National Math Camp 2021 Journal

Md. Shadman Shahriyar Shuvo
shadmanshahriyarshuvo@gmail.com

April 22, 2021 – May 09, 2021

Last Updated on May 17, 2021

Contents

List of Figures

1 April 23, 2021

§1.1 Triangle Center by Saad Bin Quddus

Today's topic is about basic triangle centers like circumcenter, centroid, incenter, excenter, orhtocenter, etc... (This is mostly Angle Chasing in a TRIANGLE)

§1.1.1 Circumcenter

I think, you are familiar with the circumcenter. It is the center of the circle which goes through the points A, B, C of $\triangle ABC$. It is determined by drawing the perpendicular bisectors of the line segments. The proof of concurrency is very easy. Just remember that any point on the

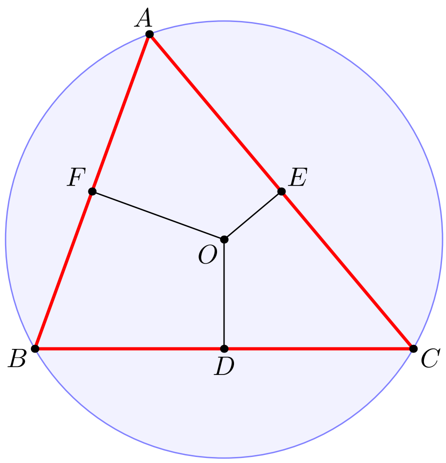


Figure 1.1: Circumcenter of $\triangle ABC$

perpendicular bisector is equidistant from two of the corresponding vertex.

§1.1.2 Centroid

Centroid is the intersection of the medians of a triangle. It is defined by G. It is also called Center of Mass or Center of Gravity.

Here we are going to see a combinatorial proof!

Let, three centroid don't concur, then they intersect in three pints let G_1, G_2, G_3. Let the midpoints of the sides are L, M, N. Then draw the medians of the triangle LMN then, their medians intersect at G_1, G_2, G_3 as $MN \parallel BC$. So we are going to infinite descent, and

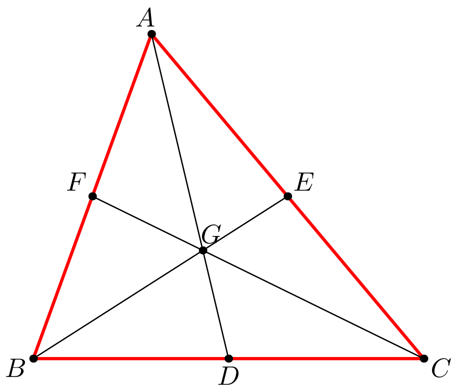
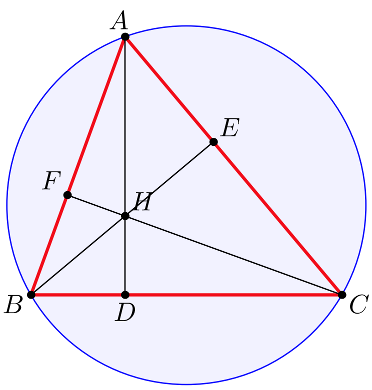


Figure 1.2: Cnetroid of $\triangle ABC$

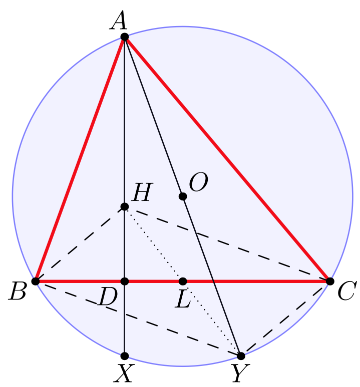
consider the median triangle of LMN. Consequently, the areas of the median triangles are going to 0. But the area of triangle $G_1G_2G_3$ remains same. which means triangle $G_1G_2G_3$ is bigger that the original triangle which is a contradiction. So centroid exists.

§1.1.3 Orthocenter

Let D, E, F be the foot of the perpendicular from A, B, C to the opposite side of the triangle. Then $BFEC$ is a cyclic quadrilateral(You can see this by $\angle FEA = B$ or by $\angle BFC = \angle BEC = 90°$). Also there are another two cyclic quadrilaterals. Find them.



Orthocenter of $\triangle ABC$



Reflection of Orthocenter lies on Circumcirlce

There are six cyclic quadrilaterals and the orthocenter is the incenter of the orthic trinagle.

Then Mentor taught us the reflection of the orthocenter across the sides and about the midpoint of the sides lie on the circumcircle of the triangle ABC. Let the reflection of H across the side BC is X then we are going to show that X lies on (ABC).

Note that $\triangle BDH \cong \triangle BDX$ by some angle chasing.

So, $\angle BXH = \angle BHD = \angle ACB$ and therefore $ABXC$ is a cyclic quadrilateral.

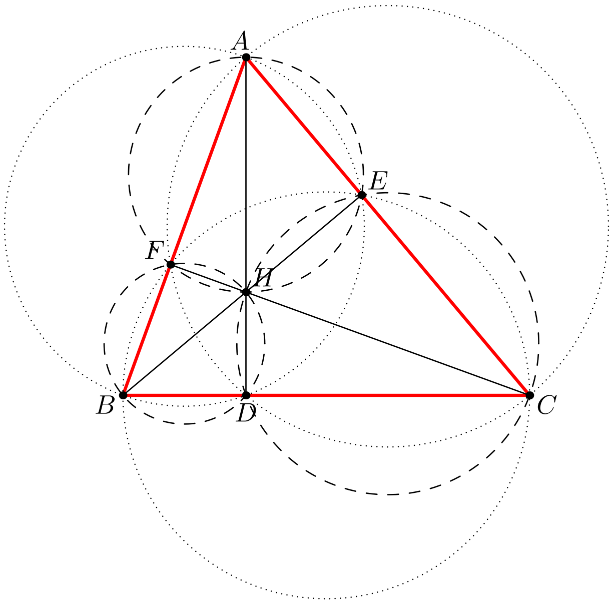


Figure 1.3: Orthocenter and 6 cyclic quadrilaterals

Let the reflection of H acroos the midpoint of BC is Y. Then,

$$\angle BAH = \angle CAO = 90^\circ - B.$$

and AY is a diameter.

$BH = CY$ hence, $BH \parallel CY$ thererfore, $BHCY$ is a parallelogram, and H, L, Y are collinear. hence Y lies on (ABC).

§1.1.4 Nine Point Circle

Our current topic is the famous Nine-Point Circle whih goes through exactly nine points.

These pints are three midpoints, three feet of the perpendicular and the three midpoints of AH, BH, CH.

Now we are going to show the first six points are concyclic. D is the reflection of A across MN so $\angle MDN = A$ we also know that $\angle MLN = A$ so L, M, N, D are concyclic . Similarly we can show that L, M, N, E and L, M, N, F are concyclic, so all six points are concyclic. Other proof $\angle BDN = \angle NML$ so L, M, N, D are concyclic points.

Now we are gonna prove that K the midpoint of AH lies on $(DEFLMN)$. $\angle NLB = C$ so we have to show that $\angle NKH = C$. but

$$\angle NKH = \angle BHD = C$$

so we are done.

Also N_9 the center of the Nine-Point Circle is the midpoint of OH where O and H are circumcenter and Orthocenter respectively.

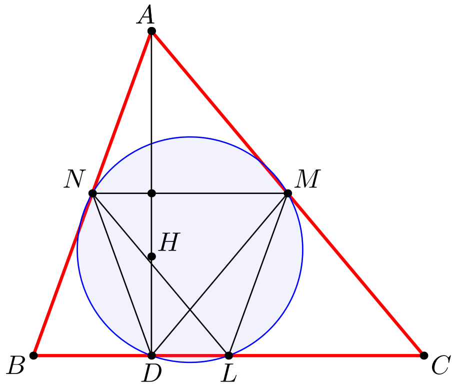


Figure 1.4: D, L, M, N lie on a circle

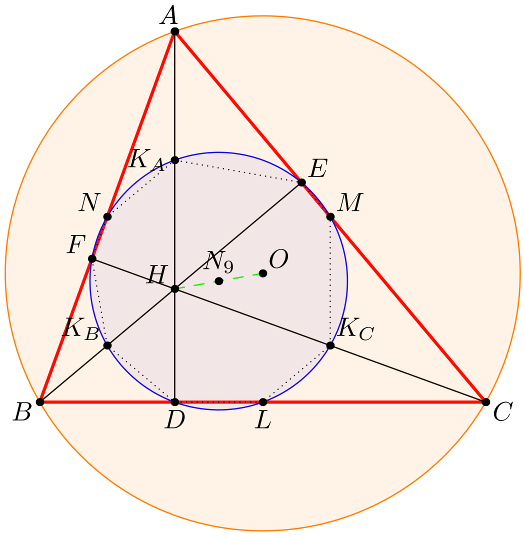


Figure 1.5: Nine Point Circle of $\triangle ABC$

§1.2 Basic Divisibility by Zim-mim Siddiqee Sowdha

§1.2.1 Basic Divisibility

For all integers a, $1|a$.

Divisibility Properties

- $a|b$ then there exista inetger k s.t $b = ak$.
- $a|b, a|c \implies a|b \pm c$
- $a|b \implies a|bc$
- $a|b, b|a \implies a = b$
- $m|(a-b), m|(c-d) \implies m|(ac-bd)$. by $m|(a-b)c-(c-d)b = ac-bd$

§1.2.2 Division Algorithm

This is one of the most famous topic. It tells that if $a, b \in \mathbb{Z}$ then there exists unique q, r s.t

$$a = bq + r; \quad 0 \le r < |b|$$

§1.2.3 Fundamental Theorem of Arithmetic (FTA)

Every integer has an unique prime power factorization which is called the Fundamental Theorem of Arithmetic.

$$N = {p_1}^{a_1}{p_2}^{a_2}{p_3}^{a_3}\cdots{p_m}^{a_m}.$$

Let assume that, the factorization is not unique. Then we have,

$$N = {p_1}^{a_1}{p_2}^{a_2}{p_3}^{a_3}\cdots{p_m}^{a_m} = {q_1}^{b_1}{q_2}^{b_2}{q_3}^{b_3}\cdots{q_n}^{b_n}.$$

Now we have,

$$p_1|q_1q_2q_3\cdots q_n$$

$$\implies p_1|q_i$$

By Euclid's Lemma

$$p_i = q_i$$

If $m \ne n$ then $1 = q_xq_yq_z$ for some x, y, z which is a contradiction.

§1.2.4 Modular Arithmetic

Modular Arithmetic means working with remainders where remainders aren't fixed.

1. **Congruence:** $m|a-b \implies a \equiv b \pmod{m}$.
2. a is divided by m and remanider is b then $a \equiv b \pmod{m}$.
3. $a = bq + r \implies a \equiv r \pmod{b}$.

Some Properties of Modular Arithmetic

1. $a \equiv b \pmod{m} \implies a + mx \equiv b + my \pmod{m}$.
2. $a \equiv b \pmod{m}; c \equiv d \pmod{m} \implies a \pm c \equiv b \pm d \pmod{m}$. Also $ka \equiv kb \pmod{m}$.
3. $a \equiv b \pmod{m}; c \equiv d \pmod{m} \implies ac \equiv bd \pmod{m}$. Which means $a^k \equiv b^k \pmod{m}$ which is very useful.

4. $ak \equiv bk \pmod{m}$and$(m,k) = 1 \implies a \equiv b \pmod{m}$.

Problem 1.2.1. $7^{259} \equiv m \pmod{5}$. Find m.

Solution.

$$7^2 \equiv 2^2 \equiv 4 \equiv -1 \pmod{5}$$

$$(7^2)^{129} \equiv (-1)^{129} \equiv -1 \pmod{5}$$

$$7^{259} \equiv -7 \equiv -7 + 10 \equiv 3 \pmod{5}$$

. □

§1.2.5 Residue Class/System Modulo m

n is an integer. n divided by 6 we can get 6 residue. They are $0, 1, 2, 3, 4, 5$. This set is called Residue system modulo 6. Let S be the set, then

$$S = \{0, 1, 2, 3, 4, 5\} \equiv \{0, 1, 8, 3, 4, -1\} \pmod{6}.$$

The set is defined by $RS_{(m)}$

And as an example,

$$RS_{(12)} = \{0, 1, 2, 3, \dots, 11\}$$

Note that here $1, 5, 7, 11$ are coprime to 12 and if we consider this set of $\{1, 5, 7, 11\}$ which is called as reduced Residue System modulo 12.

$$RRS_{(12)} = \{1, 5, 7, 11\}$$

$\varphi(m)$ is called the Euler's Totient Function and it is the number of elements in the set $RRS_{(m)}$. As an example $RRS_{(12)} = 4$.

For prime p we have $\varphi(p) = p - 1$.

Theorem 1.2.2 (Euler's Theorem)

For any integer a coprime to m, we have,

$$a^{\varphi(m)} \equiv 1 \pmod{m}$$

. Which also means that $a^{p-1} \equiv 1 \pmod{p}$.

Here is Fermat's Little Theorem. It comes from Euler's phi function.

Theorem 1.2.3 (Fermat's Little Theorem)

Let a be a positive integer and p be a prime then,

$$a^p \equiv a \pmod{p}.$$

✠2 April 24, 2021

§2.1 Induction by Muhaiminul Islam Ninad

Today's Topic is Basic Induction. Our mentor started with showing an inductive proof of sum of positive integers:

$$1 + 2 + 3 + \ldots + n = \frac{n(n+1)}{2}.$$

It is easy and left as an exercise.

§2.1.1 Induction/Weak Induction

Our next problem is:

Example 2.1.1

Let, $a_1 = \sqrt{2}, a_{i+1} = \sqrt{2 + a_i}$. Prove that,

$$a_n = 2\cos\frac{\pi}{2^{n+1}}.$$

Solution. Here we show that, base case is true as $a_1 = 2\cos\frac{\pi}{2^2} = 2\cos\frac{\pi}{4} = 2 \cdot \frac{1}{\sqrt{2}} = \sqrt{2}$.

Now assume that it is true for a_k and $a_k = 2\cos\frac{\pi}{2^{k+1}}$. Then we will show that $a_{k+1} = 2\cos\frac{\pi}{2^{k+2}}$.

□

Example 2.1.2

Show that for all positive integer n,

$$1 + \frac{1}{\sqrt{2}} + \frac{1}{\sqrt{3}} + \frac{1}{\sqrt{4}} + \ldots \frac{1}{\sqrt{n}} \leq 2\sqrt{n}.$$

Solution. Here, after showing the base case true, assume that it's true for integer k. Then for $k+1$, add $\frac{1}{\sqrt{k+1}}$ to both side.

After these, show that, $2\sqrt{k} + \frac{1}{k+1} \leq 2\sqrt{k+1}$ Done! □

Example 2.1.3

Prove that for all positive integer n,

$$\frac{1}{2} \cdot \frac{3}{4} \cdot \frac{5}{6} \cdot \dots \cdot \frac{2n-1}{2n} < \frac{1}{\sqrt{3n}}.$$

Solution. Here assume that it's tru for $k-1$ then show for k.

Then do some algebra which is left as exercise! □

§2.1.2 Strong Induction

In this tecknique, we will assume that the statement is true for all integers from base case to k (in general). Then we will show that its true for $k+1$, and often we use the assertion that the statement is true for all integers from base case to k.

Example 2.1.4

The Fiobonacci sequence is defined as $F_1 = 1, F_2 = 2$ and for $n \geq 1$, $F_{m+2} = F_{m+1} + F_m$. Show that every natural number n can be written as a sum of distinct fiobonacci numbers, with no 2 Fiobonacci numbers being consecutive (F_n and F_{n+1} are consecutive).

Solution. We proceed by strong induction. Let $P(n)$ be the statement that n can be written as a sum of distinct fiobonacci numbers with no 2 consecutive. It is easy to verify $P(1)$ and $P(2)$. We now proceed by strong induction, so assume $P(i)$ for all $1 \leq i \leq n$. Now consider the number $n+1$ and the highest F_m such that $F_m \leq n+1$. Then if $n+1 = F_m$ we are done. Otherwise, $n+1-F_m$ is a positive integer less than $n+1$, and so $P(n+1-F_m)$ is true by assumption. Therefore, we can write $n+1-F_m = F_{i_1} + F_{i_2} + \cdots + F_{i_k}$ for distinct Fiobonacci numbers, no 2 of which are consecutive. Now we have written $n+1$ as a sum of distinct fiobonacci numbers

$$n+1 = F_{i_1} + F_{i_2} + \ldots + F_{i_k} + F_m.$$

such that no 2 are consecutive execpt possibly the largest 2, if $F_{i_k} = F_{m-1}$. But the latter case would imply that $n \leq F_m + F_{m-1} = F_{m+1}$, contradicting the choice of m. This completes the induction. □

The above soln is from Jacob Tsimerman's *A closer look at Induction* note.

§2.1.3 Real Induction

Example 2.1.5

There are n lamps in a room, with certain lamps connected by wires. Initially all lamps are off. You can press the on/off button on any lamp A, but this also switches the state of all the lamps connected to lamp A from on to off and vice versa. Prove that by pressing enough buttons you can make all the lamps on. (Connections are such that if lamp A is connected to lamp B, then lamp B is also connected to lamp A.)

Solution. We use induction on n. The base case of $n = 1$ is trivial (just turn the lamp on). Now assume the case of $n - 1$ lamps. Now look at the set of n lamps and ignore some lamp A. Then by induction, we can turn the remaining lamps on by pressing the buttons on some subset of them. Now if at the end of doing this A is also on, we are done. So we can assume that at the end of doing this A is off. Since A was an arbitrary lamp, we can assume that by pressing a sequence of buttons we can flip the states of all lamps except one of our choosing. Now, taking A and B to be 2 different lamps and flipping the states first of all lamps different from A and then all lamps different from B, we see that we can flip the states of only A and B. So this means we can flip the states of any number of even lamps. Now we have 2 cases:

- n is even: Then we are already done, since we can flip the states of any number of even lamps.
- n is odd: In this case, there must be some lamp A connected to an even number of lamps (prove this!) so first press the button on lamp A. Now, including A, an odd number of lamps are on, so an even number of lamps that are off remain. Flip their states to finish the proof!

$\square$

The above solution is from Jacob Tsimerman's *A closer look at Induction* note.

Our class ended!

§2.2 Invariants and Monovariants by Raiyan Jamil

This topic covers the trick of Invariant and Monovariants which are very powerful weapons to tackle hard combinatorial problems.

Invariant means which doesn't change after some steps or operations.

Monovariants means the value changes only in one direction, either it increases or decreases.

§2.2.1 Invariants

Example 2.2.1

You have an equilateral triangle. In each "step", you can:

- Draw a line on the current shape and cut it into two pieces along the line.
- Then flip one of the pieces and join the two pieces again along the line.

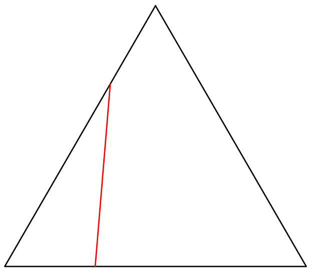


Figure 2.1: An Equilateral Triangle

Solution. After some move you may realize that, the perimeter and the area of the shape remains same as initial position.

SO if we want to make it a square then let the sise length of the square is x, and the length of the side of the equilateral triangle is a, so w havefollowing two equation:

$$\frac{\sqrt{3}}{4}a^2 = x^2$$

$$3a = 4x$$

. which have no common solution. So it is not possible to make it a square.

□

Example 2.2.2

In an empty room, in every minute either 4 people enter or 3 people leave. Can there be $7^{125} + 5$ people in the room after 7^{666} minutes?

Solution. The trick in htis problem is to work with mod 7, per 7 minutes.

Let ititially there are x people in the room. So in 7 minutes there let 4 people inter a times and $7-a$ people leave the room. So after seven minutes there are $x+4a-3(7-a) = x+7(a-3)$ people. This leads us to work with modulo seven.

As initially there are zero people in the room so $x \equiv 0 \pmod 7$ but $7^{125}+5 \not\equiv 0 \pmod 7$ so the answer is no. □

Example 2.2.3

An 8×8 chessboard has two opposite corners removed. Is it possible to tile the remaining 62 squares with 31 dominoes?

Solution. The answer is NO. Color the board with black-white. And there are 31 black and 30 white squares but the number of black and white squares should be the same for tiling. □

Example 2.2.4

In a cube there are seven vertices amrked 0 and one marked 1. It is permitted to add 1 to any two neighbouring vertices (that is two vertices connected by edge). Is it possible that all the numbers are divisible by 3 after a finite number of steps?

Solution. Here, the answer is also NO.

Alternately color the vertices with black and white. Then after each move we add 1 to white and 1 to black. Let S_b and S_w denote the sum of the numbers in Black and White vertices respectively. Then $S_b - S_w = 1$ remains constant as initially there was the sum 1. Which means it is not possible that all the numbers are divisible by three. □

Example 2.2.5

The numbers $1, 2, 3, \ldots, n$ are written in a row. It is permitted to swap any two numbers. If 2007 such operations are performed, is it possible that the final arrangement of numbers coincides with the original.

Solution. The answe is NO.

Here we define *inversion* which is the number of such pair of consecutive elements in the row such that for x, y the sequence:

$$1, 2, 3, \ldots, y, x, \ldots, n$$

y is left to x and $y > x$.

Now you can observe that after each move inversion can increase or decrease by 1.

Initially there was inversion=0, but after 2007 move the inversion will be odd. So it is not possible. □

Example 2.2.6

A natural number is written in each square of an $m \times n$ chessboard. The allowed move is to add an integer k to each of two adjacent numbers in such a way that nonnegative numbers are obtained (two squares are adjacent if they share a common side). Find a necessary and sufficient condition for it to be possible for all the numbers to be zero after finitely many operations.

Solution. Note that in each move, we are adding the same number to 2 squares, one of which is white and one of which is black (if the chessboard is colored alternately black and white). If S_b and S_w denote the sum of numbers on black and white squares respectively, then $S_b - S_w$ is an invariant. Thus if all numbers are 0 at the end, $S_b - S_w = 0$ at the end and hence $S_b - S_w = 0$ in the beginning as well. This condition is thus necessary; now we prove that it is sufficient.

Suppose a, b, c are numbers in cells A, B, C respectively, where A, B, C are cells such that A and C are both adjacent to B. If $a \leq b$, we can add $(-a)$ to both a and b, making a 0. If $a \geq b$, then add $(a - b)$ to b and c. Then b becomes a, and now we can add $(-a)$ to both of them, making them 0. Thus we have an algorithm for reducing a positive integer to 0. Apply this in each row, making all but the last 2 entries 0. Now all columns have only zeroes except the last two. Now apply the algorithm starting from the top of these columns, until only two adjacent nonzero numbers remain. These last two numbers must be equal since $S_b = S_w$. Thus we can reduce them to 0 as well. □

§2.2.2 Monovariants

Example 2.2.7

Several positive integer numbers are written on a blackboard. One can erase any two distinct integers and write their greatest common divisor and least common multiple instead.

(a) Prove that eventually the numbers will stop changing.

(b) Prove that the values of the numbers, once they stop changing, do not depend on what moves were made.

Solution. For (a) observe that gcd and lcm increasing or decreasing (why?). By playing with numbers you will find a mnovariant. The rest is left as an execise. □

Example 2.2.8 (Stanford Putnam Training 2007)

On an $n \times n$ board, there are n^2 squares, $n - 1$ of which are infected. Each second, any square that is adjacent to at least two infected squares becomes infected. Show that at least one square always remains uninfected.

Solution. Left as an exercise! $\square$

✠3 April 25, 2021

§3.1 Extremal Principle and Pigeonhole Principle by Nishat Anjum Bristy

§3.1.1 Extreme Principle

Every finite set has a least value and a greatest value. This is the basis of extreme principle.

As an example $\mathbb{N}$ has the least value 1.

Here is a motivating example of how to use extreme principle in Problem Solving.

Example 3.1.1

n students are sitting in a field such that the distance betweeen each pair of students is distinct. each student is holding a ball. When the teacher whistle, students throw their ball to the nearest student. Prove that there is a pair of students that throws their ball to each other.

Here starting with small values of n, we may guess the solution. The main idea is finding the least distance between two students. By extereme principle, there is a least distance betweeen two students. So, this 2 students throw their balls to each other. Done!

Example 3.1.2

Find all the possible positive solutions to the equations.

$$x_1 + x_2 = x_3^2$$
$$x_2 + x_3 = x_4^2$$
$$x_3 + x_4 = x_5^2$$
$$x_4 + x_5 = x_1^2$$
$$x_5 + x_1 = x_2^2$$

Here you should guess the solution. You will find that $x_1 = x_2 = x_3 = x_4 = x_5 = 2$.

We will show that the solution must be equal to 2, it can't be less that or grater that 2.

By extremal principle, WLOG assume, x_2 is the least value here. So, we have,

$$x_1 \leq x_2, x_3, x_4, x_5$$

$$x_1 \leq x_4$$

$$x_1 \leq x_5$$

So,

$$2x_1 \leq x_4 + x_5 = x_1^2$$

$$\implies x_1 \geq 2$$

Similarly we can assume that x_2 is the gretest value here, and show that $x_2 \leq 2$.

Then by the same argument, $x_3 = x_4 = x_5 = x_1 = x_2 = 2$.

So we are done.

Example 3.1.3

There are n red points and n blue points in a plane such that no three are collinear. Show that we can choose n line segments so that, every line segment connects a red point with a blue point and no two line intersect .

First, start with samll values of n, you can find a monovariant here, that, if there is no intersectins, then the sum of the lengths of the segments is least(by triangle inequality).

Let, assume a configuration with some intersections. Then, select an intersection, and then un-intersect it. In this process, we care about the sum of the lengths of the segments, by triangle inequality you can easily show that, with 4 points, if they intersects(2 line segments) then, in-intersect it and measure the sum, you can show that the last sum is obviously lesser than the previous.

It some point the sum become least. So we have to show that there is no intersection. Assume there is an inersection. Then using triangle inequality, there is a configuration with lesser sum, but we assumed the sum is least here. Contradiction!

Example 3.1.4

A finite set of points S in a plane has the property that triangle determined by any thrree points in S has area at most 1. Prove that, there exists a triangle with area 4 that contains all the points

I am giving the solution with a diagram. :D

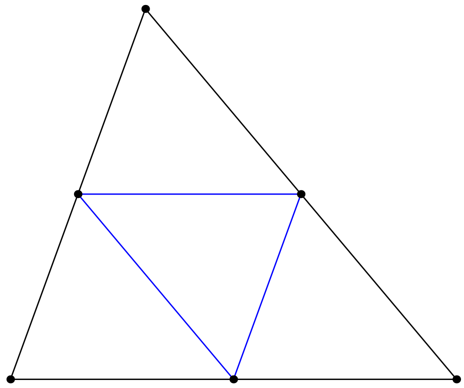


Figure 3.1: Guess the solution

§3.1.2 Pigeonhole Principle

Suppose there are n pigeons to be placed within n_1 holes. Then you can easily say that there is hole which contains two pigeons. It is a trivial but very useful idea in solving combinatorial problems.

Example 3.1.5

A box has three pair of shocks colored red, blue and green. If the shocks are choosen without looking, at least how many shocks must be chosen to gurantee that at least one matching pair is there?

The answer is FOUR.

Example 3.1.6

SHow that given a set of n positive integers, there exists a non-empty subset where the sum of the elements is divisible by n.

Let, the set is $S = \{a_1, a_2, a_3, \ldots, a_n\}$ And consider the followig:

$$s_1 = a_1$$
$$s_2 = a_1 + a_2$$
$$s_3 = a_1, a_2, a_3$$
$$\ldots$$
$$s_n = a_1 + a_2 + \ldots + a_n$$

$s_1, s_2, \ldots, _n$ may leave n distinct residue modulo n then one of them is 0, done.

But if there are some two s_i, s_j for which $s_i \equiv s_j \pmod{n}$ and $i < j$ then we have $s_j - s_i$ divisible by n.

Example 3.1.7

10 points are placed within an equilateral triangle of side length one. Show that, there exists two points with distance at most $\frac{1}{3}$ apart.

Look at the diagram. You may find the solution!

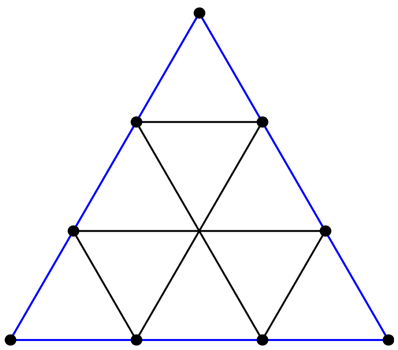


Figure 3.2: There are nine triangle and ten points ot be placed here!

Class ended!

§3.2 PoP, Radical Axis, Cyclic Quads by Raiyan Jamil

What is Power of a Point? Well, its not the Microsoft Office's Power Point. Its the most famous Power of a Point theorem which deals with a circle and a point. It tells that the power of a fixed point with respect to a fixed circle is constant. Let P be a fixed point a circle be ω then, let a line through P intersects the circle at A, B and another line through P intersects the circle at C, D respectively. Now, we have,

$$PA \cdot PB = PC \cdot PD.$$

which is called the Power of a Point.

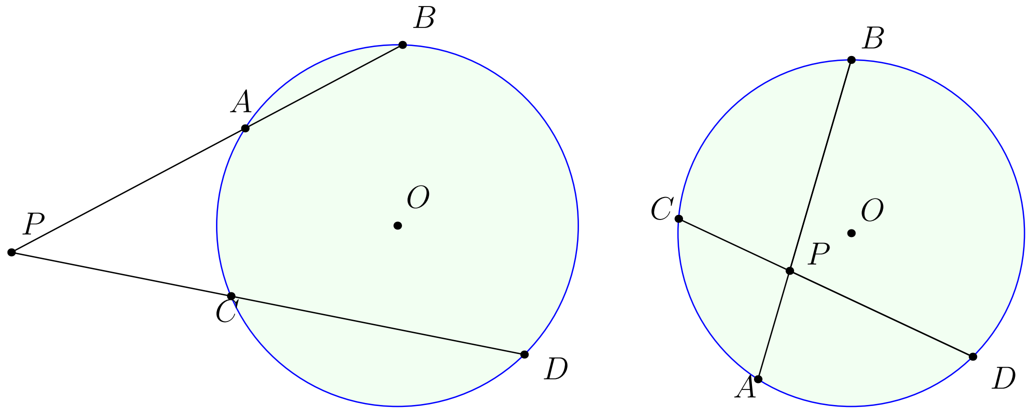


Figure 3.3: Power of a Point

§3.2.1 Radical Axis

What is radical axis? Radical axis is a set of points which have equal power with respect to two circles. It is a straight line and easy to prove using cartesian co-ordinates.

It is easy to draw the radical axis of two intersecting circles, but if thye are not intersecting then we have to draw another circelwhich intersect the two circles, then by the radical center, we can find hte radical axis.

Suppose that we have given three distinct circle, where pairwise radical axes are not parallel then they must concur. This (the point of concurrency) is called **Radical Center** of three circles.

Now we are going to see some example of problem solving using power of a point.

Example 3.2.1

Let ABC be an acute triangle. Let the line through B perpendicular to AC meet the circle with diameter AC at points P and Q, and let the line through C perpendicular to AB meet the circle with diameter AB at points R and S. Prove that P, Q, R, S are concyclic.

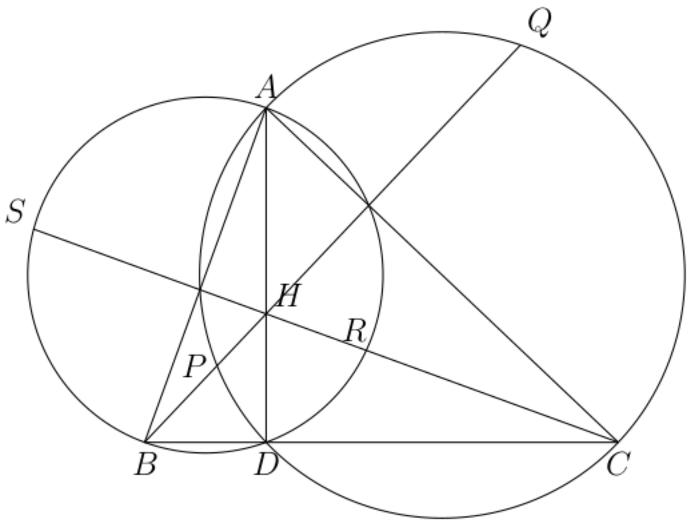


Figure 3.4: Soving a problem using PoP

Solution. Let D be the foot of the perpendicular from A to BC andlet H be the orthocenter of ABC. Since, $\angle ADB = 90°$, the circle with diameter AB passes through D, so $HS \cdot HR = HA \cdot HD$ by power of a point.

Similarly the circle with diameter AC passes through D as well, so $HP \cdot HQ = HA \cdot HD$ as well. Hence $HP \cdot HQ = HR \cdot HS$, and therefore by the converse of power of a point, P, Q, R, S are concyclic. □

§3.2.2 PoP for showing Concurrency

Example 3.2.2 (IMO 1995)

Let A, B, C, and D be four distinct points on a line, in that order. The circles with diameters AC and BD intersect at X and Y . The line XY meets BC at Z. Let P be a point on the line XY other than Z. The line CP intersects the circle with diameter AC at C and M , and the line BP intersects the circle with diameter BD at B and N . Prove that the lines AM, DN , and XY are concurrent.

Solution. By power of a point we have $PM \cdot PC = PX \cdot PY = PN \cdot PB$. So, B, C, M, N are concyclic. Note that $\angle AMC = \angle BND = 90°$ since they are subtended by diameters AC and BD, respectively. Hence $\angle MND = 90° + \angle MNb = 90° + \angle MCA = 180° - \angle MAD$.

Therefore, A, D, N, M are concyclic. Since AM, DN, XY are thethree radical axes for the circumcircles of $AMXC, BXND$ and $AMND$, they concur at the radical center.

□

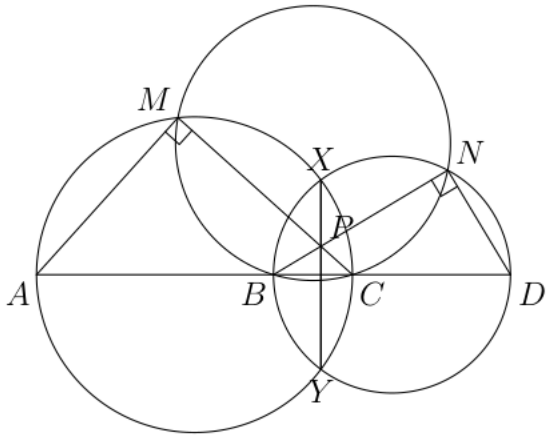


Figure 3.5: PoP for showing Concurrency

§3.2.3 PoP for showing Collinearity

Example 3.2.3

Let ABC be a triangle and let D and E be points on the sides AB and AC, respectively, such that DE is parallel to BC. Let P be any point interior to triangle ADE, and let F and G be the intersections of DE with the lines BP and CP , respectively. Let Q be the second intersection point of the circumcircles of triangles PDG and PFE. Prove that the points A, P, and Q are collinear.

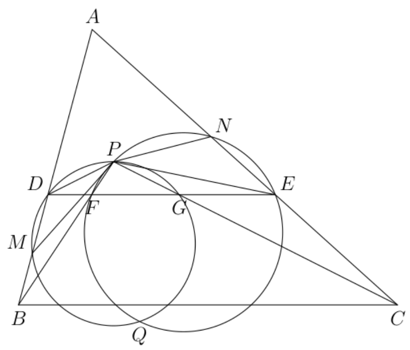


Figure 3.6: PoP for showing Collinearity

Solution. Let the circumcircle of DPG meet line AB again at M , and let the circumcircle of EPF meet line AC again at N . Assume the configuration where M and N lie on sides AB and AC respectively (the arguments for the other cases are similar). We have $\angle ABC = \angle ADG = 180° - \angle BDG = 180° - \angle MPC$, so $BMPC$ is cyclic. Similarly, $BPNC$ is cyclic as well. So $BCNPM$ is cyclic. Hence $\angle ANM = \angle ABC = \angle ADE$, so M, N, D, E are concyclic. By power of a point, $AD \cdot AM = AE \cdot AD$. Therefore, A has equal power with respect to the circumcircles of DPG and the EPF , and thus A lies on line PQ, the radical axis. $\square$

Here I am going to include some problems which can be solved using Power of a Point.

Problem 3.2.4 (IMO 2000/1). Two circles G_1 and G_2 intersect at two points M and N . Let AB be the line tangent to these circles at A and B, respectively, so that M lies closer to AB than N . Let CD be the line parallel to AB and passing through the point M, with C on G_1 and D on $_2$. Lines AC and BD meet at E; lines AN and CD meet at P ; lines BN and CD meet at Q. Show that $EP = EQ$.

Problem 3.2.5 (USAMO 1997/2). Let ABC be a triangle. Take points D, E, F on the perpendicular bisectors of BC, CA, AB respectively. Show that the lines through A, B, C perpendicular to EF, FD, DE respectively are concurrent.

Problem 3.2.6 (USAJMO 2012/1). Given a triangle ABC, let P and Q be points on segments AB and AC, respectively, such that $AP = AQ$. Let S and R be distinct points on segment BC such that S lies between B and R, $\angle BPS = \angle PRS$, and $\angle CQR = \angle QSR$. Prove that P, Q, R, S are concyclic.

✠4 April 26, 2021

§4.1 Polynomials by Mursalin Habib

What is a polynomial? Well, an example of a polynomial is given below:

$$x^2 - 5x + 6.$$

Generally a polynomial is a form of:

$$a_n x^n + a_{n-1}x^{n-1} + a_{n-2}x^{n-2} + \ldots + a_2x^2 + a_1x + a_0.$$

where $a_n \neq 0$. Also assume that $a_n, a_{n-1}, \ldots$ are generally real numbers. Here comes some definitions:

Definition 4.1.1 (Coefficient). $a_n, a_{n-1}, \ldots$ are called coefficients.

Definition 4.1.2 (Leading Coefficient). a_n is called the leading coefficient.

Definition 4.1.3 (Degree of a polynomial). Maximum power n is called the degree of a polynomial.

Definition 4.1.4 (Monic Polynomial). A polynomial with leading coefficient 1 is called a monic polynomial.

Here we are introduced with some techniques to solve polynomial problems:

§4.1.1 Exploiting Symmetry

Example 4.1.5

Find all real x that satisfy the equation

$$(x-1)(x^2+1)(x^3+1) = 30x^3.$$

Here do some algebra to get:

$$x^6 + x^5 + x^4 - 28x^3 + x^2 + x + 1 = 0.$$

It is apolynomial of degree 6 which is messy. But you can see that here is a symmetry left to the term $-28x^3$ with the right part of the equation. Also observe that, if x is a root then $\frac{1}{x}$ is also a root. So, we are going to divide the equation by x^3 and we get:

$$x^3 + x^2 + x - 28 + \frac{1}{x} + \frac{1}{x^2} + \frac{1}{x^3} = 1.$$

Here we pair up x^3 with $\frac{1}{x^3}$ and so on. We get the following:

$$\left(x^3+\frac{1}{x^3}\right)+\left(x^2+\frac{1}{x^2}\right)+\left(x+\frac{1}{x}\right)-28=0.$$

Now we assume $x+\frac{1}{x}=y$ and you see that, $x^3+\frac{1}{x^3}=y^3-3y, x^2+\frac{1}{x^2}=y^2-2y, x+\frac{1}{x}=y$ and we proceed by following:

$$\begin{aligned}\left(x^3+\frac{1}{x^3}\right)+\left(x^2+\frac{1}{x^2}\right)+\left(x+\frac{1}{x}\right)-28&=0\\ y^3-3y+y^2-2y+y-28&=0\\ y^3+y^2-2y-30&=0\end{aligned}$$

But it is a polynomial with degree 3, which is also not so easy to solve. But we have a theorem for this: Rational Root Theorem.

Theorem 4.1.6 (Rational Root Theorem)

A polynomial $P(x)$ has a rational root $\frac{p}{q}$ if and only if $p|a_0$ and $q|a_n$.

if we can find a root of our polynomial then it comes easy to solve a quadratic eqaution.

After playing with numbers, you can find a root 3 which works! Then we have,

$$(y-3)(\dots)=y^3+y^2-2y-30.$$

Now, you can solve the problem and the rest is a good exercise so left as an exercise.

Here we see another problem:

Example 4.1.7

Find all real solution to the eqaution,

$$x^4+(x-2)^4=34.$$

It is a 4 degree polynomial, so we have to think wisely. An idea coomes that, we can rewrite the equation by folling,

$$(y+1)^4+(y-1)^4=34$$

where, $x=y+1$ and so $x-2=y-1$ After doing some algebra we get a polynomial where all the degrees of y is even, and assume $y^2=z$ then the polynomial is a quadratic and do some algebra.

§4.1.2 Polynomial Division

You probably know that for a number a we can find q such that $q|a$ and we can write a as follows:

$$a = bq + r$$

where $0 \leq r < b$.

Similarly for a polynomial $a(x)$ we can find $b(x), q(x)$ and $r(x)$ such that,

$$a(x) = b(x)q(x) + r(x).$$

Here note that if $b(x)$ has degree 2 then $r(x)$ is linear.

By using these facts we can solve a problem now:

Example 4.1.8

Find the remainder when the polynomial $x^{81} + x^{49} + x^{25} + x^9 + x$ is divided by the polynomial $x^3 - x$.

Here observe that we can write the polynomial by $Q(x)(x^3 - x) + r(x)$ and also observe that $r(x)$ has degree 2. So,

$$x^{81} + x^{49} + x^{25} + x^9 + x = Q(x)(x^3 - x) + ax^2 + bx + c.$$

Now we factor,

$$x^3 - x = x(x+1)(x-1).$$

Now, pluging $x = 0, x = 1, x = -1$ in the above equation we get,

$$a = 0, b = 5, c = 0$$

so, the remainder is $5x$.

Always remember to write a polynomial $a(x)$ by $b(x)q(x) + r(x)$.

Also remember the vieta's formulas. It Assume that the polynomial

$$a_n x^n + a_{n-1}x^{n-1} + a_{n-2}x^{n-2} + \ldots + a_2x^2 + a_1x + a_0.$$

has roots $r_1, r_2, r_3, \ldots, r_n$ we have

$$r_1 + r_2 + r_3 + \ldots + r_n = -\frac{a_{n-1}}{a_n}$$

and,

$$r_1r_2 + r_2r_3 + \ldots + r_{n-1}r_n = \frac{a_{n-2}}{a_n}$$

and similarly analogous...

Here are going to solve a problem using the above proposition.

Example 4.1.9

Given that, $a+b+c>0$, $ab+bc+ca>0$ and $abc>0$. Prove that, $a,b,c>0$.

Here we will use method of contradiction!

We are going to construct a polynomial:

$$P(x)=x^3-(a+b+c)x^2+(ab+bc+ca)x-abc$$

which has roots a,b,c.

And assume that a is negative. But then $P(a)$ is negative which is supposed to be zero(as a is a root of $P(x)$). Which is a contradiction!

Example 4.1.10

Let n be a positive integer and for $1\le k\le n$ let s_k be the sum of the products of the numbers $1,1/2,1/3,\ldots,1/n$ taken k at a time. For example,

$$s_2=1\cdot\frac{1}{2}+1\cdot\frac{1}{3}+\ldots\frac{1}{n-1}\cdot\frac{1}{n}$$

Find $s_1+s_2+\ldots+s_n$.

It is left as an exercise for the interested readers.

Theorem 4.1.11 (Identity Theorem)

Two polynomials $f(x),g(x)$ have degree less than n. If they intersect at $n+1$ points $(x_1,x_2,\ldots x_{n+1})$ so, $f(x_1)=g(x_1),f(x_2)=g(x_2),\ldots$.

Then two polynomials are the same i.e. $f(x)=g(x)$.

Here let $P(x)=f(x)-g(x)$, it results that, $P(x)$ has $n+1$ roots which is not possible unless $P(x)$ is identically zero. (as $P(x)$ has degree at most n.)

Here, we solve a problem using the above result.

Example 4.1.12

If $f(x)$ is a monic quartic polynomial such that $f(-1)=-1,f(2)=-4,f(-3)=-9$ and $f(4)=-16$. Find $f(1)$.

$f(-1)=-1,f(2)=-4,f(-3)=-9$ and $f(4)=-16$ So, $f(x)=-x^2$ which is not a monic polynomial.

We asssume $f(x)=x^4+bx^3+cx^2+dx+e$ as it is monic and quartic.

Then, consider the polynomial $f(x) + x^2 = P(x)$ which is a 4 degree polynomial which has roots $-1, 2, -3, 4$.

At these points $P(x)$ is zero, and as it is a quartic so we have,

$$P(x) = c(x+1)(x-2)(x+3)(x-4)$$

where c is obviously zero as $f(x)$ is a monic.

Example 4.1.13

If $P(x)$ denotes a polynomial of degree n such that

$$P(k) = \frac{k}{k+1}$$

for $k = 0, 1, 2, \ldots, n$. Determine $P(n+1)$.

Here conisder a polynomial

$$(x+1)P(x) - x = f(x)$$

by the above argument, we get,

$$f(x) = cx(x-1)(x-2)(x-3)\cdots(x-n)$$

Plugging $x = -1$ we get, $1 = c(-1)^{n+1}(n+1)!$ so,

$$c = \frac{1}{(-1)^{n+1}(n+1)!}$$

The rest is a good exercise.

§4.1.3 Polynomial Interpolation, Polynomial Functional Equation

Suppose you are given that $f(1) = 7, f(2) = 4, f(10) = -5$ and you are told to find the function. This process is called Polynomial Interpolation. The above problem asks you to find the polynomial which graph goes through the points $(1,7), (2,4), (10,-5)$.

Example 4.1.14

What is the next term of the sequence $2, 5, 11, 23, \ldots$?

The answer is what you want!

We write n term as a_n and let

$$a_n = (A_1 \times 2) + (A_2 \times 5) + (A_3 \times 11) + (A_4 \times 23) + (A_5 \times 42)$$

Take $A_{1,2}$, A_3, A_4, A_5 such that if we plug $n = 1$ then we get $A_1 = 1$ and $A_2 = A_3 = A_4 = A_5 = 0$. Similarly for $n = 2, 3, 4, 5$. Magically take

$$A_1 = \frac{(n-2)(n-3)(n-4)(n-5)}{(1-2)(1-3)(1-4)(1-5)}$$

and analogous for $A_2, A_3, \ldots$

Example 4.1.15

f be a function such that $f(1) = 7, f(2) = 4, f(10) = -5$

From the above example it is easy. So,

$$f(x) = \frac{(x-2)(x-10)}{(1-2)(1-10)} \times 7 + \frac{(x-1)(x-10)}{(2-1)(2-10)} \times 4 + \frac{(x-1)(x-2)}{(10-1)(10-2)} \times (-5)$$

It is known as Lagrange Interpolation. It is useful in finding an algebraic form of a sequence.

Example 4.1.16

$$f(x) = \frac{(x-b)(x-c)}{(a-b)(a-c)} + \frac{(x-a)(x-c)}{(b-a)(b-c)} + \frac{(x-a)(x-b)}{(c-a)(c-b)}$$

and $a \neq b \neq c$. $\deg(f) \leq 2$.

We get, $f(a) = f(b) = f(c) = 1$. So, it is not possible to have degree 2. As it has same value at three points.

Consider $f(x) - 1 = p(x)$, and $p(a), p(b), p(c)$ is zero. So, $p(x)$ is identically zero and $f(x) = 1$.

Example 4.1.17

Let a, b, c, d be distinct real numbers. Show that

$$\frac{a^4}{(a-b)(a-c)(a-d)} + \frac{b^4}{(b-a)(b-c)(b-d)} + \frac{c^4}{(c-a)(c-b)(c-d)} + \ldots = a+b+c+d.$$

$$P(x) = \frac{a^4(x-b)(x-c)(x-d)}{(a-b)(a-c)(a-d)} + \frac{b^4(x-a)(x-c)(x-d)}{(b-a)(b-c)(b-d)} + \frac{c^4(x-a)(x-b)(x-d)}{(c-a)(c-b)(c-d)} + \ldots$$

The coefficient of x^3 in $P(x)$

$$f(x) = x^4 - P(x) = (x-a)(x-b)(x-c)(x-d).$$

. . . Lagrange Interpolation . . .

§4.2 Transformation by Mugdho Tanjim Shorif

There are generally 5 kind of Transformation, namely:

- Translation
- Rotation
- Reflection
- Homothety
- Spiral Similarity

§4.2.1 Translation

This is the most common and easy of the transformations, you can translate a point along with a line. Let the point is P and the line is AB, then if you translate P wrt AB, we write this as $T(AB)$ and here P maps to a point Q such that $AB \parallel PQ$, and $AB = PQ$.

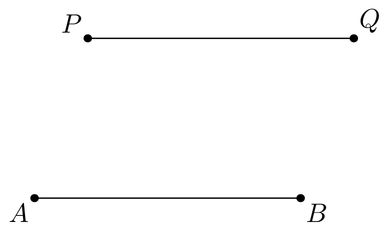


Figure 4.1: Translation along with AB maps P to Q.

Here we are going to solve some problem.

Example 4.2.1

In the figure below, what is the minimal distance from A to B with a bridge that can be made in anywhere over the river perpendicular to the parallel lines.

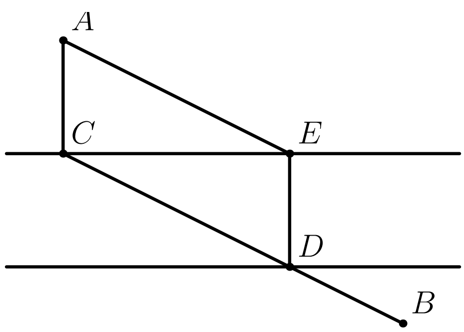


Figure 4.2: Find shortest path from A to B.

Problem 4.2.2. Similarly above find the shrtest distance from A to B with more that one river between them.

Example 4.2.3

Let $ABCDEF$ be a hexagon such that, $AB \parallel DE, BC \parallel EF, CD \parallel FA$ and $AF - CD = DE - AB = BC - EF > 0$. Prove that the hexagon is equiangular that is all the angles of the hexagon is equal to $120°$.

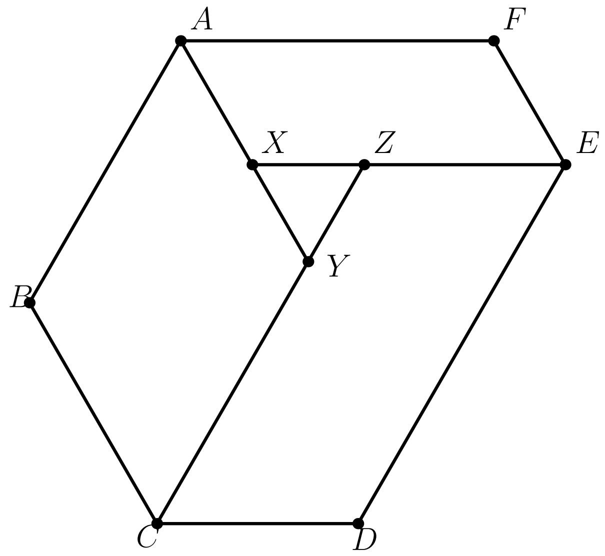


Figure 4.3: Finding an equilateral triangle

Here the opposite sides configuration is very disgusting to handle. So we want such a translation which makes the subtraction of th opposite sides to the side of an equilateral triangle. We are going to translate E along with AF to map E to X, similarly define Y, Z. Now observe that XYZ is an equilateral triangle. Now it is easy to conclude.

Example 4.2.4

In quadrilateral $ABCD$, let M, N be the midpoints of AB and CD respectively. Given that, $@MN = AD + BC$. Prove that, $AD \parallel BC$.

§4.2.2 Rotation

Rotation deals with a center point and an angle. Let a point be P and another center point O. You may rotate P wrt O with angle $50°$ which means you draw an arc with center O and goes from P to Q. And $\angle POQ = 50°$. It is defined by

$$R(O, \alpha)$$

Example 4.2.5

Let, $ABCD$ be a square and P be a point inside the square such that, $PA = 1, PB = 2, PC = 3$. Find $\angle APB$.

Here we are going to rotate the points A, C, P with center B and angle of $90°$. Which means $A \mapsto C, P \mapsto P'$. Now note that as $\angle PBP' = 90°$ and $PB = BP'$, we have, $\angle BPP' = 45° = BP'P$. By Pythagoras, $PP' = 2\sqrt{2}$. As $AP = CP' = 1$, by the converse of Pythagoras we have, $\angle PP'C = 90°$. So $\angle APB = \angle CP'B = 90°$.

Example 4.2.6

Let ABC be an equilateral triangle and a point inside the triangle P such that $PA = 5, PB = 4, PC = 3$. Find the area of the triangle.

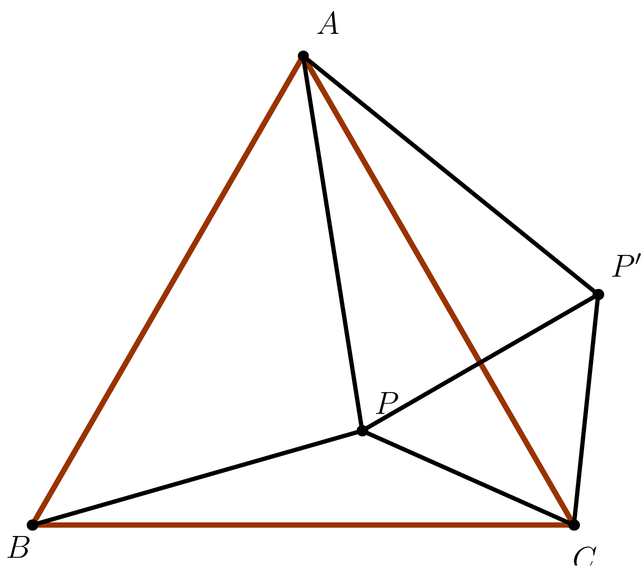


Figure 4.4: Rotate the point P

Consider a rotation with center C and angle $60°$, $P \mapsto P', B \mapsto A$ and see that,

$$CP' = CP$$

$$CA = CB$$

$$\angle P'CA = \angle PCB$$

Here you see that,

$$AP' = BP = 4$$

$$PP' = 3$$

and APP' is a right angular triangle with $\angle AP'P = 90°$. So,

$$\angle AP'C = 150° = \angle BPC$$

By cosine law we are done!

Example 4.2.7

Let $ABCD$ be a square and W, X, Y, Z be four points on AB, BC, CD, DA respectively such that $BW + BX + DY + DZ = 2BC$. Prove that, $WY \perp ZX$.

Here rotate the diagram with center B and angle $90°$. We denote the rotation of A with A' and analogous...

AND we are giong to show that $WY \parallel Z'X'$ Here we let $AB = BC = CD = DA = a$. And

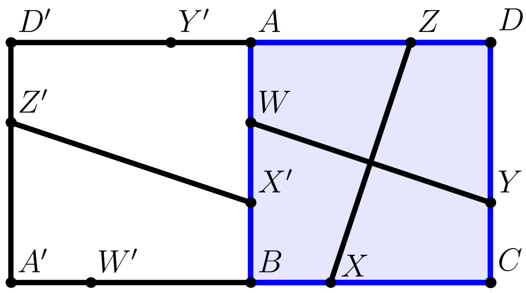


Figure 4.5: Perpendicularity to Parallelism!

doing some calculation:

$$BW + BX + DY + DZ = 2BC = 2a$$
$$BW' + BX + D'Y' + DZ = 2a$$
$$BW' + BX + (a - AY') + (a - AZ) = 2a$$
$$BW' + BX = AY' + AZ$$
$$XW' = Y'Z$$

Now it is easy to see that $XZY'W'$ is a parallelogram. And that's why $ZX \parallel W'Y'$.

§4.2.3 Reflection

Example 4.2.8

Let $ABCD$ be a quadrilateral such that, $AB = BC = CD$ and $AC \neq BD$ but $AE = DE$ where E is the intersection of the diagonals. Find $\angle BAD + \angle ADC$.

Here we are goingt to reflect C with respect to AD and we get that $BD \parallel AC'$ and $C'D = AB$. SO $ABDC'$ is either a parallelogram or trapezoid.

But there is a contradiction that if it is a paralleogram then $AC' = AC = BD$ which is absurd.

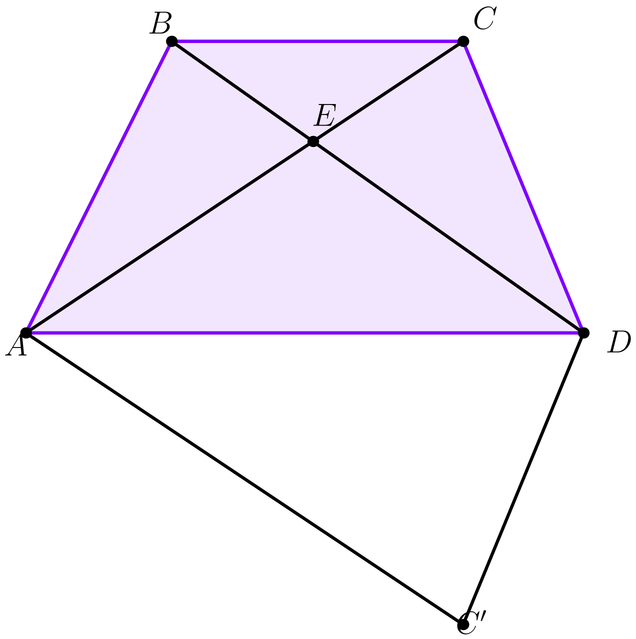


Figure 4.6: A reflection problem

So it is an isosceles trapezoid which is obviously cyclic. Here we denote $\angle BAC = \beta = \angle BCA$, $\angle CAD = \angle DAC' = \angle BDA = \alpha$, $\angle DBC = \gamma$.

So we get $\angle ADC' = \alpha + \gamma$ Using cyclic quads, we get $4\alpha = 120°$. (Yes, there is some angle chasing which is a good exercise and left to the reader.)

Here is a problem you can try:

Problem 4.2.9. A circle with center O passes through vertices A and C of $\triangle ABC$ and cuts sides AB, BC, CA at K and N respectively. The circumcircles of ABC and KBN intersect at B and M. Prove that $\angle OMB = 90°$.

§4.2.4 Homothety

Homothety (also known as dilation) is a transformation consisting of two variables- a center O and a real number k such that O sends a point A to A'. Homothety is denoted by-

$$H(O, k)$$

Remember that k can be negative

We have,

$$\frac{OA'}{OA} = k.$$

1. After homothety AB and $A'B'$ are parallel.
2. Triangles are similar after homothety.

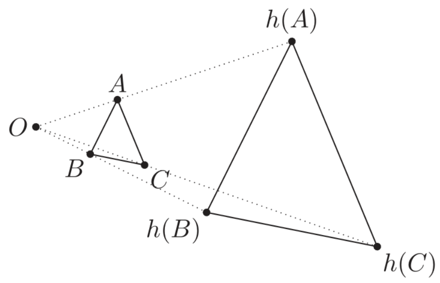


Figure 4.7: $\triangle ABC$ and $\triangle h(A), h(B), h(C)$ are homothetic similar

See the diagram. Here O sends A, B, C to $h(A), h(B), h(C)$ respectively.

As said before k can be negative. See the diagram-

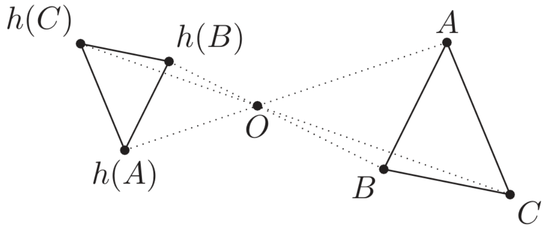


Figure 4.8: A negative homothety

Also remember that homothetic center can be a point at infinity. Where $AB = A'B'$ and the scale factor of the homothety is not equal to -1.

Example 4.2.10

Two circles C_1, C_2 are such that C_2 is internally tangent to C_1 at P. A chord AB of C_1 touches C_2 at E. Prove that ray PE bisects the arc AB which doesn't contains P.

We are going to use homothety here. Look that P is the homothetic center of two circles that sends C_2 to C_1. Let O_1, O_2 vare the centers of C_1, C_2 respectively, see that P, O_1, O_2 are collinear. Also P, E, F (where F is the intersection point of PE with C_1) are collinear. Consequently PO_2E and PO_1F are homothetic. Here note that $\angle O_2EA = 90°$ similarly F is the tangent point of a line parallel to BA whch is tangent to C_1.

Here we see a proof of the nine point circle.

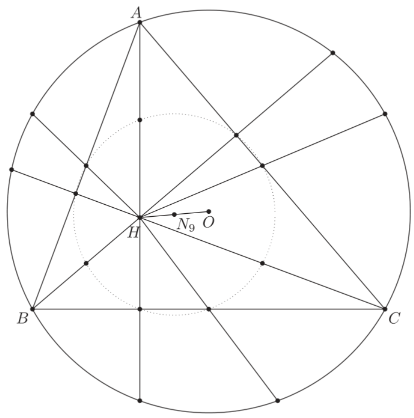


Figure 4.9: Nine Point Circle Homothetic to (ABC) with center H.

You probably know the fact that the reflection of the orthocenter on the line BC and with respect to the midpoint of BC lies on the circumcircle of ABC. Similarly, define analogous points. Here you get nine points on the circumcircle of ABC. Consider a homothety with center H and scale factor $\frac{1}{2}$. So we get nine points still concyclic. Done!

Problem 4.2.11. Let the incircle of triangle ABC touches BC at D. T is the antipode of D with respect to the incircle. Let ray AT meets BC at P. Prove that $BD = CP$.

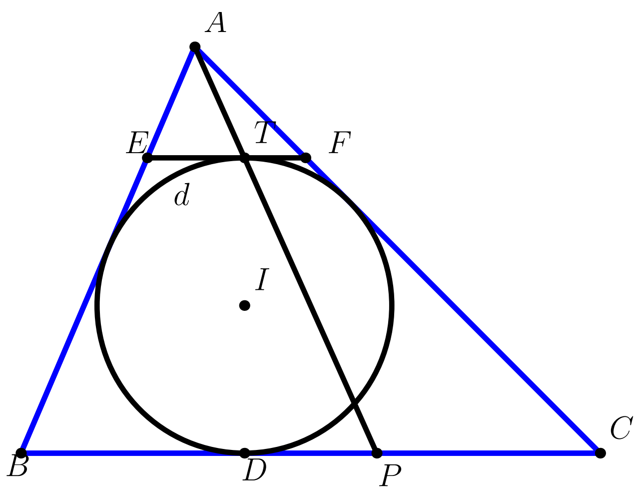


Figure 4.10: Problem 4.2.11 for exercise

§4.2.5 Spiral Similarity

Spiral similarity isa special kind of similarity consisiting of a rotation and a dilation(homothety). It is denoted by

$$S(O, \alpha, k)$$

where O is the center of the spiral similarity.

Example 4.2.12

P is an internal point in the plane of a triangle ABC such that $\angle APC = \angle BPC = \angle APB = 120°$ and $\angle BAC = 60°$. Let, D, E be the midpoints of the segments AC, AB respectively. Show that $AEPD$ cyclic.

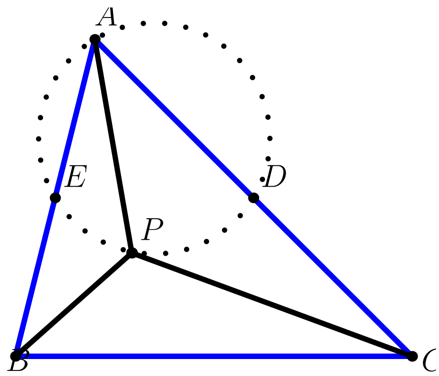


Figure 4.11: A spiral similarity problem

Here see that $\triangle APB$ and $\triangle CPA$ aer similar. So we can take a spiral similarity that takes APB to CPA with center P and angle $120°$.

$$S(P, 120°, \frac{PC}{PA})$$

$$A \mapsto C$$

$$B \mapsto A$$

So we can say that

$$E \mapsto D.$$

So, as our angle of rotation was $120°$ so $\angle EPD = 120° = 180° - \angle EAD$. Done!

And class ends here!

§5 April 27, 2021

§5.1 Bijection by Ahsan Al Mahir

(This class is taught by following Yufei Zhao's Bijection Note. This note is a great resource for further reading) Bijection means a function which is injective and surjective at the same time. Let you are told to find the number of ways to walk from $(0,0)$ to $(5,4)$. Which is called grid walking. It is difficult to find the answer unless you find some bijection. You may let the right move R and up move U which means all the ways are of $RURURRRUU$ this type. Which is in fact a binary string. Now it is easier to tackle the problem. And there are $\binom{9}{4}$ ways.

Our next example is about Triangular Grid.

Example 5.1.1

A triangular grid is obtained by tiling an equilateral triangle of side length n by n^2 equilateral triangles of side length 1. Determine the number of parallelograms bounded by line segments of the grid.

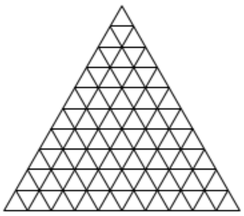


Figure 5.1: Three different oriented parallelograms

Here observe that there are 3 different types(orientation) of parallelograms. If you can find the number of parallelograms of a single orientation, by symmetry the total number is thrice the number.

Figure 5.2: Three different oriented parallelograms

Let us just count the paralellograms with the middle type of orientation (i.e., no horizontal sides).

Extend the triangular grid by one extra row at the bottom. The key (and clever) observation is that starting from any such parallelogram in the original grid, we can extend its sides to meet the lines to meet the bottom edge of the new row in the large triangular grid, and there would be four distinct intersection points, as shown below.

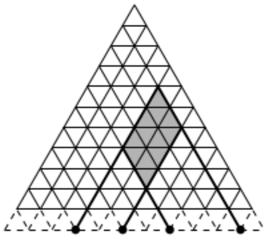


Figure 5.3: An added row and the solution

Conversely, starting from any four distinct grid points in new bottom edge, we can extend $60°$ lines from the first two points and $120°$ lines from last two points to obtain a parallologram in the original grid. This gives us a bijection between the set of parallelograms in the original grid with no horizontal sides with set of four distinct points in the new bottom edge, and hence there must be $\binom{n+2}{4}$ of them. Accounting for all three orientations, we find that the total number of parallolograms in the original grid is $3\binom{n+2}{4}$.

(The above solution taken from Zhao's Note.)

Example 5.1.2

Let n be a positive integer. Determine the number of lattice paths from $(0,0)$ to (n,n) using only unit up and right steps, such that the path stays in the region $x \geq y$.

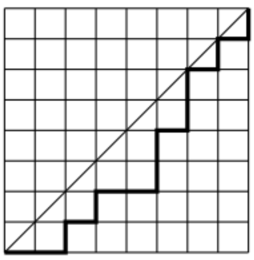


Figure 5.4: The Problem

We saw previously that the total number of lattice paths from $(0,0)$ to (n,n) without the $x \geq y$ restriction is equal is $\binom{2n}{n}$. Let us count the number of paths that goes into the $x < y$ region. Call these paths |*bad paths*.

Suppose that P is a bad path. Since P goes into the region $x < y$, it must hit the line $y = x+1$ at some point. Let X be the first point on the path P that lies on the line $y = x+1$.

Now, reflect the portion of path P up to X about the line $y = x + 1$, keeping the latter portion of P the same. This gives us a new path P'.

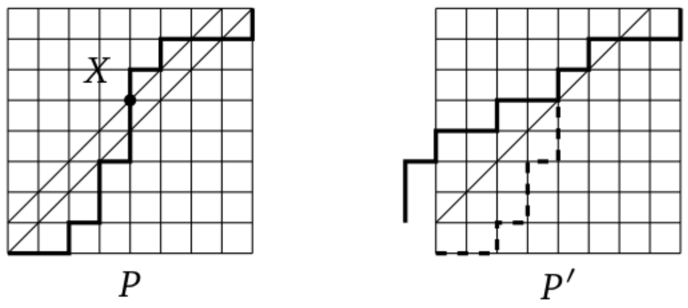


Figure 5.5: The Solution

We claim that this gives us a bijection between the set of bad paths to the set of lattice paths from $(-1, 1)$ to (n, n) using only up and right unit steps.

Here is the inverse construction. For any lattice path Q from $(-1, 1)$ to (n, n), let X be the first point on the path lying on the line $y = x + 1$, and let Q' be constructed from Q by reflecting the first portion of Q up to X through the line $y = x + 1$ and keeping the rest the same. Then the inverse of the bijection given above sends Q to Q'.

To complete the proof of this claim, we need to check a number of details, which we outline below. The reader should think about why claim is true.

- The inverse construction is well defined. That is, we can always find such a point X , and also, the resulting Q' is a always a bad path.
- The two constructions are inverses of each other.

The number of bad paths is equal to the number of lattice paths from $(-1, 1)$ to (n, n) using only unit up and right steps, and there are $\binom{2n}{n+1}$ such paths.

Therefore, the total number of "good" paths, i.e., those that do not go into the region $x < y$, is equals to

$$\binom{2n}{n} - \binom{2n}{n+1} = \binom{2n}{n} - \frac{n}{n+1}\binom{2n}{n} = \frac{1}{n+1}\binom{2n}{n}.$$

The above number is called the Catalan Number. There are many more counting problems which are counted by Catalan Numbers.

Now you can solve some problems from Yufei Zhao's Bijection Note. This note contains many problems. I am ading some of them.

Problem 5.1.3. Show that the n-th Catalan number counts the number of expressions containing n pairs of parentheses which are correctly matched. E.g., for $n = 3$,

$$((())) \quad (()()) \quad (())() \quad ()(()) \quad ()()()$$

A plane tree is an object with the following structure. We start with a root vertex (drawn at the top), and then with each node we attach a number of new vertices (possibly none), where the order of the attached vertices matters. For instance, there are exactly 5 plane trees with 4 vertices

Problem 5.1.4. Show that the n-th Catalan number counts the number of plane trees with $n+1$ vertices.

Problem 5.1.5. Show that the number of ways of stacking coins in the plane so that the bottom row consists of n consecutive coins is C_n .

Problem 5.1.6. Show that the number of triangulations of a convex $(n+2)$-gon into n triangles by $n-1$ diagonals that do not intersect their interiors is the n-th Catalan number, C_n.

Problem 5.1.7. Let n be a positive integer. Prove that the number of partitions of n equals the number of partitions of $2n$ with n parts.

§5.2 Prime Numbers by DS Hasan

(We followed the text *Olympiad Number Theory* by Justin Stevans)

Prime numbers are the heart of Number Theory. They form the atom of the numbers and understaning them is equivalent to understanding all the numbers.

§5.2.1 p-adic Valuation

Here we see some advanced functions related to prime numbers. The **p-adic valuation.**

Definition 5.2.1 (p-adic Valuation)**.** We define the p-adic valuation of m to be the highest power of p that divides m. The notation for this is $v_p(m)$.

It is also known as the largest exponent function.

As an example since $20 = 2^2 \cdot 5$ we have $v_2(20) = 2$ and $v_5(20) = 1$.

Point to be noted that the above function is an additive function. So,

Theorem 5.2.2 (v_p is an Additive Function)

$v_p(ab) = v_p(a) + v_p(b)$.

Proof. Set, $v_p(a) = e_1$ and $v_p(b) = e_2$. Then, $a = p^{e_1}a_1$ and $b + p^{e_2}b_1$ where a_1 and b_1 are relavtively prime to p. We get,

$$ab = p^{e_1+e_2}a_1b_1 \implies v_p(ab) = e_1 + e_2 = v_p(a) + v_p(b).$$

□

Theorem 5.2.3

If $v_p(a) > v_p(b)$ then, $v_p(a+b) = v_p(b)$.

Proof. Again write $v_p(a) = e_1$ and $v_p(b) = e_2$. We therefore have $a = p^{e_1}a_1$ and $b = p^{e_2}b_1$. Notice that

$$a + b = p^{e_1}a_1 + p^{e_2}b_1 = (p^{e_2})(p^{e_1-e_2}a_1 + b_2.$$

Since $e_1 \geq e_2 + 1$ we have $p^{e_1-e_2}a_1 + b_2 \equiv b_2 \neq 0 \pmod p$ therefore $v_p(a+b) = e_2 = b$ as desired. □

§5.2.2 Example Problems

Example 5.2.4

Prove that $\sum_{i=1}^{n} \frac{1}{i}$ is not an integer for $n \geq 2$.

The key idea for the problems is to find a prime that divides into the denominator more than in the numerator.

Notice that

$$\sum_{i=1}^{n} \frac{1}{i} = \sum_{i=1}^{n} \frac{\frac{n!}{i}}{n!}$$

We consider $v_2\left(\sum_{i=1}^{n} \frac{n!}{i}\right)$. From Theorem 5.2.3, we get

$$v_2\left(\frac{n!}{2i-1} + \frac{n!}{2i}\right) = v_2\left(\frac{n!}{2i}\right)$$

We then get $v_2(\frac{n!}{4i-2} + \frac{n!}{4i}) = v_2(\frac{n!}{4i})$ and reepating to sum up the factorial in this way we arrive at

$$v_2\left(\sum_{i=1}^{n} \frac{n!}{i}\right) = v_2\left(\frac{n!}{2^{\lfloor \log_2 n \rfloor}}\right)$$

However for $\sum_{i=1}^{n} \frac{1}{i}$ to be an integer we need

$$v_2\left(\sum_{i=1}^{n} \frac{n!}{i}\right) \geq v_2(n!)$$

$$v_2\left(\frac{n!}{2^{\lfloor \log_2 n \rfloor}}\right) \geq v_2(n!)$$

$$0 \geq \lfloor \log_2 n \rfloor$$

which is a contradiction since $n \geq 2$.

Example 5.2.5

Prove that $\sum_{i=0}^{n} \frac{1}{2i+1}$ is not am integer for $n \geq 1$.

Define parity factorial i.e. $4!! = 4 \cdot 2$ and $5!! = 5 \cdot 3 \cdot 1$ and take the product of all odd numbers upto $2i+1$ and define as $(2i+1)!!$.

Same as above example rewrite the summation using parity factorial.

Then take v_3 and contradict that $0 \geq \lfloor \log_3(2n+1) \rfloor$.

You can solve some problems from the text "Olympiad Number Theory" by Justin Stevans.

✠6 April 28, 2021

§6.1 Double Counting and PIE by Nishat Anjum Bristy

§6.1.1 Double Counting

Double counting is also known as counting in two ways. By this technique, we count something in two ways!

Here is our first example:

Example 6.1.1

Show that,

$$1 + 2 + 3 + \ldots + n = \frac{n(n+1)}{2}$$

You can easily solve this by induction. but here we present a solution with double counting.

By writing the left side as S_n we proceed as follows:

$$S_n = 1 + 2 + \ldots + n$$

$$S_n = n + (n-1) + \ldots + 1$$

Thus,

$$S_n = \frac{n(n+1)}{2}.$$

But now, we want to think the right side of the equation in combinatorial arguments. Here we see that the right side is equal to the number of ways to choose 2 things from $n+1$ given things. If we can establish a bijection between them then we are done!

Here we take two empty cells, and we want to place the numbers in the cells. Suppose the cells:

$$\boxed{i}\boxed{j}$$

such that, $i < j$. Now if we place $i = 1$ then we see that, there are n choice for j. By similar arguments, we calculate,

$$\binom{n+1}{2} = 1 + 2 + 3 + \ldots + n.$$

Example 6.1.2

In a given series th esum of any 7 consecutive number is negative and the sum of any 11 consecutive numbers is positive. Prove that the series can't have 17 terms.

Here we make a matrix of the numbers of the series by writing consecutive terms.

$$\begin{matrix} t_1 & t_2 & t_3 & \dots & t_{11} \\ t_2 & t_3 & t_4 & \dots & t_{12} \\ \dots & \dots & \dots & \dots & \dots \\ \dots & \dots & \dots & \dots & \dots \\ t_7 & t_8 & t_9 & \dots & t_{17} \end{matrix}$$

Then sum up all the rorws and all the columns. See that, the rows sum up to a positive number but the columns sum up to a negative number. Which is a contardiction!

Remark. In the above example, we used the Fubini's Principle.

Example 6.1.3

Determine the total number of fixed points in all the permutations of

$$\{1, 2, 3, \dots, n\}$$

Here observing with smaller n you can find the answer. It is just $n!$.

Try to make a table here. You probably find that, in each column there is $(n-1)!$ number of fixed points. So the total is $n(n-1)! = n!$.

§6.1.2 Principle of Inclusion-Exclusion

A, B are two set and we know that $|a \cup B| = |A| + |B| - |A \cap B|$. This called inclusion exclusion pirinciple.

For three sets A, B, C we have

$$|A \cup B \cup C| = |A| + |B| + |C| - |A \cap B| - |B \cap C| - |C \cap A| + |A \cap B \cap C|$$

For larger number of sets we have:

$$|A_1 \cup A_2 \cup \dots A_n| = |A_1| + |A_2| + \dots + |A_n| - |A_1 \cap A_2| - |A_2 \cap A_3| - \dots - |A_{n-1} \cap A_n| + |A_1 \cap A_2 \cap A_3| + \dots + \dots$$

So positive for evens and negative for odds.

The above identity can be written as

$$|A_1 \cup A_2 \cup \ldots \cup A_n = \sum_{k=1}^{n} \sum_{a_i \neq a_j} (-1)^{k+1} |S_{a_1} \cap \ldots \cap S_{a_k}$$

In problem solving it is also an useful trick!

§6.2 Big Picture by Saad Bin Quddus

(This class is taught by following Yufei Zhao's *Cyclic Quadrilateral: The Big Picture Note.*) Here Saad vai started with Spiral Similarity. A very common trick in Olympiad Geometry. Then he went to the Miquels theorem for Triangle and Quadrilateral.

§6.2.1 Spiral Similarity

What is a spiral similarity. It is a special type of similarity which arise anturally. Spiral Similarity is a rotation with a dilation or homothety centered at a single point.

Lemma 6.2.1

Let AB and CD be segments, and suppose $X = AC \cap BD$. If (ABX) and (CDX) intersect again at O, then O is the center of the unique spiral similarity taking AB into CD.

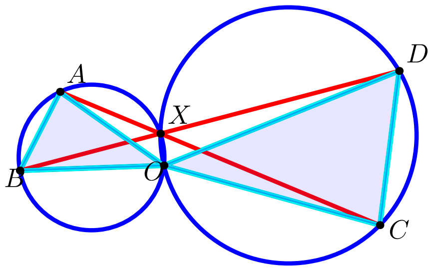


Figure 6.1: Spiral Similarity Lemma

You may wonder that spiral similarity comes in pairs. As the next proposition says:

Proposition 6.2.2

The center of spiral similarity takin AB to CD is also the center of the spiral similarity taking AC to BD.

§6.2.2 Miquel's Theorem

Theorem 6.2.3 (Miquel's Theorem)

Let ABC be a triangle and D, E, F eb the points on BC, CA, AB respectively. Then the circumcircles of the triangles AEF, BDF, CDE are concurrent.

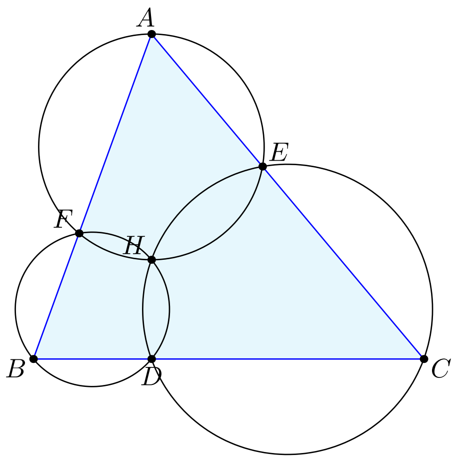


Figure 6.2: Miquel's Theorem on $\triangle ABC$.

Proof. Let $(BDF) \cap (CDE) = H$. Here we angle chase:

$$\angle EHF = \angle B + \angle C = 180 - \angle A.$$

done! Another aproah is :

$$\angle AFH = \angle HDB, \angle AEH = \angle HDC.$$

which sum to $180°$. □

Note that D, E, F can lie on the extension of the segments.

Here we are going to the Miquel's Quadrilateral Theorem which arise naturally.

Theorem 6.2.4 (Miquel's (Quadrilateral) Theorem)

The four circles $(PAB), (PDC), (QAD), (QBC)$ concur at the Miquel point M. Furthermore, M is the center of the spiral similarity sending AB to DC and BC to AD. (In particular, $\triangle MAB \sim \triangle MDC$ and $\triangle MBC \sim \triangle MAD$.)

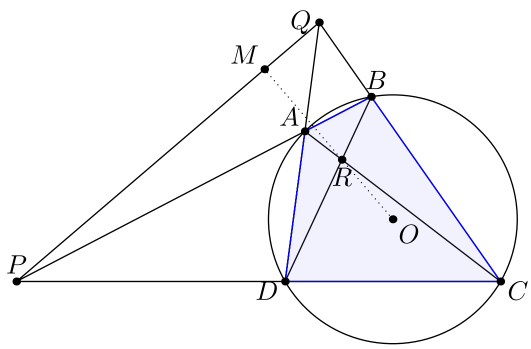


Figure 6.3: Miquel's Theorem in Complete Quadrilateral.

The above theorem is same as the theorem for triangle's. Just consider thriangle QDC and P, A, B on the corresponding segments!

Proof. Let M be the second intersection between (QAB) and (QCD) and by spiral similarity, M is the center of the spiral similarity taking AB to CD. SO, it is also the center of spiral similarity taking BC to DA. By converse direction of the lemma M lies on (PAD) and (ABC). □

Now we are going to see some properties of Miquel Point of a cyclic quadrilaral. It is known that *One of the most powerful configurations in olympiad geometry is the Miquel point when complete quadrilateral ABCD is cyclic.*

Theorem 6.2.5 (Miquel's Theorem on a Cyclic Quadrilateral)

Miquel's Point has more properties in a cyclic quadrilateral. Beacuse of the fact that, M is the inverse of R (intersection of the diagonals) with respect to inversion around $(ABCD)$.

- The six circles $(OAC), (OBD), (PAD), (PBC), (QAB), (QCD)$ goes through a single point i.e. M.
- M is the center of a spiral similarity taking AB to CD, as well as the spiral similarity taking BC to DA.
- M is the inverse of $R = AC \cap BD$ with respect to an inversion around $(ABCD)$. By Brocard's theorem, M is the foot of O onto PQ.
- $OM \perp PQ$.

These results also can be proved by angle chasing as well as spiral similarity.

§7 April 29, 2021

§7.1 Harder Divisibility by Atonu Roy Chowdhury

Prerequisities:

1. Residue System
2. Reduced Residue System
3. Fermat's Little Theorem(FLT: $a^{p-1} \equiv 1 \pmod{p}$ where $(a,p) = 1$) and Euler's Theorem($a^{\varphi(m)} \equiv 1 \pmod{m}$ where $(a,m) = 1$ and m is not necessarily prime).
4. Wilson's Theorem(p prime $\Leftrightarrow (p-1)! \equiv -1 \pmod{p}$)

All of these topics are covered in Basic Divisibility Class: section 1.2.

§7.1.1 Order

By Fermat's Little Theorem and Euler's Totient Function,

$$a^{\varphi(m)} \equiv 1 \pmod{m}$$

If we are going to calculate $a^1, a^2, a^3, \ldots, a^{\varphi(m)} \pmod{m}$ we find that, $a^n \equiv 1 \pmod{m}$ where $m < \varphi(m)$.

As an example $2^3 \equiv 1 \pmod{7}$ but $2^{\varphi(7)} \equiv 2^6 \equiv 1 \pmod{7}$

Here we find that 3 is more special than 6 in our example. Actually 3 is order of 2 modulo 7. Which is denoted by $\operatorname{ord}_7(2) = 3$.

Definition 7.1.1 (Order). $\operatorname{ord}_m(a) = \min\{x : a^x \equiv 1 \pmod{m}\}$

here a point to be noted that $\gcd(a,m) = 1$. If they aren't co-prime then no power of a wil be 1 modulo m. Which is left as an exercise for the readers.

Theorem 7.1.2 (Fundamental Theorem of Orders)

$\operatorname{ord}_m(a) = d$ then, $d|N \Leftrightarrow a^N \equiv 1 \pmod{m}$.

Let assume $N = dk$ and we know $a^d \equiv 1 \pmod{m}$ then, we have $a^{dk} \equiv 1 \pmod{m}$.

Assume for the sake of contradiction $d \not| N \implies N = dq + r$ such that $0 < r < d$. Now, $a^d \equiv 1 \pmod{m}$. as d is the order. Then we have $a^{dq} \equiv 1 \pmod{m} \implies a^N = a^{dq+r} \equiv 1 \cdot a^r \pmod{m}$

$$\implies a^r \equiv 1 \pmod{m}$$

which is a contradiction as r can't be the order as $r < d$.

Here, we learn:

1. $d \mid \varphi_(m)$ which means $d \in \{\text{divisorsof}\varphi_(\text{m})\}$
2. $a^x \equiv a^y \pmod{m} \Leftrightarrow x \equiv y \pmod{d}$ where $\gcd(m, n) = 1$. WLOG, $x \geq y$ so, $a^{x-y} \equiv 1 \pmod{m}$ then, $d \mid x - y$ and then we get $x \equiv y \pmod{d}$.

Example 7.1.3

Given that $\gcd(a, m) = 1$. Prove that $n \mid \varphi(a^n - 1)$.

Let, $N = a^n - 1$, so, $n \mid \varphi(N)$ and $\text{ord}_N(a) \mid \varphi(N)$

So, we have to show that $a^n \equiv 1 \pmod{N}$

Assume for the sake of contradiction that, $k < n$ then we have, $a^k \equiv 1 \pmod{N} \implies N \mid a^k - 1$

But, which means, $a^k - 1 \geq N = a^n - 1$

Contradiction as we assumed that $k < n$.

Example 7.1.4

Find all n $n \mid 2^n - 1$.

Here we find that n must be odd and $n = 1$ works. We let $n = 2k + 1$, so, $2k + 1 \mid 2^{2k+1} - 1$

Here we will use a lemma.

Lemma 7.1.5

If $a^x \equiv 1, a^y \equiv 1$ all are taken modulo m. Then we have $a^{\gcd(x,y)} \equiv 1 \pmod{m}$

Let, p be the smallest prime factor of n (this trick is called the smallest prime factor(spf trick) of n)

$d = \text{ord}_p(2) \implies d \mid \varphi(p) = p - 1$ By FLT, $p \mid n \mid 2^n - 1 \implies 2^n \equiv 1 \pmod{p} \implies d \mid n$

.

But then,

$$d \mid p - 1, \quad d \mid n$$

which is a contradiction!

§7.1.2 Primitive Root

Definition 7.1.6. Let g is a positive integer and $\gcd(g, n) = 1$. Then we shall call g "Primitive Root modulo m" if $\text{ord}_m(g) = \varphi(m)$.

As an example, $\gcd(3, 7) = 1$, $3^6 \equiv 1 \pmod 7$. We also know that $\varphi(7) = 6$. So, we can say that 3 is a primitive root modulo 7.

Theorem 7.1.7 (Primitive Root)

Let, p be a prime. Then $\exists g \in \{1, \ldots, p-1\}$ such that g is a primitive root modulo p.

> **Remark 7.1.8.** $\{1, \ldots, p-1\}$ is the reduced residue system of p denoted by $RRS(p)$.

Usage and Properties of Primitive Root:

Property 1. If g is a primitive root modulo m and $\varphi(m)$ is even then,$g^{\varphi(m)/2} \equiv -1 \pmod m$.

Let, $\varphi(m) = 2n$ So we have,

$$g^{2n} \equiv 1 \pmod m \implies m \mid g^{2n} - 1 = (g^n + 1)(g^n - 1)$$

Which means, $m \mid g^n + 1$ or $m \mid g^n - 1$. So we have, $g^n \equiv -1$ or $g^n \equiv +1$ modulo m.

Now, AFTSOC (Assume for the sake of contradiction) that $g^n \equiv 1 \pmod m$ Then, $\varphi(m) = \text{ord}_m(g) \le n$

But now we get $2n \le n$ which is absurd.

Property 2. $S = \{g, g^2, g^3, \ldots, g^{\varphi(m)}\}$ is $RRS(m)$ where g is primitive root modulo m.

§7.1.3 Wilson's Theorem

Theorem 7.1.9 (Wilson's Theorem)

If p is a prime then $(p-1)! \equiv -1 \pmod p$.

You can find a proof from Brilliant.org

Problem 7.1.10. Let p be an odd prime. Find all k such that

$$p \mid 1^k + 2^k + 3^k + \ldots + (p-1)^k$$

Here solving the above problem, you assume that you don't know any formula.

✠8 April 30, 2021

The Combinatorics Exam of The National Camp. Problems are given below:

BGD TSTST Problem 1. You have a set S of 19 points in the plane such that given any three points in S, there exist two of them whose distance from each other is less than 1. Prove that there exists a circle of radius 1 that encloses at least 10 points of S.

BGD TSTST Problem 2. There are 2021 stones in a pile. At each step, Lazim chooses a pile with at least two stones, splits it into two piles, and multiplies the sizes of the resulting two piles. He keeps doing this until there are 2021 piles each containing exactly one stone. Finally, he adds up all the products he has obtained during the process and ends up with the number N. Find, with proof, all the possible values of N.

BGD TSTST Problem 3. Show that for all positive integers $n \geq 2$, you can cut any quadrilateral into n isosceles triangles.

BGD TSTST Problem 4. Let $n \geq 1$ be an integer. A non-empty set is called "good" if the arithmetic mean of its elements is an integer. Let T_n be the number of good subsets of $\{1, 2, 3 \ldots, n\}$. Prove that for all integers n, T_n and n leave the same remainder when divided by 2.

BGD TSTST Problem 5. We place some checkers on an $n \times n$ checkerboard so that they follow the conditions:

- every square that does not contain a checker shares a side with one that does;
- given any pair of squares that contain checkers, we can find a sequence of squares occupied by checkers that start and end with the given squares, such that every two consecutive squares of the sequence share a side.

Prove that at least $(n^2 - 2)/3$ checkers have been placed on the board.

✠9 May 1, 2021

§9.1 Length Chase by Raiyan Jamil

§9.1.1 Ceva's and Menelaus's Theorem

A line through a vertices connecting a point on the opposite side of a vertex is called a **cevian**.

Three cevian may concurrent or not. It is detremined my the ceva's theorem.

Theorem 9.1.1 (Ceva's Theorem)

Let D, E, F be arbitrary points on the line BC, CA, AB. AD, BE, CF are concurrent if and only if

$$\frac{BD}{DC} \cdot \frac{CE}{EA} \cdot \frac{AF}{FB} = 1.$$

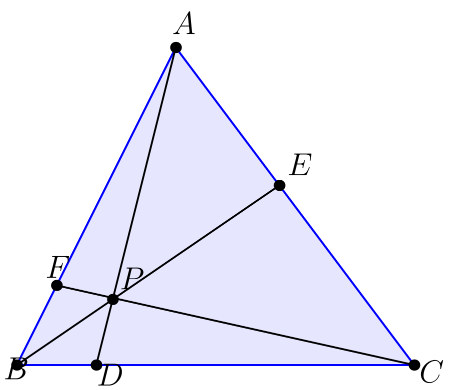


Figure 9.1: Ceva's Theorem

You can prove the formula using areal ratios.

Theorem 9.1.2 (Menelaus's Theorem)

Let D, E, F be arbitrary points on the line BC, CA, AB. D, E, F are collinear if and only if

$$\frac{BD}{DC} \cdot \frac{CE}{EA} \cdot \frac{AF}{FB} = -1.$$

where the distances are directed.

Same as above.

§9.1.2 Trigonometric Ceva's Theorem

Theorem 9.1.3 (Trigonometric form of Ceva's Theorem)

Let D, E, F be arbitrary points on the line BC, CA, AB. AD, BE, CF are concurrent if and only if

$$\frac{\sin \angle BAD}{\sin \angle DAC} \cdot \frac{\sin \angle CBE}{\sin \angle EBA} \cdot \frac{\sin \angle ACF}{FCB} = 1.$$

For proving the formula, you have to use the fact that $\triangle ABC$ has area $= \frac{1}{2} AB \cdot AC \sin BAC$.

§9.1.3 Isotomic Conjugate

Let D be a point on the line BC and M eb the midpoint o the line segment. M' be the reflection of D over M. Then, AD' is called the isotomic of AD.

Theorem 9.1.4 (Isotomic Conjugate)

Let AD, BE, CF are concurrent cevians of a triangle ABC. Then the isotomics AD', BE', CF' are also concurrent. The point of concurrency is called the Isotomic Conjugate of the first one.

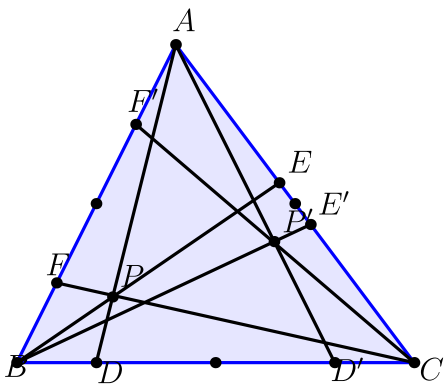


Figure 9.2: Isotomic conjugate P'.

§9.1.4 Isogonal Conjugate

Let AD be a cevian of ABC. Angle bisector of $\angle BAC$ is AI. Then, the reflection of the line AD over AI is called the isogonal of AD.

Theorem 9.1.5 (Isogonal Conjugate)

Let AD, BE, CF are concurrent cevians of a triangle ABC. Then the isogonals AD', BE', CF' are also concurrent. The point of concurrency is called the Isogonal Conjugate of the first one.

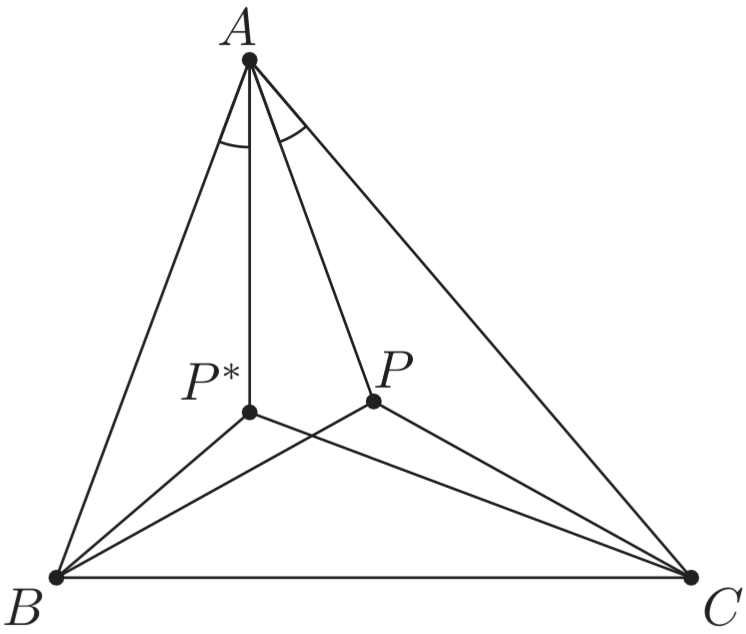


Figure 9.3: Isogonal Conjugate of P.

§9.1.5 Projective Plane

Here is a long discussion.

I write in a brief.

The summary of the discussion is:

1. There are infinitely many points at infinity.
2. There is exactly 1 line at infinity.
3. All points at infinity lie on the line at infinity.

$$\textbf{Projective Geometry} = \textbf{Euclidean Geometry} + \textbf{point at } \infty + \textbf{line at } \infty$$

There is an another perspective.

Line at infinity is a circle with radius ∞ which goes htrough all the points at infinity.

✠10 May 2, 2021

§10.1 Quadratic Residue and Diophantine Equation by Atonu Roy Chowdhry

§10.1.1 Quadratic Residue

(Note: here *qr* means quadratic residue)

Definition 10.1.1 (Quadratic Residue). a is called quadratic residue modulo n if $\exists x : x \equiv a \pmod{n}$.

Definition 10.1.2 (Quadratic Residue Class). $qr(n) = \{a : a \text{is a qr in mod} n\}$.

As an example $qr(5) = \{0, 1, 4\}$.

Theorem 10.1.3

If -1 is a qr in mod p where p is an odd prime. Then, $p \equiv 1 \pmod{4}$.

AFTSOC, $p \equiv -1 \pmod{4}$ or $p = 4k - 1$. So $\exists x : x^2 \equiv -1 \pmod{p}$.

$$x^{p-1} \equiv 1 \pmod{p} \text{ By FLT}$$

$$\implies x^{4k-2} \equiv 1 \pmod{p}$$

$$\implies (x^2)^{2k-1} \equiv 1 \pmod{p}$$

$$\implies (-1)^{2k-1} \equiv 1 \pmod{p}$$

$$-1 \equiv 1 \pmod{p}$$

which is absurd.

The converse of the above theorem is also true.

Theorem 10.1.4

If $p \equiv 1 \pmod{4}$ is a prime then -1 is a quadratic residue mod p

The proof is constructive...

§10.1.2 Legendre's Formula

Definition 10.1.5 (Legendre Symbol).

$$\left(\frac{n}{p}\right) = \begin{cases} 0 & p \mid n \\ 1 & n \in qr(p) \\ -1 & n \notin qr(p) \end{cases}$$

Theorem 10.1.6

$$a^{\frac{p-1}{2}} \equiv \left(\frac{a}{p}\right) \pmod p$$

Lemma 10.1.7

$$\left(\frac{ab}{p}\right) = \left(\frac{a}{p}\right)\left(\frac{b}{p}\right)$$

The meaning of the above lemma is if a, b are both qr then ab is also qr.

If a, b both are not qr then ab is a qr.

But, if only one of them is qr, then, ab is not qr.

Lemma 10.1.8

$$\left(\frac{-1}{p}\right) = \begin{cases} -1 & p = 4kk + 1 \\ 1 & p = 4k - 1 \end{cases}$$

Lemma 10.1.9

$$\left(\frac{2}{p}\right) = (-1)^{\frac{p-1}{8}}$$

Lemma 10.1.10

$$\left(\frac{p}{q}\right)\left(\frac{q}{p}\right) = (-1)^{\frac{p-1}{2}} \cdot (-1)^{\frac{q-1}{2}}$$

Techniques: Whenever you see squares you shoul take moulo 2^n.

§10.1.3 Diophantine Equation

Here we are going to solve some diophantine equation problems (i.e. problems asking for integer solutions)

Example 10.1.11

$d \neq 2, 5, 13$, $S = \{2, 5, 13, d\}$. Prove that, $\exists a, b \in S$ such that $ab - 1 \neq k^2$

Here you have to show that there is no such d that satisfies all the equations:

$$2d - 1 = x^2$$
$$5d - 1 = y^2$$
$$13d - 1 = z^2$$

AFTSOC, exists such d. First take mod 4,

$qr(4) = \{0, 1\}$

So, $2d - 1 \pmod 4 \in \{0, 1\}$ Here, $2d - 1$ doesn't congruent to 0 modulo 4.

So, $2d - 1 \equiv 1 \pmod 4 \implies d \equiv 1 \pmod 2$

But, then mod 4 and mod 8 aren't useful. Then take mod 16. Then some exercise left for the readers.

Example 10.1.12

Find all solutions to the equation:

$$x^3 + y^4 = 7$$

Here we need to find a prime p such that $3|p - 1$ and $4|p - 1$. $p = 13$ is a good choice.

So we work with mod 13. We get: $x^3 \pmod{13} = \{0, 1, 5, 8, 12\}$ and $y^4 \pmod{13} = \{0, 1, 3, 9\}$.

But no such summation of two elements from the sets is equal to 7. So, there is n such solution.

Example 10.1.13

Find all solutions to the equation:

$$x^5 - y^2 = 4$$

Here the magical mod is 11. We get $x^5 \pmod{11} = \{0, 1, -1\}$. And $y^2 = x^5 - 4 \pmod{11} = \{6, 7, 9\}$

But quadratic residue $\pmod{11} = \{0, 1, 4, 9, 5, 3\}$.

So, there is no such solution.

✠11 May 4, 2021

§11.1 Advanced Theorems in Geometry by Raiyan Jamil

Here we aer going to learn some advanced theorems in geometry which are mostly belong to Projective Geometry.

- Desargues's Theorem
- Pascal's Theorem
- Pappu's theorem
- Brianchon's Theorem
- Butterfly Theorem

§11.1.1 Desargues's Theorem

Theorem 11.1.1 (Desargues's theorem)
$\triangle ABC$ and $\triangle XYZ$ are such that $AB \cap XT = U, BC \cap YZ = V, CA \cap ZX = W$ then, X, Y, Z are collinear if and only if AX, BY, CZ are concurrent.

Here we call that ABC and XYZ are perspective from a line if U, V, W are collinear and the line is called the line of perspectivity.

And if AX, BY, CZ are concurrent then we say, ABC and XYZ are persepctive from a point.

But, the Desargues's Theorem establishes a realtion between these two perspectivity which is useful in problem solving. As, concurrency proof can be given using collinearity. It is really a very useful theorem.

§11.1.2 Pascal's Theorem

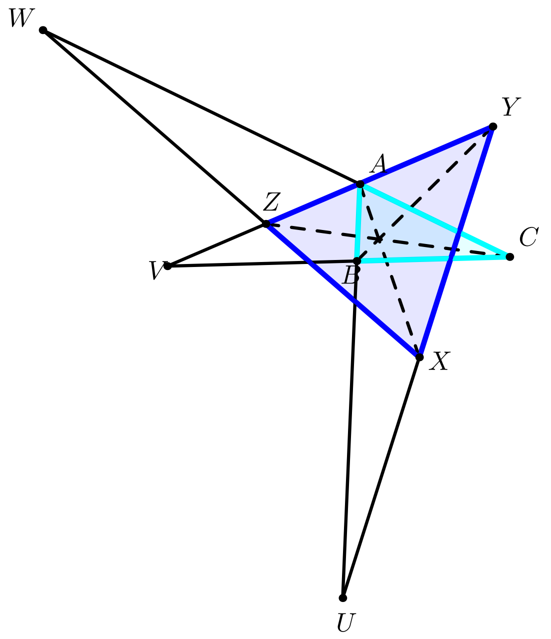


Figure 11.1: The Desargues' Theorem

Theorem 11.1.2 (Pascal's Theorem)

If hexagon $ABCDEF$ lies on a circle then $AB \cap DE = X, BC \cap EF = Y, CD \cap FA = Z$ are collinear.

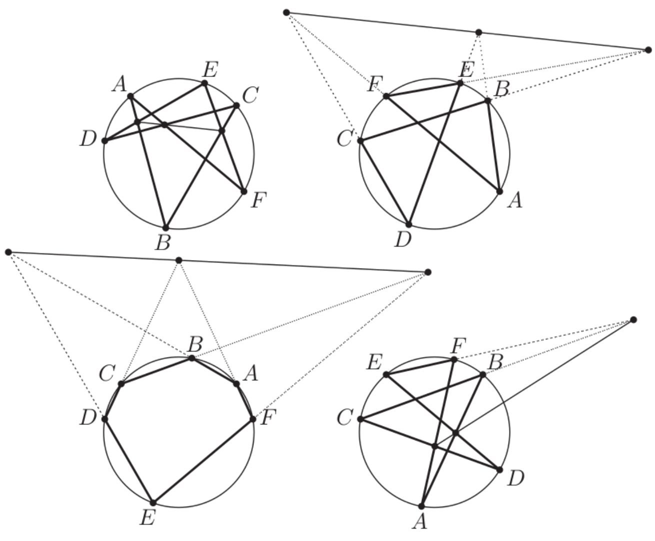


Figure 11.2: Many Faces of Pascal's Theorem (adapted from Evan Chen's EGMO)

> **Remark.** If X, Y, Z are collinear then you can not say that $ABCDEF$ lies on a circle.

Pascal's Theorem is most useful of these five theorem. It can be applied to as well as triangles, quadrilaterals and pentagons. Where as an example we apply Pascal's on $AABBCC$ we get $AA \cap BC$ $AB \cap CC$ and $BB \cap CA$ are collinear where AA means the tangent to the circumcircle at A, and so on.

So, it seems very useful in different problems containing triangles, quadrilaterals, pentagons and hexagons.

§11.1.3 Pappu's theorem

Theorem 11.1.3 (Pappu's Theorem)

A, B, C, D, E, F are six poins on the plane. Let $AB \cap DE = X, BC \cap EF = Y, CD \cap FA = Z$. Then, A, C, E and B, D, F are collinear if and only if X, Y, Z are collinear.

You may wonder that, Problem 2 of IMO 2019 can be solved using Pappu's Theorem along with some other facts.

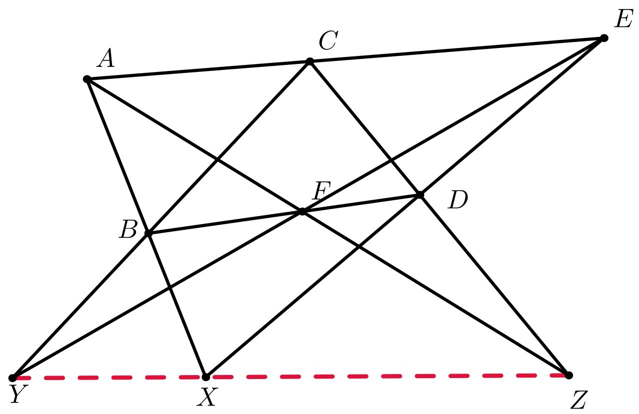


Figure 11.3: Pappu's Theorem

§11.1.4 Brianchon's Theorem

Theorem 11.1.4 (Brianchon's Theorem)

$ABCDEF$ is a tangential hexagon (i.e. Sides of the hexagon are externally tangent to a common circle). Then, AD, BE, CF are concurrent.

Brianchon's Theorem can be derived directly from Pascal's Theorem by only interchanging the words 'points' and 'line', and making whatever grammatical adjustments that are necessary.

Brianchon's and Pascal's theorem form Pole Polar duality of Projective Geometry. Point to be noted that, we can take C, D, E collinear, then the polygon becomes a pentagon. We also can take A, B, C and D, E, F collinear, then the polygon becomes a tangential quadrilateral.

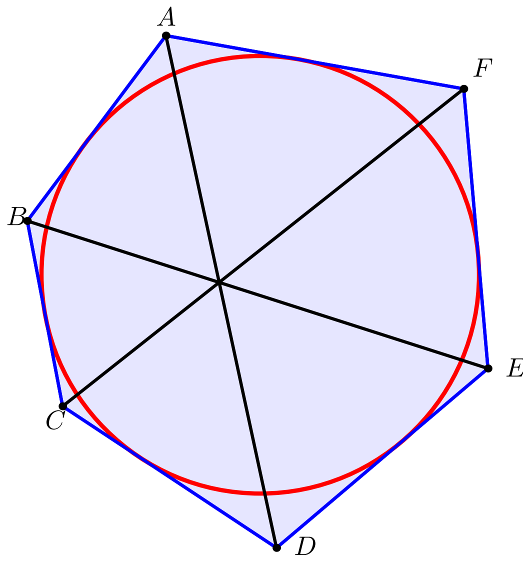


Figure 11.4: Brianchon's Theorem

Here, B, E become point of tangency. Let, CD and FA touches the circle at G, H then, AD, CF, BE, GH all are concurrent.

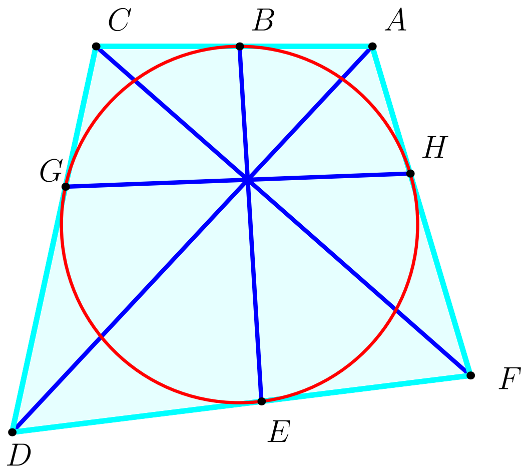


Figure 11.5: Brianchon's Theorem on a quadrilateral.

§11.1.5 Butterfly Theorem

Theorem 11.1.5 (Butterfly Theorem)

AB be a chord of a circle with midpoint M. Let two chords through M of the circle are CD and EF. $CE \cap AB = X$ and $DF \cap AB = Y$. Then, $MX = MY$.

The Theorem is also tru if the chord is not a chord of the circle i.e. the line lies outside the circle, as the next theorem says.

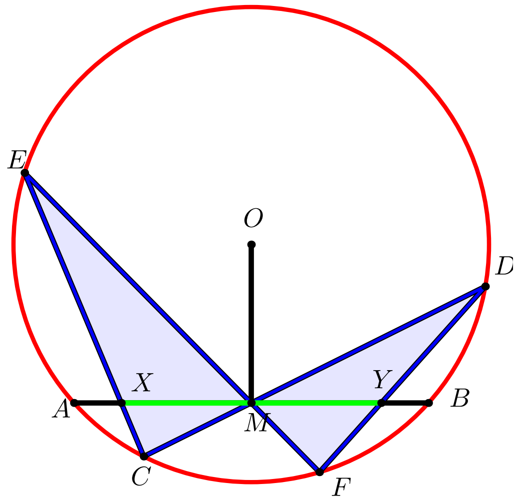


Figure 11.6: The butterfly theorem, look polygon $CEFD$ looks like a butterfly!

Theorem 11.1.6 (Extended Butterfly Theorem)

Let ℓ be a line on the plane of a circle ω. O is the center of the circle. Let M be a point on ℓ such that $OM \perp \ell$. Let two lines through M intersects the circle at C, E and D, F respectively. Let DE and CF meet ℓ at B, A respectively. And CD and EF meet ℓ at H, G respectively. Now, $AM = BM$ and $GM = HM$.

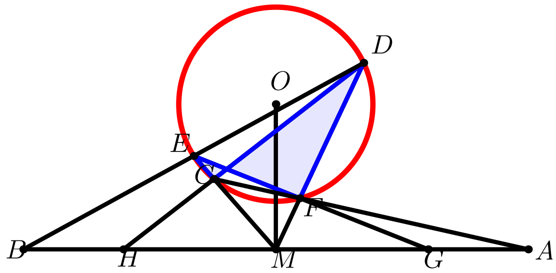


Figure 11.7: Extended Butterfly Theorem

✠12 May 6, 2021

The Number Theory Exam of The National Camp. Problems are given below:

BGD TSTST Problem 6. Let N be an integer. Given any a, b such that $\gcd(a, b, N) = 1$. Prove that you can find m, n such that $(m, n) = 1$ and $N \mid m - a, N \mid n - b$.

BGD TSTST Problem 7. Let p be a prime number. We call a subset S of $\{1, 2, \ldots, p-1\}$ "good" if it satisfies the property that for every $x, y \in S$, $xy \pmod p$ is also in S. How many "good" sets are there?

BGD TSTST Problem 8. Let $P(x)$ be a nonzero integer polynomial, that is, the coefficients are all integers. We call a prime q "interesting" if there exists some natural number n for which $q|2^n + P(n)$. Prove that there exist infinitely many "iner- esting" primes.

§13 May 7, 2021

§13.1 Inversive & Projective Geometry by Saad Bin Quddus

§13.1.1 Inversion

An inversion wrt a circle send a point(A) inside to a point(A^*) outside the circle such that $OA \cdot OA^* = r^2$, where r is the radius of the circle.

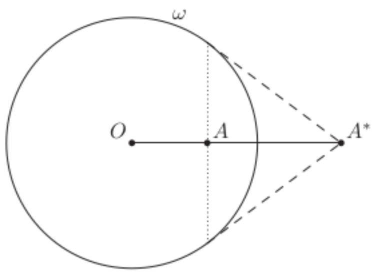


Figure 13.1: A^* is the inverse of A with respect to ω.

Remember that O, A, A^* lie on a line but O doesn't lie between A and A^*.

An interesting result about inversion is if A^*, B^* are the inverse of A, B respectively then A, B, B^*, A^* are concyclic. Inverse of a circle with respect to circle ω (intersecting ω at A, B)

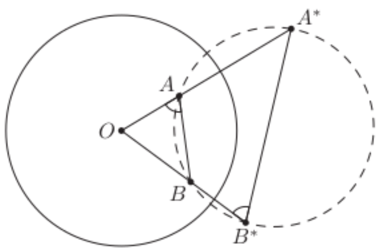


Figure 13.2: A cyclic quadrilateral

is a line through A, B.

Remember that the inverse of the center with respect to ω is a point at infinity.

Also another fact that two circle orthogonal to each other are overlaying with respect to the other circle.

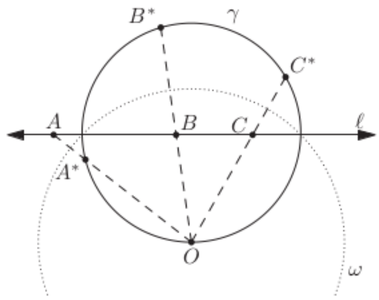


Figure 13.3: A circle inverts to a line and vice-versa

§13.1.2 Projective Geometry

> **Theorem 13.1.1** (La Hire's Theorem)
>
> A point X lies on the polar of a point Y if and only if Y lies on the polar of X.

Harmonic Division Let four points A, C, B, D lie on a line in that order. These points are called harmonic if $\frac{AC}{BC} \div \frac{AD}{BD} = -1$ where the lengths are directed. And denoted by $(A, B; C, D) = -1$

We can solve lots of problems with this, litteraly.

Pencil Let four collinear points are A, B, C, D and another line ℓ. An another point(not neccessarily distinct) P. Line through P connecting A, B, C, D intersects ell at A', B', C', D' respectively. Then

$$(A, B; C, D) = (A', B'; C', D')$$

So their cross ratio remain same!

> **Lemma 13.1.2** (Cevian Induces Harmonic Bundle)
>
> Let AD, BE, CF are concurrent cevians, $EF \cap BC = G$ then, $(B, C; D, G) = -1$

> **Lemma 13.1.3** (Midpoints and Parralel Lines)
>
> Given points A and B, let M be the midpoint of AB and P_∞ the point at infinity of line AB. Then $(A, B; M, P_\infty)$ is a harmonic bundle.

> **Proposition 13.1.4** (Harmonic Quadrilateral)
>
> $ABCD$ cyclic quadrilateral and $AC/BC = AD/BD$ then $ABCD$ is called harmonic quadrilateral.

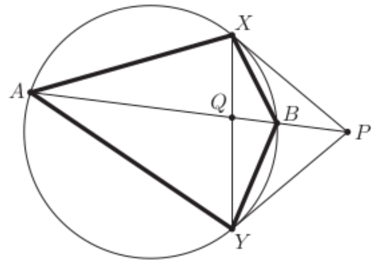


Figure 13.4: Here $AXBY$ is a harmonic quadrilateral

Harmonic Quadrilateral has many nice and cute properties:

(a) If tangent at B and D meet at T then, A, C, T are collinear. The intersection of the diagonals (S) is also collinear with A, C, T.

(a) S and T are inverse of each other with respect to $(ABCD)$.

(a) AC is an A-Symmedian of DAB and C-Symmedian of BCD. Analogous for BC.

Lemma 13.1.5 (Right Angles and Bisectors)

Let X, A, Y, B be collinear points in that order and let C be any point not on this line. Then any two of the following conditions implies the third condition.

i $(A, B; X, Y)$ is a harmonic bundle.

ii $\angle XCY = 90°$.

iii CY bisects $\angle ACB$.

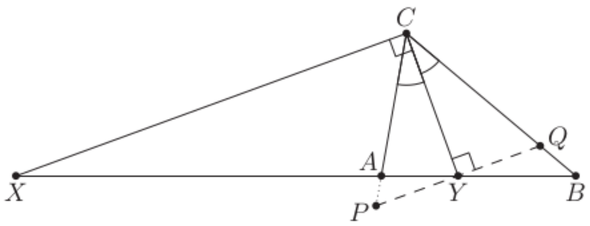


Figure 13.5: CX and CY are external and internal angle bisectors.

Lemma 13.1.6

$(A, B, C, D) = -1$ and M is the midpoint of AB, then

- $MA^2 = MB^2 = MC \cdot MD$.
- $DA \cdot DB = DC \cdot DM$.

Theorem 13.1.7 (Brocard's Theorem)

Let $ABCD$ be an arbitrary cyclic quadrilateral inscribed in a circle with center O, and set $P = AB \cap CD, Q = BC \cap DA$, and $R = AC \cap BD$. Then P, Q, R are the poles of QR, RP, PQ, respectively. In particular, O is the orthocenter of triangle PQR.

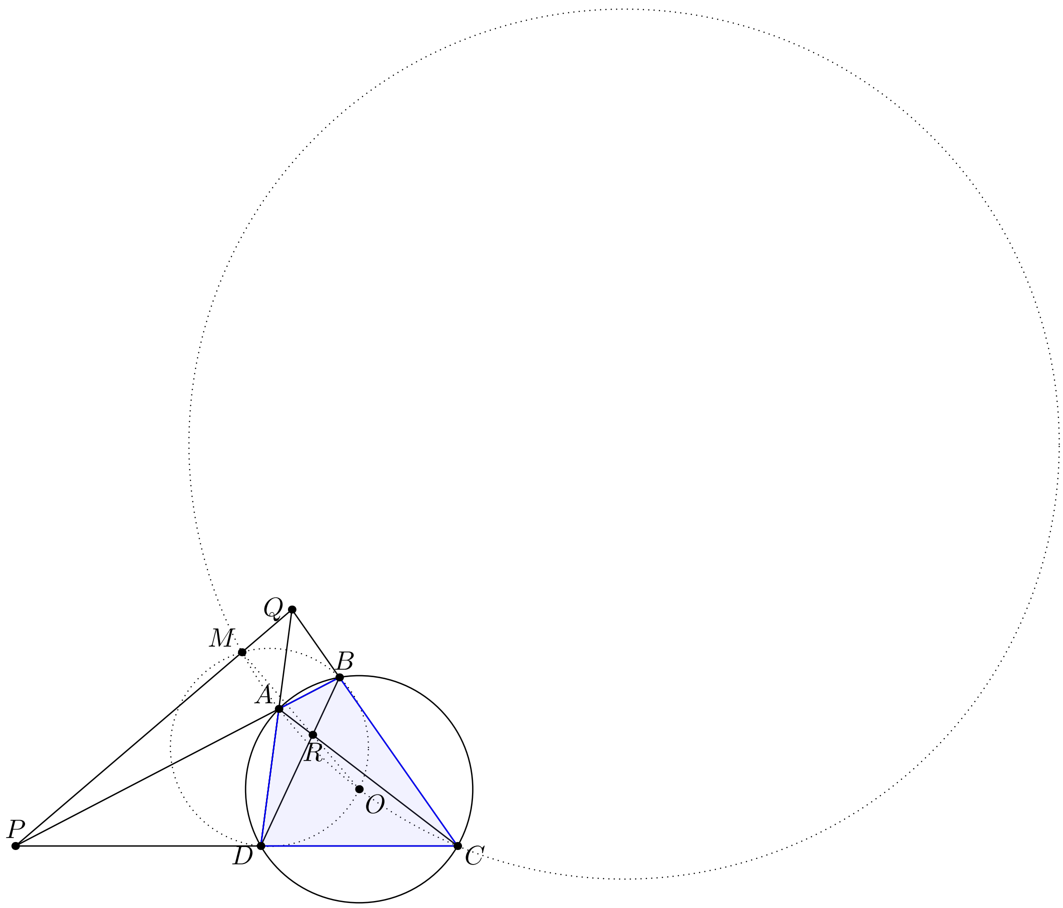


Figure 13.6: $(OAMC)$ and $(OBMD)$ are the inverses of AC and BD respectively.

Here we see that R is the inverse of M. So, O, R, M are collinear.

And consequently, PQ is the polar of R.

We shall prove that PR is polar of Q and QR is polar of P.

$Q, R \in$ polar of P So, we have from La Hire's Theorem that P belongs to polar of both Q, R.

Then, join Q, R and they intersect the circle and AB, CD at four points and then doing some harmonic bundle chase gives the desired result and left as an exercise!

§13.2 Algorithm by Ahsan Al Mahir

(We followed the note *Algorithms* by Cody Johnson from France IMO Training Camp 2015. This note is a great resource for further reading.) An algorithm is a set of steps to perform a procedure.

You may know the **Binary Search Algorithm**.(the number guessing game is a game in which your opponent thinks of a integer n on an interval $[a, b]$, and you try to guess his number with the rule that after every guess he must tell you if your guess was correct, too high, or too low. you can win this game by at most $\log_2(b - a + 1)$ guesses.)

§13.2.1 Greedy Algorithms

The greedy algorithm is an algorithm that chooses the optimal choice in the short run. It arises naturally. You can solve many of the problems appear in various olympiads by greedy-approch.

Example 13.2.1 (Binary Number System)

Prove that every positive integer can be written uniquely as the sum of one or more distinct powers of 2.

Here, we take the highest power of 2 (say m) less than or equal to the integer n. Then, apply the algorithm to the number $(n - m)$. And consequntly we are done! (by strong induction)

Example 13.2.2 (Zeckendorf's Theorem)

Prove that every positive integer can be written uniquely as the sum of one or more Fibonacci numbers, no two of which are consecutive Fibonacci numbers.

Here, work similarly a sthe above example, lsrgest power of 2 replaced by the largest Fibonacci number less than or equal to n.

Here, we comes to a graph coloring problem. Algorithms are hugely applied in graph theoretic problems especially in graph coloring.

Example 13.2.3

Let $\triangle$ be the maximum degree of the vertices of a given graph. Devise a method to color this graph using at most $\triangle + 1$ colors such that no two neighboring vertices are of the same color.

We shall use the following greedy algorithm: for each vertex, we shall color it with any color that has not been used by any of its neighbors. Since each vertex has at most $\triangle$ neighbors, at least one of the $\Delta+1$ colors has not been used, so such a color will always exist. Thus, we are done.

§13.2.2 Reduction Algorithms

Algorithms can be used to reduce a complex configuration to a simple one while preserving its combinatorial function in the problem.

Example 13.2.4 (Cody Johnson)

Consider an ordered set S of 6 integers. A move is defined by the following rule: for each element of S, add either 1 or -1 to it. Show that there exists a finite sequence of moves such that the elements of the resulting set, $S' = (n_1, n_2, \ldots, n_6)$, satisfy $n_1n_5n_6 = n_2n_4n_6 = n_3n_4n_5$.

Here show that, we can reduce all the elements to noly 0 and 1. Now it is easy to tackle the problem. Then you can assume for the sake of contradiction that the products are not equal. After this some case works solve the problem.

Example 13.2.5 (Canada MO)

Let $n \times n$ be grid of squares. Their is some barricades such that none of the squares are isolated. There is two robots arbitrarily placed on two square. You can perform up, down, left, right commands to control the robots but it is simutaneous. Prove that it is possible to take 2 robots at the lower left corner of the grid.

Here are two ideas to solve it.

First one is to take the robot which is furthest from the lower left square, then take it to the rquired square. And then the other.

Another approach is to show that, we can restrict (or take) two robots at a single square sometime. Then we are done by giving the commands U,R,L,D.

§13.2.3 Invariant and Monovariant

See section 2.2. This class covered invariants and mnonovariants.

✠14 May 9, 2021

The Geometry Exam of The National Camp. Problems are given below:

BGD TSTST Problem 9. Let $\triangle ABC$ be a triangle inscribed in a circle ω. D, E are two points on the arc BC of ω not containing A. Points F, G lie on BC such that

$$\angle BAF = \angle CAD \text{and } \angle BAG = CAE$$

Prove that the two lines DG and EF meet on ω.

BGD TSTST Problem 10. ABC is a triangle where $\angle BAC = 90°$. A line through the midpoint D of BC meets AB at X and AC at Y . The point P is taken on XY such that PD and XY have the same midpoint M. The perpendicular from P to BC meets BC at T .

Prove that AM bisects $\angle TAD$.

BGD TSTST Problem 11. Let ABC be a triangle with BC being the longest side. Let O be the circumcenter of ABC. P is an arbitrary point on BC. The perpendicular bisector of BP meet AB at Q and the perpendicular bisector of PC meet AC at R. Prove that $AQOR$ is cyclic.

After solving all of the three problems above, you may try this bonus problem. Beware though, any work done on Problem 4 with incomplete solutions of the first three won't receive any points.

BGD TSTST Problem 12. Let ABC be a triangle with circumcircle (O). The midpoints of BC, CA, AB are A', B', C' respectively. The medians AA', BB', CC' cut the circumcircle (O) at $A, A_1; B, B_1; C, C_1$ respectively. The line of tangency to (O) at A_1 meets the perpendicular to AO through A at X. Define Y, Z similarly. Prove that X, Y, Z are collinear.