

# Algebra

**A1** (IMO 1) Find all function  $f : \mathbb{R} \rightarrow \mathbb{R}$  such that for all  $x, y \in \mathbb{R}$  the following equality holds

$$f(\lfloor x \rfloor y) = f(x) \lfloor f(y) \rfloor$$

where  $\lfloor a \rfloor$  is greatest integer not greater than  $a$ .

**Solution.** Plugging  $x = y = 0$  gives  $f(0) = f(0)\lfloor f(0) \rfloor$ , i.e.  $f(0)(\lfloor f(0) \rfloor - 1) = 0$ . This means either  $f(0) = 0$  or  $\lfloor f(0) \rfloor = 1$ .

In the second case with  $\lfloor f(0) \rfloor = 1$ , plugging just  $y = 0$  gives  $f(0) = f(x)\lfloor f(0) \rfloor = f(x)$ , so  $f(x) = f(0)$  for all  $x$  and we have  $f \equiv c$  for some constant  $c \in [1, 2)$ . Otherwise,  $f(0) = 0$ . Let  $0 \leq x < 1$  be arbitrary, then  $\lfloor x \rfloor = 0$  so in this case plugging  $y = x$  gives  $0 = f(0) = f(x)\lfloor f(x) \rfloor$ , meaning that  $f(x) = 0$  or  $\lfloor f(x) \rfloor = 0$ , though the first condition actually means  $\lfloor f(x) \rfloor = 0$  too. Therefore  $0 \leq x < 1$  means  $\lfloor f(x) \rfloor = 0$  for all  $x$ . Now for any real number  $z$ , choose an integer  $x$  such that  $|x| > |z|$  and both  $x$  and  $z$  have the same sign. Then  $0 < z/x < 1$ . Let  $y = z/x$  and we have  $f(z) = f(xy) = f(\lfloor x \rfloor y) = f(x) \lfloor f(y) \rfloor = f(x)(0) = 0$ , so  $f \equiv 0$ .

Finally, to show these work, if  $f \equiv 0$  then LHS=RHS=0 and if  $f \equiv c$  for some  $c \in [1, 2)$  we have LHS=RHS=  $c$ .

**A2** Let the real numbers  $a, b, c, d$  satisfy the relations  $a + b + c + d = 6$  and  $a^2 + b^2 + c^2 + d^2 = 12$ . Prove that

$$36 \leq 4(a^3 + b^3 + c^3 + d^3) - (a^4 + b^4 + c^4 + d^4) \leq 48.$$

**Solution.** For the right inequality, all we need is the following AM-GM inequality:

$$\begin{aligned} \frac{a^4 + b^4 + c^4 + d^4 + 48}{2} &= \frac{(a^4 + 4a^2) + (b^4 + 4b^2) + (c^4 + 4c^2) + (d^4 + 4d^2)}{2} \\ &\geq \sqrt{4a^6} + \sqrt{4b^6} + \sqrt{4c^6} + \sqrt{4d^6} \\ &\geq 2|a^3| + 2|b^3| + 2|c^3| + 2|d^3| \\ &\geq 2a^3 + 2b^3 + 2c^3 + 2d^3 \end{aligned}$$

rearranging gives  $4(a^3 + b^3 + c^3 + d^3) - (a^4 + b^4 + c^4 + d^4) \leq 48$ .

For the left inequality, we notice the following:  $(a-1)^4 = (a^4 - 4a^3) + 6a^2 - 6a + 1$  and if we denote  $S_k = a^k + b^k + c^k + d^k$  we have  $(a-1)^4 + (b-1)^4 + (c-1)^4 + (d-1)^4 = S_4 - 4S_3 + 6S_2 - 6S_1 + 4 = S_4 - 4S_3 + 6(12) - 4(6) + 4 = S_4 - 4S_3 + 52$ . This means,

$$4S_3 - S_4 = 52 - [(a-1)^4 + (b-1)^4 + (c-1)^4 + (d-1)^4]$$

On the other hand,  $(a-1)^2 + (b-1)^2 + (c-1)^2 + (d-1)^2 = S_2 - 2S_1 + 4 = 12 - 2(6) + 4 = 4$ . Considering the following identity for all reals  $x_1, \dots, x_n$

$$\left( \sum_{i=1}^n x_i^2 \right)^2 = \sum_{i=1}^n x_i^4 + 2 \sum_{i < j} x_i x_j \geq \sum_{i=1}^n x_i^4$$

(since all squares are nonnegative), we have  $(a-1)^4 + (b-1)^4 + (c-1)^4 + (d-1)^4 \leq ((a-1)^2 + (b-1)^2 + (c-1)^2 + (d-1)^2)^2 = 4^2 = 16$ , so  $4S_3 - S_4 \geq 52 - 16 = 36$ , as desired.

**A4** A sequence  $x_1, x_2, \dots$  is defined by  $x_1 = 1$  and  $x_{2k} = -x_k, x_{2k-1} = (-1)^{k+1}x_k$  for all  $k \geq 1$ . Prove that  $\forall n \geq 1 \ x_1 + x_2 + \dots + x_n \geq 0$ .

**Solution.** Let  $s_n = x_1 + x_2 + \dots + x_n$ . Suppose on the contrary, there exists  $n$  such that  $s_n < 0$ . Choose the smallest such  $n$ . Note that all  $x_i$ 's are  $\pm 1$ , so it must be that  $s_{n-1} = 0$  and  $x_n = -1$ . In addition,  $s_n \equiv n \pmod{2}$  since all terms are  $\pm 1$ , so  $n$  must be odd. We follow up with the following observations:

- $x_{4k+1} = (-1)^{2k+1+1}x_{2k+1} = x_{2k+1}$  while  $x_{4k+2} = -x_{2k+1}$ , so  $s_{4k} = s_{4k+2}$  for all  $k \geq 0$ .
- $x_{4k-1} = (-1)^{2k+1}x_{2k} = -x_{2k} = x_{4k}$ , so we actually have:

$$s_{4k} = \sum_{i=1}^k x_{4i-3} + x_{4i-2} + x_{4i-1} + x_{4i} = \sum_{i=1}^k x_{2i-1} - x_{2i-1} - x_{2i} - x_{2i} = -2 \sum_{i=1}^k x_{2i} = 2 \sum_{i=1}^k x_i = 2s_k$$

In particular, if  $s_{4k} = 0$ , so is  $s_k$  and therefore  $k$  is even.

If  $n - 1 = 4k$  for some  $k$ , then  $0 = s_{n-1} = s_{4k} = s_k$  and  $s_n = x_n = x_{4k+1} = (-1)^{2k+2}x_{2k+1} = x_{2k+1} = (-1)^{k+2}x_{k+1} = x_{k+1}$  (since  $k$  is even), and if  $n - 1 = 4k + 2$  for some  $k$  then  $0 = s_{4k+2} = s_{4k} = s_k$  and  $s_n = x_n = x_{4k+3} = (-1)^{2k+3}x_{2k+2} = -x_{2k+2} = x_{k+1}$ . In both cases we have  $s_n = x_{k+1}$  and since  $s_k = 0$ ,  $x_{k+1} = s_{k+1}$  too. Since  $s_n = -1$ , we must have  $s_{k+1} = -1$ , too. By the minimality of  $n$ , we have  $4k + 1 \leq n \leq k + 1$ , which can only happen when  $k = 0$ . However, when  $k = 0$ , we have  $s_1 = x_1 = 1$ , contradiction. This means  $s_n$  must be nonnegative for all  $n$ .

## Combinatorics

**C2** On some planet, there are  $2^N$  countries ( $N \geq 4$ ). Each country has a flag  $N$  units wide and one unit high composed of  $N$  fields of size  $1 \times 1$ , each field being either yellow or blue. No two countries have the same flag. We say that a set of  $N$  flags is diverse if these flags can be arranged into an  $N \times N$  square so that all  $N$  fields on its main diagonal will have the same color. Determine the smallest positive integer  $M$  such that among any  $M$  distinct flags, there exist  $N$  flags forming a diverse set.

**Answer.**  $M = 2^{N-2} + 1$ .

**Solution.**  $M = 2^{N-2}$  is not enough: consider all the  $2^{N-2}$  distinct flags where the top field is blue and the bottom field is yellow. No matter how we choose the  $N$  flags and arrange them, the top top-left corner of the diagonal will be blue and the bottom-right yellow.

To show that  $M = 2^{N-2} + 1$  is enough, consider an arbitrary set of  $M$  flags. Consider a bipartite graph with one side being the  $M$  flags and the other side being the  $k$  fields. In a blue matching, an edge exists between a flag and the  $i$ -th node if and only if the  $i$ -field of the flag is blue. Define yellow matching similarly. The goal is to find either a blue or yellow matching such that all the nodes on the right (the fields) are matched. By Hall's marriage theorem, this is possible if and only if for any  $k$  with  $1 \leq k \leq N$  and any subset of fields of size  $k$ , at least  $k$  of the flags have an edge to at least one of the  $k$  fields.

Suppose the condition fails for blue matching. That is, there exists  $k$  fields such that less than  $k$  flags have at least one of the  $k$  fields being blue. W.L.O.G. let the  $k$  fields be the first  $k$  fields. Now, we know that all but at most  $k - 1$  of the flags have the first  $k$  fields being yellow, while there are  $2^{N-k}$  distinct flags with first  $k$  fields being yellow. Thus we have  $2^{N-2} + 1 \leq 2^{N-k} + k - 1$ . Since  $2^{N-k} < 2^{N-k+1}$  for all real numbers  $k$ , for  $k \leq N$ , both  $2^{N-k}$  and  $2^{N-k+1}$  are integers, we have  $2^{N-k} \leq 2^{N-k+1} - 1$  and therefore  $2^{N-k} + k - 1 \leq 2^{N-k+1} - 1 + k - 1 = 2^{N-(k-1)} + (k-1) - 1$ , which means that the function  $2^{N-k} + k - 1$  is decreasing. But when  $k = 2$  we have  $2^{N-k} + k - 1 = 2^{N-2} + 1$ , so we have  $k = 2$  here. We now split into cases:

- If  $k = 1$ , then all the  $M$  flags have top field yellow. Consider, now, the Hall condition on the yellow matching, and consider an arbitrary subset of  $\ell$  fields. If this  $\ell$  fields contain the first field then all (i.e.  $2^{N-2} + 1 \geq N$ ) flags match to the first field and the Hall condition is easily satisfied. Otherwise, among the  $2^{N-1}$  flags with first field yellow, there are only  $2^{N-1-\ell}$  flags with all of the  $\ell$  fields blue. In addition,  $2^{N-2} + 1 - (2^{N-1-\ell} + \ell) \leq 2^{N-2} + 1 - (2^{N-1-1} + 1) = 0$  (we use the fact from above that  $2^{N-\ell} + \ell$  is decreasing), hence always nonnegative. This means, there will always be  $\ell$  flags with at least one of the  $\ell$  fields yellow.
- If  $k = 2$ , then all (except possible one) flags have top two fields yellow, meaning we have at least  $2^{N-2}$  flags with top two fields yellow. However, there are only  $2^{N-2}$  distinct flags with the top two fields yellow, so we have all the distinct collection of flags with the first two fields yellow. Now, choose two

of the  $2^{N-2}$  flags arbitrarily, and for  $3 \leq i \leq N$ , the  $i$ -th flag is chosen as the one with 1st, 2nd,  $i$ -th field yellow and the rest blue. This gives the desired diagonalization.

**C3** 2500 chess kings have to be placed on a  $100 \times 100$  chessboard so that

- no king can capture any other one (i.e. no two kings are placed in two squares sharing a common vertex);
- each row and each column contains exactly 25 kings.

Find the number of such arrangements. (Two arrangements differing by rotation or symmetry are supposed to be different.)

**Answer.** There are (only) two such arrangements.

**Solution.** Now, partition our chessboard into 2500  $2 \times 2$  squares and call each of them megasquare. We call the  $2 \times 100$  squares containing the 50 megasquares a megarow, and define a megacolumn similarly. Within each megasquare, any two of the four squares share a vertex, so one megasquare cannot have more than a king. Since we need 2500 chess kings in total, each megasquare must have exactly a king.

Now, we have four types of megasquares: top-left (TL), top-right (TR), bottom-left (BL), bottom-right (BR), depending where we put our king. TL megasquares and TR megasquares are called T-megasquares, define B-, L-, R- megasquares similarly. We need the following lemmas:

*Step 1.* Each megarow consists of 25 T-megasquares and 25 B-megasquares. This is because each row contains exactly 25 kings. Similarly, each megacolumn consists of 25 L-megasquares and 25 R-megasquares. This means the number of T-, B-, L-, R-megasquares are each  $25 \times 50 = 1250$ .

*Step 2.* Consider any B-megasquare  $M_1$ , and consider either of the two bottom squares of the megasquare (the bottom row). If there is a megasquare  $M_2$  located below this megasquare, each square of the top row of this megasquare will have a common vertex with the bottom row of the original megasquare. Hence, this megasquare must also be a B-megasquare.

*Step 3.* With steps 1 and steps 2 in mind, consider the top megarow, with 25 of them being B-megasquares. For each of the B-megasquares, by the lemma above, all the 49 megasquares below it (in the same row) must also be B-megasquares, so these 25 megarows will have all B-megasquares. These 25 megarows give rise of  $25 \times 50$  megasquares, and therefore the remaining 25 megarows must all be T-megasquares. This means the notion of T- and B-megacolumns are well-defined: the megarow with either all T-megasquares or B-megasquares. Similarly the notion of L- and R-megarows are also well-defined.

*Step 4.* Obviously, the intersection of a T-megacolumn and a L-megarow is a TL-megasquare (and similarly for other combinations). Now that there are 25 T- and 25 B-megacolumns, we consider the adjacent megarows of different types: either T-megacolumn followed by B-megacolumn or vice versa. Consider also the adjacent megarows of different type: either L-megarow followed by R-megarow or vice versa. Their intersections together give rise of 4 megasquares. The bottom-right corner of the top-left megasquare shares a vertex with the top-left corner of the bottom-right corner, so the condition that top-left megasquare is BR and the bottom-right megasquare is TL cannot happen simultaneously: in other words, we cannot have B-megacolumn left to T-megacolumn and R-megarow above L-megarow simultaneously (call this a BT-switch and RL-switch). Similarly, by considering the top-right and bottom-left megasquares we cannot have TB-switch and LR-switch simultaneously.

*Step 5.* Now consider the 50 megacolumns from left to right. If the switch happens more than once, then the switches must alternate, which means both TB- and BT-switch must happen. Given that either LR- or RL-switch must also happen, this violates our finding in step 4. Hence only once switch can happen, which means that the leftmost 25 megacolumns are T-types and rightmost 25 megacolumns B-types, or vice versa. Similarly, only one switch (LR- or RL) can happen, which means the uppermost 25 megarows are L and bottommost R, or vice versa. In the case where the leftmost 25 megacolumns are T-types and rightmost 25 megacolumns B-types, TB-switch happens so LR-switch cannot happen: it must be an RL switch. In the other case, BT-switch happens so we must only have RL-switch. Each of these cases give rise of one configuration, so two configurations are possible.

To show that these two configurations work, each megasquare has only a king, so any two kings that could possibly attack each other must be put in two different megasquares. These two megasquares must also share a vertex, which gives two main cases to consider:

- One is above the other, hence in the same megacolumn. By our construction, each megacolumn is either T-type or B-type, so either both are on the top row of their respective megacolumns or on the bottom row, hence cannot attack each other. The case where one is to the left of the other is completely analogous.
- The two megasquares share exactly one vertex, and WLOG (the other case is similar) let's say one is on the top left of the other. If the kings were to attack, then we have BT-switch and RL-switch simultaneously. Both our configurations avoid that.

**C6** Given a positive integer  $k$  and other two integers  $b > w > 1$ . There are two strings of pearls, a string of  $b$  black pearls and a string of  $w$  white pearls. The length of a string is the number of pearls on it. One cuts these strings in some steps by the following rules. In each step:

- The strings are ordered by their lengths in a non-increasing order. If there are some strings of equal lengths, then the white ones precede the black ones. Then  $k$  first ones (if they consist of more than one pearl) are chosen; if there are less than  $k$  strings longer than 1, then one chooses all of them.
- Next, one cuts each chosen string into two parts differing in length by at most one. (For instance, if there are strings of 5, 4, 4, 2 black pearls, strings of 8, 4, 3 white pearls and  $k = 4$ , then the strings of 8 white, 5 black, 4 white and 4 black pearls are cut into the parts (4, 4), (3, 2), (2, 2) and (2, 2) respectively.) The process stops immediately after the step when a first isolated white pearl appears.

Prove that at this stage, there will still exist a string of at least two black pearls.

**Solution.** Throughout the solution we use black string to denote string of black pearls. We consider the following two cases: the first case is when  $k$  is large enough that at each step, all the pearls are chosen to be cut, and at the last step a first isolated white pearl appears. At step  $i$ , the shortest white pearl has length  $\lfloor \frac{w}{2^i} \rfloor$ . Therefore if  $m$  steps have been taken, then the shortest white pearl after step  $m - 1$  has length  $\lfloor \frac{w}{2^{m-1}} \rfloor \geq 2$  and therefore  $w \geq 2^{m-1}$ . Now the longest black pearl after step  $m$  has length  $\lceil \frac{b}{2^m} \rceil \geq \lceil \frac{w+1}{2^m} \rceil \geq \lceil \frac{2^{m-1}+1}{2^m} \rceil = 2$  so there's a string of at least 2 black pearls will exist after step  $m$ , where at least one white pearl is isolated.

Now consider the case where  $k$  is not large enough: at one point there will be more than  $k$  strings of pearls of length  $> 1$ . Suppose on the contrary that our conclusion doesn't hold. We investigate the following two steps:

- The first point where there are more than  $k$  pearls and we don't cut them all. Given  $b > w$  and the assumption that conclusion doesn't hold, we may assume all strings (black or white) have lengths at least 2 right before that. We see that for all  $i$  with  $2^i \leq k$ , the  $i$ -step sees  $2^i$  cuts, half of which to black strings and half for white strings (resulting in  $2^i$  white and  $2^i$  black strings). Then the next step,  $k \geq 2^i$  strings are being cut, so at least  $k - 2^i$  of the white strings are being cut, resulting in at least  $k$  white strings in total (we may still assume that all white strings have length at least 2; we can show that the previous assumption of all strings having length  $\geq 2$  implies that after this step some black strings have length at least 2).
- The step at which all black pearls become isolated. This means before this step, all black strings of length  $> 1$  must have length 2, and must be cut. By (i), all strings of length  $> 1$  must be cut (which means there cannot be more than  $k$  of them). We also know that we have at least  $k$  black strings, none of them is isolated, so the presence of at least one white string of length  $> 1$  means not all strings can be cut, contradiction.

## Geometry

**G1** Let  $ABC$  be an acute triangle with  $D, E, F$  the feet of the altitudes lying on  $BC, CA, AB$  respectively. One of the intersection points of the line  $EF$  and the circumcircle is  $P$ . The lines  $BP$  and  $DF$  meet at point  $Q$ . Prove that  $AP = AQ$ .

**Solution.** We let  $P_1$  to be the  $P$  closer to  $B$  and  $P_2$  the further one, and define  $Q_1$  and  $Q_2$  correspondingly. Now,

$$\angle Q_1PA = \pi - \angle APB = \angle ACB = \angle BFD = \angle AFQ_1$$

so quadrilateral  $Q_1P_1FA$  is cyclic. Moreover  $\angle ACB = \angle AFE$  since  $BCFE$  is cyclic. With respect to the circumcircle of  $Q_1P_1FA$ ,  $AP_1$  subtends  $\angle AFP_1 = \pi - \angle AFE = \pi - \angle ACB$  and  $AQ_1$  subtends  $\angle AFQ_1 = \angle ACB$ , hence supplementary and therefore  $AP_1 = AQ_1$ .

Regarding  $P_2$  and  $Q_2$ , we also have  $\angle AP_2B = \angle AP_2Q_2 = \angle ACB = \angle AFD = \angle AFQ_2$  and therefore  $Q_2P_2FA$  is cyclic. Using the well-known fact that  $AF$  is the external angle bisector of  $\angle DFE$  which is identical to  $\angle Q_2EP_2$  due to collinearity, and that this external angle bisector intersects the circumcircle of  $Q_2FP_2$  at  $A$ , we must have  $AP_2 = AQ_2$ . (Essentially, the idea of solving these two are similar, but worded rather differently).

**G2** (IMO 4) Let  $P$  be a point interior to triangle  $ABC$  (with  $CA \neq CB$ ). The lines  $AP, BP$  and  $CP$  meet again its circumcircle  $\Gamma$  at  $K, L$ , respectively  $M$ . The tangent line at  $C$  to  $\Gamma$  meets the line  $AB$  at  $S$ . Show that  $SC = SP$  if and only if  $MK = ML$ .

**Solution.** Now we have the following equivalence:

$$\begin{aligned} MK = ML &\leftrightarrow \angle MLK = \angle MKL \leftrightarrow \angle MLB + \angle KLB = \angle LKA + \angle AKM \\ &\leftrightarrow \angle MCB + \angle KAB = \angle LBA + \angle ACM \leftrightarrow \angle PCB + \angle PAB = \angle PBA + \angle ACP \end{aligned}$$

**G3** Let  $A_1A_2 \dots A_n$  be a convex polygon. Point  $P$  inside this polygon is chosen so that its projections  $P_1, \dots, P_n$  onto lines  $A_1A_2, \dots, A_nA_1$  respectively lie on the sides of the polygon. Prove that for arbitrary points  $X_1, \dots, X_n$  on sides  $A_1A_2, \dots, A_nA_1$  respectively,

$$\max \left\{ \frac{X_1X_2}{P_1P_2}, \dots, \frac{X_nX_1}{P_nP_1} \right\} \geq 1.$$

**Solution.** We have  $\sum_{i=1}^n \angle X_iPX_{i+1} = \sum_{i=1}^n \angle P_iPP_{i+1} = 2\pi$  with indices taken modulo  $n$ . This implies an index  $j$  (again taken modulo  $n$ ) with  $\angle X_jPX_{j+1} \geq \angle P_jPP_{j+1}$ . We show that this follows that  $XX_{j+1} \geq PP_{j+1}$ .

Consider the circle  $A_{j+1}P_jP_{j+1}$ ; its diameter is the segment  $A_{j+1}P$ . Moreover, from the sine rule extended to the circumcircle of  $A_jPP_{j+1}$  we have

$$A_{j+1}P = \frac{A_{j+1}P}{\sin \angle A_{j+1}P_jP} = \frac{P_jP_{j+1}}{\sin \angle P_jA_{j+1}P_{j+1}} = \frac{P_jP_{j+1}}{\sin \angle A_jA_{j+1}P_{j+2}}$$

and similarly if  $A_{j+1}X$  were to be the diameter of the circle  $A_{j+1}X_jX_{j+1}$  then

$$A_{j+1}X = \frac{A_{j+1}X}{\sin \angle A_{j+1}X_jX} = \frac{X_jX_{j+1}}{\sin \angle X_jA_{j+1}X_{j+1}} = \frac{X_jX_{j+1}}{\sin \angle A_jA_{j+1}A_{j+2}}$$

Now,  $\angle X_jPX_{j+1} \geq \angle P_jPP_{j+1} = \angle X_jXX_{j+1}$ , the last equality are both the same as  $\pi - \angle A_jA_{j+1}A_{j+2}$ . This means, with respect to the circle  $A_{j+1}X_jXX_{j+1}$ ,  $P$  is either on or inside the circle. From the fact that  $A_{j+1}X$  is the diameter of the circle we have that  $A_{j+1}P \leq A_{j+1}X$ , and therefore  $P_jP_{j+1} \leq X_jX_{j+1}$ .

- G4** (IMO 2) Given a triangle  $ABC$ , with  $I$  as its incenter and  $\Gamma$  as its circumcircle,  $AI$  intersects  $\Gamma$  again at  $D$ . Let  $E$  be a point on the arc  $BDC$ , and  $F$  a point on the segment  $BC$ , such that  $\angle BAF = \angle CAE < \frac{1}{2}\angle BAC$ . If  $G$  is the midpoint of  $IF$ , prove that the meeting point of the lines  $EI$  and  $DG$  lies on  $\Gamma$ .

**Solution.** Let  $EI$  intersect  $\Gamma$  again at  $H$  (this  $H$  is unique once  $A, B, C, E$  are fixed). All we need to show is that  $D, G, H$  are collinear.

Now, we have  $\angle BAF = \angle CAE$  and since  $DI$  bisects  $\angle BAC$ , we also have  $\angle FAI = \angle EAI = \angle DHI$ ; the last equality follows from that  $A, H, D, E$  are concyclic. This means if  $J$  is the intersection of  $HD$  and  $AF$  then  $\angle JHI = \angle JAI$  and therefore  $J, H, A, I$  are concyclic.

Now, extend  $AJ$  to intersect  $\Gamma$  again at  $K$ , we get  $\angle AKE = \angle AHE = \angle AHI = \angle AJI$ , showing that  $JI \parallel KE$ . With  $\angle KBC = \angle KAC = \angle BAE = \angle BCE$  we have  $KE \parallel BC$  too and therefore  $JI \parallel BC$ . This means, if  $AD$  and  $BC$  intersect at  $L$  we have  $\frac{FJ}{JA} = \frac{LI}{IA}$ . Finally, using the well-known fact  $BI = DI = IC$ , and that  $\angle LBD = \angle CAD = \angle LAB$ , so  $DBL$  and  $DAB$  are, in fact, similar. This means that  $DI^2 = BI^2 = DL \cdot DA$ , i.e.  $\frac{DI}{DL} = \frac{DA}{DI}$ . Therefore,

$$\frac{FJ}{JA} = \frac{LI}{IA} = \frac{DI - DL}{DA - DI} = \frac{DI(1 - DL/DI)}{DA(1 - DI/DA)} = \frac{DI}{DA}$$

and by Menelaus theorem on  $\triangle FIA$ , the line  $DJ$  will intersect  $FI$  in its midpoint, i.e.  $G$ .

- G5** Let  $ABCDE$  be a convex pentagon such that  $BC \parallel AE$ ,  $AB = BC + AE$ , and  $\angle ABC = \angle CDE$ . Let  $M$  be the midpoint of  $CE$ , and let  $O$  be the circumcenter of triangle  $BCD$ . Given that  $\angle DMO = 90^\circ$ , prove that  $2\angle BDA = \angle CDE$ .

**Solution.** Denote the reflection of  $D$  in  $M$  as  $F$ . Since  $M$  is the common midpoint of lines  $CE$  and  $DF$ ,  $CDEF$  is a parallelogram. Moreover, from  $\angle DMO = 90^\circ$  we get  $MO$  as the perpendicular bisector of  $DF$ , hence  $DO = FO$ . This means  $F$  lies on the circumcenter of triangle  $BCD$ .

The other observation is that, if  $G$  on segment  $AB$  is such that  $BC = BG$ , then from  $AB = BC + AE$  we have  $GA = AE$ . But since  $BC \parallel AE$ , we have  $\angle CBG + \angle GAE = 180^\circ$  and therefore

$$\angle CGE = 180^\circ - \angle CGB - \angle AGE = 180^\circ - (90^\circ - \angle CBG/2) - (90^\circ - \angle GAE/2) = 90^\circ$$

which means  $CE$  is the diameter of the circumcircle of  $CGE$ . With  $M$  as the midpoint of  $CE$  we have  $CM = MG = ME$ . From  $BG = BC$ , too,  $MB$  is the perpendicular bisector of  $CG$ ; in particular,  $MB \perp CG$  and similarly  $MA \perp EG$  and with  $CG \perp EG$  we have  $MA \perp MB$ . That is,  $\angle AMB = 90^\circ$ . We also have  $MB$  bisects  $\angle ABC$  for this reason.

Now with the first two points set up, define  $H$  as the point on ray  $BD$  and satisfying  $BH = BF$ . Let  $L$  be the intersection of  $AM$  and  $FH$ . We claim that  $M$  is the midpoint of  $AL$ . Let  $N$  be the midpoint of  $FH$ , and by  $BF = BH$  we have  $BN \perp FH$ , or  $\angle BNL = 90^\circ = \angle BML$ , which means  $B, N, M, L$  are concyclic. Since  $M$  is the midpoint of  $FD$ , we also have  $MN \parallel HD$ , and therefore  $\angle BFH = \angle BHF = \angle KHD = \angle HNM = \angle LBM$ , the last equality following from that  $B, N, M, L$  concyclic. In addition, from the fact that  $MB$  bisects  $\angle ABC$  we have

$$\angle MBC = \frac{1}{2}\angle ABC = \frac{1}{2}\angle CDE = \frac{1}{2}(180^\circ - \angle FCD) = \frac{1}{2}(180^\circ - \angle FBD) = \angle BFH = \angle MBL$$

(we subtly used the fact that  $FCDE$  is a parallelogram and that  $F, B, C, D$  are concyclic). This means that  $B, L, C$  are actually collinear! I.e.  $BM$  bisects  $\angle ABL$  too, so with  $A, M, L$  collinear by definition and that  $BM \perp AL$  we have  $AM = ML$  as required.

Finally, with  $M$  as the common midpoint of  $AL$  and  $DF$ ,  $AFLD$  is a parallelogram. Thus

$$\angle BDA = \angle BDF + \angle FDA = \angle HDF + \angle LFD = \angle BHF = \frac{1}{2}\angle CDE$$

(the last step is due to the previous equation), as desired.

**G7** Three circular arcs  $\gamma_1, \gamma_2$ , and  $\gamma_3$  connect the points  $A$  and  $C$ . These arcs lie in the same half-plane defined by line  $AC$  in such a way that arc  $\gamma_2$  lies between the arcs  $\gamma_1$  and  $\gamma_3$ . Point  $B$  lies on the segment  $AC$ . Let  $h_1, h_2$ , and  $h_3$  be three rays starting at  $B$ , lying in the same half-plane,  $h_2$  being between  $h_1$  and  $h_3$ . For  $i, j = 1, 2, 3$ , denote by  $V_{ij}$  the point of intersection of  $h_i$  and  $\gamma_j$  (see the Figure below). Denote by  $\widehat{V_{ij}V_{kj}}\widehat{V_{kl}V_{il}}$  the curved quadrilateral, whose sides are the segments  $V_{ij}V_{il}$ ,  $V_{kj}V_{kl}$  and arcs  $V_{ij}V_{kj}$  and  $V_{il}V_{kl}$ . We say that this quadrilateral is *circumscribed* if there exists a circle touching these two segments and two arcs. Prove that if the curved quadrilaterals  $\widehat{V_{11}V_{21}}\widehat{V_{22}V_{12}}$ ,  $\widehat{V_{12}V_{22}}\widehat{V_{23}V_{13}}$ ,  $\widehat{V_{21}V_{31}}\widehat{V_{32}V_{22}}$  are circumscribed, then the curved quadrilateral  $\widehat{V_{22}V_{32}}\widehat{V_{33}V_{23}}$  is circumscribed, too.

**Solution.** Consider  $\gamma_1, \gamma_2, \gamma_3$  as in the problem, and consider the following claim: consider  $O_1$  as the set of all circles tangent to  $\gamma_1$  externally and to  $\gamma_2$  internally, and  $O_2$  as the set of all circles tangent to  $\gamma_2$  externally and to  $\gamma_3$  internally. If the exsimilicenter (that is, the intersection of common external tangent) of  $\omega_1$  and  $\omega_2$  lies on  $AC$  for *some*  $\omega_1 \in O_1$  and  $\omega_2 \in O_2$ , then the exsimilicenter of  $\omega_1$  and  $\omega_2$  lies on  $AC$  for *all*  $\omega_1 \in O_1$  and  $\omega_2 \in O_2$ .

To show this, consider  $\omega_A$  and  $\omega_B$  both in  $O_1$ . Let  $A_1$  and  $A_2$  be the tangency points of  $\omega_A$  with  $\gamma_1$  and  $\gamma_2$ , respectively. Define  $B_1$  and  $B_2$  similarly. By Monge Alembert's theorem,  $A_1$  and  $A_2$  passes through the insimilicenter of the circles determined by arcs  $\gamma_1$  and  $\gamma_2$ ; we name them as  $\Gamma_1$  and  $\Gamma_2$ .

Let the intersection of  $A_1A_2$  and  $B_1B_2$  as  $X$ , the insimilicenter of  $\Gamma_1$  and  $\Gamma_2$ . By this definition, if  $A_2X$  intersects  $\Gamma_2$  at  $A'_2$  again and  $B_2X$  intersects  $\Gamma_2$  again at  $B'_2$  then  $\frac{A_1X}{A_2X'} = \frac{B_1X}{B_2X'} = \frac{r_1}{r_2}$  with  $r_1, r_2$  denoting the radii of  $\Gamma_1$  and  $\Gamma_2$  respectively. We now have:

$$XA_1 \cdot XA_2 = \frac{A_1X}{A_2X'}(XA'_2 \cdot XA_2) = \frac{A_1X}{A_2X'}(XB'_2 \cdot XB_2) = \frac{B_1X}{B_2X'}(XB'_2 \cdot XB_2) = XB_1 \cdot XB_2$$

where the equality  $XA'_2 \cdot XA_2 = XB'_2 \cdot XB_2$  follows from the fact that  $A_2, B_2, A'_2B'_2$  all on  $\Gamma_2$  and that  $A_2A'_2$  and  $B_2B'_2$  intersect at  $X$ . Therefore,  $A_1, A_2, B_1, B_2$  are concyclic. Now, consider this circle containing the four points as  $\Gamma_0$ , we know that  $\Gamma_0$  and  $\Gamma_1$  intersect at  $A_1B_1$ ,  $\Gamma_0$  and  $\Gamma_2$  at  $A_2B_2$ ,  $\Gamma_1$  and  $\Gamma_2$  at  $AC$ . This means  $A_1B_1$  and  $A_2B_2$  concur on  $AC$  by the radical axis theorem. Finally,  $A_1, B_1$  are the exsimilicenters of  $\Gamma_1$  and  $\omega_A, \omega_B$ , respectively, so by Monge-Alembert theorem again the exsimilicenter of  $\omega_A$  and  $\omega_B$  must be on  $A_1B_1$ . Similarly, the same exsimilicenter must be on  $A_2B_2$  (except  $A_2, B_2$  are actually the insimilicenters of  $\Gamma_2$  and the  $\omega$ s). This means  $A_1B_1$  and  $A_2B_2$  intersect at the the exsimilicenter of  $\omega_1$  and  $\omega_2$ : in other words, by the previous points,  $\omega_1$  and  $\omega_2$  have exsimilicenter on  $AC$ . By a similar logic, any two difference circles in  $O_2$  also have their exsimilicenter on  $AC$ .

Now, suppose that  $\omega_1$  and  $\omega_2$  are such that the exsimilicenter lies on  $AC$ , say  $B$ . Consider all  $\omega'_2 \in O_2$  varying from  $A$  to  $C$ . From above, the exsimilicenter of  $\omega_2$  and  $\omega'_2$  will also lie on  $AC$  (except when  $\omega_2 = \omega'_2$ ). At most one of the circle  $\omega'_2$  will have their exsimilicenter coincide with  $B$ . In other words, for all  $\omega'_2$  except this circle and the circle coincide with  $\omega_2$ , the exsimilicenter of  $\omega_2$  and  $\omega'_2$  lies on  $AC$  other than  $B$ . By Monge-Alembert theorem again, the exsimilicenter of  $\omega_1$  and  $\omega'_2$  will also be on  $AC$  for all those  $\omega'_2$ . As  $\omega'_2$  varies continuously, the exsimilicenter of  $\omega_1$  and  $\omega'_2$  will also vary continuously. This means that this exsimilicenter of the two circles will also be on  $AC$  even for the two edge cases. Finally, if  $\omega'_1$  is any other circle in  $O_1$ , then a similar logic yields that  $\omega'_1$  and  $\omega'_2$  have exsimilicenters on  $AC$ , which solves the lemma.

Now go back to the problem. Despite the fancy formulation of the problem, really all we need is this: let the circle inscribed in  $\widehat{V_{11}V_{21}}\widehat{V_{22}V_{12}}$  as  $\omega_{11}$  and  $\widehat{V_{12}V_{22}}\widehat{V_{23}V_{13}}$  as  $\omega_{12}$ ; their exsimilicenters intersect at  $B$ . Let the circle inscribed in  $\widehat{V_{21}V_{31}}\widehat{V_{32}V_{22}}$  be  $\omega_{21}$ , and let  $\omega_{22}$  to be the unique circle tangent to  $h_2, \gamma_2$  and  $\gamma_3$ . By our lemma above, the exsimilicenter must be on  $AC$ . Since  $h_2$  is an external common tangent of  $\omega_{21}$  and  $\omega_{22}$  and  $h_2$  intersect  $AC$  at  $B$ ,  $B$  is indeed the exsimilicenter. Thus, the other common tangent must also pass through  $B$ , and so must be  $h_3$ . This means  $h_3$  is also tangent to  $\omega_{22}$ . In other words,  $\widehat{V_{22}V_{32}}\widehat{V_{33}V_{23}}$  is circumscribed. Q.E.D.

## Number Theory

**N1** Find the least positive integer  $n$  for which there exists a set  $\{s_1, s_2, \dots, s_n\}$  consisting of  $n$  distinct positive integers such that

$$\left(1 - \frac{1}{s_1}\right) \left(1 - \frac{1}{s_2}\right) \cdots \left(1 - \frac{1}{s_n}\right) = \frac{51}{2010}.$$

**Answer.** 39.

**Solution.** We need  $s_1 > 1$  since  $s_1 = 0$  will make the product equal 0. If we sort  $s_1, s_2, \dots$  in increasing order then we have  $s_i \geq i + 1$  for all  $i$  and therefore

$$\prod_{i=1}^n \left(1 - \frac{1}{s_i}\right) \geq \prod_{i=1}^n \left(1 - \frac{1}{i+1}\right) = \prod_{i=1}^n \left(\frac{i}{i+1}\right) = \frac{1}{n+1}$$

and therefore  $\frac{51}{2010} \geq \frac{1}{n+1}$ , i.e.  $n+1 \geq \frac{2010}{51} = 39 + \frac{21}{51}$ . Thus  $n \geq 39$ .

Now let's show that  $n = 39$  works. They are the numbers 2, 3, ..., 33, 35, 36, 37, 38, 39, 40, 67, which telescopes into this somewhat nice form:

$$\frac{1}{33} \cdot \frac{34}{40} \cdot \frac{66}{67} = \frac{17}{670} = \frac{51}{2010}$$

**N2** Find all pairs  $(m, n)$  of nonnegative integers for which

$$m^2 + 2 \cdot 3^n = m(2^{n+1} - 1).$$

**Answer.**  $(6, 3), (9, 3), (9, 5), (54, 5)$

**Solution.** Solving the quadratic equation in  $m$  gives  $m = \frac{2^{n+1} - 1 \pm \sqrt{(2^{n+1} - 1)^2 - 8 \cdot 3^n}}{2}$ , so the term  $(2^{n+1} - 1)^2 - 8 \cdot 3^n$  needs to be a perfect square. Now, if  $(2^{n+1} - 1)^2 - 8 \cdot 3^n = a^2$  then  $(2^{n+1} - 1 - a)(2^{n+1} - 1 + a) = 8 \cdot 3^n$ . We now have the following observation:

- Given that  $2^{n+1} - 1 - a \equiv 2^{n+1} - 1 + a \pmod{2}$ , both must be even for their product to be divisible by 8. This means one of the numbers  $2^{n+1} - 1 - a$  and  $2^{n+1} - 1 + a$  must be  $2 \cdot 3^{n_1}$  and the other  $4 \cdot 3^{n_2}$ , with  $n_1 + n_2 = n$ .
- Adding  $2^{n+1} - 1 - a$  and  $2^{n+1} - 1 + a$  together gives  $2(2^{n+1} - 1) = 2 \cdot 3^{n_1} + 4 \cdot 3^{n_2}$ , so  $2^{n+1} - 1 = 2 \cdot 3^{n_1} + 2 \cdot 3^{n_2}$ , and therefore  $3^{\min(n_1, n_2)} \mid 2^{n+1} - 1$ .

We now consider the following lemma: for each  $k \geq 1$ , the order of 2 modulo  $3^k$  is  $2 \cdot 3^{k-1}$ . We will prove by induction that the minimum  $\ell$  with  $3^k \mid 2^\ell - 1$  is  $\ell = 2 \cdot 3^{k-1}$  and at the same time for this  $\ell$ ,  $3^{k+1} \nmid 2^\ell - 1$ .

Base case:  $k = 1$  we have  $2^1 - 1$  not divisible by 3, and  $2^2 - 1$  divisible by 3 not 9. Now suppose that this is true for some  $k \geq 1$ , such that  $\ell = 2 \cdot 3^{k-1}$  we have  $3^k \mid 2^\ell - 1$  but  $3^{k+1} \nmid 2^\ell - 1$ . Let  $2^\ell = 3^k x + 1$  with  $3 \nmid x$ . Let  $\ell_1$  be the smallest number with  $3^{k+1} \mid 2^{\ell_1} - 1$ ; we have  $\ell \mid \ell_1$  so let  $\ell_1 = y\ell$ . This means:

$$2^{\ell_1} - 1 = 2^{y\ell} - 1 = (3^k x + 1)^y - 1 = \sum_{i=1}^y \binom{y}{i} (3^k x)^i$$

and for the purpose of modulo  $3^{k+2}$ , for all  $k \geq 1$  we have  $3k \geq k + 2$  so we have

$$\sum_{i=1}^y \binom{y}{i} (3^k x)^i \equiv \binom{y}{2} (3^k x)^2 + \binom{y}{1} (3^k x) \pmod{3^{k+2}}$$



now if this is divisible by  $3^{k+1}$ , since  $2k \geq k+1$ , we have  $\binom{y}{2}(3^k x)^2 + \binom{y}{1}(3^k x) \equiv 3^k xy \pmod{3^{k+1}}$ . This means  $3 \mid xy$  and with  $3 \nmid x$  we have  $3 \mid y$ . Thus the smallest such  $y$  is  $y = 3$ . Now, for this  $y = 3$  we have

$$\sum_{i=1}^y \binom{y}{i} (3^k x)^i \equiv \binom{3}{2} (3^k x)^2 + \binom{3}{1} (3^k x) = 3(3^{2k})x^2 + 3^{k+1}x = 3^{k+1}(3^k x^2 + x) \pmod{3^{k+2}}$$

and since  $3^k x^2 + x \equiv x \not\equiv 0 \pmod{3}$ , we have  $3^{k+2} \nmid 2^{3\ell} - 1$ , as desired.

Now going back to the problem, where we left off at  $3^{\min(n_1, n_2)} \mid 2^{n+1} - 1$ . If  $k = \min(n_1, n_2)$  then we have  $2 \cdot 3^{k-1} \mid n+1$ . In particular,  $n+1 \geq 2 \cdot 3^{k-1}$ . Moreover, we have

$$2^{n+1} - 1 = 3^{n_1} + 2 \cdot 3^{n_2} \leq 3^{n-k} + 2 \cdot 3^k > 3^{n-k}$$

In other words  $8^{(n+1)/3} > 2^{n+1} - 1 > 3^{n-k} = 9^{(n-k)/2}$  so  $\frac{n+1}{3} > \frac{n-k}{2}$ , i.e.  $2n+2 > 3n-3k$  so  $n < 3k+2$ .

On the other hand we have  $n+1 \geq 2 \cdot 3^{k-1}$  so  $2 \cdot 3^{k-1} - 1 \leq n \leq 3k+1$ . It's not hard to see that this only works when  $k \geq 2$ . We would now have the  $2^{n+1} - 1 > 3^{n-k} \geq 3^{n-2}$  but by above,  $n < 3k+2 \geq 3(2)+2 = 8$  so we only need to test all  $n \leq 7$ . Nevertheless, for  $n = 6, 7$  we have  $n+1 = 7, 8$  which is not divisible by 6, so for them  $k \geq 1$  and  $3(1)+2 = 5 < 6$  so these cases can be disregarded and we have  $n \leq 5$  to test.

Recall that the discriminant is  $(2^{n+1}-1)^2 - 8 \cdot 3^n$ . For  $n = 0, 1, 2, 3, 4, 5$  these discriminants are  $-7, -15, -23, 9, 313, 202$  so only  $n = 3, 5$  work as perfect squares. Plugging these into the quadratic formula we have:

$$n = 3 : \frac{2^{3+1} - 1 \pm \sqrt{(2^{3+1} - 1)^2 - 8 \cdot 3^n}}{2} = \frac{15 \pm 3}{2} = 6, 9;$$

$$n = 5 : \frac{2^{5+1} - 1 \pm \sqrt{(2^{5+1} - 1)^2 - 8 \cdot 3^n}}{2} = \frac{63 \pm 45}{2} = 9, 54.$$

Since these are obtained from the quadratic equations, they work as fine, giving us our desired pairs.

**N4** Let  $a, b$  be integers, and let  $P(x) = ax^3 + bx$ . For any positive integer  $n$  we say that the pair  $(a, b)$  is  $n$ -good if  $n \mid P(m) - P(k)$  implies  $n \mid m - k$  for all integers  $m, k$ . We say that  $(a, b)$  is *very good* if  $(a, b)$  is  $n$ -good for infinitely many positive integers  $n$ .

(a) Find a pair  $(a, b)$  which is 51-good, but not very good.

(b) Show that all 2010-good pairs are very good.

**Solution.** (a) (Courtesy of the official solution). The desired pair is  $x^3 - 51^2x = x(x^2 - 51)$ . Since  $P(0) = P(51)$ , it is only  $m$ -good for  $m$  that are divisors of 51, i.e. finite. On the other hand, to show it's 51-good, notice that  $x^3 - 51x^2 \equiv x^3 \pmod{17}$ .

- $x^3 \equiv 0, 1, 2$  for  $x = 0, 1, 2 \pmod{3}$  so it's 3-good.
- If  $x^3 \equiv y^3 \pmod{17}$  (here assume  $x, y \neq 0$ ; the 0 case can be isolated), then raising both sides to the power of 11 we have  $x^{33} \equiv y^{33} \pmod{17}$ . But by Fermat's little theorem we have  $x^{32} \equiv y^{32} = 1$  so  $x \equiv x^{33} \equiv y^{33} \equiv y$ , so this is also 17-good.

Finally, as  $\text{lcm}(3, 17) = 51$  and  $(a, b)$  is both 3- and 17-good, it's 51-good.

(b) Let  $(a, b)$  be 2010-good. We split this into the following steps:

*Step 1.* It's also 67-good.

Proof: Now,  $\{P(0), \dots, P(2009) \pmod{2010}\} = \{0, 1, \dots, 2009\}$ . In particular, since  $67 \mid 2010$ , the numbers  $0, 1, \dots, 66$  appears the same number of times (i.e. 30) in the sequence  $i \pmod{67}$  with  $i = 0, 1, \dots, 2009$ . Bearing in mind that  $n - m \mid P(n) - P(m)$  for all  $n \neq m$  and all integer polynomials  $P$ , if we consider the sequence  $P(0), \dots, P(2009)$  modulo 67, it will simply be  $P(0), \dots, P(66)$  repeated 30 times. But since  $P(0), \dots, P(2009)$  modulo 67 is also  $0, 1, \dots, 66$  repeated 30 times, we have  $\{P(0), \dots, P(66) \pmod{67}\} = \{0, \dots, 66\}$ . Hence  $(a, b)$  is 67-good.

*Step 2.*  $67 \mid a$  and  $67 \nmid b$ .

Proof: now that  $(a, b)$  is 67-good, for each  $m, n$  with  $67 \nmid m - n$  we have  $67 \nmid P(m) - P(n) = a(m^3 - n^3) + b(m - n) = (m - n)(a(m^2 - mn + n^2) + b)$ , i.e.  $67 \nmid a(m^2 + mn + n^2) + b$ . We now have two cases:

- If  $67 \mid b$  then  $P(m) - P(n) \equiv a(m^3 - n^3) \pmod{67}$ . Choose  $n = 1$  and  $m = g^{22}$  where  $g$  is a primitive root modulo 67, then  $m^3 \equiv g^{66} \equiv 1 \equiv n^3 \pmod{67}$ , so  $67 \mid P(m) - P(n)$ . But then  $67 \nmid m - n$  since  $m \not\equiv 1 \pmod{67}$ . Thus this case gives rise of a contradiction.
- Now assume  $67 \nmid b$ . We recall the identity  $67 \nmid a(m^2 + mn + n^2) + b$  for all  $m \not\equiv n \pmod{67}$ . If, there exist  $x$  such that  $67 \mid a(3x^2) + b$ , from  $b \not\equiv 0$  we have  $3ax^2 \not\equiv 0$  and therefore  $x \not\equiv 0$ . Now, choose  $m = 2x$  and  $n = -x$  we have  $a((2x)^2 - 2x^2 + x^2) + b = 3ax^2 + b \equiv 0 \pmod{67}$ . But  $m - n = 3x \not\equiv 0 \pmod{67}$ , contradicting that  $(a, b)$  is good. Thus we can further assume that  $67 \nmid a(m^2 + mn + n^2) + b$  for any integer pairs  $(m, n)$ .

We now claim that  $\{m^2 + mn + n^2 : m, n \in \mathbb{Z}\}$  attains all integers in  $\mathbb{Z}_{67}$ . For 0 it's easy: take  $m = n = 0$ . Choosing  $m = 0$  we have  $n^2$ , which gives all the quadratic residues modulo 67. Choosing  $m = n$  we have  $3m^2$ , which gives  $3 \times$  all the quadratic residues modulo 67. Now,  $8^2 = 64 \equiv -3 \pmod{67}$  is a quadratic residue modulo 67, and since  $67 \equiv 3 \pmod{4}$ ,  $-1$  is a quadratic non-residue modulo 67, and therefore  $3 = (-1)(-3)$  is also a quadratic non-residue modulo 67. Thus for all  $n$  with  $67 \nmid n$ ,  $3n^2$  is a quadratic non-residue mod 67, so  $\{3n^2 : n = 1, \dots, 66\}$  covers all quadratic non-residues modulo 67. Thus,  $(m, n) = (0, 0), (0, n), (n, n)$  together covers all integers in  $\mathbb{Z}_{67}$ .

If  $67 \nmid a$ , then we can choose a number  $x$  such that  $67 \mid ax + b$ . From the previous point, there exists  $m, n$  such that  $m^2 + mn + n^2 \equiv x \pmod{67}$ , and thus  $67 \mid a(m^2 + mn + n^2) + b$ , which is a contradiction. Therefore, we need  $67 \mid a$ .

Combining the two cases yields the results of this lemma.

*Step 3.*  $(a, b)$  is  $67^k$  good for all  $k \geq 1$ , which finishes the solution.

Proof: Let's say,  $67^k \mid P(m) - P(n) = a(m^3 - n^3) + b(m - n) = (m - n)(a(m^2 + mn + n^2) + b)$ . In modulo 67, we have  $67 \mid a$  but  $67 \nmid b$ , so  $a(m^2 + mn + n^2) + b \equiv b \not\equiv 0 \pmod{67}$ . This means,  $a(m^2 + mn + n^2) + b$  is relatively prime to 67, and therefore same to  $67^k$ . This means,  $67^k \mid m - n$ , as desired.