

# Solution to IMO 2018 shortlisted problems.

Anzo Teh

## Algebra

- A1** Let  $\mathbb{Q}_{>0}$  denote the set of all positive rational numbers. Determine all functions  $f : \mathbb{Q}_{>0} \rightarrow \mathbb{Q}_{>0}$  satisfying

$$f(x^2 f(y)^2) = f(x)^2 f(y)$$

for all  $x, y \in \mathbb{Q}_{>0}$ .

**Answer.** The only function is the constant function  $f(x) = 1$ .

**Solution.** It's not hard to see that the aforementioned function works, so let's show that it's the only working function. Substituting  $x = \frac{1}{f(y)}$  gives  $f(1) = f(\frac{1}{f(y)})^2 f(y)$  and substituting  $y = 1$  gives  $f(\frac{1}{f(1)})^2 = 1$  (since all function values are positive, hence nonzero), and therefore  $f(\frac{1}{f(1)}) = 1$ . This means there's a value  $c_0$  such that  $f(c_0) = 1$ . Therefore plugging  $y = c_0$ , we get  $f(x^2) = f(x)^2$  for all  $x$ , and this gives

$$f(x)^2 f(y) = f(x^2 f(y)^2) = f((xf(y))^2) = f(xf(y))^2$$

and since both  $f(xf(y))^2$  and  $f(x)^2$  are squares of positive rationals,  $f(y)$  is also a square of positive rationals for all  $y$ .

Now suppose that  $f(x) \neq 1$  for some  $x$ . Then there is a maximum positive integer  $n$  such that for all  $x \in \mathbb{Q}^+$ ,  $f(x)$  is a  $2^n$ -th power of a rational. This means for all  $y \in \mathbb{Q}^+$ ,

$$f(y) = \frac{f(xf(y))^2}{f(x)^2}$$

is a square of the  $2^n$ -th power of a rational number. This gives  $f(y)$  as a  $2^{n+1}$ -th power of a rational, contradiction.

- A2** (IMO 2) Find all integers  $n \geq 3$  for which there exist real numbers  $a_1, a_2, \dots, a_{n+2}$  satisfying  $a_{n+1} = a_1$ ,  $a_{n+2} = a_2$  and

$$a_i a_{i+1} + 1 = a_{i+2},$$

for  $i = 1, 2, \dots, n$ .

**Answer.** All  $n$  that are multiples of 3.

**Solution.** (Modified from my solution on AoPS). For  $3 \mid n$  we have the construction that's a repetition of  $(2, -1, -1)$ . For the rest of the solutions we visualize the numbers on a circle. We'll now eliminate the following cases:

**Case  $a_i = 0$  for some  $i$ .** By the cyclic condition above we may assume that  $a_1 = 0$ . Then we must have  $a_2 = a_3 = 1$  and  $a_4 = 2$ , etc. Now some inductive statement shows that if  $a_i, a_{i+1} > 0$  then  $a_{i+2} > 0$ , and we also have  $a_2 > 0$  too. Hence  $a_i > 0$  for all  $i > 0$ , including when  $i = n + 1$ , contradiction.

**Case  $a_i, a_{i+1} > 0$  for some  $i$ .** Again here we consider indices mod  $n$ . Now  $a_{i+2} > 1$ , and therefore  $a_{i+3} > 1$ . Subsequently, we have  $a_{i+4} = a_{i+2}a_{i+3} + 1 > a_{i+2}a_{i+3} \geq a_{i+3} \geq 1$ , which shows that this sequence is actually increasing after  $a_{i+3}$ . This cannot happen since the sequence of real numbers are on a circle.

This therefore implies that between any two positive numbers there must be at least one negative number; if  $a_i, a_{i+1} < 0$  then  $a_{i+2} = a_i a_{i+1} + 1 > 1$ , so there must be at most two negative numbers between any two consecutive positive numbers. As the goal is to show that there are exactly two negative numbers between any two consecutive positive numbers, it suffices to show that the configuration  $+ - +$  cannot happen. To do this we do 'backtracking', i.e. consider  $a_i, a_{i-1}, a_{i-2}$ , etc, given the circular structure of our sequence.

Now suppose that  $a_{i+2} > 0$  and  $a_{i+1} < 0$  and  $a_i > 0$ . We first see that  $a_i a_{i+1} < 0$  so  $a_{i+2} < 1$ . Also  $a_{i+3} < 0$  by the "no consecutive positive" lemma we established in the beginning. This means,  $a_{i+1} a_{i+2} < -1$  and with  $a_{i+2} < 1$  (comparing modulus) we get  $a_{i+1} < -1$ , actually. Now that  $a_i = \frac{a_{i+2}-1}{a_{i+1}}$  with  $|a_{i+2} - 1| < 1$  (since  $0 < a_{i+2} < 1$ ) and  $|a_{i+1}| > 1$  as proven we have  $|a_i| < 1$ ; combining this with  $a_i > 0$  we get  $0 < a_i < 1$ . Going a bit further,  $a_{i-1} = \frac{a_{i+1}-1}{a_i}$ ;  $a_{i+1} < 0$  so  $|a_{i+1} - 1| = |a_{i+1}| + 1$ ; and  $0 < a_i < 1$  so  $|a_{i-1}| = \frac{|a_{i+1}-1|}{|a_i|} > |a_{i+1}| + 1$ , and bear in mind that  $a_{i-1} < 0$  here. Therefore  $a_{i-1} < a_{i+1} - 1$ , i.e. getting more negative. Continuing this backtracking process, we see that the numbers must be alternating in sign, with positive numbers bounded above by 1, and negative numbers given by  $a_{i-1} < a_{i+1} - 1$  whenever both numbers are negative. This cannot happen on a circle, reaching our contradiction.

**A3** Given any set  $S$  of positive integers, show that at least one of the following two assertions holds:

- (1) There exist distinct finite subsets  $F$  and  $G$  of  $S$  such that  $\sum_{x \in F} 1/x = \sum_{x \in G} 1/x$ ;
- (2) There exists a positive rational number  $r < 1$  such that  $\sum_{x \in F} 1/x \neq r$  for all finite subsets  $F$  of  $S$ .

**Solution.** Suppose that there exists a set  $S$  such that both (1) and (2) fail. That is, finite subset sums are pairwise distinct (or injective, if you like), and for each  $r < 1$  there's finite  $F$  with  $\sum_{x \in F} 1/x = r$ . This second contrapositive can be extended to include  $r = 0$  as all we need is the empty set. This  $S$  is infinite because there are at most  $2^n$  subset sums that can be attained by a set of size  $n$  and there are infinitely many positive rational numbers  $r < 1$ . Since  $S \subseteq \mathbb{N}$ , it's countable so we can enumerate  $S \setminus \{1\}$  as  $\{a_1 < a_2 < a_3 < \dots\}$ .

Denote  $s(F)$  as  $\sum_{x \in F} \frac{1}{x}$ , and  $t(F) = \{s(G) : G \subseteq F\}$ . Given that for all  $r < \frac{1}{a_1}$  there is  $F$  such that  $s(F) = r$ , such  $F$  must not contain  $a_1$  (here,  $a_1 > 1$ ). Thus  $\{r \in \mathbb{Q}^+ : r < \frac{1}{a_1}\} \subseteq t(S \setminus \{1, a_1\})$ . Now consider the sum  $s(S \setminus \{1, a_1\})$ . If this diverges, or is  $> \frac{1}{a_1}$ , then we can choose  $N$  (minimal possible) such that

$$s(\{a_2, \dots, a_N\}) = \sum_{i=2}^N \frac{1}{a_i} \geq \frac{1}{a_1}$$

and by the minimality of  $N$ ,  $s(\{a_2, \dots, a_N\}) < \frac{1}{a_N} + \frac{1}{a_1} < \frac{2}{a_1}$ . Therefore  $0 \leq s(\{a_2, \dots, a_N\}) - \frac{1}{a_1} < \frac{1}{a_1}$ . By assumption, there's a finite set  $F_0 \subseteq \{a_2, a_3, \dots\}$  with  $s(F_0) = s(\{a_2, \dots, a_N\}) - \frac{1}{a_1}$ , so  $s(F_0 \cup \{a_1\}) = s(\{a_2, \dots, a_N\})$ . But  $F_0 \cup \{a_1\} \neq \{a_2, \dots, a_N\}$  as one contains  $a_1$  while the other does not, contradiction. Therefore,  $s(S \setminus \{1, a_1\}) \leq \frac{1}{a_1}$  and since  $t(S \setminus \{1, a_1\}) \supseteq \{r \in \mathbb{Q} : r < \frac{1}{a_1}\}$ , equality must hold, and so  $s(S \setminus \{1, a_1\}) = \frac{1}{a_1}$ . This means  $s(S \setminus \{1\}) = \frac{1}{a_1} + \frac{1}{a_1} = \frac{2}{a_1} \leq \frac{2}{2} = 1$  (as  $a_1 \geq 1$ ). But then we have

$$t(S \setminus \{1\}) \supseteq \{r \in \mathbb{Q} : r < 1\}$$

(a set that includes 1 cannot have reciprocal sum less than 1), we have  $a_1 = 2$  and consequently

$$s(S \setminus \{1, a_1\}) = s(S \setminus \{1, 2\}) = \frac{1}{2}$$

Now, we repeat the above for  $a_2$ , and the same logic can be applied to get

$$s(S \setminus \{1, a_1, a_2\}) = \frac{1}{a_2} = s(S \setminus \{1, a_1\}) - \frac{1}{a_2} = \frac{1}{2} - \frac{1}{a_2}$$

which means  $a_2 = 4$ . Continuing this, we get  $a_i = 2^i$  for all  $i \geq 1$ . But then for finite  $F$ , the denominator of  $s(F)$  is a power of 2 in this case, contradiction.

- A4** Let  $a_0, a_1, a_2, \dots$  be a sequence of real numbers such that  $a_0 = 0, a_1 = 1$ , and for every  $n \geq 2$  there exists  $1 \leq k \leq n$  satisfying

$$a_n = \frac{a_{n-1} + \dots + a_{n-k}}{k}.$$

**Answer.**  $\frac{2016}{2017^2}$ .

**Solution.** We'll show a more general statement whereby for each  $m \geq 2$ , the maximum possible value of  $a_{m+1} - a_m$  is  $\frac{(m-1)}{m^2}$ . The equality case can be taken following the following recursive manner: for all  $k \geq 2$  we have

$$a_k = \begin{cases} a_{k-1} & k \leq m-1 \\ \frac{a_{k-1} + \dots + a_0}{k} & k = m \\ \frac{a_{k-1} + \dots + a_1}{k-1} & k = m+1 \end{cases} \quad (1)$$

This means  $a_k = 1$  for all  $k \leq m-1$ ,  $a_m = \frac{m-1}{m} = 1 - \frac{1}{m}$  and  $a_{m+1} = \frac{m-1}{m} = 1 - \frac{1}{m^2}$ . It then follows that the desired difference is  $\frac{1}{m} - \frac{1}{m^2} = \frac{(m-1)}{m^2}$ .

It then remains to prove the bound. We claim the following: conditioned on  $a_0, \dots, a_{m-1}$  (i.e. fixing these variables),

$$\max a_{m+1} - a_m = \frac{(a_{m-1} + \dots + a_1) - (m-1)a_0}{m^2} \quad (2)$$

That is,  $a_m$  is the average of  $a_0, \dots, a_{m-1}$  and  $a_{m+1}$  the average of  $a_1, \dots, a_m$ . Let's first determine when would  $a_{m+1} - a_m$  be maximized. Conditioned on  $a_0, \dots, a_m$  (i.e. fixing these numbers), we need to maximize  $a_{m+1}$ . Next, let  $a_{m+1} = \frac{a_m + \dots + a_{m-k+1}}{k}$  for some  $k$ . Then  $a_{m+1} - a_m = \frac{a_{m-1} + \dots + a_{m-k+1} - (k-1)a_m}{k}$ . Thus conditioned on  $a_1, \dots, a_{m-1}$ , maximizing  $a_{m+1} - a_m$  would require minimizing  $a_m$  too. It follows that to obtain the optimal answer, we take the minimal possible  $a_m$ , and conditioned on  $a_0, \dots, a_m$ , take the maximal possible  $a_{m+1}$ .

Next, we show that, regardless of how  $a_0, \dots, a_m, \dots$  are constructed, the following two sequences:

$$\left\{ \frac{a_0 + \dots + a_m}{m+1} \right\}_{m \geq 1} \quad \left\{ \frac{a_1 + \dots + a_m}{m} \right\}_{m \geq 1} \quad (3)$$

are, respectively, nondecreasing and nonincreasing. By rearranging the terms, we see that an equivalent statement is that for all  $m \geq 1$ ,

$$\frac{a_0 + \dots + a_m}{m+1} \leq a_{m+1} \leq \frac{a_1 + \dots + a_m}{m} \quad (4)$$

We'll do induction on  $m$  for each of them: base case is where  $m = 1$ , and  $\frac{a_0 + a_1}{2} = \frac{1}{2}$ ,  $a_1 = 1$ . Since  $a_2$  can either be  $\frac{1}{2}$  or 1, the conclusion follows.

Inductive step: suppose that our statement holds for all  $m = 1, \dots, m_0$ . Suppose for some  $k \geq 1$  we have  $a_{m_0+1} = \frac{a_{m_0} + \dots + a_{m_0-k+1}}{k}$  with  $1 \leq k \leq m_0 + 1$ . If  $k = m_0 + 1$  we have equality. Otherwise, by our induction hypothesis,

$$\frac{a_0 + \dots + a_{m_0}}{m_0 + 1} \geq \frac{a_0 + \dots + a_{m_0-k}}{m_0 - k + 1} = \left( \frac{m_0 + 1}{m_0 - k + 1} \right) \frac{a_0 + \dots + a_{m_0}}{m_0 + 1} - \frac{k}{m_0 - k + 1} \cdot a_{m_0+1} \quad (5)$$

i.e. rearranging, yields  $a_{m_0+1} \geq \frac{a_0+\dots+a_m}{m_0+1}$ .

The proof for the other sequence is similar (with all signs reverse) with a catch: if only works for  $k \leq m_0$ . The non-covered case is  $k = m_0 + 1$ , so we need to show that  $\frac{a_{m_0}+\dots+a_0}{m_0+1} \leq \frac{a_{m_0}+\dots+a_1}{m_0}$ , or equivalently,  $a_0 \leq \frac{a_{m_0}+\dots+a_1}{m_0}$ . This nevertheless follows from the fact that with  $a_0 < a_1$ , we always have  $a_0 \leq a_m \leq a_1$  (since  $a_m$  is simply the averages of some previous terms for all  $m \geq 2$ ). This finishes the induction step.

Finally, the sequence lemma entails that for each  $m$ , the maximum  $a_{m+1}$  is obtained by taking  $a_{m+1} = \frac{a_1+\dots+a_m}{m}$  and the minimum, by taking  $a_{m+1} = \frac{a_0+\dots+a_m}{m+1}$ . Thus to determine the maximum of  $a_{m+1} - a_m$ , we do

$$a_m = \frac{a_0 + \dots + a_{m-1}}{m} \quad a_{m+1} = \frac{a_1 + \dots + a_m}{m} = \frac{a_1 + \dots + a_{m-1}}{m} + \frac{1}{m^2}(a_0 + \dots + a_{m-1}) \quad (6)$$

It then follows that  $a_{m+1} - a_m = \frac{a_1+\dots+a_{m-1}-(m-1)a_0}{m^2}$ . Finally, to determine the choices of  $a_2, \dots, a_{m-1}$  that maximizes this difference, we take  $a_2, \dots, a_{m-1}$  to be maximum possible, i.e. all  $= a_1$ . Given also  $a_0 = 0$  we have  $\frac{a_1+\dots+a_{m-1}-(m-1)a_0}{m^2} = \frac{m-1}{m^2}$ , as desired.

**A5** Determine all functions  $f : (0, \infty) \rightarrow \mathbb{R}$  satisfying

$$\left(x + \frac{1}{x}\right) f(y) = f(xy) + f\left(\frac{y}{x}\right)$$

for all  $x, y > 0$ .

**Answer.**  $f(x) = Ax + \frac{B}{x}$  for some real constants  $A, B$ .

**Solution.** We first see that this function works since in our equation we have LHS = RHS =  $A(xy + \frac{y}{x}) + B(\frac{x}{y} + \frac{1}{xy})$ . We will now focus on showing that these are the only working ones.

Fixing  $x > 1$  and an integer  $n$ , we substitute  $y = x^n$  into the original equation, letting  $a_n = f(x^n)$  we get the recurrence relation

$$a_{n+1} - \left(x + \frac{1}{x}\right)a_n + a_{n-1} = 0$$

so this has characteristic polynomial (in  $z$ )  $z^2 - (x + \frac{1}{x})z + 1 = 0$ , which has roots  $x$  and  $\frac{1}{x}$ . Thus we have  $f(x^n) = a(x)x^n + \frac{b(x)}{x^n}$  for all integers  $n$ , with  $a(x)$  and  $b(x)$  are real constants. Note that  $f(1) = a(x) + b(x)$  so we may write  $b(x) = C - a(x)$  for all  $x$ , with  $C = f(1)$ . In addition  $a(x) = a(y)$  for all  $y = x^n$  where  $n$  integer.

We now show that  $a(x) = a(y)$  for all  $x, y \neq 1$ . By before, we may assume that  $x \neq y$  and  $x \neq \frac{1}{y}$ . Consider substituting  $x^n$  into  $x$  and  $y^n$  into  $y$  in the original equation, we get

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

$$\left(x^n + \frac{1}{x^n}\right) \left(a(y)y^n + \frac{C - a(y)}{y^n}\right) = a(xy)x^n y^n + \frac{C - a(xy)}{x^n y^n} + a(y/x)(y/x)^n + \frac{C - a(y/x)}{(y/x)^n}$$

Rearranging, we get

$$(a(xy) - a(y))(x^n y^n - \frac{1}{x^n y^n}) + (a(\frac{y}{x}) - a(y))((\frac{y}{x})^n - (\frac{x}{y})^n) = 0$$

In addition, by comparing  $n = 1$  and  $n = 2$  we get

$$(a(xy) - a(y))(xy - \frac{1}{xy})(xy + \frac{1}{xy}) + (a(\frac{y}{x}) - a(y))(\frac{y}{x} - \frac{x}{y})(\frac{y}{x} + \frac{x}{y}) = 0$$

Note that  $xy - \frac{1}{xy}$  and  $\frac{y}{x} - \frac{x}{y}$  are nonzero since  $x \neq y$  and  $xy \neq 1$ . This subsequently implies that  $xy + \frac{1}{xy} \neq \frac{y}{x} + \frac{x}{y}$  since both  $x, y$  are not equal to 1. Consequently, we must have  $a(xy) = a(y/x) = a(y)$ . By considering all possible  $x$  and  $y$ 's we have  $a(x)$  constant for all  $x \neq 1$ , which will then show that  $f$  is indeed in the form  $Ax + \frac{B}{x}$ .

## Combinatorics

- C1** Let  $n \geq 3$  be an integer. Prove that there exists a set  $S$  of  $2n$  positive integers satisfying the following property: For every  $m = 2, 3, \dots, n$  the set  $S$  can be partitioned into two subsets with equal sums of elements, with one of subsets of cardinality  $m$ .

**Solution.** We use the following:

$$\{2 \cdot 3^{n-1}, 3^{n-1}, 2 \cdot 3^{n-2}, 3^{n-2}, \dots, 2 \cdot 3, 3, a, b\}$$

where  $a$  and  $b$  are simply any pair of numbers such that the sum of the set is  $2 \cdot 3^n$ . This is possible because the first  $2(n-1)$  elements have sum

$$3^n + 3^{n-1} + \dots + 3^2 = 3^2 \left( \frac{3^{n-1} - 1}{3 - 1} \right) = \frac{3 \cdot 3^n - 9}{2} < 2 \cdot 3^n$$

(To avoid  $a, b$  being the same as any other elements in the set we could just take  $a, b$  both not divisible by 3). A set with  $m$  elements can be taken as:

$$\{2 \cdot 3^{n-1}, 2 \cdot 3^{n-2}, \dots, 2 \cdot 3^{n-m+1}, 3^{n-m+1}\}$$

which all has sum  $3^n$ .

- C2** (IMO 4) A site is any point  $(x, y)$  in the plane such that  $x$  and  $y$  are both positive integers less than or equal to 20.

Initially, each of the 400 sites is unoccupied. Amy and Ben take turns placing stones with Amy going first. On her turn, Amy places a new red stone on an unoccupied site such that the distance between any two sites occupied by red stones is not equal to  $\sqrt{5}$ . On his turn, Ben places a new blue stone on any unoccupied site. (A site occupied by a blue stone is allowed to be at any distance from any other occupied site.) They stop as soon as a player cannot place a stone.

Find the greatest  $K$  such that Amy can ensure that she places at least  $K$  red stones, no matter how Ben places his blue stones.

**Answer.**  $K = 100$ .

**Solution.** If we colour the whole lattice space in chessboard fashion, then Amy can focus on putting all the stones on white grid (any sites with distance  $\sqrt{5}$  must have different colours). Since there are 200 white grids and players take alternate turns, then Amy can achieve at least 100.

Now let's design a strategy that prevents Amy from achieving more than 100. We first consider partitioning the  $20 \times 20$  grid into 25  $4 \times 4$  grid. For each of the  $4 \times 4$  grid, we do the following labelling:

A1	C2	D1	B2
D2	B1	A2	C1
C1	A2	B1	D2
B2	D1	C2	A1

Ben's strategy is to place the stone at the location with the same label where Amy put the stone at (e.g. if Amy put it in the topleft corner, A1, then Ben would do the bottomright corner).

Let's now show that Amy can only place one stone in each of A, B, C, and D-labelled stones. Consider a grid with label  $XY$  which Amy places a stone ( $X \in \{A, B, C, D\}$  and  $Y \in \{1, 2\}$ ). Then Ben would put in another  $XY$  grid. Both the grids with label  $XY'$  ( $Y'=1$  if  $Y=2$  and vice versa) are distance  $\sqrt{5}$  away from both the  $XY$  grid, thereby forbidden to be placed by Amy by our rules. It then follows that Amy cannot place more than  $25 \times 4 = 100$  stones.

- C3** Let  $n$  be a given positive integer. Sisyphus performs a sequence of turns on a board consisting of  $n + 1$  squares in a row, numbered 0 to  $n$  from left to right. Initially,  $n$  stones are put into square 0, and the other squares are empty. At every turn, Sisyphus chooses any nonempty square, say with  $k$  stones, takes one of these stones and moves it to the right by at most  $k$  squares (the stone should stay within the board). Sisyphus' aim is to move all  $n$  stones to square  $n$ . Prove that Sisyphus cannot reach the aim in less than

$$\left\lceil \frac{n}{1} \right\rceil + \left\lceil \frac{n}{2} \right\rceil + \left\lceil \frac{n}{3} \right\rceil + \cdots + \left\lceil \frac{n}{n} \right\rceil$$

turns. (As usual,  $\lceil x \rceil$  stands for the least integer not smaller than  $x$ .)

**Solution.** Label the stones as  $1, 2, \dots, n$ . At each turn, all it matters is the square where a stone is chosen to be thrown (and not a particular stone from that square). Therefore we can assume that at each turn when a particular square is chosen, the stone with the largest label in the square is chosen to be moved. If the square has  $k$  stones, then the stone with largest label has at label at least  $k$  but it can only be moved at most  $k$  steps. We then conclude that for each stone with label  $i$ , it can only be moved by at most  $i$  steps to the right.

Thus we conclude that  $\lceil \frac{n}{i} \rceil$  steps is required to move stone labelled  $i$  from 0 to  $n$ , and summing up gives the inequality.

## Geometry

- G1** (IMO 1) Let  $\Gamma$  be the circumcircle of acute triangle  $ABC$ . Points  $D$  and  $E$  are on segments  $AB$  and  $AC$  respectively such that  $AD = AE$ . The perpendicular bisectors of  $BD$  and  $CE$  intersect minor arcs  $AB$  and  $AC$  of  $\Gamma$  at points  $F$  and  $G$  respectively. Prove that lines  $DE$  and  $FG$  are either parallel or they are the same line.

**Solution.** (Paraphrased from my post on AoPS). Skipping angle-chasing algebra here, it suffices to show that  $\angle AFD = \angle AGE$ . We first show that these two angles must be at most  $90^\circ$ . To begin with, the fact that  $D$  lies on line segment  $AB$  means that  $\angle AFD \leq \angle AFB = 180^\circ - \angle ACB$ , so we may assume that  $\angle ACB < 90^\circ$ . Next, we have  $BF = FD$  (by the definition of perpendicular bisector), and  $\angle FBA \leq \angle ACB$  (think of the angle subtended by  $AB$  and angle subtended by  $AF$ ). This gives  $\angle BFD \geq 180^\circ - 2\angle ACB$  and thus  $\angle AFD \leq \angle ACB \leq 90^\circ$ . Similarly  $\angle AGE \leq 90^\circ$ . Now that the sin function is injective in  $[0, 90^\circ]$ , it's enough to prove that  $\sin \angle AFD = \sin \angle AGE$ . This isn't hard either: by sine rule we have

$$\frac{\sin \angle AFD}{AD} = \frac{\sin \angle FAD}{FD} = \frac{\sin \angle FAB}{FB} = \frac{\sin \angle GAC}{GC} = \frac{\sin \angle GAE}{GE} = \frac{\sin \angle AGE}{AE}$$

where the desired equality follows from that  $AD = AE$ . (Notice the implicit use of the facts  $FD = FB, GC = GE$ , and  $\frac{\sin \angle FAB}{FB} = \frac{\sin \angle GAC}{GC}$  follows from that  $FB$  and  $GC$  are chords of the same circle.

- G2** Let  $ABC$  be a triangle with  $AB = AC$ , and let  $M$  be the midpoint of  $BC$ . Let  $P$  be a point such that  $PB < PC$  and  $PA$  is parallel to  $BC$ . Let  $X$  and  $Y$  be points on the lines  $PB$  and  $PC$ , respectively, so that  $B$  lies on the segment  $PX$ ,  $C$  lies on the segment  $PY$ , and  $\angle PXM = \angle PYM$ . Prove that the quadrilateral  $APXY$  is cyclic.

**Solution.** Consider the circumcircle  $\Gamma$  of  $PXY$ , and consider the antipode  $D$  of  $P$  w.r.t.  $\Gamma$ . Consider  $A_1$  as the second intersection of  $DM$  and  $\Gamma$ . We'll show that  $A = A_1$ .

Let's first see how would  $A$  be defined if only  $P, X, Y, M$  are given: we have  $BM = MC$  so  $PM$  is the median line to  $BC$ . With  $AP \parallel BC$ , the lines  $(PA, PM; PB, PC)$  is a harmonic bundle. Therefore the line  $PA$  can be constructed this way, and also  $PA \perp AM$  since

$PA \parallel BC$  and  $AM \perp BC$ . Therefore all it remains to show is that  $(PA_1, PM; PB, PC)$  is harmonic bundle, and that  $PA_1 \perp A_1M$ , The second relation  $PA_1 \perp A_1M$ , or equivalently  $\angle PA_1M = 90^\circ$ , follows from that  $PM$  is the antipode of  $\Gamma$  so we're left with showing  $(PA_1, PM; PB, PC)$  is harmonic bundle.

Using directed angles,  $\angle(A_1P, PX) = \angle(A_1D, DX)$  and  $\angle(A_1P, PY) = \angle(A_1D, DY)$ . Using the relation  $\angle PXM = \angle PYM$ , and  $\angle PXD = \angle PYD = 90^\circ$ , we have  $\angle MXD = \angle MYD$ . We also have the relation (consider the concurrent lines  $DM, MX, MY$  and the triangle  $DMY$ )

$$\begin{aligned} 1 &= \frac{\sin \angle XDM}{\sin \angle YDM} \cdot \frac{\sin \angle DYM}{\sin \angle XYM} \cdot \frac{\sin \angle MXY}{\sin \angle MXD} \\ &= \frac{\sin \angle XDM}{\sin \angle YDM} \cdot \frac{\sin \angle MYD}{\sin \angle MXD} \cdot \frac{\sin \angle MXY}{\sin \angle XYM} \\ &= \frac{\sin \angle XDM}{\sin \angle YDM} \cdot \frac{\sin \angle MXY}{\sin \angle MYX} \end{aligned}$$

due to Ceva because  $\angle MYD = \angle MXD$ . By looking at point  $M$  and triangle  $PXY$  we also have

$$\begin{aligned} 1 &= \frac{\sin \angle MXY}{\sin \angle MYX} \cdot \frac{\sin \angle MYP}{\sin \angle YPM} \cdot \frac{\sin \angle XPM}{\sin \angle PXM} \\ &= \frac{\sin \angle MXY}{\sin \angle MYX} \cdot \frac{\sin \angle XPM}{\sin \angle YPM} \end{aligned}$$

because  $\angle MYP = \angle PXM$ . Thus considering the two equations give

$$\frac{\sin \angle XDM}{\sin \angle YDM} = \frac{\sin \angle XPM}{\sin \angle YPM}$$

and by the earlier directed angle identity

$$\frac{\sin \angle XPA_1}{\sin \angle YPA_1} = \frac{\sin \angle XDM}{\sin \angle YDM} = \frac{\sin \angle XPM}{\sin \angle YPM}$$

which then show that  $(PA_1, PM; PX, PY)$  is a harmonic bundle.

**G3** A circle  $\omega$  with radius 1 is given. A collection  $T$  of triangles is called good, if the following conditions hold:

- each triangle from  $T$  is inscribed in  $\omega$ ;
- no two triangles from  $T$  have a common interior point.

Determine all positive real numbers  $t$  such that, for each positive integer  $n$ , there exists a good collection of  $n$  triangles, each of perimeter greater than  $t$ .

**Answer.** Any  $t \leq 4$ .

**Solution.** Let's first construct a series of solution for  $t = 4$ . Set  $A$  and  $C_0$  as the diameter of the circle, and focus on just one side of the arc separated by  $A$  and  $C_0$  (i.e. a semicircle). Then for any  $B$  on the semicircle, the perimeter of  $ABC_0$  is  $> 4$  (so long as this is not degenerate).

Consider, now, the following algorithm: start with  $B_1$  anywhere on the semicircle. Thereafter, suppose we have  $B_i$  on the semicircle not equal to  $A$  or  $C_0$ . Consider moving  $C_i$  on the minor arc from  $B_i$  to  $C_0$ . The perimeter would move continuously (and increasing) from  $2AB_i$  (i.e.  $< 4$ ) to the perimeter of  $AB_iC_0$  (which is  $> 4$ ), so there by intermediate value theorem there's a point  $C'_i$  in this minor arc such that  $AB_iC'_i$  has perimeter 4. This means we may choose  $C_i \in$  the minor arc  $(C'_i, C_0)$  to ensure perimeter of  $AB_iC_i$  is  $> 4$ , and choose  $B_{i+1}$  strictly in the minor arc  $(C_i, C_0)$ , thereby making sure that the triangles

$AB_iC_i$  do not intersect in interior point. Thus we can construct arbitrarily many such triangles.

Now suppose  $t > 4$ . Consider  $\epsilon = t - 4 > 0$ . Since the total length of any two sides is at most 4, the shortest side must have length at least  $\epsilon$ , i.e. the angle subtended by the center must exceed  $\epsilon$ . Now we proceed with the following:

**Lemma 1.** *Given an arc of unit circle of measure  $\theta$ , the number of triangles with all angles  $\geq \epsilon$  that can be placed on this circle (with no intersection), denoted by  $f(\theta)$ , is no more than  $\max(0, \lfloor \frac{\theta}{\epsilon} \rfloor - 1)$ .*

*Proof.* Within an arc of  $< 2\epsilon$ , among three vertices, two of them is  $< \epsilon$  apart. It then follows that we need an arc of measure at least  $2\epsilon$  to place a single triangle of the said criterion.

For induction purpose, assume that our statement is true for all  $\theta' \leq k\epsilon$  for some  $k \geq 2$ . Consider, now, an arc with measure  $\theta$  such that  $\theta \leq (k+1)\epsilon$ . Consider any triangle  $ABC$  satisfying the condition, and let the endpoints of arc be  $D$  and  $E$ . Here, we may pick such  $ABC$  such that  $D, A, B, C, E$  are in that order, and  $(DA) + (CE)$  is as small as possible. Given also that the triangles do not intersect each other in the interior, it follows that no other triangles are in the  $(DA)$  or  $(CE)$  region.

In addition, any triangle with a vertex in  $AB$  must have all vertices in  $AB$ , similarly for  $BC$ . Given also that  $(AB)$  and  $(BC)$  have measures  $\geq \epsilon$ , by induction hypothesis the number of valid triangles is bounded by

$$1 + (\lfloor \frac{(AB)}{\epsilon} \rfloor) - 1 + (\lfloor \frac{(BC)}{\epsilon} \rfloor) - 1 \leq \lfloor \frac{(AB) + (BC)}{\epsilon} \rfloor - 1 \leq \lfloor \frac{(DE)}{\epsilon} \rfloor - 1$$

as desired. □

In particular, considering the whole circle, we cannot have more than  $\frac{2\pi}{\epsilon} - 1$  such triangles. Therefore, any  $n$  with  $n > \frac{2\pi}{\epsilon} - 1$  would fail.

- G4** A point  $T$  is chosen inside a triangle  $ABC$ . Let  $A_1, B_1$ , and  $C_1$  be the reflections of  $T$  in  $BC, CA$ , and  $AB$ , respectively. Let  $\Omega$  be the circumcircle of the triangle  $A_1B_1C_1$ . The lines  $A_1T, B_1T$ , and  $C_1T$  meet  $\Omega$  again at  $A_2, B_2$ , and  $C_2$ , respectively. Prove that the lines  $AA_2, BB_2$ , and  $CC_2$  are concurrent on  $\Omega$ .

**Solution.** Denote  $\omega_A, \omega_B, \omega_C$  as the circumcircles of  $TB_1C_1, TA_1C_1$ , and  $TA_1B_1$ , respectively. These circles have centers  $A, B, C$  by the definition of reflection.

Consider, now, the common chord of  $\omega_A$  and  $\omega_C$ , i.e.  $TB_1$ . The angle subtended by  $TB_1$  (on the circumference) on  $\omega_A$  and  $\omega_C$  are  $\angle TC_1B_1$  and  $\angle TA_1B_1$ , respectively. In other words, since  $AC$  is the perpendicular bisector of  $TB_1$ , we have

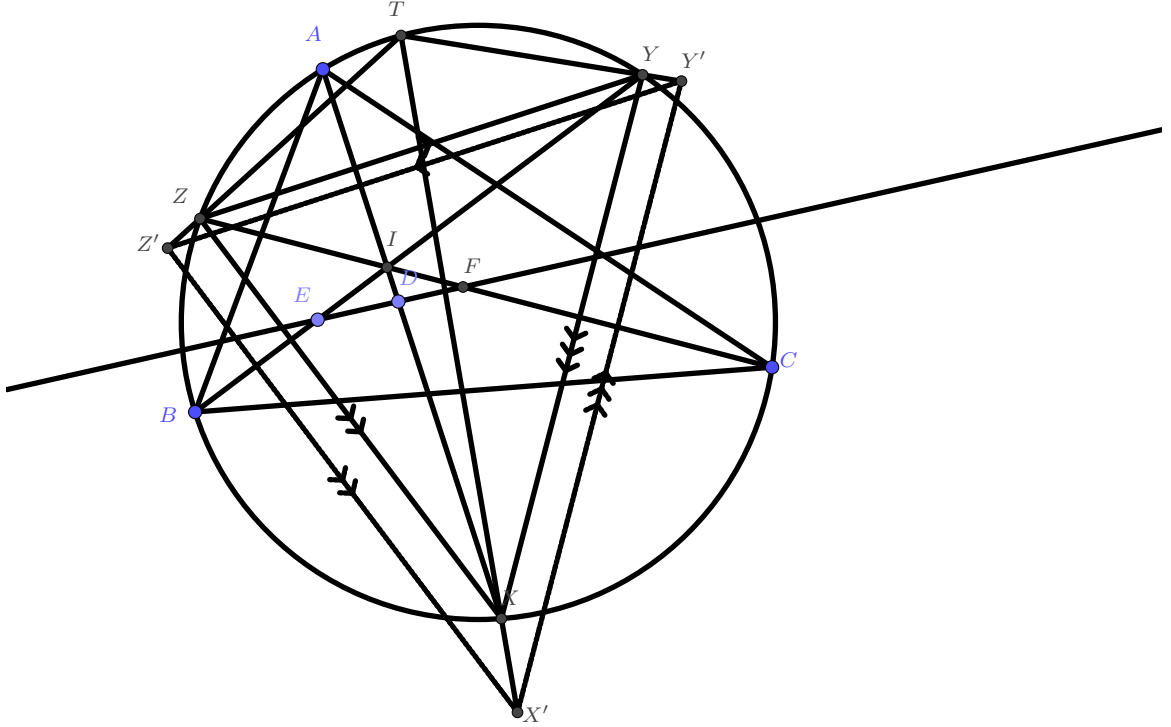
$$\angle CAB_1 = \frac{1}{2} \angle TAB_1 = \angle TC_1B_1 = \angle C_2C_1B_1 = \angle C_2A_2B_1$$

and similarly  $\angle ACB_1 = \angle A_2C_2B_1$ . It follows that triangles  $ACB_1$  and  $A_2C_2B_1$  are similar (and in fact, determined by spiral similarity under center  $B_1$ ). This means we have  $\angle(B_1A_2, AA_2) = \angle(B_1C_2, CC_2)$ , which means that  $AA_2$  and  $CC_2$  will meet on the circumcircle of  $AB_1A_2C_2$ , i.e.  $\Omega$ . Similarly we can deduce that the other two pairs  $AA_2$  and  $BB_2$ , and  $BB_2$  and  $CC_2$ , will meet on  $\Omega$ .

- G5** Let  $ABC$  be a triangle with circumcircle  $\Omega$  and incentre  $I$ . A line  $\ell$  intersects the lines  $AI, BI$ , and  $CI$  at points  $D, E$ , and  $F$ , respectively, distinct from the points  $A, B, C$ , and  $I$ . The perpendicular bisectors  $x, y$ , and  $z$  of the segments  $AD, BE$ , and  $CF$ , respectively determine a triangle  $\Theta$ . Show that the circumcircle of the triangle  $\Theta$  is tangent to  $\Omega$ .



**Solution.** Let  $AI, BI, CI$  intersect  $\Omega$  again at  $X, Y, Z$  (i.e. the midpoints of arcs  $BC, CA, AB$  not containing the other point). Then  $XY, YZ, ZX$  are perpendicular bisectors of  $CI, AI, BI$ , respectively. Now let  $x \cap y = Z', y \cap z = X'$  and  $x \cap z = Y'$ , then  $XYZ$  and  $X'Y'Z'$  are homothetic with each other, so it suffices to show that the homothetic center,  $T$ , lies on  $\Omega$ .



Now we consider just the angle  $\angle(ZX, XT)$  vs  $\angle(XT, XY)$ . Let  $d(a, b)$  be the distance between parallel lines  $a, b$ , then

$$\frac{\sin \angle(ZX, XT)}{\sin \angle(XT, XY)} = \frac{d(ZX, Z'X')}{d(XY, X'Y')} = \frac{IE}{IF} = \frac{\sin \angle IFE}{\sin \angle IEF}$$

and since  $\angle IFE + \angle IEF = \angle ZXY$ , we have  $\angle(ZX, XT) = \angle(EF, IE) = \angle(\ell, IF)$  and similarly  $\angle(XT, XY) = \angle(IE, \ell)$ . Then similarly,  $\angle(ZY, YT) = \angle(\ell, IF)$ , so  $\angle(ZX, XT) = \angle(ZY, YT)$  and  $T$  lies on  $\Omega$ .

- G6** (IMO 6) A convex quadrilateral  $ABCD$  satisfies  $AB \cdot CD = BC \cdot DA$ . Point  $X$  lies inside  $ABCD$  so that

$$\angle XAB = \angle XCD \quad \text{and} \quad \angle XBC = \angle XDA.$$

Prove that  $\angle BXA + \angle DXC = 180^\circ$ .

**Solution.** Now consider the second intersection (namely  $Y$ ) of the circles  $ABX$  and  $CDX$ , we get (using oriented angles to prevent case distinction)  $\angle(YB, YX) = \angle(AB, AX) = \angle(CD, CX) = \angle(YD, YX)$  (the first and the last inequality follows from that  $A, B, Y, X$  and  $C, D, Y, X$  are each concyclic; the middle one follows from the problem condition). Thus we get that  $YD, YB$  are actually the same line (so  $Y, D, B$  collinear). Also from we have  $\angle XBC = \angle XDA$  which translates into  $\angle(XB, BC) = \angle(XD, AD)$  so we get  $\angle(AY, YX) = \angle(AB, BX) = \angle(AB, BC) - \angle(XB, BC)$  and  $\angle(CD, AD) - \angle(XD, AD) = \angle(CD, DX) = \angle(CY, YX)$  This gives the important property:

$$\angle(AY, CY) = \angle(AY, YX) - \angle(CY, YX) = \angle(AB, BC) - \angle(CD, AD)$$

Now the condition  $AB \cdot CD = \angle BC \cdot DA$  means that the tangents to triangle  $ABD$  and the tangents to triangle  $BCD$  will intersect at a point  $Z$  on line  $BD$  (think of Apollonius circle) and by the properties of tangents we have  $\angle(BD, AD) = \angle(AB, BZ)$  so  $\angle(AB, BD) - \angle(BD, AD) = \angle(AB, BD) - \angle(AB, AZ) = \angle(AZ, BD)$  and similarly we have  $\angle(BD, BC) - \angle(CD, BD) = \angle(BD, CZ)$  so adding these two up we get

$$\begin{aligned}\angle(AY, CY) &= \angle(AB, BC) - \angle(CD, AD) = \angle(AB, BD) - \angle(BD, AD) + \angle(BD, BC) - \angle(CD, BD) \\ &= \angle(AZ, BD) + \angle(BD, CZ) = \angle(AZ, CZ)\end{aligned}$$

Thus  $Y$  lies on the circle  $ACZ$ , and the fact that  $Z$  is the centre of Apollonius circle means that  $AZ = ZC$ . WLOG assume that  $Z$  is closer to  $B$  than  $D$ . Now  $\angle BXA = \angle BYA = \angle AYZ = \angle ZCA = \angle ZAC = \angle ZYC = 180^\circ - \angle DYC = \angle DXC$ , the second last inequality follows from our earlier claim that  $B, Y, D$  are collinear. So  $\angle BXA + \angle DXC = 180^\circ$ , Q.E.D.

**G7** Let  $O$  be the circumcentre, and  $\Omega$  be the circumcircle of an acute-angled triangle  $ABC$ . Let  $P$  be an arbitrary point on  $\Omega$ , distinct from  $A, B, C$ , and their antipodes in  $\Omega$ . Denote the circumcentres of the triangles  $AOP$ ,  $BOP$ , and  $COP$  by  $O_A$ ,  $O_B$ , and  $O_C$ , respectively. The lines  $\ell_A, \ell_B, \ell_C$  perpendicular to  $BC, CA$ , and  $AB$  pass through  $O_A, O_B$ , and  $O_C$ , respectively. Prove that the circumcircle of triangle formed by  $\ell_A, \ell_B$ , and  $\ell_C$  is tangent to the line  $OP$ .

**Solution.** The solution will be elaborated, but the end goal is to prove that the point of tangency will be the point  $P$ .

First, denote  $\ell$  as the perpendicular bisector of  $OP$ , then  $O_A, O_B$  and  $O_C$ . We'll use the fact that the orthocenter and circumcenter are harmonic conjugates of each other w.r.t. a triangle. Let's first do some angle chasing: given that  $OA = OP = OB$ ,  $OO_A, OO_B$  is internal angle bisector of  $\angle OAP$  and  $\angle OPB$ , respectively. If  $m_C$  is the perpendicular bisector of  $AB$  then  $m_C$  is also the angle bisector of  $\angle AOB$  and some angle chasing yields that  $m_C$  and  $OP$  are conjugates w.r.t.  $\angle O_A O O_B$ . Since  $OP \perp O_A O_B$ , the circumcenter of  $OO_A O_B$  lies on  $m_C$ , which is perpendicular to  $AB$  and therefore parallel to  $\ell_C$ .

We now consider the point  $O$ , the line  $\ell$  with points  $O_A, O_B, O_C$  on it, and the lines  $\ell_A, \ell_B, \ell_C$ . Consider the point  $C_1$  as the intersection of  $\ell_A$  and  $\ell_B$ ; we first show that  $O_A, O_B, C_1, P$  are concyclic. Since  $O$  and  $P$  are symmetric w.r.t.  $\ell$ ,  $\angle(O_A P, O_B P) = -\angle(O_A O, O_B O)$ . If we name  $m_A, m_B$  as how we name  $m_C$  before (that is, these lines pass through  $O$ , and contain the circumcenters of triangles  $OO_B O_C, OO_C O_A$  and  $OO_A O_B$ , respectively), then  $\ell_A \parallel m_A$  and similarly for the others. Therefore:

$$\angle(O_A C_1, O_B C_1) = \angle(\ell_A, \ell_B) = \angle(m_A, m_B)$$

The last angle might be hard to gauge, but given  $m_A$  contain the circumcenter of triangle  $OO_B O_C$ , it also contains the antipode of  $O$  w.r.t. this circumcircle, namely,  $X_A$ . This means  $90^\circ = \angle(OO_B, O_B X_A) = \angle(OO_C, O_C X_A)$ . This gives

$$\begin{aligned}\angle(m_A, OO_C) &= \angle(OX_A, OO_C) = \angle(O_B X_A, O_B O_C) \\ &= \angle(O_B X_A, OO_B) + \angle(OO_B, O_B O_C) = 90^\circ + \angle(OO_B, O_B O_C) = 90^\circ + \angle(OO_B, \ell)\end{aligned}$$

and similarly  $\angle(m_B, OO_C) = 90^\circ + \angle(OO_A, \ell)$ . Therefore

$$\begin{aligned}\angle(m_A, m_B) &= \angle(m_A, OO_C) - \angle(m_B, OO_C) = \angle(OO_B, \ell) - \angle(OO_A, \ell) \\ &= \angle(OO_B, OO_A) = \angle(O_A P, O_B P)\end{aligned}$$

which then gives  $\angle(O_A P, O_B P) = \angle(m_A, m_B) = \angle(O_A C_1, O_B C_1)$  so  $C_1$  lies on the circle  $O_A O_B P$ , as claimed.

Define  $A_1, B_1$  similarly above and we get identities like above; we are now in a position to show that  $P$  lies on the circumcircle of  $A_1B_1C_1$ . To see why:

$$\begin{aligned}\angle(C_1P, A_1P) &= \angle(C_1P, PO_B) - \angle(A_1P, PO_B) = \angle(C_1O_A, O_AO_B) - \angle(A_1P_C, O_BO_C) \\ &= \angle(C_1O_A, \ell) - \angle(A_1P_C, \ell) = \angle(C_1O_A, A_1P_C) = \angle(C_1B_1, A_1B_1)\end{aligned}$$

which shows  $C_1, B_1, A_1, P$  are indeed concyclic. To show that  $OP$  is tangent to this circle, we need to show that  $\angle(A_1P, OP) = \angle(A_1C_1, C_1P)$ . We first have

$$\angle(A_1P, OP) = \angle(A_1P, A_1O_B) + \angle(A_1O_B, OP) = \angle(O_CP, O_CO_B) + \angle(\ell_B, OP)$$

Notice that the last equality is the same as  $\angle(O_CP, O_CO_B) + \angle(\ell_B, OP) = \angle(O_CP, \ell) + \angle(\ell_B, OP) = -\angle(OO_C, \ell) + \angle(\ell_B, OP)$  as  $O$  and  $P$  are symmetric w.r.t  $\ell$ . But by before,  $\angle(m_B, OO_C) = 90^\circ + \angle(OO_A, \ell)$  so by similar logic  $90^\circ + \angle(OO_C, \ell) = \angle(m_B, OO_A) = \angle(\ell_B, OO_A)$ . Thus

$$\begin{aligned}\angle(A_1P, OP) &= -\angle(OO_C, \ell) + \angle(\ell_B, OP) = 90^\circ - \angle(\ell_B, OO_A) + \angle(\ell_B, OP) \\ &= 90^\circ + \angle(OO_A, OP) = \angle(OO_A, \ell)\end{aligned}$$

the last equality because  $OP$  perpendicular  $\ell$ . Meanwhile,

$$\begin{aligned}\angle(A_1C_1, C_1P) &= \angle(\ell_B, C_1P) = \angle(\ell_B, O_AC_1) + \angle(O_AC_1, C_1P) \\ &= \angle(\ell_B, \ell_A) + \angle(\ell, O_BP) = \angle(OO_A, OO_B) + \angle(OO_B, \ell) = \angle(OO_A, \ell)\end{aligned}$$

where  $\angle(\ell_B, \ell_A) = \angle(O_BP, \angle O_AP) = \angle(OO_A, OO_B)$  and  $\angle(\ell, O_BP) = \angle(OO_B, \ell)$  are because  $O$  and  $P$  are symmetric w.r.t.  $\ell$ . Thus  $\angle(A_1P, OP) = \angle(OO_A, \ell) = \angle(A_1C_1, C_1P)$ , Q.E.D.

## Number Theory

**N1** Determine all pairs  $(n, k)$  of distinct positive integers such that there exists a positive integer  $s$  for which the number of divisors of  $sn$  and of  $sk$  are equal.

**Answer.** All pairs  $(n, k)$  such that neither of them divides each other.

**Solution.** If  $k \mid n$  then  $sk$  is a proper divisor of  $sn$ , so  $sn$  always has strictly more divisors than  $sk$ .

Now we show that if  $n$  and  $k$  do not divide each other then there exists such an  $s$ . To do this, let primes  $p_1, \dots, p_k$  and  $q_1, \dots, q_\ell$  be all the primes such that the power dividing  $n$  and  $k$  are not equal. such that the power of  $p_i$  dividing  $n$  and  $k$  are  $a_i$  and  $b_i$ , respectively, and power of  $q_i$  dividing  $n$  and  $k$  are  $c_i$  and  $d_i$ , respectively. Also consider  $a_i < b_i$ ,  $c_i > d_i$ . We have  $k, \ell \geq 1$  by our problem condition.

Now consider the number  $N = k\ell(\max(\max a_i, \max b_i, \max c_i, \max d_i) + 1)$ , and integers  $e_1, \dots, e_k, f_1, \dots, f_\ell$  such that

$$\frac{a_i + e_i + 1}{b_i + e_i + 1} = \frac{N - i\ell}{N - (i-1)\ell} \quad \frac{d_i + f_i + 1}{c_i + f_i + 1} = \frac{N - ki}{N - k(i-1)}$$

These have solutions  $e_i = \frac{(b_i - a_i)N}{\ell} - 1$  and  $f_i = \frac{(c_i - d_i)N}{k} - 1$ , which are nonnegative integers since  $N$  is divisible by both  $k$  and  $\ell$ . Thus, if  $s = \prod_{i=1}^k p_i^{e_i} \prod_{j=1}^\ell q_j^{f_j}$  then

$$\begin{aligned}\frac{d(sn)}{d(sk)} &= \frac{\prod_{i=1}^k (a_i + e_i + 1) \prod_{i=1}^\ell (c_i + f_i + 1)}{\prod_{i=1}^k (b_i + e_i + 1) \prod_{i=1}^\ell (d_i + f_i + 1)} \\ &= \frac{\prod_{i=1}^k (N - i\ell) \prod_{i=1}^\ell (N - k(i-1))}{\prod_{i=1}^k (N - (i-1)\ell) \prod_{i=1}^\ell (N - ki)} = \frac{N - k\ell}{N} \cdot \frac{N}{N - k\ell} = 1\end{aligned}$$

as desired.

**N2** Let  $n > 1$  be a positive integer. Each cell of an  $n \times n$  table contains an integer. Suppose that the following conditions are satisfied:

- Each number in the table is congruent to 1 modulo  $n$ .
- The sum of numbers in any row, as well as the sum of numbers in any column, is congruent to  $n$  modulo  $n^2$ .

Let  $R_i$  be the product of the numbers in the  $i^{\text{th}}$  row, and  $C_j$  be the product of the number in the  $j^{\text{th}}$  column. Prove that the sums  $R_1 + \cdots + R_n$  and  $C_1 + \cdots + C_n$  are congruent modulo  $n^4$ .

**Solution.** A routine algebra exercise. The  $ij$ -th entry can be written as  $na_{ij} + 1$  for some positive integer  $a_{ij}$ , which satisfies that for all  $i$  and  $j$ ,

$$n \mid \sum_{k=1}^n a_{ik} \quad n \mid \sum_{k=1}^n a_{kj}$$

We also have

$$\begin{aligned} R_i &= \prod_{k=1}^n (na_{ik} + 1) \equiv 1 + n \sum_{k=1}^n a_{ik} + n^2 \sum_{1 \leq k < \ell \leq n} a_{ik} a_{i\ell} + n^3 \sum_{1 \leq k < \ell < m \leq n} a_{ik} a_{i\ell} a_{im} \\ C_j &= \prod_{k=1}^n (na_{kj} + 1) \equiv 1 + n \sum_{k=1}^n a_{kj} + n^2 \sum_{1 \leq k < \ell \leq n} a_{kj} a_{\ell j} + n^3 \sum_{1 \leq k < \ell < m \leq n} a_{kj} a_{\ell j} a_{mj} \end{aligned}$$

both taken modulo  $n^4$ . We now compare the coefficients of  $1, n, n^2, n^3$  in  $R_1 + \cdots + R_n$  and  $C_1 + \cdots + C_n$ . We will, in fact, show that the difference of each term is divisible by  $n^4$ . The coefficient of 1 in both expressions are 1, and the coefficient of  $n$  in  $R_1 + \cdots + R_n$  is:

$$\sum_{i=1}^n \sum_{k=1}^n a_{ik} = \sum_{j=1}^n \sum_{k=1}^n a_{kj}$$

which is the also the coefficeint of  $n$  in  $R_1 + \cdots + R_n$ . Next, we notice that

$$\sum_{1 \leq k < \ell \leq n} a_{ik} a_{i\ell} = \frac{1}{2} \left( \left( \sum_{k=1}^n a_{ik} \right)^2 - \sum_{k=1}^n a_{ik}^2 \right)$$

so summing this across all  $i$  gives the coefficient of  $n^2$  in  $R_1 + \cdots + R_n$  as

$$\frac{1}{2} \left( \sum_{i=1}^n \left( \sum_{k=1}^n a_{ik} \right)^2 - \sum_{i=1}^n \sum_{k=1}^n a_{ik}^2 \right)$$

and similarly for  $C_1 + \cdots + C_n$ :

$$\frac{1}{2} \left( \sum_{j=1}^n \left( \sum_{k=1}^n a_{kj} \right)^2 - \sum_{j=1}^n \sum_{k=1}^n a_{kj}^2 \right)$$

Notice that  $\sum_{i=1}^n \sum_{k=1}^n a_{ik}^2 = \sum_{j=1}^n \sum_{k=1}^n a_{kj}^2$  are simply sum of squares of all  $a_{ik}$  so it suffices to show that  $2n^2$  divides

$$\sum_{i=1}^n \left( \sum_{k=1}^n a_{ik} \right)^2 - \sum_{j=1}^n \left( \sum_{k=1}^n a_{kj} \right)^2$$

By before,  $n \mid \sum_{k=1}^n a_{ik}$  and  $n \mid \sum_{k=1}^n a_{ij}$  so we can name  $\sum_{k=1}^n a_{ik} = nr_i$  and  $\sum_{k=1}^n a_{ij} = nc_j$ . Substituting this and factoring  $n^2$  term, all it needs is to show that

$$2 \mid \sum_{i=1}^n r_i^2 - \sum_{j=1}^n c_j^2$$

However,  $r_i$  and  $r_i^2$  have the same parity, and  $\sum_{i=1}^n r_i = \sum_{j=1}^n c_j$  is the sum of all the  $a_{ij}$ s.

Therefore

$$\sum_{i=1}^n r_i^2 \equiv \sum_{i=1}^n r_i = \sum_{j=1}^n c_j \equiv \sum_{j=1}^n c_j^2 \pmod{2}$$

as desired.

Finally we need to tackle the coefficient of  $n^3$ . Again we have that for a set of variables  $x_1, \dots, x_n$  then

$$\begin{aligned} \sum_{i < j < k} x_i x_j x_k &= \frac{1}{6} \left( \left( \sum_{i=1}^n x_i \right)^3 - \sum_{i=1}^n x_i^3 - 3 \sum_{i \neq j} x_i^2 x_j \right) = \frac{1}{6} \left( S_1^3 - S_3 - 3 \sum_{i=1}^n x_i^2 (S_1 - x_i) \right) \\ &= \frac{1}{6} (S_1^3 + 2S_3 - 3S_1 S_2) \end{aligned}$$

where  $S_k$  is the sum of  $k$ -th power  $\sum_{i=1}^n x_i^k$ . Using the  $r_i$  and  $c_j$  notations before we now have the coefficient of  $n^3$  in  $R_i$  as

$$\sum_{i \leq k < \ell < m \leq n} a_{ik} a_{i\ell} a_{im} = \frac{1}{6} ((nr_i)^3 + 2 \sum_{k=1}^n a_{ik}^3 - 3nr_i S_i^{r(2)})$$

where  $S_i^{r(2)}$  is simply the sum of square of squares of row  $i$ . Similarly the coefficient of  $n^3$  in  $C_j$  is

$$\frac{1}{6} ((nc_j)^3 + 2 \sum_{k=1}^n a_{kj}^3 - 3nc_j S_j^{c(2)})$$

with the  $c$  in  $S_j^{c(2)}$  denoting the notion of column. Thus we are essentially comparing

$$\frac{1}{6} (n^3 \sum_{i=1}^n r_i^3 + 2 \sum_{i=1}^n \sum_{k=1}^n a_{ik}^3 - 3n \sum_{i=1}^n r_i S_i^{r(2)})$$

vs

$$\frac{1}{6} (n^3 \sum_{j=1}^n c_j^3 + 2 \sum_{j=1}^n \sum_{k=1}^n a_{kj}^3 - 3n \sum_{j=1}^n c_j S_j^{c(2)})$$

now  $\sum_{i=1}^n \sum_{k=1}^n a_{ik}^3 = \sum_{j=1}^n \sum_{k=1}^n a_{kj}^3$  because they are just the sum of cubes of all  $a_{ij}$ s. The other

two terms on each side has factor  $n$  so it suffices to show that  $\sum_{i=1}^n r_i^3 \equiv \sum_{j=1}^n c_j^3 \pmod{6}$ ,

and  $\sum_{i=1}^n r_i S_i^{r(2)} \equiv \sum_{j=1}^n c_j S_j^{c(2)} \pmod{2}$ . The first one is due to the fact that for all integers  $k$ ,  $k^3 \equiv k \pmod{6}$  and therefore

$$\sum_{i=1}^n r_i^3 \equiv \sum_{i=1}^n r_i = \sum_{j=1}^n c_j \equiv \sum_{j=1}^n c_j^3 \pmod{6}$$

where the middle equality is because they are the same as the overall sum of squares on grid. The second one is due to the fact that  $S_i^{r(2)}$  is the sum of squares of row which has same parity of sum of row  $r_i$  so in mod 2 (and also  $x \equiv x^3 \pmod{2}$ ),

$$\sum_{i=1}^n r_i S_i^{r(2)} \equiv \sum_{i=1}^n r_i r_i (r_i^2) = \sum_{i=1}^n r_i^3 \equiv \sum_{i=1}^n r_i = \sum_{j=1}^n c_j \equiv \sum_{j=1}^n c_j^3 \equiv \sum_{j=1}^n c_j S_j^{c(2)}$$

as desired.

**N3** Define the sequence  $a_0, a_1, a_2, \dots$  by  $a_n = 2^n + 2^{\lfloor n/2 \rfloor}$ . Prove that there are infinitely many terms of the sequence which can be expressed as a sum of (two or more) distinct terms of the sequence, as well as infinitely many of those which cannot be expressed in such a way.

**Solution.** Throughout, we focus on writing  $a_n$  in terms of sum of distinct  $a_k$ 's for  $k < n$ , and  $n$  odd.

*Lemma 1.* If  $a_{2\ell+1}$  can be written as sum of distinct  $a_k$  for  $k < 2\ell+1$ , then this sum must contain  $a_k$  for all  $k = \ell+1, \dots, 2\ell$ .

Proof: here, we have  $a_{2\ell+1} = 2^{2\ell+1} + 2^\ell$ , and

$$\begin{aligned} \sum_{i=0}^{2\ell} a_i &= (2^0 + \dots + 2^{2\ell}) + 2(2^0 + \dots + 2^{\ell-1}) + 2^\ell = 2^{2\ell+1} - 1 + 2^\ell + 2(2^\ell - 1) \\ &= a_{2\ell+1} + 2^{\ell+1} - 3 \end{aligned}$$

which means all  $a_k > 2^{\ell+1} - 3$  cannot be omitted from summation. This would be the case for all  $k \geq \ell+1$ .

*Lemma 2.*  $a_{2\ell+1}$  can be written in our desired sum if and only if  $2^{2\ell}$  can be written as sum of distinct  $a_k$ 's for  $k < 2\ell$ .

Proof: from lemma 1, the summation for  $a_{2\ell+1}$  necessarily contains  $a_{2\ell}$ , and the difference now is  $a_{2\ell+1} - a_{2\ell} = 2^{2\ell}$ .

Thus the problem now becomes showing that there exists infinitely many  $\ell$  such that  $2^{2\ell}$  can be represented this way.

*Lemma 3.* Call  $\ell$  good if we can write  $2^{2\ell}$  as sum of distinct  $a_k$ 's. Then  $\ell$  is good if and only if  $4\ell - 3$  is good.

Proof: again consider

$$a_0 + \dots + a_{2\ell-1} = (2^0 + \dots + 2^{2\ell-1}) + 2(2^0 + \dots + 2^{\ell-1}) = 2^{2\ell} - 1 + 2(2^\ell - 1) = 2^{2\ell-1} + 2^{\ell+1} - 3$$

so like above, anything  $a_{\ell+1}$  and above must be part of sum of  $2^{2\ell}$ .

Now consider, instead,  $2^{2(4\ell-3)}$ . Then  $a_{4\ell-2}, \dots, a_{8\ell-7}$  all be part of the sum. Now consider

$$a_{4\ell-2} + \dots + a_{8\ell-7} = (2^{4\ell-2} + \dots + 2^{8\ell-7}) + 2(2^{2\ell-1} + \dots + 2^{4\ell-4}) = (2^{8\ell-6} - 2^{4\ell-2}) + 2^{4\ell-2} - 2^{2\ell} = 2^{8\ell-6} - 2^{2\ell}$$

which follows that  $4\ell - 3$  is good if and only if  $\ell$  is good.

Now we can complete the solution. Observe, first, that 2 is good since  $16 = 10 + 6 = a_3 + a_2$ . This gives us the sequence of good numbers  $2, 5, 17, \dots$ . Conversely, we show that 6 is not good. From before, we see that  $a_7$  to  $a_{11}$  must all be part of  $2^{12}$ , so

$$a_7 + \dots + a_{11} = (2^7 + \dots + 2^{11}) + 2^3 + 2(2^4 + 2^5) = 2^{12} - 2^7 + 2^5 + 2^6 + 2^3 = 2^{12} - 24$$

we have  $a_0, \dots, a_4$  as 2, 3, 6, 10, 20, which we can manually verify that there's no subset of  $\{2, 3, 6, 10, 20\}$  sums to 24.

**N4** (IMO 5) Let  $a_1, a_2, \dots$  be an infinite sequence of positive integers. Suppose that there is an integer  $N > 1$  such that, for each  $n \geq N$ , the number

$$\frac{a_1}{a_2} + \frac{a_2}{a_3} + \dots + \frac{a_{n-1}}{a_n} + \frac{a_n}{a_1}$$

is an integer. Prove that there is a positive integer  $M$  such that  $a_m = a_{m+1}$  for all  $m \geq M$ .

**Solution.** Let the sum  $d(n) = \frac{a_1}{a_2} + \frac{a_2}{a_3} + \dots + \frac{a_{n-1}}{a_n} + \frac{a_n}{a_1}$ . Then  $d(n+1) - d(n) = \frac{a_n}{a_{n+1}} + \frac{a_{n+1}-a_n}{a_1}$ . It follows that this difference is an integer for all  $n \geq N$ . Effectively, for all primes  $p$ , one of the two following situations must happen:

- $v_p(a_n) \geq v_p(a_{n+1})$  and  $v_p(a_{n+1} - a_n) \geq v_p(a_1)$ .
- $v_p(a_{n+1}) - v_p(a_n) = v_p(a_1) - v_p(a_{n+1} - a_n) > 0$ .

Consider, now, the scenario where  $v_p(a_n) \neq v_p(a_{n+1})$ , so  $v_p(a_{n+1} - a_n) = \min(v_p(a_n), v_p(a_{n+1}))$ . The first scenario essentially means

$$v_p(a_n) \geq v_p(a_{n+1}) \geq v_p(a_1)$$

and the second means  $v_p(a_{n+1}) = v_p(a_1) > v_p(a_n)$ . This means, given fixed  $v_p(a_n)$ , we either have  $v_p(a_{n+1}) = v_p(a_n)$ , or have  $v_p(a_n) \geq v_p(a_{n+1}) \geq v_p(a_1)$  if  $v_p(a_n) \geq v_p(a_1)$ , or  $v_p(a_{n+1}) = v_p(a_1)$ . It then follows that there are only finitely many  $n \geq N$  with  $v_p(a_n) \neq v_p(a_{n+1})$ . (either at most 1 if  $v_p(a_N) < v_p(a_1)$ , or at most  $v_p(a_N) - v_p(a_1)$  otherwise).

We also note that only those  $p$  dividing  $a_1 a_N$  are relevant, i.e. only finitely many those primes. It then follows that for all but finitely many  $n$ ,  $v_p(a_n) = v_p(a_{n+1})$  for all  $p$ , i.e.  $a_n = a_{n+1}$ . Thus the sequence is eventually constant.

**N5** Four positive integers  $x, y, z$  and  $t$  satisfy the relations

$$xy - zt = x + y = z + t$$

Is it possible that both  $xy$  and  $zt$  are perfect squares?

**Answer.** No.

**Solution.** Suppose otherwise, write  $xy = a^2$  and  $zt = b^2$ . Then  $(x-y)^2 = (x+y)^2 - 4xy = (a^2 - b^2)^2 - 4a^2$  is a perfect square, say  $c^2$ . Similarly,  $(a^2 - b^2) - 4b^2$  is a perfect square, say  $d^2$ .

The relation above can be best summarized into:

$$X^2 = p^2 + q^2 = r^2 + s^2$$

where  $X = a^2 - b^2$ , and  $|p^2 - r^2| = 4(a^2 - b^2) = 4X$ . It's also important to note that since  $x, y, z, t > 0$ ,  $a^2 - b^2, a, b$  are all positive. We further write  $p = p_1 2^{p_0}$  and  $q = q_1 2^{q_0}$  where  $p_1, q_1$  both odd. Then

$$X^2 = (p_1 2^{p_0})^2 + (q_1 2^{q_0})^2$$

If  $p_0 = q_0$  then  $X^2 = 2^{2p_0}(p_1^2 + q_1^2)$  and given that  $2^{2p_0} = (2^{p_0})^2$  is a perfect square, so is  $p_1^2 + q_1^2 \equiv 1 + 1 = 2 \pmod{4}$  (as both  $p_1, q_1$  odd). This contradicts that no square can be congruent to 2 mod 4. Hence  $p_0 \neq q_0$  and w.l.o.g. let  $p_0 > q_0$ , which will imply that the highest power dividing  $X^2$  is  $2^{2q_0}$ . In other words, if  $k$  is the highest power of 2 dividing  $X$  then each  $p, q, r, s$  are divisible by  $k$ , so they can be written as  $2^k p_0, 2^k q_0, 2^k r_0, 2^k s_0$ .

Write  $X = 2^k X_0$  with  $X_0$  odd. Dividing  $2^k$  from both sides give

$$X_0^2 = p_0^2 + q_0^2 = r_0^2 + s_0^2$$

with  $|p_0^2 - r_0^2| = \frac{4X}{2^{2k}} = \frac{4X_0}{2^k}$  and given  $X_0$  odd, we have  $k \leq 2$ . We'll use the fact that, since  $X_0$  odd, one of  $p_0$  and  $q_0$  must be odd, and the other even. Similarly, one of  $r_0$  and  $s_0$  odd and the other even.

- If  $k = 0$ , we have  $|p_0^2 - r_0^2| = |q_0^2 - s_0^2| = 4X_0 \equiv 4 \pmod{8}$ . To satisfy  $|p_0^2 - r_0^2| = 4X_0$  we will need  $p_0, r_0$  both even or both odd, so w.l.o.g. let them be both odd because  $|q_0^2 - s_0^2| = 4X_0$  must be satisfied too. However,  $p_0^2 \equiv r_0^2 \equiv 1 \pmod{8}$  whenever  $p_0, r_0$  odd, contradicting  $|p_0^2 - r_0^2| \equiv 4 \pmod{8}$ .
- $k = 1$  means  $2X_0 \equiv 2 \pmod{4}$  is impossible: difference of squares cannot have  $\equiv 2 \pmod{4}$ .
- $k = 0$  means  $|p_0^2 - r_0^2| = |q_0^2 - s_0^2| = X_0$ , which is odd. Now consider  $p_0^2 + q_0^2 = X^2$  and w.l.o.g. let  $p_0 > q_0$ , which also means  $p_0 > X_0\sqrt{\frac{1}{2}}$ . Now, assuming  $r_0 \neq p_0$

$$|r_0^2 - p_0^2| \geq \min\{|(p_0+1)^2 - p_0^2|, |(p_0-1)^2 - p_0^2|\} = \min\{|2p_0-1|, |2p_0+1|\} = 2p_0-1 > 2X_0\sqrt{\frac{1}{2}}-1$$

which gives  $X_0 > 2X_0\sqrt{\frac{1}{2}} - 1 = \sqrt{2}X_0 - 1$  which means  $X_0 \leq 2$ . But since  $X_0$  is odd,  $X_0 = 1$  and the only solution is  $1^2 + 0^2$ . This gives  $X = 4$ , and the only possible combinations of  $(p, q)$  and  $(r, s)$  are  $(4, 0, 0, 4)$  which we can solve as  $a = 2, b = 0$ . Now  $b = 0$  means  $zt = 0$ , contradiction.

Therefore the contradiction above means a solution does not exist.

**N6** Let  $f : \{1, 2, 3, \dots\} \rightarrow \{2, 3, \dots\}$  be a function such that  $f(m+n) | f(m) + f(n)$  for all pairs  $m, n$  of positive integers. Prove that there exists a positive integer  $c > 1$  which divides all values of  $f$ .

**Solution.** We first start with the following lemma.

**Lemma 2.**  $\lim_{n \rightarrow \infty} \frac{f(n)}{n}$  exists and is either  $f(1)$  or  $0$ . In addition, this limit is  $f(1)$  precisely when  $f(n) = nf(1)$  for all  $n$ .

*Proof.* Let's first show the existence of such limit. Let  $L_0 = \liminf \frac{f(n)}{n}$  and  $L_1 = \limsup \frac{f(n)}{n}$ , i.e.  $L_0 \leq L_1$ . An important property is the sublinearity of the function, i.e.  $f(m+n) \leq f(m) + f(n)$ . Now suppose that  $c, n$  are such that  $f(n) \leq cn$ . We show that for all  $c' > c$  and  $m$  sufficiently large (threshold depending on  $c'$ ),  $f(m) \leq c'm$ . Using repeated iteration of this inequality, by setting  $m = kn + r$  with  $0 \leq r < n$  we have

$$f(m) \leq f(n) + \dots + f(n) + f(r) = kf(n) + r \leq kcn + f(r) \quad (7)$$

and therefore choosing  $k \geq \frac{\max(f(1), \dots, f(n-1))}{n(c'-c)}$  we get  $f(m) \leq kc'n \leq c'(kn + r) = c'm$  (i.e.  $f(m) \leq c'm$  for all  $m \geq kn$  for this choice of  $k$ ). Since  $c'$  can be anything greater than  $c$ , it then follows that  $L_1 \leq c$  (by definition of  $\limsup$ ). Since  $c$  can also be taken arbitrarily close to  $L_0$  (by definition of  $\liminf$ ), this implies  $L_1 \leq L_0$  too. We then have  $L_0 = L_1$ , i.e. the limit is indeed  $L_0$  (call this  $L$  from now).

From the proof above we can also deduce that  $\frac{f(n)}{n} \geq L$  for all  $n$ . In particular we also have  $L \leq f(1)$ . Suppose, now,  $L > 0$ . We claim that  $f(n+1) = f(n) + f(1)$  for  $n$  sufficiently large. Consider  $L' = 1.01L$  (i.e.  $L > \frac{L'}{2}$ ), which then follows that there exists an  $N$  such that  $f(n) \leq L'n$  for all  $n \geq N$ . For all  $n > \max(N, \frac{f(1)/2-L}{L-L'/2})$ , consider the relation  $f(n+1) | f(n) + f(1)$ , i.e.  $f(n+1) = f(n) + f(1)$  or  $f(n+1) \leq \frac{f(n)+f(1)}{2}$ . In the latter case we have

$$L(n+1) \leq f(n+1) \leq \frac{f(n) + f(1)}{2} \leq \frac{L'n + f(1)}{2} < L(n+1) \quad (8)$$

i.e. a contradiction. This then show that  $f(n+1) = f(n) + f(1)$  for  $n$  sufficiently large, which will then entail  $L = f(1)$ .

Finally, we have seen that  $\frac{f(n)}{n} \leq f(1) = L$  for all  $n$ , on the other hand  $\frac{f(n)}{n} \geq L$  too. Thus the equality holds here, i.e.  $\frac{f(n)}{n} = L$ .  $\square$



Now in view of the lemma, we either have  $f(n) \equiv cn$  or  $\lim_{n \rightarrow \infty} \frac{f(n)}{n} = 0$ . In the first case, using  $f(1) \geq 2$ , we have  $c \geq 2$ , which implies the conclusion. We now focus on the second case, which brings us into the following.

**Lemma 3.** *Denote the set of primes as  $\mathcal{P}$ , and for each  $n \geq 1$ ,  $\mathcal{P}_n = \mathcal{P} \cap \{n, n+1, \dots\}$ . Suppose that the conclusion is false. Then there exists an  $M$  and an injective mapping  $\varphi : \mathcal{P}_M \rightarrow \mathcal{P}$  such that  $\varphi(p) \mid f(p)$  for all  $p$ .*

*Proof.* We first see that

$$\dots \mid \gcd(f(n), f(1)) \mid \dots \mid \gcd(f(2), f(1)) \mid \gcd(f(1), f(1)) \quad (9)$$

Indeed  $f(n+1) \mid f(1) + f(n)$ , so from  $\gcd(f(n+1), f(1))$  dividing both  $f(n+1)$  and  $f(1)$  follows that it also divides  $f(n)$ . Thus there exists a constant  $c$  such that for  $n$  sufficiently large,  $\gcd(f(n), f(1)) = c$ . If  $c > 1$  then we have  $c \mid f(n)$  for all  $n$  and we're done. We now assume  $c = 1$ , so there exists an  $M$  such that  $\gcd(f(n), f(1)) = 1$  for all  $n \geq M$ .

Next, let's show that for all  $p \geq M$  we have  $\gcd(f(p), f(n)) = 1$  for all  $n < p$ . A more general claim is that for each pair  $(m, n)$ , we have  $\gcd(f(m), f(n)) \mid f(\gcd(m, n))$ . Indeed, starting from  $(m_0, n_0) = (m, n)$ , consider the pair  $(m_0, n_0), \dots$  via the following Euclidean iteration:

$$(m_{k+1}, n_{k+1}) = \begin{cases} (m_k, n_k) & m_k = n_k \\ (m_k - n_k, n_k) & m_k > n_k \\ (m_k, n_k - m_k) & n_k > m_k \end{cases} \quad (10)$$

Assume that  $m_k > n_k$ , then

$$\gcd(m_k - n_k, n_k) = \gcd(m_k, n_k) \quad f(m_k) \mid f(n_k) + f(m_k - n_k) \rightarrow \gcd(f(m_k), f(n_k)) \mid f(m_k - n_k) \quad (11)$$

So considering all the 3 cases we have

$$\gcd(f(m_k), f(n_k)) \mid \gcd(f(m_{k+1}), f(n_{k+1})) \quad \gcd(m_k, n_k) = \gcd(m_{k+1}, n_{k+1}) \quad (12)$$

Notice by Euclid's algorithm, there exists a  $K$  such that  $m_k = n_k$  for all  $k \geq K$ . For those  $k$ ,  $\gcd(f(m_k), f(n_k)) = f(\gcd(m_k, n_k)) = f(m_k)$ . This means we have

$$\gcd(f(m), f(n)) = \gcd(f(m_0), f(n_0)) \mid \gcd(f(m_K), f(n_K)) = f(\gcd(m_K, n_K)) = f(\gcd(m, n)) \quad (13)$$

as claimed.

In particular, for any prime  $p \geq M$ , for any  $n$  with  $p \nmid n$ , we have  $\gcd(f(n), f(p)) \mid f(\gcd(n, p)) = f(1)$ . But since  $\gcd(f(p), f(1)) = 1$  we do have  $\gcd(f(n), f(p)) = 1$ . Since  $f(p) > 1$ , there's a prime  $q \mid f(p)$ ; we may define  $\varphi(p) = q$ . Such a mapping is an injection since  $\gcd(f(p), f(q)) = 1$  for different primes  $p, q$  and  $p, q \geq M$ .  $\square$

Now we may complete our proof. Let threshold  $M$  as per Lemma 3, As per Lemma 2, choose  $N$  such that  $\frac{f(n)}{n} \leq \frac{1}{3}$ . Let  $M_1 = \max(M, N)$ ; we see that the mapping  $\varphi|_{\geq M_1}$  (that is,  $\varphi$  restricted to  $\geq M_1$ ) is still an injection. It then follows that for each  $n \geq M_1$ ,

$$\begin{aligned} & |\mathcal{P} \cap \{1, \dots, n\}| - |\mathcal{P} \cap \{1, \dots, M_1 - 1\}| |\mathcal{P} \cap \{M_1, \dots, n\}| \\ &= |\{\varphi(p) : M_1 \leq p \leq n\}| \leq |\mathcal{P} \cap \{1, 2, \dots, \frac{1}{3}n\}| \end{aligned} \quad (14)$$

So rearranging yields that for each  $n$ ,  $|\mathcal{P}_{\leq n}| - |\mathcal{P}_{\leq \frac{1}{3}n}| \leq |\mathcal{P}_{\leq M_1-1}|$  (where  $\mathcal{P}_{\leq n} = \mathcal{P} \cap \{1, \dots, n\}$ ). This means for  $n$  sufficiently large, there are only bounded number of prime numbers between  $\frac{1}{3}n$  and  $n$ . But this contradicts the prime number theorem, which states that the number of prime numbers between  $\frac{1}{3}n$  and  $n$  is  $\simeq (\frac{n}{\log n} - \frac{n}{3(\log n - \log 3)})(1 + o(1))$ , which is unbounded as  $n$  large.