

SMMC online camp

JYOTI PRAKASH SAHA

23 August 2025

List of problems and examples

1.1	Exercise (IOQM 2023 P16, AoPS, cf. ARML 2010 Team Problems P4)	2
1.2	Exercise (RMO 2013d P6, AoPS)	4
1.3	Example (Putnam 2002 A2)	5
1.4	Exercise (RMO 2018a P4, AoPS)	5
1.5	Exercise (USAMO 2000 P4, AoPS)	8
1.6	Exercise (SMMC 2017 A1, AoPS)	10
1.7	Exercise (RMO 2023b P6, AoPS)	11
2.1	Example (Moscow MO 2015 Grade 11 Day 1 P5)	13
2.2	Exercise (IMOSL 1995 N5, AoPS)	17
2.3	Exercise (Tournament of Towns Fall 2013, Senior A Level P4, AoPS)	18
2.4	Exercise (SMMC 2020 A1, AoPS)	18
3.1	Example	19
3.2	Example	20
3.3	Example	20
3.4	Exercise (SMMC 2018 A1)	21
4.1	Exercise (British Mathematical Olympiad Round 1 2004/5 P5)	21
5.1	Exercise (SMMC 2018 A2)	23
5.2	Exercise (Putnam 1999 A2, AoPS)	23
5.3	Exercise (Tournament of Towns Spring 2014, Senior A Level P7, by D. A. Zvonkin)	25
5.4	Exercise (SMMC 2024 C2)	25
5.5	Exercise (ELMO 2009, AoPS, proposed by Evan O’Dorney)	26
6.1	Example	26
6.2	Example	27
6.3	Example	27
6.4	Exercise (China TST 1995 Day 2 P2, AoPS)	28
7.1	Exercise (USAMO 1976 P5, AoPS)	29
7.2	Exercise (Leningrad Math Olympiad 1991)	30

8.1	Exercise (USAMO 2018 P4, AoPS, proposed by Ankan Bhat-tacharya)	31
8.2	Exercise (Tournament of Towns Fall 2019, Junior, O Level P4, by Boris Frenkin)	33
8.3	Example (India RMO 2017a P2)	33
8.4	Exercise (USAJMO 2013 P1, proposed by Titu Andreescu)	34
8.5	Exercise (China TST 1995 Day 1 P1, AoPS)	35
8.6	Exercise (SMMC 2017 B2, AoPS)	36

Contents

1	Coloring problems	2
2	Combinatorics again	13
3	Tiling problems	19
4	Rationals	21
5	Polynomials	23
6	Crossing the x -axis/Intermediate value theorem	26
7	Roots of unity	29
8	Congruences	31

§1 Coloring problems

Exercise 1.1 (IOQM 2023 P16, AoPS, cf. ARML 2010 Team Problems P4). The six sides of a convex hexagon $A_1A_2A_3A_4A_5A_6$ are colored red. Each of the diagonals of the hexagon is colored either red or blue. If N is the number of such colorings such that every triangle $A_iA_jA_k$, where $1 \leq i < j < k \leq 6$, has at least one red side, find the sum of the squares of the digits of N .

Summary — It suffices to (observe and then!!) show that for a coloring of the diagonals of the hexagon using red and blue, if each of the triangles $A_1A_2A_3$ and $A_2A_4A_6$ has at least one red side, then each of the triangles $A_iA_jA_k$, where $1 \leq i < j < k \leq 6$, has at least one red side too. Count the number of colorings of the diagonals of the hexagon using red and blue such that each of the triangles $A_1A_3A_5$ and $A_2A_4A_6$ has at least one red side.

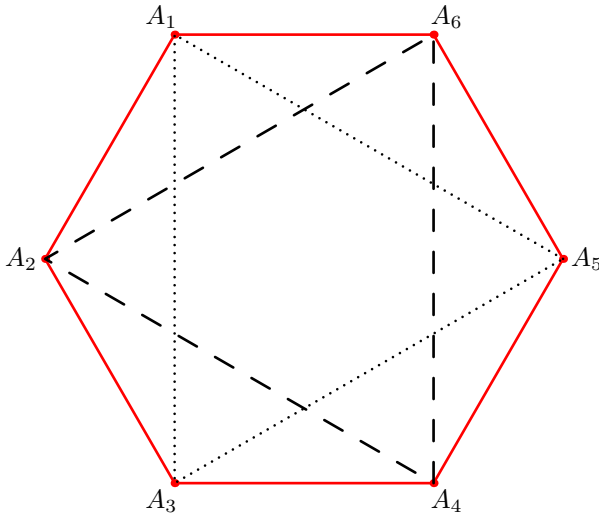


Figure 1: India IOQM 2023 P16, Exercise 1.1

Walkthrough —

- (a) The sides of the hexagon has been colored red.
- (b) Note that if $A_iA_jA_k$ is such that some two of its vertices are consecutive, then it has at least one red side.
- (c) If $A_iA_jA_k$ is such that no two of its vertices are consecutive, then any two of its vertices are exactly one vertex apart. Note that there precisely two such triangles, namely, $A_1A_3A_5$ and $A_2A_4A_6$.
- (d) Observe that if each of these two triangles have at least one red side, then the required condition is satisfied.
- (e) Moreover, if the required condition is satisfied, then each of these two triangles has at least one red side.
- (f) It follows that N is equal to the number of colorings of the diagonals of the hexagon using red and blue such that each of the triangles $A_1A_2A_3$ and $A_2A_4A_6$ have at least one red side.
- (g) This shows that

$$N = (2^3 - 1)(2^3 - 1)(2^{\binom{6}{2} - 6 - (3+3)}) = 7 \cdot 7 \cdot 8 = 392.$$

- (h) The sum of the squares of the digits of N is equal to $3^2 + 9^2 + 2^2 = 9 + 81 + 4 = 94$.

Solution 1. Consider one coloring of the diagonals of the hexagon using red and blue. If this coloring satisfies the given condition, then each of the triangles $A_1A_2A_3$ and $A_2A_4A_6$ has at least one red side. Let us establish the claim

below.

Claim — For any coloring of the diagonals of the hexagon using red and blue, if each of the triangles $A_1A_2A_3$ and $A_2A_4A_6$ has at least one red side, then each of the triangles $A_iA_jA_k$, where $1 \leq i < j < k \leq 6$, has at least one red side.

Proof of the Claim. Consider a triangle $A_iA_jA_k$ with $1 \leq i < j < k \leq 6$. Note that if $A_iA_jA_k$ is such that some two of its vertices are consecutive, then it has at least one red side. If $A_iA_jA_k$ is such that no two of its vertices are consecutive, then any two of its vertices are exactly one vertex apart. Note that there are precisely two such triangles, namely, $A_1A_3A_5$ and $A_2A_4A_6$. This proves the Claim. $\square$

Hence, it follows that N is equal to the number of colorings of the diagonals of the hexagon using red and blue such that each of the triangles $A_1A_2A_3$ and $A_2A_4A_6$ have at least one red side. Note that the sides of $A_1A_2A_3$ can be colored in $2^3 - 1 = 7$ ways such that at least one of its sides is red. Similarly, the sides of $A_2A_4A_6$ can be colored in $2^3 - 1 = 7$ ways such that at least one of its sides is red. Note that there are precisely $\binom{6}{2} - 6 - 3 - 3$ diagonals in the hexagon which are not a side of these two triangles. Hence, the number of ways to color these 15 diagonals using red and blue satisfying the given condition is equal to

$$N = (2^3 - 1)(2^3 - 1)(2^{\binom{6}{2} - 6 - (3+3)}) = 7 \cdot 7 \cdot 2^{15} = 392.$$

The sum of the squares of the digits of N is equal to

$$3^2 + 9^2 + 2^2 = 9 + 81 + 4 = 94.$$

■

Exercise 1.2 (RMO 2013d P6, AoPS). Suppose that the vertices of a regular polygon of 20 sides are coloured with three colors red, blue and green, such that there are exactly three red vertices. Prove that there are three vertices A, B, C of the polygon having the same colour such that triangle ABC is isosceles.

Walkthrough — Decompose the set of vertices of the 20-gon using the vertices of the pentagons as in Fig. 2. Apply the pigeonhole principle. It would be useful to note that any three vertices of a regular pentagon form the vertices of an isosceles triangle.

Solution 2. Since there are exactly three red vertices and any of the remaining 17 vertices are blue or green, it follows that at least 9 of these 17 vertices are of the same color, say blue. Note that the set of vertices of a regular 20-gon

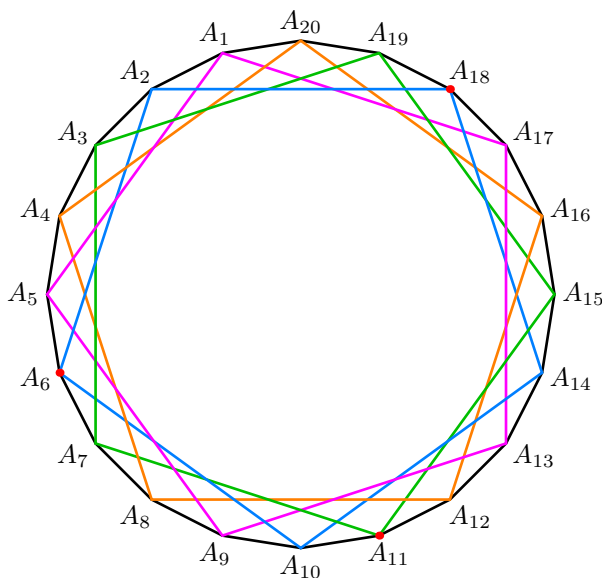


Figure 2: India RMO 2013, Exercise 1.2

can be written as the union of the four pairwise disjoint sets, each of them consisting of the vertices of a regular pentagon (as in Fig. 2). Since there are nine blue vertices, by the pigeonhole principle, at least one of these four sets contains three blue points. Since any three points on a regular pentagon form the vertices of an isosceles triangle, the statement follows. ■

Example 1.3 (Putnam 2002 A2). Given any five points on a sphere, show that some four of them must lie on a closed hemisphere.

Walkthrough —

- Draw a great circle passing through at least two of the five points.
- At least one closed hemisphere contains at least two of the remaining three points.
- Conclude!

Solution 3. Draw a great circle passing through at least two of the five points. Then at least one closed hemisphere contains at least two of the remaining three points. This proves the result. See [AN10, Example 3.2]. ■

Exercise 1.4 (RMO 2018a P4, AoPS). Let E denote the set of 25 points (m, n) in the xy -plane, where m, n are natural numbers, $1 \leq m \leq 5, 1 \leq n \leq 5$.

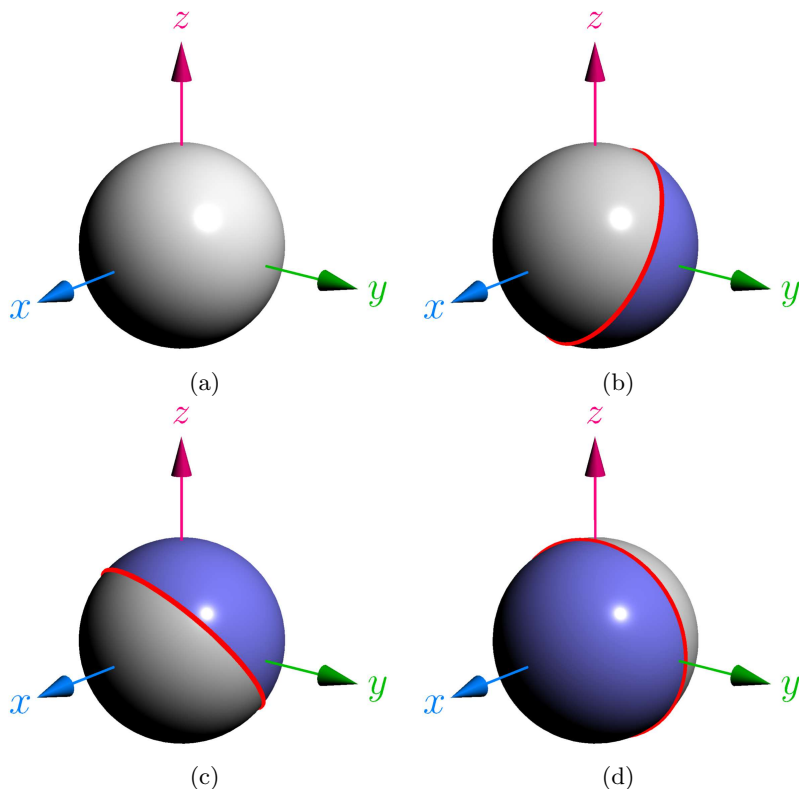


Figure 3: USA Putnam 2002 A2, Example 1.3

Suppose the points of E are arbitrarily coloured using two colours, red and blue. Show that there always exist four points in the set E of the form (a, b) , $(a + k, b)$, $(a + k, b + k)$, $(a, b + k)$ for some positive integer k such that at least three of these four points have the same colour. (That is, there always exist four points in the set E which form the vertices of a square and having at least three points of the same colour.)

Walkthrough —

- (a) Assume that the conclusion is false, and by interchanging the colors (if necessary), assume that there are more red points than the blue ones.
- (b) Show that one of the four corners is red, and assume without loss of generality that the point E (as in Fig. 4) is red.
- (c) Considering the number of red points in each of the sets $\{A, A'\}$, $\{B, B'\}$, $\{C, C'\}$, $\{D, D'\}$, prove that these four sets together contain at most 4 red points, and conclude that the green square (as in Fig. 4) contains at

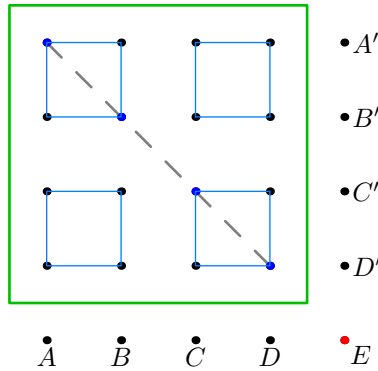


Figure 4: India RMO 2018, Exercise 1.4

least 8 red points.

- (d) Consider the blue squares in the green square, to show that the green square contains exactly 8 red points.
- (e) Conclude that there are exactly 13 red points, and each of the sets $\{A, A'\}$, $\{B, B'\}$, $\{C, C'\}$, $\{D, D'\}$ contains exactly one red point, and the green square contains exactly 8 red points.
- (f) For each point on the dashed diagonal (as in Fig. 4), consider the square having this point and E as the endpoints of one of its diagonals to show that the points on the dashed diagonal are blue.
- (g) Note that each point within the green square lying outside the dashed diagonal, is a vertex of a square having two of its remaining vertices on the dashed diagonal. Conclude that each such point is red.
- (h) Obtain a contradiction to conclude that the assumption is false.

Solution 4. On the contrary, let us assume that there is no axes-parallel square having at least three vertices of the same color.

Note that at least 13 among those 25 points are of the same color. Without loss of generality, assume that those are red. By our hypothesis, it follows that among the four vertices at the corners, there is at least one red vertex. Without loss of generality¹, let us assume that the bottom-right vertex is red, and denote this vertex by E (as in Fig. 4).

Note that each of the sets $\{A, A'\}$, $\{B, B'\}$, $\{C, C'\}$, $\{D, D'\}$ (as in Fig. 4) contains at most one red point, otherwise, we can form an axes-parallel square with at least three vertices of the same color. Consequently, the green square (as in Fig. 4) contains at least $13 - 5 = 8$ red points.

If the green square contains at least 9 red points, then at least one of the four blue squares (as in Fig. 4) contains at least three red points, which is not the

¹Convince yourself that there is **indeed no loss of generality** in assuming so.

case by our hypothesis. Hence, the green square contains exactly 8 red points. Consequently, there are precisely 13 red points among the 25 points, and each of the sets $\{A, A'\}$, $\{B, B'\}$, $\{C, C'\}$, $\{D, D'\}$ contains exactly one red point.

For any given point on the dashed diagonal (as in Fig. 4), consider the square having this point and E as the endpoints of one of its diagonals. Note that one of the other two vertices of this square is red. By our hypothesis, it follows that all the points on the gray diagonal (as in Fig. 4) are blue.

Note that each point within the green square lying outside the dashed diagonal, is a vertex of a square having two of its remaining vertices on the dashed diagonal. This shows that all the points within the green square, lying outside the gray diagonal, are red. Hence, there exists an axes-parallel square, all whose vertices are red. This contradicts our hypothesis, and hence, it follows that there exists an axes-parallel square having at least three vertices of the same color. ■

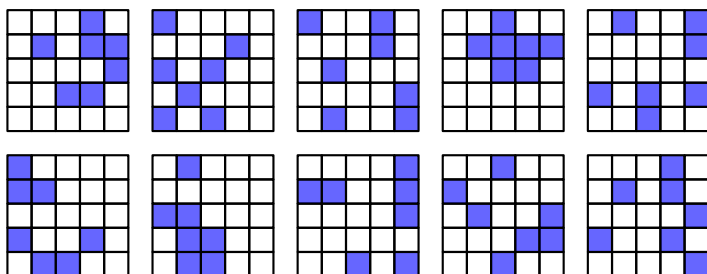
Exercise 1.5 (USAMO 2000 P4, AoPS). Find the smallest positive integer n such that if n squares of a 1000×1000 chessboard are colored, then there will exist three colored squares whose centers form a right triangle with sides parallel to the edges of the board.

Walkthrough —

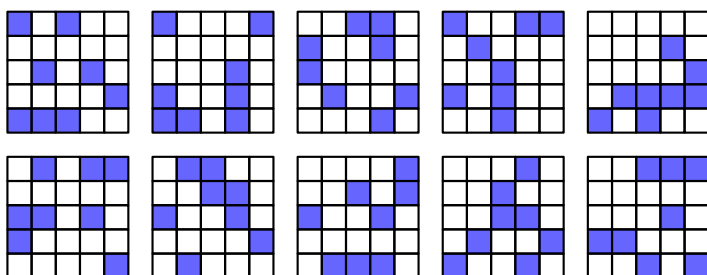
- (a) Does Fig. 5 help?
- (b) Consider a suitable coloring to show that $n \geq 1999$.
- (c) Does coloring 1999 squares suffice?
- (d) What happens when there are two columns, each containing at least two colored squares, and some row contains one colored square from each of these columns?
- (e) Consider the columns which contain at least two colored squares. How many colored squares can they contain together?
- (f) What about the remaining colored squares? How many are they in total?

Solution 5. Note that if all the squares on the top row and on the left column, excluding the square common to them, are colored, then the required condition is not satisfied. This shows that n is at least 1999.

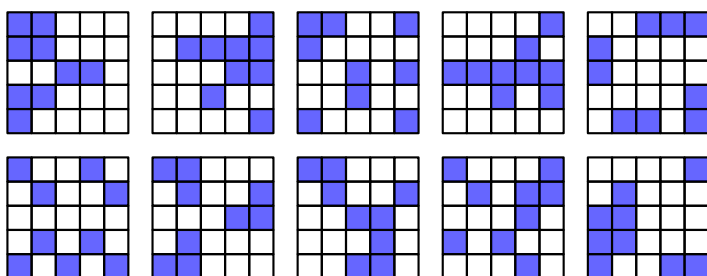
Suppose precisely 1999 squares of the chessboard have been colored. Note that there are columns containing at least two colored squares. Consider the columns containing at least two colored squares. If there are two among these columns, such that some row contains one colored square from each of these columns, then we are done. It remains to consider the case that no two of these columns have this property, which we assume from now on. Hence, the colored squares lying on these columns, lie in different rows. This shows that these columns together contain at most 1000 colored squares. Consequently, there



The above chessboards have 7 of its squares colored



The above chessboards have 8 of its squares colored



The above chessboards have 9 of its squares colored

Figure 5: USAMO 2000 P4, Exercise 1.5

are at least 999 colored squares, each lying on a column containing no more colored squares. This implies that there are precisely 999 such colored squares. Moreover, there is only one column containing at least two colored squares, and it contains the remaining 1000 colored squares. One among the 999 colored squares, together with two suitable squares from these 1000 squares, have the required property. This shows that $n = 1999$. ■

Exercise 1.6 (SMMC 2017 A1, AoPS). The five sides and five diagonals of a regular pentagon are drawn on a piece of paper. Two people play a game, in which they take turns to colour one of these ten line segments. The first player colours line segments blue, while the second player colours line segments red. A player cannot colour a line segment that has already been coloured. A player wins if they are the first to create a triangle in their own colour, whose three vertices are also vertices of the regular pentagon. The game is declared a draw if all ten line segments have been coloured without a player winning. Determine whether the first player, the second player, or neither player can force a win.

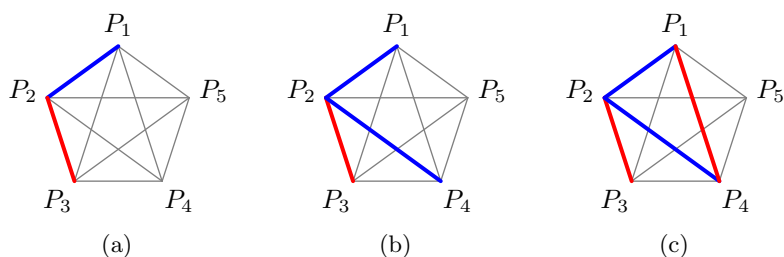


Figure 6: SMMC 2017 A1, Exercise 1.6, First two colored segments share a common vertex

Walkthrough — To force a win, the first player colors a side of the pentagon in blue in the first move.

Let us first consider the case that the two edges coloured in the first two moves have a common endpoint.

- (a) Show that there is no loss of generality in assuming that the first player colours P_1P_2 in blue and the second player colours P_2P_3 in red, where $P_1P_2P_3P_4P_5$ denotes the pentagon.
- (b) Next, the first player colours P_2P_4 in blue.
- (c) If the second player does not color P_1P_4 , then in the next move the first player colours P_1P_4 in blue and wins. It remains to consider the case that the second player colours P_1P_4 in red, which we assume from now on.
- (d) The first player colours P_2P_5 in blue.

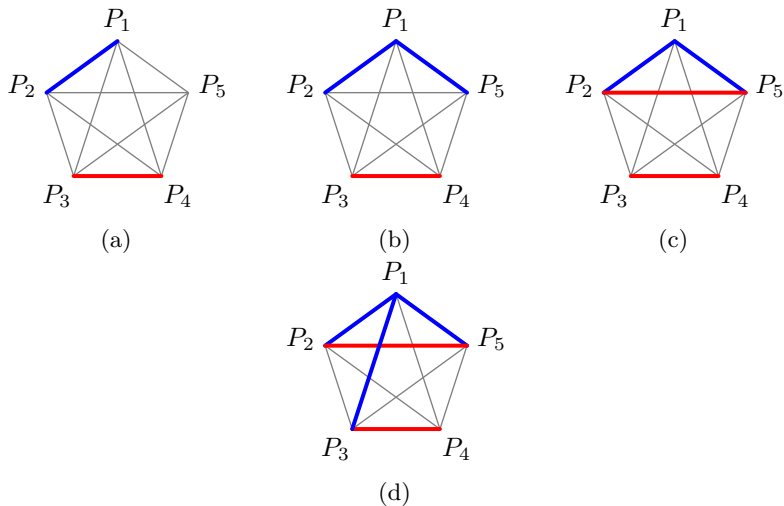


Figure 7: SMMC 2017 A1, Exercise 1.6, First two colored segments share no common vertex

- (e) During the next turn of the first player, one of the edges P_1P_5 and P_4P_5 is coloured in blue, thus creating a blue triangle.

We are still left with the case that the two edges coloured in the first two moves do not have a common endpoint.

- (a) Show that there is no loss of generality in assuming that the first player colours P_1P_2 in blue and the second player colours P_3P_4 in red.
- (b) Next, the first player colours P_1P_5 in blue.
- (c) If the second player does not color P_2P_5 , then in the next move the first player colours P_2P_5 in blue and wins. It remains to consider the case that the second player colours P_2P_5 in red, which we assume from now on.
- (d) The first player colours P_1P_3 in blue.
- (e) During the next turn of the first player, one of the edges P_2P_3 and P_3P_5 is coloured in blue, thus creating a blue triangle.

Solution 6. ■

Exercise 1.7 (RMO 2023b P6, AoPS). Consider a set of 16 points arranged in a 4×4 square grid formation. Prove that if any 7 of these points are coloured blue, then there exists an isosceles right-angled triangle whose vertices are all blue.

The following is from [AoPS](#), is due to Rohan (Goyal?) as mentioned [here](#) by [L567](#).

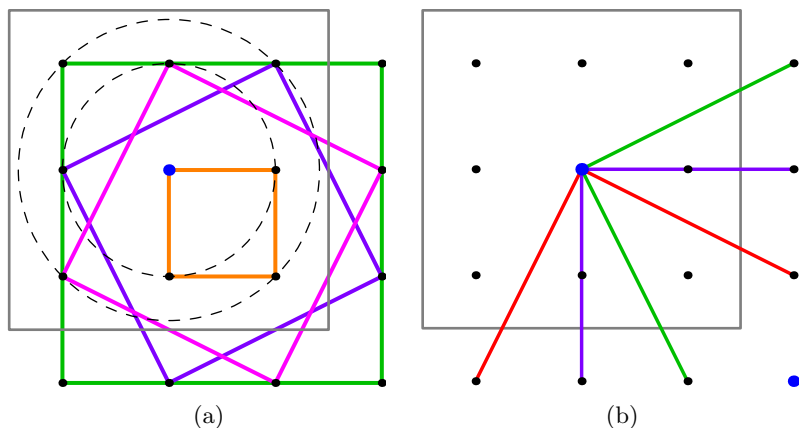


Figure 8: India RMO 2023, Exercise 1.7

Walkthrough —

- (a) Show that if the small square (as in Fig. 8a) does not contain a blue point, then we are done.
- (b) It remains to consider the case when the small square (as in Fig. 8a) contains at least one blue point.
- (c) Rotating the configuration about the center of the small square (if necessary), assume that the top-left vertex of the small square (as in Fig. 8a) is blue.
- (d) Prove that the gray square contains at most three blue points.
 - Consider the case when at least two blue points lie on the bigger dashed circle. Show that the smaller dashed circle does not contain any blue point, in this case. Hence, the gray square contains at most three blue points.
 - Similarly, if the smaller dashed circle contains at least two blue points, then the gray square (as in Fig. 8b) contains at most three blue points.
- (e) It suffices to consider that each one of the red, purple, and green L -shapes, has at most one end-point which is blue (otherwise, we are done).
- (f) Use the above to show that the bottom-right point (as in Fig. 8b) is blue.
- (g) Consider the point at the bottom-right corner, and the center of the gray square, and a blue end-point of an L -shape, to show that these three points form the vertices of an isosceles triangle having the required properties.

Solution 7. Note that the 16 points are the vertices of the four squares as in Fig. 8a. If no vertex of the small square is blue, then by the pigeonhole principle, at least one of the remaining three squares has at least three blue

vertices, and hence there exists an isosceles right-angled triangle with blue vertices.

Let us assume that the small square (as in Fig. 8a) has a blue vertex. Rotating the configuration about the center of the small square (if necessary), we may and do assume that the top-left vertex of the small square is blue. Henceforth, on the contrary, let us assume that there are no isosceles right-angled triangles with blue vertices.

Claim — The gray square (as in Fig. 8a) contains at most three blue points.

Proof of the Claim. Note that the points within the gray square lie on the two dashed circles (as in Fig. 8a). Therefore, to prove the Claim, it suffices to show that if one of the dashed circles (as in Fig. 8a) contains at least two blue points, then the other dashed circle does not contain any blue point.

If at least two blue points lie on the bigger dashed circle, then using the assumption, it follows that no more blue points lie on it, and hence these two blue points lie along a diameter. It follows that no blue point lies on the other dashed circle.

If at least two blue points lie on the smaller dashed circle, then using a similar argument, it follows that no blue point lies on the bigger dashed circle.

The Claim follows. $\square$

Note that if both the end-points of one of the red, purple, and green L -shapes (as in Fig. 8b) are blue, then these points together with the center of gray square form the vertices of an isosceles right-angled triangle, contradicting the assumption. Hence, each one of these three L -shapes has at most one end-point which is blue. Since there are 7 blue points, using the Claim, it follows that the bottom-right point is blue. Note that the center of the gray square, the bottom-right point, and a blue end-point of the “purple” L -shape, form the vertices of a triangle having the required properties. $\blacksquare$

§2 Combinatorics again

Example 2.1 (Moscow MO 2015 Grade 11 Day 1 P5). Prove that it is impossible to put the integers from 1 to 64 (using each integer once) into an

8×8 table so that for any 2×2 square $\begin{array}{|c|c|} \hline a & b \\ \hline c & d \\ \hline \end{array}$, the difference $ad - bc$ is equal to 1 or -1 .

Remark.

a	b
c	d

p	q
r	s

Figure 9: $ad - bc = \pm 1, ps - qr = \pm 1$, Example 2.1

a	b
c	d

p	q
r	s

Figure 10: $ad - bc = \pm 1, ps - qr = \pm 1$, Example 2.1

- Given a 2×2 square

a	b
c	d

, the difference $ad - bc$ is equal to

the product of the diagonal terms

– the product of the anti-diagonal terms.

Let us call this difference *the determinant* of the 2×2 square.

- For instance,
 - $\begin{pmatrix} 1 & 2 \\ 3 & 4 \end{pmatrix}$ has determinant equal to -2 ,
 - $\begin{pmatrix} 8 & 9 \\ 7 & 12 \end{pmatrix}$ has determinant equal to $96 - 63 = 33$,
 - $\begin{pmatrix} 13 & 14 \\ 5 & 7 \end{pmatrix}$ has determinant equal to $91 - 70 = 21$.
 - Did you notice that if the determinant is odd, then the diagonal entries are odd or the anti-diagonal entries are odd?
- We need to show that there is no filling of an 8×8 table using the integers from 1 to 64, using each integer once, such that any 2×2 square (such squares have been marked in Fig. 9, Fig. 10, note that there $9 + 16 = 25$ such 2×2 squares.) has a determinant equal to 1 or -1 . Equivalently^a, no matter how one may fill an 8×8 table using the integers from 1 to 64, using each integer once, some 2×2 square has to have a determinant other than 1, -1 .

^aIs the equivalence clear? Try to think about it!

Summary — If such a filling exists, then divide the 8×8 table into 16 pairwise disjoint 2×2 squares (as in Fig. 11). Due to parity constraints, each square contains precisely two evens along its diagonal or anti-diagonal, and their product is at most one more than the product of the odd entries. Consequently, for any of these 16 squares, the product of its even entries is less than the product of the successors of its odd entries. Multiplying across the squares gives a contradiction.

Walkthrough —

- (a) Assume that such a filling exists.

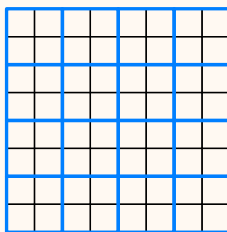


Figure 11: Moscow MO 2015 Grade 11 Day 1 P5, Example 2.1

- (b) Recall that the determinant of a 2×2 square $\begin{bmatrix} a & b \\ c & d \end{bmatrix}$ is
- the product of the diagonal terms
– the product of the anti-diagonal terms.
- (c) Note that $\boxed{\text{even} - \text{even} \neq \pm 1, \text{odd} - \text{odd} \neq \pm 1}$, and hence any square contains two odd numbers along the diagonal  or on the anti-diagonal .
- (d) Divide the 8×8 table into 16 pairwise disjoint 2×2 squares.
- (e) Each of these 16 squares contains at least two odd integers, and hence, they together contain at least 32 odd integers.
- (f) Conclude that each of these 16 squares contains precisely two odd integers, and precisely two even integers.
- (g) Consider a square among them. It is of the form

$$\begin{bmatrix} a & b \\ c & d \end{bmatrix} \text{ with } a, d \text{ both odd, and } b, c \text{ both even,}$$

or of the form

$$\begin{array}{|c|c|} \hline b & a \\ \hline d & c \\ \hline \end{array} \text{ with } a, d \text{ both odd, and } b, c \text{ both even.}$$

- (h) The product of its even entries is at most one more than the product of its odd entries.
- (i) Note that for any two odd positive integers b, c , the inequality $bc + 1 < (b + 1)(c + 1)$ holds.
- (j) This shows that

the product of two evens between 1 and 64
 $<$ the product of
 two (possibly different) evens between 1 and 64.

- (k) Multiply all the even entries of the 16 squares to obtain

$$2 \cdot 4 \cdot \dots \cdot 64 < (1 + 1) \cdot (3 + 1) \cdot \dots \cdot (63 + 1) = 2 \cdot 4 \cdot \dots \cdot 64.$$

Solution 8. Let us assume that an 8×8 table admits a filling by the integer from 1 to 64, using each integer once, such that each 2×2 square, considered as a matrix, has determinant equal to 1 or -1 .

Claim — Any 2×2 square contains at least two odd integers.

Proof of the claim. Since the difference of two integers can be odd only when they are of different parity (i.e. one of them is odd, and the other is even), it follows that for any 2×2 square, the product of its diagonal entries and the product of its anti-diagonal entries are of different parity, and hence of these two products is odd, and consequently, the diagonal entries are odd or the anti-diagonal entries are odd. In particular, any 2×2 square contains at least two odd integers. $\square$

Let us divide the 8×8 table into 16 pairwise disjoint 2×2 squares (as in Fig. 11).

Claim — Each of these 16 squares contains exactly two even integers, lying along its diagonal or anti-diagonal.

Proof of the claim. By the previous Claim, each of these 16 squares contains at least two odd integers, and they contain at least $16 \times 2 = 32$ odd integers. Since there are precisely 32 odd integers between 1 and 64, it follows that each of these 16 squares contains exactly two odd integers along its diagonal or anti-diagonal, and hence exactly two even integers along its anti-diagonal or diagonal. $\square$

Since the determinant of any 2×2 square is 1 or -1 , it follows that for any of the 16 squares as in Fig. 11, the product of its even entries is at most one more than the product of its odd entries. Note that for any two odd positive integers b, c , the inequality $bc + 1 < (b + 1)(c + 1)$ holds. Consequently, for any of the 16 squares as in Fig. 11, the product of its even entries is less than the product of the successors of its odd entries. This implies that the product of the even entries of all the 16 squares is less than the product of the successors of the odd entries of these boxes. Note that the even entries of these squares are the even integers lying between 1 and 64, so are the successors of the odd entries of these squares. It follows that

$$2 \cdot 4 \cdot \dots \cdot 64 < (1 + 1) \cdot (3 + 1) \cdot \dots \cdot (63 + 1) = 2 \cdot 4 \cdot \dots \cdot 64.$$

This contradicts the assumption that an 8×8 table admits a filling by the integer from 1 to 64, using each integer once, such that each 2×2 square, considered as a matrix, has determinant equal to 1 or -1 . Hence, no such filling is possible. ■

Exercise 2.2 (IMOSL 1995 N5, AoPS). At a meeting of $12k$ people, each person exchanges greetings with exactly $3k + 6$ others. For any two people, the number who exchange greetings with both is the same. How many people are at the meeting?

Walkthrough —

- (a) Count the number of triples (a, b, c) where a exchanges greetings with b and c in two different ways.
- (b) Show that $12k - 1$ divides 525 and deduce the value of k .

Solution 9. Let λ denote the integer such that for any two people, precisely λ persons exchange greetings with them. Counting the number of triples of the form (a, b, c) where a exchanges greetings with b and c , we obtain

$$12k \binom{3k+6}{2} = \lambda \binom{12k}{2},$$

which yields

$$\begin{aligned} \lambda &= \frac{(3k+5)(3k+6)}{12k-1} \\ &= \frac{1}{4} \frac{36k^2 + 132k + 120}{12k-1} \\ &= \frac{1}{4} \left(3k + 11 + \frac{3k+131}{12k-1} \right) \\ &= \frac{3k+11}{4} + \frac{1}{16} \left(1 + \frac{525}{12k-1} \right). \end{aligned}$$

This shows that $12k - 1$ divides 525 and the quotient $525/(12k - 1)$ is congruent to 3 modulo 4, that is, for some integer $\ell \geq 0$, we have

$$525 = (12k - 1)(4\ell + 3).$$

Noting that $525 = 3 \cdot 5^2 \cdot 7$, it follows that one of $12k - 1, 4\ell + 3$ is a multiple of 3 and the other one is a multiple of 7. This shows that $12k - 1$ is equal to one of

$$3, 15, 45, 7, 35, 105,$$

and hence $12k - 1 = 35$, which gives $k = 3$. It follows that there are 36 people at the meeting. ■

Exercise 2.3 (Tournament of Towns Fall 2013, Senior A Level P4, AoPS).

Integers $1, 2, \dots, 100$ are written on a circle, not necessarily in that order. Can it be that the absolute value of the difference between any two adjacent integers is at least 30 and at most 50?

Walkthrough —

- (a) Assume that such an arrangement is possible.
- (b) Consider the integers $1, 2, \dots, 25, 76, 77, \dots, 100$.
- (c) Show that no two of these integers are adjacent.
- (d) Conclude that the integers $1, 2, \dots, 25, 76, 77, \dots, 100$ and $26, 27, \dots, 75$ are placed alternately along the circle.
- (e) Show that 26 is adjacent to 76 only.
- (f) Derive a contradiction.

Solution 10. Let us assume that the integers $1, 2, \dots, 100$ can be arranged along the circumference of a circle in some order such that the absolute value of the difference between any two adjacent integers is at least 30 and at most 50.

Since the difference of any two of the integers $1, 2, \dots, 25, 76, 77, \dots, 100$ is less than 30 or greater than 50 it follows that no two of these integers are adjacent. Consequently, the elements of the sets

$$\{1, 2, \dots, 25, 76, 77, \dots, 100\}, \{26, 27, \dots, 75\}$$

are placed alternately along the circle. However, 26 is adjacent to 26 only, which is impossible. This shows that there is no arrangement of the integers $1, 2, \dots, 100$ along the circumference of a circle satisfying the given condition. ■

Exercise 2.4 (SMMC 2020 A1, AoPS). There are 1001 points in the plane such that no three are collinear. The points are joined by 1001 line segments

such that each point is an endpoint of exactly two of the line segments. Prove that there does not exist a straight line in the plane that intersects each of the 1001 line segments in an interior point. An **interior point** of a line segment is a point of the line segment that is not one of the two endpoints.

Walkthrough —

- (a) On the contrary, let us assume that there exists a straight line L in the plane that intersects each of the 1001 line segments in an interior point.
- (b) Show that L cannot pass through any of the 1001 points.
- (c) Color the points on one side of L red, and the points on the other side of L blue.
- (d) Show that the number of the line segments is equal to twice the number of red points, to obtain a contradiction.

Solution 11. On the contrary, let us assume that there exists a straight line L in the plane that intersects each of the 1001 line segments in an interior point. Note that L cannot pass through any of the 1001 points. Indeed, if L passes through one of the 1001 points, then the two line segments that have this point as an endpoint, cannot intersect L at their interior points, since no three of the given points are collinear. Let us color the points on one side of L red, and the points on the other side of L blue. Since L intersects each of the 1001 line segments in an interior point, each of the 1001 line segments has one red endpoint and one blue endpoint. Moreover, each of the 1001 points is an endpoint of exactly two of the line segments. Therefore, the number of line segments is equal to twice the number of red points, which is impossible since 1001 is odd. This completes the proof. ■

§3 Tiling problems

Example 3.1. Show that for any integer $n \geq 1$, a $2^n \times 2^n$ chessboard with one square removed can be tiled by non-overlapping trominos, that is, L -shaped pieces consisting of three squares.

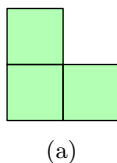
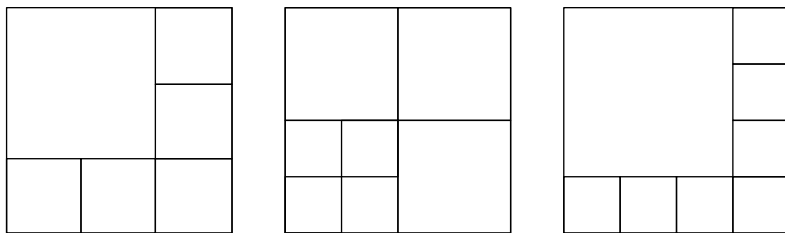


Figure 12: Tiling a $2^n \times 2^n$ chessboard with one square removed using trominos.



(a) Tiling using 6 squares. (b) Tiling using 7 squares. (c) Tiling using 8 squares.

Figure 13: Tiling a square using 6, 7, and 8 squares.

Walkthrough —

- (a) Can a 2×2 chessboard with one square removed be tiled by trominos?
- (b) Can a 4×4 chessboard with one square removed be tiled by trominos?
- (c) Can a 8×8 chessboard with one square removed be tiled by trominos?
- (d) What about tiling a $2^n \times 2^n$ chessboard with one square removed using trominos for $n \geq 4$? Does induction help?

Solution 12. ■

Example 3.2. For any integer $n \geq 6$, show that a square can be cut into n squares, not necessarily of the same size.

Walkthrough —

- (a) Try to work it out for small values of n , for instance $n = 6, 7, 8, 9$.
- (b) What happens if you want to go from n to $n + 3$?

Solution 13. Note that if we can do it for n , then we can do it for $n + 3$ by cutting one of the squares into four smaller squares. So it suffices to do it for $n = 6, 7, 8$, which is shown in Fig. 13. By induction, we are done. ■

Example 3.3. Can a 12×15 chessboard be covered by non-overlapping trominos? A tromino is an L -shaped piece consisting of three squares, where these squares are of the same size as the smallest squares in the chessboard.

Walkthrough —

- (a) Does Fig. 14 help?

Solution 14. Note that a 2×3 rectangle can be tiled by two non-overlapping trominos. Since a 12×15 chessboard can be covered by non-overlapping 2×3

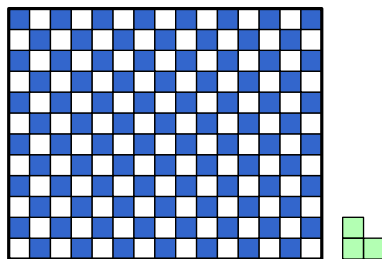


Figure 14: Tiling a 12×15 chessboard using trominos.

rectangles, it follows that a 15×15 chessboard can be tiled by non-overlapping trominos. ■

Exercise 3.4 (SMMC 2018 A1). Call a rectangle *dominant* if it is similar to a 2×1 rectangle. For which integers $n \geq 5$ is it possible to tile a square with n dominant rectangles, which are not necessarily congruent to each other?

Walkthrough —

(a)

Solution 15. ■

§4 Rationals

Exercise 4.1 (British Mathematical Olympiad Round 1 2004/5 P5). Let S be a set of rational numbers with the following properties:

1. $\frac{1}{2} \in S$,
2. If $x \in S$, then both $\frac{1}{x+1} \in S$ and $\frac{x}{x+1} \in S$.

Prove that S contains all rational numbers in the interval $0 < x < 1$.

Walkthrough —

- (a) Since $\frac{1}{2}$ lies in S , by the second condition, it follows that $\frac{2}{3}$ lies in S and so does $\frac{1}{3}$.
- (b) Taking $x = \frac{1}{3}$, it follows that

$$\frac{3}{4}, \frac{1}{4}$$

lie in S . **Note that we have showed that S contains all the rationals between 0 and 1 with denominator at most 4.**

- (c) Taking $x = \frac{2}{3}$, it follows that

$$\frac{2}{5}, \frac{3}{5}$$

lie in S . We are **not in a position** to conclude that S contains all the rationals between 0 and 1 with denominator at most 5.

- (d) Taking $x = \frac{1}{4}$, it follows that

$$\frac{1}{5}, \frac{4}{5}$$

lie in S . It follows that S contains all the rationals between 0 and 1 with denominator at most 5.

- (e) Does the above provide any insight to conclude that S contains all the rationals between 0 and 1? For instance, can one expect the following (and then prove, or realize that it is false, or argue along different lines)?

For a rational number x lying in S , the rationals

$$\frac{1}{x+1}, \frac{x}{x+1}$$

have denominators larger^a than that of x .

^aOften, while being naive, one takes the liberty to write **larger** to mean **no smaller**, that is, **greater than or equal to**. But this is **NOT allowed** while writing down a solution.

Or, stated in a different way,

A rational number lying in $(0, 1)$ can be obtained from a rational number lying in $(0, 1)$ with smaller denominator by applying one of the maps

$$x \mapsto \frac{1}{x+1}, x \mapsto \frac{x}{x+1}.$$

Solution 16. It suffices to establish the following.

Claim — For any integer $k \geq 2$, all the rationals lying in $(0, 1)$ with denominators not exceeding k lie in S , that is, we have

$$\left\{ \frac{1}{\ell}, \frac{2}{\ell}, \dots, \frac{\ell-2}{\ell}, \frac{\ell-1}{\ell} \right\} \subseteq S \quad \text{for all } 2 \leq \ell \leq k. \quad (1)$$

Proof of the Claim. Eq. (1) holds for $k = 2$ from condition (1). Suppose Eq. (1) holds for $k = n - 1$ for some integer $n \geq 3$. Let m be an integer satisfying $1 \leq m < n$. Using the induction hypothesis, we will show that $\frac{m}{n}$ lies in S . Note that for $0 < x < 1$, the inequalities

$$0 < \frac{x}{x+1} < \frac{1}{2}, \frac{1}{2} < \frac{1}{x+1} < 1$$

hold. Using Condition (1), it follows that $\frac{m}{n}$ lies in S if $\frac{m}{n} = \frac{1}{2}$. If $0 < \frac{m}{n} < \frac{1}{2}$, then

$$\frac{x}{x+1} = \frac{m}{n}$$

holds for $x = \frac{m}{n-m}$, which is a rational number lying in $(0, 1)$ with denominator $\leq n-1$, and by induction hypothesis, the set S contains $\frac{m}{n}$. Moreover, if $\frac{1}{2} < \frac{m}{n} < 1$, then

$$\frac{1}{x+1} = \frac{m}{n}$$

holds for $x = \frac{n-m}{m}$, which is a rational number lying in $(0, 1)$ with denominator $\leq n-1$, and by induction hypothesis, the set S contains $\frac{m}{n}$. We conclude that for any integer $n \geq 3$, Eq. (1) holds for $k = n$ if it holds for $k = n-1$. $\square$

§5 Polynomials

Exercise 5.1 (SMMC 2018 A2). Ada and Byron play a game. First, Ada chooses a non-zero real number a and announces it. Then Byron chooses a non-zero real number b and announces it. Then Ada chooses a non-zero real number c and announces it. Finally, Byron chooses a quadratic polynomial whose three coefficients are a, b, c in some order.

- Suppose that Byron wins if the quadratic polynomial has a real root and Ada wins otherwise. Determine which player has a winning strategy.
- Suppose that Ada wins if the quadratic polynomial has a real root and Byron wins otherwise. Determine which player has a winning strategy.

Walkthrough — Without loss of generality, we may assume that $a = 1$.

- In (a), Byron has a winning strategy by choosing $b = -1$, and then considering the polynomial $ax^2 + cx + b$.
- In (b), Ada has a winning strategy by choosing c

$$\begin{cases} -4\sqrt{b} & \text{if } b > 0, \\ \frac{b^2}{8} & \text{if } b < 0. \end{cases}$$

In any of the above cases, one can check that the discriminant of each of the three possible polynomials is positive.

Solution 17.

Exercise 5.2 (Putnam 1999 A2, AoPS). Show that for some fixed positive integer n , we can always express a polynomial with real coefficients which is nowhere negative as a sum of the squares of n polynomials.

Walkthrough —

- (a) Show that the real roots of P have even multiplicity.
- (b) Conclude that P can be expressed as a product of monic quadratic polynomials with real coefficients having nonreal roots, and even powers of linear polynomials with real coefficients.
- (c) Show that a monic quadratic polynomial with real coefficients having nonreal roots is the sum of the squares of two polynomials with real coefficients.

Solution 18. Note that if P is a constant polynomial, then it is clear. Henceforth, let us assume that P is a nonconstant polynomial.

Claim — The polynomial P can be written as the product of polynomials, each of which can be expressed as the sum of the squares of two polynomials with real coefficients.

Proof of the Claim. Since P has real coefficients, it follows that if $\alpha \in \mathbb{C} \setminus \mathbb{R}$ is a root of P , then so is $\bar{\alpha}$. Thus, the nonreal complex roots of P form pairs of complex conjugates. Note that

$$(x - \alpha)(x - \bar{\alpha}) = (x - \operatorname{Re}(\alpha))^2 + \operatorname{Im}(\alpha)^2.$$

Decomposing P over the pairs of nonreal complex conjugate roots, and the real roots, it follows that P can be expressed as the product

$$cf(x) \prod_{a \in A} (x - a)^{m_a},$$

where c denote the leading coefficient of P , $f(x)$ denotes the product of (possibly no) quadratic polynomials of the form $(x - a)^2 + b^2$ with $a \in \mathbb{R}, b \in \mathbb{R} \setminus \{0\}$, and A denotes the set of real roots of P , and for an element $a \in A$, the multiplicity of a is denoted by m_a .

Evaluating P at a suitable real number (for instance, at $1 + \sum_{a \in A} a$ (resp. 1) if A is nonempty (resp. empty)), it follows that $c > 0$.

Let a be an element of A . Since A is finite, there exists a real number $\varepsilon > 0$ such that the interval $(a - \varepsilon, a + \varepsilon)$ contains no real roots of P other than a . If m_a were odd, then the sign of $P(x)$ would not remain constant as x ranges over in $(a - \varepsilon, a + \varepsilon) \setminus \{a\}$. Hence, it follows that m_a is even.

Since $c > 0$ and m_a is even for any $a \in A$, the Claim follows. $\square$

Claim — Let $f_1(x), g_1(x), f_2(x), g_2(x)$ be polynomials with real coefficients. Then the following holds.

$$(f_1(x)^2 + g_1(x)^2)(f_2(x)^2 + g_2(x)^2)$$

$$= (f_1(x)f_2(x) - g_1(x)g_2(x))^2 + (f_1(x)g_2(x) - f_2(x)g_1(x))^2$$

Proof of the Claim. Note that

$$\begin{aligned} & (f_1(x)^2 + g_1(x)^2)(f_2(x)^2 + g_2(x)^2) \\ &= f_1(x)^2 f_2(x)^2 + g_1(x)^2 g_2(x)^2 - 2f_1(x)f_2(x)g_1(x)g_2(x) \\ & \quad + f_1(x)^2 g_2(x)^2 + f_2(x)^2 g_1(x)^2 + 2f_1(x)g_2(x)f_2(x)g_1(x) \\ &= (f_1(x)f_2(x) - g_1(x)g_2(x))^2 + (f_1(x)g_2(x) + f_2(x)g_1(x))^2. \end{aligned}$$

□

Combining the above Claims, and using induction, the result follows. ■

Exercise 5.3 (Tournament of Towns Spring 2014, Senior A Level P7, by D. A. Zvonkin). Consider a polynomial $P(x)$ such that

$$P(0) = 1, \quad (P(x))^2 = 1 + x + x^{100}Q(x),$$

where $Q(x)$ is also a polynomial. Prove that in the polynomial $(P(x) + 1)^{100}$, the coefficient of x^{99} is zero.

Walkthrough —

- (a) Since $P(x)^2$ is congruent to $1 + x$ modulo x^{100} , show that $(P(x) + 1)^{100} + (1 - P(x))^{100}$ is congruent to a polynomial of degree 50 in $1 + x$ modulo x^{100} .
- (b) Prove that $(P(x) + 1)^{100}$ is congruent to a polynomial of degree 50 in $1 + x$ modulo x^{100} .

Solution 19. Note that

$$(P(x) + 1)^{100} + (1 - P(x))^{100}$$

is a polynomial in $P(x)^2$ of degree 50. Given three polynomials $f(x), g(x), h(x)$ having complex coefficients, with $h(x) \neq 0$, we say that $f(x)$ is congruent to $g(x)$ modulo $h(x)$ if $h(x)$ divides $f(x) - g(x)$, that is, $f(x) - g(x)$ is the product of $h(x)$ and a polynomial in x with complex coefficients. Since $P(x)^2$ is congruent to $1 + x$ modulo x^{100} , it follows that $(P(x) + 1)^{100} + (1 - P(x))^{100}$ is congruent to a polynomial of degree 50 in $1 + x$ modulo x^{100} . Using that $P(x) \equiv 1 \pmod{x}$, we obtain that $(P(x) + 1)^{100}$ is congruent to a polynomial of degree 50 in $1 + x$ modulo x^{100} . This shows that the coefficient of x^{99} in $(P(x) + 1)^{100}$ is zero. ■

Exercise 5.4 (SMMC 2024 C2). Define the function $f : \mathbb{R} \rightarrow \mathbb{R}$ by

$$f(x) = x^3 - 3x^2 + \frac{7}{2}x - \frac{1}{2}.$$

Determine all real numbers r such that $f(f(r)) = r$.

Walkthrough —

- (a) Show that f is an increasing function.

Solution 20. ■

Here is a problem that can be solved using Gauss's lemma.

Exercise 5.5 (ELMO 2009, AoPS, proposed by Evan O'Dorney). Let a, b, c be positive integers such that $a^2 - bc$ is a square. Prove that $2a + b + c$ is not prime.

Walkthrough —

- (a) Consider the quadratic polynomial $p(x) = bx^2 + 2ax + c$.
- (b) Show that its discriminant is a perfect square.
- (c) Use Gauss's lemma to show that $p(x)$ can be factored into linear polynomials with integer coefficients.
- (d) Note that the roots of $p(x)$ are negative rationals.
- (e) Conclude that $p(x)$ can be factored into linear polynomials with positive integer coefficients.
- (f) Conclude that $p(1) = 2a + b + c$ is not a prime

Solution 21. Consider the quadratic polynomial $p(x) = bx^2 + 2ax + c$ with integer coefficients. Since its discriminant is a perfect square, it follows that its roots are rational, that is, it can be factored over the rationals. By Gauss's lemma, $p(x)$ can be factored into linear polynomials with integer coefficients. Since the leading coefficient of $p(x)$ is positive, it follows that it can be factored into linear polynomials with integer coefficients and having positive leading coefficients. Note that the roots of $p(x)$ are negative rationals. This proves that $p(x)$ can be factored into linear polynomials with positive integer coefficients. Noting that $p(1) = 2a + b + c$, it follows that $2a + b + c$ is not a prime. ■

Remark. Note that in the above, one may prove that $p(x)$ can be factored into linear polynomials with integer coefficients without using Gauss's lemma, possibly by establishing the lemma in this specific case. In fact, the above problem could serve as an introduction to Gauss's lemma.

§6 Crossing the x -axis/Intermediate value theorem

Example 6.1. Suppose $P(x)$ is a polynomial with real coefficients such that $P(x) = x$ has no real solution. Show that $P(P(x)) = x$ has no real solutions.

Example 6.2. Let $P(x)$ and $Q(x)$ be monic polynomials of degree 10 having real coefficients. Assume that the equation $P(x) = Q(x)$ has no real roots. Prove that the equation $P(x+1) = Q(x-1)$ has at least one real root.

Walkthrough —

- (a) Consider the difference $P(x) - Q(x)$ to show that the coefficient of x^9 in these polynomials are equal.
- (b) Prove that the polynomial $P(x+1) - Q(x-1)$ is of degree 9.

Solution 22. Note that $P(x) - Q(x)$ is a polynomial of degree at most 9 having real coefficients. Since $P(x) - Q(x)$ has no real root, it follows that it has degree at most 8. In other words, the coefficients of x^9 in $P(x), Q(x)$ are the same. Note that $P(x+1) - Q(x-1)$ is of degree ≤ 9 , and the coefficient of x^9 in $P(x+1) - Q(x-1)$ is equal to the coefficient of x^9 in $(x+1)^{10} - (x-1)^{10}$, which is equal to 20. This shows that $P(x+1) - Q(x-1)$ is a polynomial of degree 9 with real coefficients. Consequently, it has at least one real root. ■

Example 6.3. Let $P(x)$ be a nonconstant polynomial with real coefficients having a real root. Suppose it does not vanish at 0. Show that the monomial terms appearing in $P(x)$ can be erased one by one to obtain its constant term such that the intermediate polynomial have at least one real root.

Walkthrough —

- (a)

Solution 23. Write $P(x) = a_n x^n + \cdots + a_0$ with $a_n, \dots, a_0$ lying in $\mathbb{R}$, and $a_n a_0 \neq 0$. Since any polynomial of odd degree has a real root, it follows that if the degree of $P(x)$ is odd, then the nonconstant monomials, other than the leading term, can be erased one by one, and then, the leading term can be erased to obtain a_0 , and the intermediate polynomials have a real root. If a_n, a_0 are of opposite signs and n is even, then the same process can be followed, and note that any of the intermediate polynomials takes values of opposite signs at 0 and at a large enough integer, and hence has a real root.

Let us assume that n is even, and a_n, a_0 are of the same sign. Let α denote a real root of $P(x)$. Let $Q(x)$ denote the polynomial $P(x) - a_n x^n$. Note that $Q(0) = a_0$ and $Q(\alpha) = -a_n \alpha^n$. Since a_0 is nonzero, it follows that $\alpha \neq 0$, and hence, $Q(0), Q(\alpha)$ are of opposite signs. This shows that $Q(x)$ is a nonconstant polynomial with real coefficients having a real root, and it does not vanish at 0. Since the degree of $Q(x)$ is smaller than that of $P(x)$, by induction, we are done. ■

Exercise 6.4 (China TST 1995 Day 2 P2, AoPS). Alice and Bob play a game with a polynomial of degree at least 4:

$$x^{2n} + \square x^{2n-1} + \square x^{2n-2} + \cdots + \square x + 1.$$

They take turns to fill the empty boxes. If the resulting polynomial has no real root, Alice wins, otherwise, Bob wins. If Alice goes first, who has a winning strategy?

Walkthrough —

- (a) There are more odds than evens among the integers $1, 2, \dots, 2n - 1$.
- (b) Can Bob have a winning strategy using the odds in his favour?

Solution 24. Bob has a winning strategy, as described below.

Bob makes sure that at the end of each of his turns except the last one, the number of even powers of x whose coefficients have been provided by some of them is equal to the number of odd powers of x whose coefficients have been provided by some of them. This can be done, for instance, if during a turn of Bob, other than the last turn, Bob provides the coefficient of an odd (resp. even) power of x if Alice has provided the coefficient of an even (resp. odd) power of x in the preceeding turn.

Since $n \geq 2$, it follows that Bob gets at least one turn. At the beginning of the final turn of Bob, there are two powers of x whose coefficients are to be determined, denote them by x^i, x^j , their coefficients by c_i, c_j respectively. Let $Q(x)$ denote the polynomial, obtained by the erasing the terms corresponding to x^i, x^j from the polynomial that Bob had at the beginning of his final turn. Note that

$$P(x) = Q(x) + c_i x^i + c_j x^j.$$

Note that at least of i, j is odd. Interchanging i, j if necessary, let us assume that i is odd. We describe the strategy that Bob follows in the two cases below.

Let us consider the case that j is even. Bob determines c_j in such a way that for any choice of c_i , the completed polynomial $P(x)$ is guaranteed to have at least one real root. This can be done, for instance, by taking c_j satisfying

$$Q(1) + Q(-1) + 2c_j = 0.$$

For any choice of c_i , the above choice of c_j shows that $P(1) + P(-1) = 0$, which implies that $P(x)$ has a root in the interval $[-1, 1]$.

Let us consider the case that j is odd. Bob determines c_j in such a way that for any choice of c_i by Alice in the next turn, the completed polynomial $P(x)$ is guaranteed to have at least one real root. This can be done, for instance, by taking c_j satisfying

$$Q(2) + c_j 2^j + 2^i Q(-1) - c_j 2^i = 0.$$

Since $i \neq j$, the above holds for some $c_j \in \mathbb{R}$. For any choice of c_i , note that

$$P(2) + 2^i P(-1) = 0$$

holds, which implies that $P(x)$ has a root in $[-1, 2]$. ■

§7 Roots of unity

Exercise 7.1 (USAMO 1976 P5, AoPS). If $P(x)$, $Q(x)$, $R(x)$, and $S(x)$ are all polynomials such that

$$P(x^5) + xQ(x^5) + x^2R(x^5) = (x^4 + x^3 + x^2 + x + 1)S(x),$$

prove that $x - 1$ is a factor of $P(x)$.

Summary — The primitive 5-th roots of unity can be used to show that $P(1) = 0$.

Walkthrough —

- (a) Substituting primitive 5-th roots of unity (that is, the 5-th roots of unity other than 1) for x , yields several linear equations in $P(1), Q(1), R(1)$.
- (b) Can $Q(1)$ and $R(1)$ be eliminated to obtain that $P(1) = 0$?

Solution 25. Denote the 5-th root of unity $\cos \frac{2\pi}{5} + i \sin \frac{2\pi}{5}$ by ζ . Substituting $x = \zeta, \zeta^2, \zeta^3$, we obtain

$$\begin{aligned} P(1) + \zeta Q(1) + \zeta^2 R(1) &= 0, \\ P(1) + \zeta^2 Q(1) + \zeta^4 R(1) &= 0, \\ P(1) + \zeta^3 Q(1) + \zeta^6 R(1) &= 0. \end{aligned}$$

Eliminating $R(1)$ from the first two equations yields

$$(1 - \zeta^2)P(1) + \zeta^2(1 - \zeta)Q(1) = 0,$$

and eliminating $R(1)$ from the last two equations yields

$$(1 - \zeta^2)P(1) + \zeta^3(1 - \zeta)Q(1) = 0.$$

Eliminating $Q(1)$ from the above two equations, we obtain $(1 - \zeta)P(1) = 0$, which gives $P(1) = 0$. This shows that $x - 1$ is a factor of $P(x)$. ■

Exercise 7.2 (Leningrad Math Olympiad 1991). A finite sequence $a_1, a_2, \dots, a_n$ is called p -balanced if any sum of the form

$$a_k + a_{k+p} + a_{k+2p} + \dots$$

is the same for any $k = 1, 2, 3, \dots, p$. For instance the sequence

$$a_1 = 1, a_2 = 2, a_3 = 3, a_4 = 4, a_5 = 3, a_6 = 2$$

is a 3-balanced. Prove that if a sequence with 50 members is p -balanced for $p = 3, 5, 7, 11, 13, 17$, then all its members are equal zero.

Summary — Consider the polynomial $\sum_{i=1}^{50} a_i x^i$.

Walkthrough —

- (a) Show that the polynomial vanishes at any p -th root of unity, other than 1, for $p \in \{3, 5, 7, 11, 13, 17\}$.
- (b) How many such roots of unity are there in total?

Solution 26. Let $a_1, a_2, \dots, a_{50}$ be a sequence of complex numbers. Assume that it is p -balanced for $p \in \{3, 5, 7, 11, 13, 17\}$. For an integer $n \geq 1$, denote the root of unity $\cos \frac{2\pi}{n} + i \sin \frac{2\pi}{n}$ by ζ_n . Let $P(x)$ denote the polynomial $\sum_{i=1}^n a_i x^i$.

Let $3 \leq p \leq 17$ be a prime. Since $a_1, a_2, \dots, a_{50}$ is p -balanced, for any $1 \leq \ell < p$, we obtain

$$\begin{aligned} P(\zeta_p^\ell) &= \sum_{k=1}^p (a_k + a_{k+p} + \dots) \zeta_p^{k\ell} \\ &= (a_1 + a_{1+p} + \dots) \sum_{k=1}^p \zeta_p^{k\ell} \\ &= 0, \end{aligned}$$

where the final equality follows since $\zeta_p^\ell \neq 1$. This shows that the polynomial $P(x)$ vanishes at the elements of the set

$$\cup_{p \in \{3, 5, 7, 11, 13, 17\}} \{\zeta_p^\ell \mid 1 \leq \ell < p\},$$

which contains

$$\sum_{p \in \{3, 5, 7, 11, 13, 17\}} (p-1) = 2 + 4 + 6 + 10 + 12 + 16 = 50$$

elements. Moreover, $P(x)$ also vanishes at 0. Note that $P(x)$ is a polynomial of degree 50, and it has at least 51 zeroes. This gives that $P(x) = 0$, and hence, the terms of the sequence $a_1, a_2, \dots, a_{50}$ are all equal to zero. ■

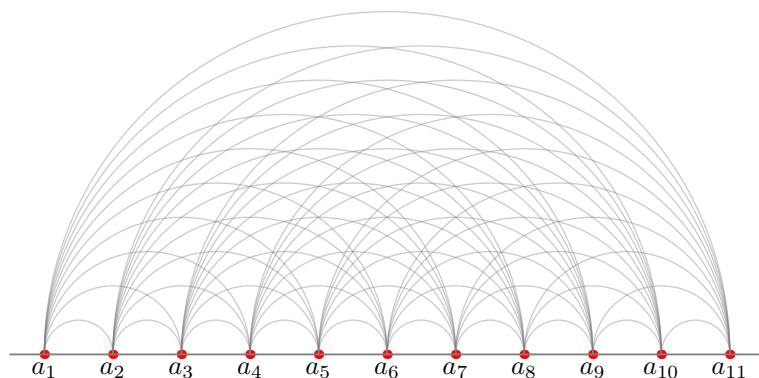


Figure 15: USAMO 2018 P4, Exercise 8.1

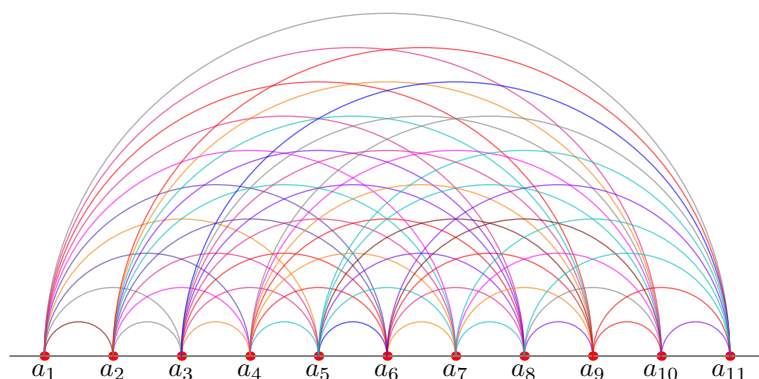


Figure 16: USAMO 2018 P4, Exercise 8.1

§8 Congruences

Exercise 8.1 (USAMO 2018 P4, AoPS, proposed by Ankan Bhattacharya).

Let p be a prime, and let $a_1, a_2, \dots, a_p$ be integers. Show that there exists an integer k such that the numbers

$$a_1 + k, a_2 + 2k, \dots, a_p + pk$$

produce at least $p/2$ distinct remainders upon division by p .

The following uses the fact that every integer not divisible by a prime p is invertible modulo p , which can be proved from first principles!

Walkthrough —

- (a) Note that it suffices to show that some integer k among $1, 2, \dots, p$ has the required property.

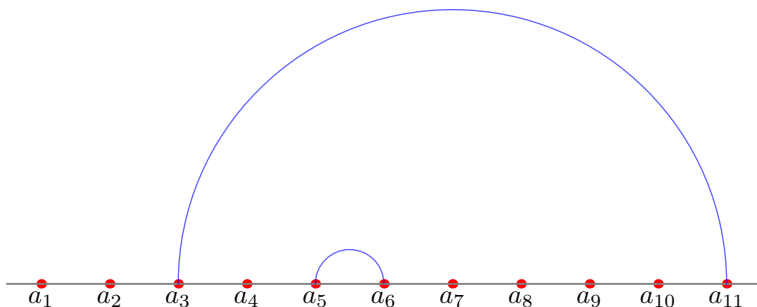


Figure 17: USAMO 2018 P4, Exercise 8.1

- (b) Consider the integers $a_1, a_2, \dots, a_p$, and we join each of them using an arc as in Fig. 15.
- (c) For any two distinct integers i, j among $1, 2, \dots, p$, show that the i -th and the j -th ones among the numbers

$$a_1 + k, a_2 + 2k, \dots, a_p + pk,$$

that is, the numbers $a_i + ik, a_j + jk$ leave the same remainder upon division by p precisely for one value of k .

- (d) Let us color the arcs (see Fig. 15). We join a_i, a_j by an arc if the numbers $a_i + ik, a_j + jk$ leave the same remainder upon division by p . We write k on that arc. See Fig. 16, where instead of writing the corresponding integers on the arcs, we have colored them. Thinking of the integers $1, 2, \dots, p$ as p colors, and we have *colored* the arcs instead of *labelling* the arcs^a.
- (e) Note that there are precisely $\frac{p(p-1)}{2}$ unordered pairs of the form $\{a_i, a_j\}$, that is, there are precisely $\frac{p(p-1)}{2}$ arcs (see Fig. 15). Moreover, on each of these arcs, one of the integers $1, 2, \dots, p$ is written. In Fig. 16, these arcs are colored using at most p colors.
- (f) Conclude that for some integer k among $1, 2, \dots, p$, at most $(p-1)/2$ arcs have the integer k written on them, that is, there are at most $(p-1)/2$ unordered pairs of the form $\{a_i, a_j\}$ such that $a_i + ik, a_j + jk$ produce the same remainder upon division by p . In Fig. 16, for some color, there are at most $(p-1)/2$ arcs of that color.
- (g) Show that^b for this integer k , the numbers

$$a_1 + k, a_2 + 2k, \dots, a_p + pk$$

produce at least $p/2$ distinct remainders upon division by p .

^aObserve that all the p colors might not have been used, for instance, if any two of $a_1, \dots, a_p$ differ by a multiple of p .

^bA graph on n vertices with m edges has at least $n - m$ connected components. This can be proved by induction on m , and observing that introducing a new edge reduces the number of connected components at most by 1.

Exercise 8.2 (Tournament of Towns Fall 2019, Junior, O Level P4, by Boris Frenkin). There are given 1000 integers $a_1, \dots, a_{1000}$. Their squares $a_1^2, \dots, a_{1000}^2$ are written along the circumference of a circle. It so happened that the sum of any 41 consecutive numbers on this circle is a multiple of 41^2 . Is it necessarily true that every integer $a_1, \dots, a_{1000}$ is a multiple of 41?

Remark. Replace 1000 by 10 and 41 by 7, and try to work on the problem.

Solution 27. For any integer m , let $\overline{m}$ denote the integer lying between 1 and 1000, which is congruent to m modulo 1000. Note that

$$a_i^2 \equiv a_j^2 \pmod{41^2}$$

holds for any integers i, j lying between 1 and 1000, and satisfying $i \equiv j \pmod{41}$. It follows that

$$a_1^2 \equiv a_{41k+1}^2 \pmod{41^2}$$

for any integer k . Since the integers 41, 1000 are relatively prime, it follows that the integers

$$41, 41 \cdot 2, 41 \cdot 3, \dots, 41 \cdot 1000$$

are pairwise distinct modulo 1000, that is, these integers are congruent to $1, 2, \dots, 1000$ modulo 1000 in some order. This shows that a_1^2 is congruent to a_i^2 modulo 41^2 for any integer $1 \leq i \leq 1000$. It follows that

$$41a_1^2 \equiv a_1^2 + a_2^2 + \dots + a_{41}^2 \pmod{41^2}$$

Since the sum $a_1^2 + a_2^2 + \dots + a_{41}^2$ is divisible by 41^2 , this shows that 41 divides a_1 . For any integer $1 \leq i \leq 1000$, 41^2 divides $a_1^2 - a_i^2$, and using that 41 divides a_1 , we obtain 41 divides a_i .

This proves that it is necessary that every integer $a_1, \dots, a_{1000}$ is a multiple of 41. ■

Example 8.3 (India RMO 2017a P2). Show that the sum of the cubes of any seven consecutive integers cannot be expressed as the sum of the fourth powers of two consecutive integers.

Walkthrough — Read it modulo ____!

Solution 28. Note that the fourth powers of the integers 0, 1, 2, 3, 4, 5, 6 are congruent to 0, 1, 2, 4, 4, 2, 1 modulo 7 respectively. This shows that the sum of the fourth powers of two consecutive integers is congruent to one of

$$0 + 1, 1 + 2, 2 + 4, 4 + 2, 2 + 1, 1 + 0$$

modulo 7. Hence, the sum of the fourth powers of two consecutive integers is not divisible by 7. Also note the cubes of seven consecutive integers is congruent to

$$0^3 + 1^3 + 2^3 + 3^3 + 4^3 + 5^3 + 6^3$$

modulo 7, which is congruent to

$$1^3 + 2^3 + 3^3 + (-3)^3 + (-2)^3 + (-1)^3 = 0$$

modulo 7. This shows that the sum of the cubes of seven consecutive integers is not equal to the sum of the fourth powers of two consecutive integers. This completes the proof. ■

Exercise 8.4 (USAJMO 2013 P1, proposed by Titu Andreescu). Are there integers a, b such that $a^5b + 3$ and $ab^5 + 3$ are both perfect cubes of integers?

Summary — Consider the integer ab modulo 3, and read $a^5b + 3, ab^5 + 3$ modulo 9.

Walkthrough —

- (a) If 3 divides ab , then consider one of the integers $a^5b + 3, ab^5 + 3$ modulo 9.
- (b) If 3 does not divide ab , then assuming the integers $a^5b + 3, ab^5 + 3$ to be perfect cubes, determine the integers a^5b, ab^5 modulo 9.

Solution 29. Let us assume that there are integers a, b satisfying the given condition. First, let us consider that 3 divides ab . Without loss of generality², let us assume that 3 divides a . Then

$$a^5b + 3 \equiv 3 \pmod{9}.$$

Since $a^5b + 3$ is a perfect cube and is divisible by 3, it follows that

$$a^5b + 3 \equiv 0 \pmod{9},$$

implying $3 \equiv 0 \pmod{9}$, which is impossible.

Next, let us consider the case that 3 does not divide ab . Since $a^5b + 3$ is a cube and is not divisible by 3, we obtain $a^5b + 3 \equiv \pm 1 \pmod{9}$, which implies

²Show that there is indeed no loss of generality in assuming what follows.

that a^5b is congruent to one of 5, 7 modulo 9. Using a similar argument, it follows that ab^5 is also congruent to one of 5, 7 modulo 9. Hence, $(ab)^6$ is congruent to one of $5 \cdot 5, 5 \cdot 7, 7 \cdot 7$ modulo 9. So, $(ab)^6$ is not congruent to 1 modulo 9. Since 3 does not divide ab , it follows that $(ab)^6$ is congruent to 1 modulo 9.

It follows that there are no integers a, b satisfying the given conditions. ■

Exercise 8.5 (China TST 1995 Day 1 P1, AoPS). Find the smallest prime number p that cannot be represented in the form $|3^a - 2^b|$, where a and b are non-negative integers.

Walkthrough —

- (a) Any prime smaller than 41 can be expressed as the absolute value of the difference of a nonnegative power of 3 and a nonnegative power of 2.
- (b) If $41 = 2^b - 3^a$, then $b \geq 3$ and hence $3^a \equiv -1 \pmod{8}$, which is impossible.
- (c) Assume that $41 = 3^a - 2^b$. Considering congruence modulo 3, show that b is an even positive integer. Reduce modulo 4 to show that a is even.
- (d) Write $a = 2x, b = 2y$, and factorize 41.
- (e) Conclude by obtaining a contradiction.

Solution 30. Note that any prime smaller than 41 can be expressed as the absolute value of the difference of a nonnegative power of 3 and a nonnegative power of 2, as shown below.

$$\begin{aligned}
 2 &= 3 - 1, \\
 3 &= 4 - 1, \\
 5 &= 9 - 4, \\
 7 &= 8 - 1, \\
 11 &= 27 - 16, \\
 13 &= 16 - 3, \\
 17 &= 81 - 64, \\
 19 &= 27 - 8, \\
 23 &= 32 - 9, \\
 29 &= 32 - 3, \\
 31 &= 32 - 1, \\
 37 &= 64 - 27.
 \end{aligned}$$

Let us prove the following claim.

Claim — The prime number 41 cannot be expressed as the absolute value of the difference of a nonnegative power of 3 and a nonnegative power of 2.

Proof of the Claim. On the contrary, let us assume that

$$41 = |3^a - 2^b|$$

holds for some nonnegative integers a, b .

First, let us consider the case that $41 = 2^b - 3^a$. Note that $b \geq 3$ holds, and reducing the above modulo 8, it follows that $3^a \equiv -1 \pmod{8}$, which is impossible.

Now, let us consider the case that $41 = 3^a - 2^b$. Reducing modulo 3, it follows that $2^b \equiv 1 \pmod{3}$, which shows that b is even. Note that b is nonzero. Next, reducing modulo 4, we obtain $3^a \equiv 1 \pmod{4}$, which implies that a is even. Writing $a = 2x, b = 2y$ for some positive integers x, y , we obtain

$$41 = 3^{2x} - 2^{2y} = (3^x - 2^y)(3^x + 2^y)$$

with $1 \leq 3^x - 2^y < 3^x + 2^y$, which yields

$$3^x - 2^y = 1, 3^x + 2^y = 41,$$

which is impossible.

Considering the above cases, the claim follows. $\square$

This proves that 41 is smallest prime that cannot be expressed in the given form. $\blacksquare$

Exercise 8.6 (SMMC 2017 B2, AoPS). Determine all pairs (p, q) of positive integers such that p and q are primes, and $p^{q-1} + q^{p-1}$ is the square of an integer.

Walkthrough —

- (a) Check that $(p, q) = (2, 2)$ works.
- (b) If p, q are odd, show that $p^{q-1} + q^{p-1} \equiv 2 \pmod{4}$, so it cannot be a perfect square.
- (c) Without loss of generality, let p be an odd prime, and $q = 2$. Then $p^{q-1} + q^{p-1} = 2^{p-1} + p$.
- (d) Write $2^{p-1} + p = m^2$.
- (e) Factorize to obtain $(m - 2^{\frac{p-1}{2}})(m + 2^{\frac{p-1}{2}}) = p$, which gives

$$m + 2^{\frac{p-1}{2}} = p.$$

- (f) Note that $p < 2^{\frac{p-1}{2}}$ holds^a for $p \geq 7$.

(g) Conclude that p can only be 3 or 5.

^aTry to show that $2^{\frac{n-1}{2}} > n$ holds for all integers $n \geq 7$.

Solution 31. First, note that $(p, q) = (2, 2)$ works since $2^{2-1} + 2^{2-1} = 4 = 2^2$.

If p and q are odd primes, then both $p - 1$ and $q - 1$ are even, and hence,

$$p^{q-1} + q^{p-1} \equiv 1 + 1 \equiv 2 \pmod{4}$$

holds. Since no perfect square is congruent to 2 modulo 4, it follows that not both of p and q are odd.

Without loss of generality³, let p be an odd prime, and $q = 2$. Then

$$p^{q-1} + q^{p-1} = p^{2-1} + 2^{p-1} = p + 2^{p-1}.$$

Write

$$p + 2^{p-1} = m^2$$

for some positive integer m . Rearranging gives

$$m^2 - 2^{p-1} = p,$$

which yields the factorization

$$(m - 2^{\frac{p-1}{2}})(m + 2^{\frac{p-1}{2}}) = p.$$

Since p is prime and

$$m - 2^{\frac{p-1}{2}} < m + 2^{\frac{p-1}{2}},$$

we obtain that

$$m + 2^{\frac{p-1}{2}} = p,$$

Using the following claim, we conclude that p can only be 3 or 5. If $p = 3$, then $p^{q-1} + q^{p-1} = 3^{2-1} + 2^{3-1} = 3 + 4 = 7$. If $p = 5$, then $p^{q-1} + q^{p-1} = 5^{2-1} + 2^{5-1} = 5 + 16 = 21$. Thus, the only solution is $(p, q) = (2, 2)$.

Claim — For any positive integer $n \geq 7$, the inequality

$$2^{\frac{n-1}{2}} > n$$

holds.

Proof. We prove this by induction. For $n = 7$, we have $2^{\frac{7-1}{2}} = 2^3 = 8 > 7$. Now, assume that the inequality holds for some $k \geq 7$. Note that

$$2^{\frac{(k+1)-1}{2}} = 2^{\frac{k-1}{2} + \frac{1}{2}} = \sqrt{2} \cdot 2^{\frac{k-1}{2}} > \sqrt{2} \cdot k$$

³Why there is no loss of generality?

holds. Observe that

$$\begin{aligned}
 (\sqrt{2}k)^2 - (k+1)^2 &= 2k^2 - (k^2 + 2k + 1) \\
 &= k^2 - 2k - 1 \\
 &= (k-1)(k-3) - 2 \\
 &\geq (7-1)(7-3) - 2 \\
 &> 0.
 \end{aligned}$$

This shows that

$$2^{\frac{(k+1)-1}{2}} > \sqrt{2} \cdot k > k+1.$$

Thus, by induction, the claim holds for all integers $n \geq 7$. □



References

- [AN10] CLAUDI ALSINA and ROGER B. NELSEN. *Charming proofs*. Vol. 42. The Dolciani Mathematical Expositions. A journey into elegant mathematics. Mathematical Association of America, Washington, DC, 2010, pp. xxiv+295. ISBN: 978-0-88385-348-1 (cited p. 5)
- [Che25] EVAN CHEN. *The OTIS Excerpts*. Available at <https://web.evanchen.cc/excerpts.html>. 2025, pp. vi+289