\Gamma$  again at  $P \neq A$ . Let  $PE$  intersect  $\Gamma$  again at  $Q \neq P$ . Prove that  $BQ$  bisects segment  $\overline{EF}$ .

(Luke Robitaille)

Here are four solutions (unedited).

**First solution (Maxwell Jiang)** Let  $R$  be the midpoint of  $AH$ . As  $HR \cdot HP = HB \cdot HE = \frac{1}{2}\text{Pow}(H)$  we have  $B, R, E, P$  cyclic. Now since  $\angle ABQ = \angle RPE = \angle RBE$  we have  $R, Q$  isogonal wrt  $\angle ABE$ . But  $AFHE$  is cyclic, and so since  $BR$  is a median of  $\triangle BAH$  we have  $BQ$  is a median of similar  $\triangle BEF$ , as desired.

**Second solution (Milan Haiman)** Let  $X$  be the midpoint of  $EF$  and let  $Y$  be the midpoint of  $AH$ . Since  $(AEHF)$ ,  $\triangle ABH \sim \triangle EBF$ .

Since  $BY$  and  $BX$  are medians, by this similarity we have  $\angle YBH = \angle FBX$ .

Let  $AH$  intersect  $BC$  at  $D$ . Note that  $HY \cdot HP = HA \cdot HD = HE \cdot HB$  since  $(AEDB)$ . Thus  $(YEPB)$ .

Now we have  $\angle ABX = \angle FBX = \angle YBH = \angle YBE = \angle YPE = \angle APE$ .

Thus  $BX$  and  $PE$  intersect on  $\Gamma$  at  $Q$ .

**Third solution (Carl Schildkraut)** Let  $K$  be the point so that  $(AK; BC) = -1$ . It is well known that  $KP$  and  $EF$  intersect at some point  $R$  on  $BC$ . Now, apply Pascal's theorem on the cyclic hexagon  $(KPQBCA)$ . We see  $KP \cap BC = R$ ,  $PQ \cap AC = E$ , so  $BQ \cap AK$  lies on  $EF$ . However, as  $EF$  and  $BC$  are anti-parallel in  $\angle BAC$ , the  $A$ -symmedian in  $\triangle ABC$  is the  $A$ -median of  $\triangle AEF$ , and as such  $AK \cap EF$  is the midpoint of  $EF$ , which  $BQ$  thus passes through.

**Fourth solution (Ankan Bhattacharya)** Let  $M$  be the midpoint of  $\overline{EF}$ . Use complex numbers with  $\Gamma$  unit circle; it's easy to obtain  $e = \frac{1}{2}(a + b + c - \frac{ac}{b})$ ,  $p = -\frac{bc}{a}$ ,  $m = \frac{1}{2}(a + b + c) - \frac{1}{4}a(\frac{b}{c} + \frac{c}{b})$ .

To show that lines  $BM$  and  $PE$  meet on  $\Gamma$ , it suffices to prove

$$\angle(\overline{BM}, \overline{PE}) = \angle BAH \iff \frac{p-e}{b-m} \div \frac{h-a}{b-a} \in \mathbb{R}.$$

Computing the left fraction, we obtain

$$\begin{aligned} \frac{p-e}{b-m} &= \frac{-\frac{bc}{a} - \frac{1}{2}(a+b+c - \frac{ac}{b})}{b - \frac{1}{2}(a+b+c) + \frac{1}{4}a(\frac{b}{c} + \frac{c}{b})} \\ &= \frac{-4b^2c^2 - 2(abc(a+b+c) - a^2c^2)}{4ab^2c - 2abc(a+b+c) + a^2(b^2+c^2)} \\ &= -2 \cdot \frac{abc(a+b+c) + 2b^2c^2 - a^2c^2}{-2a^2bc + 2ab^2c - 2abc^2 + a^2(b^2+c^2)} \\ &= -2 \cdot \frac{c(a+b)(ab-ac+2bc)}{a(b-c)(ab-ac+2bc)} \\ &= -2 \cdot \frac{c(a+b)}{a(b-c)}. \end{aligned}$$



Thus

$$-\frac{1}{2} \cdot \frac{p-e}{b-m} \div \frac{h-a}{b-a} = \frac{c(a+b)(b-a)}{a(b-c)(b+c)}$$

and its conjugate equals

$$\frac{\frac{1}{c} \frac{a+b}{ab} \frac{a-b}{ab}}{\frac{1}{a} \frac{c-b}{bc} \frac{b+c}{bc}}$$

which is clearly the same.

**G2.** Snorlax is given three pairwise non-parallel lines  $\ell_1, \ell_2, \ell_3$  and a circle  $\omega$  in the plane. In addition to a normal straightedge, Snorlax has a special straightedge which takes a line  $\ell$  and a point  $P$  and constructs a new line  $\ell'$  passing through  $P$  parallel to  $\ell$ . Determine if it is always possible for Snorlax to construct a triangle  $XYZ$  such that the sides of  $\triangle XYZ$  are parallel to  $\ell_1, \ell_2, \ell_3$  in some order, and  $X, Y, Z$  each lie on  $\omega$ .

(Vincent Huang)

The answer is yes. Here are two solutions.

**First solution (Maxwell Jiang)** We proceed in three steps.

**Claim** — Snorlax can construct the center of  $\omega$ .

*Proof.* Draw a chord and then two more parallel chords; intersecting diagonals of isosceles trapezoids gives us a line passing through the center, and repeating this gives us the center.  $\square$

**Remark** (Zack Chroman). The *Poncelet-Steiner theorem* states that using a single circle with marked center and straightedge alone, one can do any usual straightedge-compass construction. Thus quoting this theorem would complete the problem.

**Claim** — We can construct the midpoint of any segment  $s$ .

*Proof.* All you have to do is construct a parallelogram!  $\square$

**Claim** — We can construct the perpendicular bisector of any segment  $s$ .

*Proof.* By above, we can construct the midpoint  $M$  of  $s$ . We can also construct a chord  $s'$  of  $\omega$  parallel to  $s$ , and its midpoint  $M'$ . Then draw line  $M'O$ , and finally the line through  $M$  parallel to it.  $\square$

Suppose lines  $\ell_1, \ell_2, \ell_3$  determine a triangle  $X'Y'Z'$  with circumcenter  $O'$  (which we can construct by the previous claim), while  $O$  is the center of  $\omega$  (which we can construct by the first claim). We can draw radii of  $\omega$  parallel to  $X'O', Y'O', Z'O'$  and finish.

**Second solution, unedited (Vincent Huang)** Pick an arbitrary point  $A \in \omega$ . Draw  $B, C, D \in \omega$  so that  $BA \parallel \ell_1, CB \parallel \ell_2, DC \parallel \ell_3$ .

Claim: The midpoint  $M$  of arc  $AD$  is fixed regardless of the choice of  $A$ .

Proof: Suppose we had some different starting point  $A'$ , with corresponding  $B', C', D'$ . If  $A'$  is an arc measure  $\theta$  clockwise of  $A$ , then  $B'$  is an arc measure  $\theta$  counterclockwise of  $B$ , so  $C'$  is  $\theta$  clockwise of  $C$ , so  $D'$  is  $\theta$  counterclockwise of  $D$ . Thus it follows that arcs  $A'A, D'D$  have equal measure and are in opposite directions, so the midpoints of arcs  $AD, A'D'$  are the same.

Then if we choose  $X, Y, Z$  so that  $XY \parallel \ell_1, YZ \parallel \ell_2, ZX \parallel \ell_3$ , it follows from the above letting  $A = X$  that the midpoint of arc  $XX$  should also be  $M$ , i.e.  $M = X$ . So it suffices to construct the midpoint  $M$  of arc  $AD$ , as it is a choice for a vertex of  $\triangle XYZ$ .

To do this we note for any  $A', D'$  that  $ADD'A'$  is an isosceles trapezoid, so if  $E = AA' \cap DD', F = AD' \cap A'D$  then  $EF$  is the perpendicular bisector of  $AD, A'D'$ , so intersecting  $EF$  with  $\omega$  yields  $M$  as desired.

**Third solution using projective geometry, unedited (Zack Chroman)** The answer is yes. Work in  $\mathbb{RP}^2$ . We have a straightedge, a marked circle and the line at infinity. We will use the following theorem, known as the Circumcevian Ping-Pong Theorem. I can't find the reference for it, but it's real! Promise.

**Theorem**

Let  $\omega$  be a circle, and let  $P, Q, R$  lie on a fixed line. Then there exists a fixed  $S$  on the same line such that, for any  $A$  on the circle, if

$$B = AP \cap \omega, C = QB \cap \omega, D = RC \cap \omega,$$

then  $A, D, S$  are collinear. Another way to phrase this is that a combination of any even number of "second-intersection maps" on a circle, all of which come from points on a fixed line, is the identity iff it's the identity at one point.

*Proof.* Let the line intersect the circle at  $I, J$  (if the line doesn't intersect the circle, work in  $\mathbb{CP}^2$ ; it's clear that this theorem holds there iff it holds in  $\mathbb{RP}^2$ ). Then define  $S$  so that, for a fixed choice  $A_0, B_0, C_0, D_0$ ,  $S$  lies on  $A_0D_0$ . Then the combination of the projection maps through  $P, Q, R, S$  fix  $A_0$ , but also fix  $I, J$ . Moreover, they define a projective map on  $\omega$ , which is therefore the identity.

One can also prove this similarly with the Desargues Involution Theorem, which directly gives an involution on line  $PQR$  that swaps  $P, R, I, J$ , and  $Q, S_0$ ; so  $S_0$  is fixed.  $\square$

Now note that we have three points  $P_1, P_2, P_3$  lying on the line at infinity and also  $l_1, l_2, l_3$ , respectively. Then by the theorem there exists a fourth point  $P_4$  such that, for any  $X$  on the circle, projecting through  $P_1, P_2, P_3, P_4$  in this order gives  $X$  again.

Then take a fixed  $A_0$  on the circle, and define  $B_0, C_0, D_0$  as these projections, so that  $A_0, D_0, P_4$  are collinear.  $A_0 = X$  will work if and only if  $A_0 = D_0$ . It follows that we want a point  $A_0$  such that  $A_0P_4$  is tangent to  $\omega$ . We can construct this, but it's a little annoying. Our goal will be to construct the perpendicular bisector of  $A_0D_0$ ; intersecting this with the circle will give an  $A_1$  whose tangent passes through  $P_4$ , at which point we can take  $A_1 = X$  and be done.

To do this, take an arbitrary point  $W$  in the plane, and  $E \in A_0W$ . Then let  $F \in D_0W$  with  $EF \parallel A_0D_0$ . Quadrilateral  $A_0EFD_0$  is a trapezoid, so if  $G = A_0F \cap D_0E$ , it follows that  $GW$  passes through the midpoint of  $A_0D_0$ . Now we can do the same process, but replacing  $A_0D_0$  with another chord parallel to it, to get another midpoint; connecting these midpoints gives the perpendicular bisector.

Morally, we're trying here to construct the polar of  $P_4$  with respect to  $\omega$ , which is the locus of the midpoints of chords passing through  $P_4$ . Unfortunately, with only a straightedge constructing midpoints is as much work as constructing general harmonic conjugates, so we need to build the Cevalaus construction to do it.

**G3.** Let  $\triangle ABC$  be an acute triangle with incenter  $I$  and circumcenter  $O$ . The incircle touches sides  $BC, CA$ , and  $AB$  at  $D, E$ , and  $F$  respectively, and  $A'$  is the reflection of  $A$  over  $O$ . The circumcircles of  $ABC$  and  $A'EF$  meet at  $G$ , and the circumcircles of  $AMG$  and  $A'EF$  meet at a point  $H \neq G$ , where  $M$  is the midpoint of  $EF$ . Prove that if  $GH$  and  $EF$  meet at  $T$ , then  $DT \perp EF$ .

*(Ankit Bisain)*

The following harmonic solution is given by Maxwell Jiang.

Define  $T$  instead as the foot to  $EF$  from  $D$ ; we wish to show  $T \in GH$ . Let  $(AI)$  meet  $(ABC)$  a second time at a point  $T'$  so that  $I, T, T'$  are collinear, say by inversion about the incircle. By radical axis on  $(AI), (ABC), (A'EFG)$  we get a point  $X = AT' \cap EF \cap A'G$ . Since  $\angle XGA = \angle XMA = 90^\circ$ , point  $X$  lies on  $(AMG)$ .

Now note that

$$-1 = (A, I; E, F) \stackrel{T'}{=} (X, T; E, F),$$

so by properties of harmonic divisions we have  $TM \cdot TX = TE \cdot TF$ . This implies that  $T$  lies on the radical axis of  $(AMG)$  and  $(A'EFG)$ , as desired.

**G4.** Let triangle  $ABC$  have altitudes  $\overline{BE}$  and  $\overline{CF}$  which meet at  $H$ . The reflection of  $A$  over  $BC$  is  $A'$ . The circumcircles of  $\triangle AA'E$  and  $\triangle AA'F$  meet the circumcircle of  $\triangle ABC$  at  $P \neq A$  and  $Q \neq A$  respectively. Lines  $BC$  and  $PQ$  meet at  $R$ . Prove that  $\overline{EF} \parallel \overline{HR}$ .

(Daniel Hu)

Solution by Maxwell Jiang (at least for  $ABC$  acute):

Let  $D$  be the foot from  $A$ . Let  $N$  be the midpoint of  $AH$ , and let  $X = EF \cap BC$ . Let  $(AH)$  meet  $(ABC)$  again at  $Y$  so that  $A, X, Y$  collinear and define  $P' = EF \cap NC$ ,  $Q' = EF \cap NB$ . Finally, let  $AH$  hit  $EF$  at  $Z$  and  $(ABC)$  again at  $H'$ .

Note that  $-1 = (X, D; B, C) \stackrel{N}{=} (X, Z; Q', P')$ . Now consider an inversion centered at  $A$  with radius  $\sqrt{AH \cdot AD}$ , which swaps  $N, A'$  and  $P, P'$  and  $Q, Q'$  and  $X, Y$  and  $Z, H'$ . Since inversion preserves cross ratio we get  $-1 = (Y, H'; Q, P)$ , so the tangents to  $(ABC)$  at  $Y, H'$  meet on  $PQ$ . On the other hand, since  $-1 = (Y, H'; B, C)$ , these tangents also meet on  $BC$ . Thus the concurrency point is  $R$ .

To finish, note that since  $RH'$  is tangent to  $(ABC)$ , by reflection about  $BC$  we have  $RH$  is tangent to  $(BHC)$ . Then  $\angle RHB = \angle BCH = \angle FAH = \angle FEH$  so  $EF \parallel HR$ , as desired.

**G5.** Given a triangle  $ABC$  for which  $\angle BAC \neq 90^\circ$ , let  $B_1, C_1$  be variable points on  $AB, AC$ , respectively. Let  $B_2, C_2$  be the points on line  $BC$  such that a spiral similarity centered at  $A$  maps  $B_1C_1$  to  $C_2B_2$ . Denote the circumcircle of  $AB_1C_1$  by  $\omega$ . Show that if  $B_1B_2$  and  $C_1C_2$  concur on  $\omega$  at a point distinct from  $B_1$  and  $C_1$ , then  $\omega$  passes through a fixed point other than  $A$ .

(Maxwell Jiang)

The following solutions are not edited.

**First solution by quotation (Andrew Gu)** Let  $D = B_1B_2 \cap C_1C_2, E = B_1C_2 \cap B_2C_1$ . Then  $D, E$  lie on  $\omega$ . By Miquel,  $(C_1DB_2)$  and  $(B_1DC_2)$  concur on  $K \in BC$ .  $\angle B_2KC_1 = \angle B_2DC_1 = \angle B_1DC_1 = \angle BAC$  so  $ABC_1K$  is cyclic, likewise  $AB_1CK$  is cyclic. This reduces it to ELMO SL 2013 G3.

**Second solution by projective geometry (Vincent Huang)** Let  $X = B_1B_2 \cap C_1C_2$ . By spiral sim,  $Y = C_2B_1 \cap B_2C_1$  lies on  $\omega$  as well. By Brokard on  $B_1YC_1X$ , the tangents to  $\omega$  at  $B_1, C_1$  meet on  $BC$ . Now define  $Z \neq C_1$  as  $BC_1 \cap \omega$ , and let  $W = AZ \cap B_1C_1$ . By Brokard again,  $BC$  is the polar of  $W$ , and we get that  $B_1, Z, C$  collinear.

Now let  $P$  be the spiral center sending  $BC \mapsto C_1B_1$ , so that  $P \in \omega$  and  $P \in (BZC)$ . Note that

$$\angle PBC = \angle PC_1B_1 = \angle PAB, \text{ and } \angle PCB = \angle PB_1C_1 = \angle PAC.$$

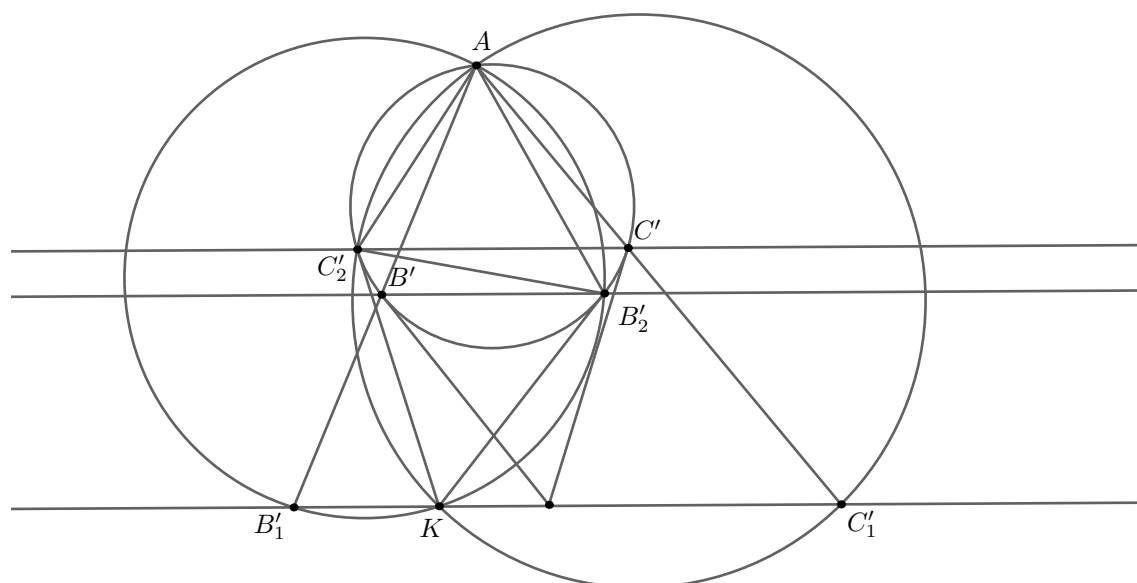
Hence  $(ABP)$  and  $(ACP)$  are tangent to  $BC$ , and  $P$  (the  $A$ -HM point) is the desired fixed point.

**Third inversion solution (Maxwell Jiang)** Let  $S = B_1C_1 \cap CB$ . By the spiral similarity,  $S$  lies on both  $(AB_1C_2)$  and  $(AC_1B_2)$ .

Now invert about  $A$  with arbitrary radius, with  $X'$  denoting the image of  $X$ . So,  $BC$  maps to a circle  $\Omega$  passing through  $A$ , and  $\omega$  maps to a line  $\ell$ . Note that  $S' = \Omega \cap (AB'_1C'_1)$ . Hence,  $S'$  is the spiral center sending  $C'C'_1$  to  $B'B'_1$ . Then,  $B_2, C_2$  are the intersections of  $S'B'_1, S'C'_1$  with  $\Omega$ . Now,  $\angle S'B'_2B' = \angle S'C'B' = \angle S'C'_1B'_1$  and similar angle equalities for  $\angle S'C'_2C'$  give

$$C'C'_2 \parallel B'B'_2 \parallel B'_1C'_1.$$

The given condition equates to  $(AB'_2B'_1)$  and  $(AC'_1C'_2)$  meeting at a point  $K$  on  $\ell$ . Note that  $\triangle AB'_2C'_2 \sim \triangle AC'_1B'_1$ . Since  $\angle AB'_2K = 180^\circ - \angle B'_1$ , we have  $\angle C'_2B'_2K = 180^\circ - \angle B'_1 - \angle C'_1 = \angle B'_2AC'_2$ , so  $KB'_2$  is tangent to  $\Omega$ . Similarly,  $KC'_2$  is tangent to  $\Omega$ .



Since the tangents to  $\Omega$  at  $B'_2, C'_2$  meet on  $\ell$ , for symmetry reasons the tangents at  $B', C'$  also meet on  $\ell$ . However, this point is fixed, so  $\ell$  passes through a fixed point, as desired.

□

Note: To show that the fixed point is the HM point, instead of taking an inversion with arbitrary radius, take the one that swaps  $(AH)$  and  $BC$ . Then use the fact that the tangents to  $(AH)$  at the feet of the altitudes meet at the midpoint of  $BC$ , which is the inverse of the HM point.

**G6.** Let  $ABC$  be an acute scalene triangle and let  $P$  be a point in the plane. For any point  $Q \neq A, B, C$ , define  $T_A$  to be the unique point such that  $\triangle T_A B P \sim \triangle T_A Q C$  and  $\triangle T_A B P, \triangle T_A Q C$  are oriented in the same direction (clockwise or counterclockwise). Similarly define  $T_B, T_C$ .

- (a) Find all  $P$  such that there exists a point  $Q$  with  $T_A, T_B, T_C$  all lying on the circumcircle of  $\triangle ABC$ . Call such a pair  $(P, Q)$  a *tasty pair* with respect to  $\triangle ABC$ .
- (b) Keeping the notations from (a), determine if there exists a tasty pair which is also tasty with respect to  $\triangle T_A T_B T_C$ .

(Vincent Huang)

The following solution is by Andrew Gu:

For (a), the answer is all  $P$  which have an isogonal conjugate (that is, any point  $P$  not on the circumcircle or sides).

Let  $(P, Q)$  be a tasty pair. Then

$$\angle BPC = \angle BPT_A + \angle T_A PC = \angle QCT_A + \angle T_A BQ = \angle BT_A C + \angle CQB = \angle BAC - \angle BQC.$$

Cyclic variants hold, and these imply  $P$  and  $Q$  are isogonal conjugates.

Conversely, let  $P$  and  $Q$  be isogonal conjugates. The same steps as above (in a different order) show that  $\angle BAC = \angle BT_A C$ , so  $T_A$  is on  $(ABC)$ , and likewise so are  $T_B$  and  $T_C$ .

For (b): Let  $T_A T_B T_C$  be the reflection of  $ABC$  about  $O$ , the circumcenter. Consider the inconic with center  $O$ . Let  $P$  and  $Q$  be its foci.



**N1.** Let  $P$  be a polynomial with integer coefficients so that  $P(0) = 1$ . Let  $x_0 = 0$ , and let  $x_{i+1} = P(x_i)$  for all  $i \geq 0$ . Show that there are infinitely many positive integers  $n$  so that  $\gcd(x_n, n + 2019) = 1$ .

(Carl Schildkraut and Milan Haiman)

We present a few solutions.

**First solution by mod-preservation** The “main” case is:

**Claim** — If there exists an index  $i$  for which  $|x_{i+1} - x_i| > 1$  then we are done.

*Proof.* Let  $p$  be any prime dividing the difference and let  $t = x_i$ , so  $P(t) \equiv t \pmod{p}$ . We have  $t \not\equiv 0$  since  $P(0) \equiv 1 \pmod{p}$ . Consequently, we get

$$0 \not\equiv x_i \equiv x_{i+1} \equiv x_{i+2} \equiv \dots \pmod{p}$$

and in this way we conclude taking  $n = p^e - 2019$  for any exponent  $e$  large enough is okay.  $\square$

So suppose that  $x_{i+1} \in \{x_i - 1, x_i, x_i + 1\}$  for every  $i$ . Then either

- The sequence  $(x_n)_n$  is periodic (with period at most 2), so the problem is easy; or
- we have  $P(x) \equiv 1 \pm x$ , which is also easy.

**Second solution by orbits (by proposer)** Let  $p > 2019$  be any prime. We claim that  $n = p$  should work, and in fact that we always have

$$x_p \not\equiv 0 \pmod{q}$$

for any  $q \mid p + 2019$ .

To see this, assume for contradiction  $x_p \equiv 0 \pmod{q}$ . Then  $(x_n \pmod{q})_n$  is periodic, with period dividing  $p$ . But the period should also be at most  $q$ , and not equal to 1 as  $P(0) = 1$ . As  $q < p$ , this is a contradiction.

**N2.** Let  $f: \mathbb{Z}_{>0} \rightarrow \mathbb{Z}_{>0}$  be a function. Prove that the following two conditions are equivalent:

- (i)  $f(m) + n$  divides  $f(n) + m$  for all positive integers  $m \leq n$ ;
- (ii)  $f(m) + n$  divides  $f(n) + m$  for all positive integers  $m \geq n$ .

*(Carl Schildkraut)*

We show that both are equivalent to  $f(x) \equiv x + c$  for a non-negative integer  $c$ . The following solution is given by Maxwell Jiang.

**Part (i):** First suppose that  $f(m) + n \mid f(n) + m$  holds for all  $m \leq n$ . This implies  $f(m) + n \leq f(n) + m \implies f(m) - m \leq f(n) - n$  for all  $m \leq n$ . Define  $g(n) = f(n) - n$  so that  $g$  is non-decreasing and the condition becomes

$$g(m) + m + n \mid g(n) + m + n \implies g(m) + m + n \mid g(n) - g(m).$$

Fix  $m \in \mathbb{N}$  and consider

$$\begin{aligned} g(m) + m + n &\mid g(n) - g(m) \\ g(m+1) + m + 1 + n &\mid g(n) - g(m+1) \end{aligned}$$

Let  $d = g(m+1) - g(m) + 1$  be the difference between the left sides; note that  $d > 0$ . Pick large  $n$  so that  $d$  divides both left sides. If  $d = 1$ , then  $g(m) = g(m+1)$ . Else, we get

$$g(n) \equiv g(m) \equiv g(m+1) \pmod{d}$$

which is impossible. Hence  $g(m) = g(m+1)$ , which applied to all  $m$  gives  $g$  constant as needed.

**Part (ii):** Now suppose  $f(m) + n \mid f(n) + m$  for all  $m \geq n$ . Fix  $n = 1$  and let  $m = p - f(1)$  for arbitrarily large primes  $p$ . Then we force  $f(p - f(1)) + 1 = p$ , so in particular we have infinitely many  $X$  such that  $f(X) = X + c$  for a constant  $c \geq 0$ . Fixing  $m$  and setting  $n = X$  gives

$$f(m) + X \mid X + c + m \implies f(m) + X \mid c + m - f(m)$$

so as  $X$  grows big we force  $f(m) = m + c$ , as desired.

**Remark.** Note that (i) and (ii) together imply that  $f(x) + y$  and  $f(y) + x$  divide each other, hence are equal, so  $f(x) + y = f(y) + x \iff f(x) \equiv x + c$ . So it is unsurprising that we are just solving two functional equations.

**N3.** Let  $S$  be a nonempty set of integers so that, for any (not necessarily distinct) integers  $a$  and  $b$  in  $S$ ,  $ab + 1$  is also in  $S$ . Show that there are finitely many (possibly zero) primes which do not divide any element of  $S$ .

(Carl Schildkraut)

The following solution is due to Ankan Bhattacharya. It's enough to work modulo  $p$ :

**Claim** — Let  $p$  be a prime and let  $G$  be a nonempty subset of  $\mathbb{F}_p$  such that if  $a, b \in G$ , then  $ab + 1 \in G$ . Then either  $G$  is a singleton, or  $G = \mathbb{F}_p$ .

*Proof.* If  $0 \in G$  then  $1 \in G$  and we get  $G = \mathbb{F}_p$ . So suppose  $0 \notin G$ , and let  $G = \{x_1, \dots, x_n\}$  be its  $n$  distinct elements.

If  $1 < n < p$ , then we get a map

$$G \rightarrow G \quad \text{by} \quad g \mapsto x_1 g + 1 \pmod{p}$$

which is injective (since  $x_1 \neq 0$ ), hence bijective. Thus, if we sum, letting  $s = x_1 + \dots + x_n$ , we find

$$s = x_1 \cdot s + n \pmod{p}.$$

If  $s \equiv 0$ , we get  $n \equiv 0 \pmod{p}$ , contradiction. Otherwise, we find  $x_1 = 1 - n/s \pmod{p}$ .

But then the same logic shows  $x_2 = \frac{n}{1-s}$ , so  $x_1 = x_2$ , contradiction.  $\square$

The problem now follows since if  $s$  is any element of  $S$  and  $p$  is any prime not dividing  $s^2 - s + 1$ , then  $S$  contains all residues modulo  $p$ .

**N4.** A positive integer  $b \geq 2$  and a sequence  $a_0, a_1, a_2, \dots$  of base- $b$  digits  $0 \leq a_i < b$  is given. It is known that  $a_0 \neq 0$  and the sequence  $\{a_i\}$  is eventually periodic but has infinitely many nonzero terms. Let  $S$  be the set of positive integers  $n$  so that the base- $b$  number  $(a_0 a_1 \dots a_n)_b$  is divisible by  $n$ . Given that  $S$  is infinite, show that there are infinitely many primes dividing at least one element of  $S$ .

(Carl Schildkraut and Holden Mui)

Let  $\gcd(x, y) = 1$  so that

$$\frac{x}{y} = \sum_{i=0}^{\infty} \frac{a_i}{b^i}.$$

Note that

$$(a_0 \cdots a_n)_b = \left\lfloor \frac{xb^n}{y} \right\rfloor,$$

unless  $\{a_i\}$  is eventually  $b - 1$ ; either way, we have

$$(a_0 \cdots a_n)_b = \frac{xb^n - t}{y}$$

for some  $0 \leq t < y$ . If  $S$  is infinite, then there exists some fixed  $0 \leq t < y$  so that the set of integers  $n$  so that

$$xb^n \equiv t \pmod{yn}$$

is infinite. Call this set  $S'$ . We see that  $t \neq 0$  (infinitely many nonzero terms condition; this condition is essential) and  $x > y > t$  (from the  $a_0 \neq 0$  condition).

Our main claim is that for any prime  $p$ , the set  $\{\nu_p(n) \mid n \in S'\}$  is bounded above. This is clear for  $p|b$ , wherein the above cannot hold if  $n > \nu_p(t)$ . Now, assume  $n = mp^k \in S'$  for some  $m, k$ . We have

$$xb^{mp^k} \equiv t \pmod{p^k} \implies x^{p-1} b^{mp^k(p-1)} \equiv t^{p-1} \pmod{p^k}.$$

As  $\gcd(p, b) = 1$ ,  $b^{p^{k-1}(p-1)} \equiv 1 \pmod{p^k}$ , so that term disappears, and we thus have

$$x^{p-1} \equiv t^{p-1} \pmod{p^k}.$$

As  $x > t$ , this cannot hold for large enough  $k$ , finishing the proof.

**N5.** Let  $m$  be a fixed even positive integer. Find all positive integers  $n$  for which there exists a bijection  $f$  from  $\{1, \dots, n\}$  to itself such that for all  $x, y \in \{1, \dots, n\}$  with  $mx - y$  divisible by  $n$ , we also have

$$(n + 1) \mid f(x)^m - f(y).$$

(Milan Haiman and Carl Schildkraut)

Solution by Andrew Gu (unedited):

We are asking for  $m, n$  such that the mapping  $x \mapsto mx$  on  $\mathbb{Z}/n\mathbb{Z}$  and the mapping  $x \mapsto x^m$  on  $U = (\mathbb{Z}/(n+1)\mathbb{Z}) \setminus \{0\}$  are isomorphic (behave in the same way by relabeling elements).

First we claim  $n + 1$  is a product of distinct primes. Otherwise, there exists  $x \in U$  for which  $x^m \equiv 0 \pmod{n + 1}$ .

Next note that the mapping  $x \mapsto mx$  on  $\mathbb{Z}/n\mathbb{Z}$  is a  $\gcd(m, n)$ -to-1 mapping, so any element in the range has a preimage of size  $\gcd(m, n)$ . We claim this is impossible for the second mapping if  $n + 1 = p_1 \cdots p_k$  is a product of  $k$  distinct primes, two of which are odd. WLOG let  $p_1, p_2$  be odd. The preimage of the element which is  $1 \pmod{p_1}, 1 \pmod{p_2}$ , and  $0$  modulo all other  $p_i$  has size  $\gcd(p_1 - 1, m) \gcd(p_2 - 1, m)$  while the preimage of the element which is  $1 \pmod{p_1}$  and  $0$  modulo all other  $p_i$  has size  $\gcd(p_1 - 1, m)$ . As  $\gcd(p_i - 1, m) \geq 2$ , these preimages have different sizes.

The remaining cases are  $n + 1 = 2p$  or  $n + 1 = p$  where  $p$  is prime. In the case where  $n + 1 = 2p$ , note that  $p > 2$  as we showed that  $n + 1$  is a product of distinct primes. Then  $p \in U$  is an  $m$ th power of one element (itself) while  $p + 1$  is an  $m$ th power of both  $p - 1$  and  $p + 1$ . Hence this case fails.

In the case where  $n + 1$  is prime, let  $f(x) = g^x$  for a primitive root  $g$ . This works, so for any  $m$ , there exists  $f$  if and only if  $n + 1$  is prime.