IMONST 2 (2020)
Reading Material

IMO ∞
0 NST

International Mathematical Olympiad
National Selection Test
MALAYSIA

Malaysia IMO Committee
contact@imo-malaysia.org

Contents

Version

Version 1.1 (author: M. Syafiq Johar), updated on 29 September 2020.

1 Principles of Mathematical Induction

The principle of mathematical induction is an important technique in proofs. Before we describe this principle, let us have give a brief discussion on mathematical proofs.

1.1 Mathematical Proofs

The essence of mathematics is proofs. The nature of mathematics is to provide a logical evidence to some phenomena. Usually this phenomena is observed via patterns. From this observation, we may then formulate a guess or a conjecture on what the general behaviour would be. To assert the truth of this guess or conjecture, we have to provide a mathematical proof by a series of implications. Arithmetic and calculations are mostly the language used to reach to this end goal.

In IMONST1, the contestants' abilities in making a conjecture, using arithmetic, and calculation were tested. In IMONST2, students are expected to be able to write proofs, which also includes the abilities tested in IMONST1. Let us give an example to the whole process as outlined above:

Example 1.1. Let n be a positive integer. Consider the sum $S(n) = 1 + 2 + 3 + \ldots + n$. Wee would like to find a general formula for this sum in terms of n. First, let us make some observation for small cases:

$$\begin{aligned}
S(1) &= 1, \\
S(2) &= 1 + 2 = 3, \\
S(3) &= 1 + 2 + 3 = 6 = 2 \times 3, \\
S(4) &= 1 + 2 + 3 + 4 = 10 = 2 \times 5, \\
S(5) &= 1 + 2 + 3 + 4 + 5 = 15 = 3 \times 5, \\
S(6) &= 1 + 2 + 3 + 4 + 5 + 6 = 21 = 3 \times 7, \\
&\vdots
\end{aligned}$$

If we continue this to any number, we can see that this sum looks like:

$$\text{Guess: } S(n) \overset{?}{=} \frac{n(n+1)}{2}.$$

At this stage, this is only a guess because we have not proven it for a general number n. We have only seen that this is true for the small cases $n = 1, 2, 3, 4, 5, 6$. We now need to mathematically show that the guess for $S(n)$ is true for any positive integer n. Of course, there are many different ways to proof this statement. We shall show a direct proof here. Note that we can rearrange the terms in $S(n)$ in any way we like since addition can be done in any order. Thus we can write $S(n)$ in two different ways:

$$S(n) = 1 + 2 + 3 + 4 + 5 + \ldots + n, \tag{1}$$

$$S(n) = n + (n-1) + (n-2) + (n-3) + (n-4) + \ldots + 1, \tag{2}$$

where the second expression is obtained by simply reversing the order of addition. Note that the number of terms in both of the expressions for $S(n)$ remains the same.

Now comes another observation. If we add the first terms of the equations (1) and (2), we would get $1 + n$. Similarly, if we add the second terms of the equations (1) and (2), we would get $2 + (n-1) = 1 + n$ as well. This remains true for the other terms as well. Thus, if we add the two equations together, we would get:

$$(1) + (2) : S(n) + S(n) = \underbrace{(n+1) + (n+1) + \ldots + (n+1)}_{n \text{ times}},$$

which then simplifies to $2S(n) = n(n+1)$. Dividing both sides of this equation with 2 implies the formula that we have before: $S(n) = \frac{n(n+1)}{2}$ for any positive integer n.

This is a valid proof because we worked in a general setting.

In the proof above, we used a series of logical arguments to get to the end product. Note a language that we used above: "implies". This means that we are making a logical argument. We had two statements $2S(n) = n(n+1)$ and $S(n) = \frac{n(n+1)}{2}$ and they are connected by a logical argument, namely:

$$2S(n) = n(n+1) \text{ implies } S(n) = \frac{n(n+1)}{2}. \tag{3}$$

This means that the second statement follows from or is a result of the first one. Essentially, a mathematical proof is a chain of implications like this: we start with what we are given or knows to be true, and logically argue sequentially with implications until we get to the desired result. Usually, mathematicians write a symbol $\Rightarrow$ to denote this implication process. This saves a lot of time and is clearer to read. So the statement (3) can also be written as:

$$2S(n) = n(n+1) \Rightarrow S(n) = \frac{n(n+1)}{2}. \tag{4}$$

Let us look at another example of proof using this new notation that we have seen.

Example 1.2. Let us find the possible remainders when we divide a perfect square by 4. We note that a perfect square is a square of any integers. So the list of perfect squares and their remainders upon division by 4 are:

$$\begin{aligned}
0^2 &= 0 \text{ leaves a remainder of } 0,\\
1^2 &= 1 \text{ leaves a remainder of } 1,\\
2^2 &= 4 \text{ leaves a remainder of } 0,\\
3^2 &= 9 \text{ leaves a remainder of } 1,\\
4^2 &= 16 \text{ leaves a remainder of } 0,\\
5^2 &= 25 \text{ leaves a remainder of } 1,\\
&\vdots
\end{aligned}$$

and we can see that for small cases the remainder is either 1 or 0. So this is our guess:

Guess: when we divide a perfect square by 4, we will get a remainder of 0 or 1.

Now let us write a proof of this using the implication sign above:

$$\begin{aligned}
N \text{ is a perfect square } &\Rightarrow N = a^2 \text{ for some integer } a\\
&\Rightarrow N = (2k)^2 \text{ or } (2k+1)^2 \text{ for some integer } k\\
&\Rightarrow N = 4k^2 \text{ or } 4k^2 + 4k + 1 \text{ for some integer } k\\
&\Rightarrow N = 4k^2 \text{ or } 4(k^2 + k) + 1 \text{ for some integer } k\\
&\Rightarrow N \text{ is a multiple of 4 or 1 more of a multiple of 4}\\
&\Rightarrow N \text{ leaves a remainder of 0 or 1 after division by 4.}
\end{aligned}$$

And so we are done. This comprises of a full proof for showing that the remainder of a perfect square upon division with 4 is either 0 or 1: we started with what we have or known to be true, namely N is a perfect square, and we reached the end conclusion via a sequence of implications using facts that we know to be true or calculations.

We have seen two different mathematical proofs. There are many different types of proofs which suits different mathematical problems. The proofs above are call direct proofs, in which we prove the desired statement directly. Some other types of proofs are via exhaustion, construction, contradiction, contrapositive, etc. In this section, we are going to show one type of mathematical proof, which is proof by induction.

1.2 Proof by Induction

Oftentimes we are asked to prove that a statement is true for all positive integers, as seen in Example 1.1. In Example 1.1, we have shown a direct method, but most problems would not be so direct. For example, show that the sum of the first n squares $1^2 + 2^2 +$

$3^2 + \ldots + n^2$ is $\frac{n(n+1)(2n+1)}{6}$. Proving this directly may be difficult, so we have to resort to a different method. This is where the proof by induction comes in handy.

Essentially, the proof of induction is obtained in three steps. Suppose that we want to prove the statement $P(n)$ is true for all positive integers n, namely we have to prove that all of $P(1), P(2), P(3), \ldots$ are true. Then, the proof via induction is comprised of four steps:

1. Base case: Prove the case $n = 1$, namely prove $P(1)$ is true.

2. Inductive hypothesis: Assume that $P(k)$ is true for some $k \geq 1$.

3. Inductive step: Using the inductive hypothesis, prove that $P(k+1)$ is true.

4. Conclusion: Since $P(1)$ is true and $P(k) \Rightarrow P(k+1)$ for all $k \geq 0$, then $P(n)$ is true for all $n \geq 1$.

This may seem very abstract and confusing at first, how did proving the case for $k+1$ bu using the case for k shows that the statement $P(n)$ is true for all n? This can be explained with a bit of imagination.

Imagine you have an infinitely many of dominoes arranged vertically in a line. Each domino represent the statement $P(n)$ for every $n \geq 1$. If a domino m has tipped over, it means that the statement $P(m)$ has been proven. Now we want to tip over all the dominoes (meaning we want to prove all of $P(n)$ are true). Using this analogy, let us examine the steps in the proof of induction.

1. Base case: Proving the base case $P(1)$ is the same as tipping the first domino over.

2. Inductive hypothesis: We assume that the k-th domino is tipped over for any $k \geq 1$. We are just assuming this happens for the time being, no actual domino has been tipped in this step.

3. Inductive step: We prove that by tipping the k-th domino, the $(k+1)$-th domino is also tipped over.

So let us go back to the first domino. We have shown that we can tip this over. Using the proven inductive step, since the first domino is tipped over, the second also tips over. By repeating this, since we know that the second domino is tipped over, the inductive step says that the third domino must tip over as well. This process is repeated again, thus creating a chain reaction that knocks down all the dominoes. So that no matter how large the number n is, the n-th domino must be tipped over eventually. Then we conclude with:

4. Conclusion: Since the first domino is tipped, and tipping the k-th domino tips the $(k+1)$-th domino as well, we conclude that all of the dominoes are tipped over.

This whole thought process is called the Principle of Mathematical Induction. Let us look at this process in a concrete example:

Example 1.3. Let us denote the sum $1^2 + 2^2 + 3^2 + \ldots + n^2$ as $S(n)$. We want to show that for any positive integer n, this sum is given by:

$$S(n) \stackrel{?}{=} \frac{n(n+1)(2n+1)}{6}. \tag{5}$$

We shall prove this via induction.

1. Base case: $S(1) = 1^2 = 1$ and $\frac{1(1+1)(2(1)+1)}{6} = 1$, so the formula $S(n) = \frac{n(n+1)(2n+1)}{6}$ is true for $n = 1$.

2. Inductive hypothesis: Let us assume that the formula is true for $n = k \geq 1$, namely the equation $S(k) = 1^2 + 2^2 + 3^2 + \ldots + k^2 = \frac{k(k+1)(2k+1)}{6}$ is true.

3. Inductive step: We shall now prove the formula for $n = k + 1$. Namely, our goal is to prove that:

$$S(k+1) \stackrel{?}{=} \frac{(k+1)((k+1)+1)(2(k+1)+1)}{6} = \frac{(k+1)(k+2)(2k+3)}{6}.$$

   We start with the left hand-side:

$$S(k+1) = 1^2 + 2^2 + \ldots + k^2 + (k+1)^2 = S(k) + (k+1)^2.$$

   But from the inductive hypothesis, we already assumed that $S(k) = \frac{k(k+1)(2k+1)}{6}$. So this sum becomes:

$$\begin{aligned} S(k+1) = 1^2 + 2^2 + \ldots + k^2 + (k+1)^2 &= S(k) + (k+1)^2 \\ &= \frac{k(k+1)(2k+1)}{6} + (k+1)^2 \\ &= \frac{(k+1)(2k^2+7k+6)}{6} \\ &= \frac{(k+1)(k+2)(2k+3)}{6} \end{aligned}$$

   which is what we wanted to prove.

4. Conclusion: Since $S(1) = 1$, and the formula in (5) for $n = k$ implies the formula for $n = k + 1$, we conclude that $S(n) = 1^2 + 2^2 + \ldots + n^2 = \frac{n(n+1)(2n+1)}{6}$ is true for all positive integers n.

There are also problems for which the base case does not start at $n = 1$, but at a different number. The principle remains the same: if we can knock down the $(k + 1)$-th domino using the preceeding k-th domino, no matter from which starting number we knock the domino, all of the dominoes will be knocked over eventually.

Example 1.4. We want to prove the following statement:

$$n^2 \overset{?}{\leq} 2^n \quad \text{for all positive integers} \quad n \geq 4. \tag{6}$$

We shall prove this via induction.

1. Base case: When $n = 4$, we have $n^2 = 16$ and $2^n = 16$, so the inequality $n^2 \leq 2^n$ is true for $n = 4$.

2. Inductive hypothesis: Let us assume that the inequality is true for $n = k$, namely the inequality $k^2 \leq 2^k$ is true for some $k \geq 4$.

3. Inductive step: We shall now prove the formula for $n = k + 1$. Namely, our goal is to prove the inequality:

   $$(k + 1)^2 \overset{?}{\leq} 2^{k+1}. \tag{7}$$

   This time, let us start from the right hand-side:

   $$2^{k+1} = 2 \times 2^k.$$

   But from the inductive hypothesis, we know that $k^2 \leq 2^k$. So term can be bounded from below as follows:

   $$2^{k+1} = 2 \times 2^k \geq 2 \times k^2 = k^2 + k^2. \tag{8}$$

   However, we know that since $k \geq 4$, we must have $k(k - 2) \geq 4 \times 2 \geq 1$ which means that $k^2 \geq 2k + 1$. Together with the inequality (8), this implies that:

   $$2^{k+1} \geq k^2 + k^2 \geq k^2 + (2k + 1) = (k + 1)^2.$$

   which is the inequality (7) that we wanted to prove.

4. Conclusion: Since the base case is true, and the inductive hypothesis for $n = k$ implies the case for $n = k + 1$, we conclude that $n^2 \leq 2^n$ is true for all positive integers $n \geq 4$.

1.3 Exercise

1. Prove using mathematical induction that for all positive integers $n \geq 1$, we have:

   $$1 + 4 + 7 + \ldots + (3n - 2) = \frac{n(3n - 1)}{2}.$$

2. Prove that for all positive integers $n \geq 1$,we have:

   $$1^3 + 2^3 + \cdots + n^3 = \frac{n^2(n + 1)^2}{4}.$$

3. Given a unit square. Show that we can always dissect this square into n smaller squares for $n \geq 6$.

4. Show that $n! > 3^n$ for all $n \geq 7$.

5. Using mathematical induction, show that for all $n \geq 1$, the number $6^n - 1$ is a multiple of 5.

6. There are n lamps labeled $1, 2, \ldots, n$. Lamp 1 can be switched on or off at any time. Lamp k, where $1 < k \leq n$ can only be switched (on or off) when lamp $k-1$ is the only lamp that is on out of lamps $1, 2, 3, \ldots, k-1$. If initially all lamps are off, how many moves does it take to switch on lamp n?

7. Prove that for every positive integer n there exists an n-digit number divisible by 5^n all of whose digits are odd.

2 Modular Arithmetic

In this section, let us look at a topic in number theory. We all know about the integers. These are just the set of whole numbers:

$$\mathbb{Z} = \{\dots, -3, -2, -1, 0, 1, 2, 3, \dots\}.$$

We can do arithmetic on this set: we can add, subtract, and multiply two integers together and this results in another integer. However, we cannot divide one non-zero integer from the other and hope that the result is also an integer: for example 1 divided by 2 is not an integer. Furthermore, these operations preserve equalities, namely if we have a, b, and c are positive integers and $a = b$, then $c \pm a = c \pm b$ and $c \times a = c \times b$.

The integers is nice, but it is a really big set. Let us consider a smaller set which can be derived from the set of integers. We divide the set of integers into classes. How do we determine which number goes in which class? First we need to fix an positive integer $n > 0$ which we call the modulus. Now we split the integers $\mathbb{Z}$ into classes. Two integers a and b are in the same class if their difference is a multiple of n.

Definition 2.1 (Congruence modulo n)**.** Two integers a and b are congruent modulo n or are members of the same class modulo n if their difference is divisible by n, namely $a - b = kn$ for some integer k. We denote this as $a \equiv b \pmod{n}$ or $a \equiv_n b$.

We do not care about the integer k in the definition above, all we care about are the integers a, b, and n. Thus we can now split all the integers into classes.

Example 2.2. Fix the modulus to be $n = 5$. Then the integers $1, 6, 11, 16, 21$ all lie in the same class because their pairwise differences are divisible by 5. In fact, there are many other integers that lie in this class. So this class is the set $\{1 + 5k : k \text{ is an integer}\}$. This is really long to write, so we usually write this down by picking a representative member from this class, say 1, and write:

$$[1] = \{1 + 5k : k \text{ is an integer}\} = \{a : a \equiv_5 1\}.$$

There are other choices for representatives of this class, for example $6, 11, 16, \dots$, but usually we choose the representative to be the non-negative integer smaller than the modulus. So, we have the equality:

$$[-9] = [-4] = [1] = [6] = [11] = [16] = [21] = \dots,$$

as all of them describe the same class.

How many classes modulo 5 are there? There are exactly 5 classes modulo 5, namely: $[0], [1], [2], [3], [4]$ and any integer is contained in exactly one of these classes.

In general, for modulo n, there would be n modulo classes, namely $[0], [1], [2], [3], \ldots,$ and $[n-1]$. This set of classes is denoted as:

$$\mathbb{Z}/n\mathbb{Z} = \{[0], [1], [2], \ldots, [n-1]\},$$

which is a much smaller set than $\mathbb{Z}$, hence why it is sometimes easier to work in modular arithmetic than integer arithmetic.

The representatives of these classes, namely $0, 1, 2, 3, \ldots, n-1$ are the possible remainders when we divide an integer by the modulus n. In particular, to decide which class an integer a belongs to, we simply divide the number a by n and find the remainder.

For example, in modulo 5, to find the class for which the number 173634281046 belong to, we find the remainder when this number leaves when divided by 5, which is 1. Hence the number 173634281046 belongs in the class [1] modulo 5.

Why do we split the numbers into classes? This construction has nice properties. Recall that any two numbers in the same class are congruent to each other modulo n, namely if a and b belong to the same class, then $a \equiv_n b$. Similar to the arithmetic on the integers, we can add, subtract, and multiply both sides of the congruence $\equiv$ just as it is $=$ instead. We call this the modular arithmetic.

Proposition 2.3. Let $n > 0$ be the modulus and a, b, c, d, k are integers such that $a \equiv_n b$ and $c \equiv_n d$. Then:

1. $k \pm a \equiv_n k \pm b$,

2. $k \times a \equiv_n k \times b$,

3. $a \pm c \equiv_n b \pm d$,

4. $a \times c \equiv_n b \times d$.

In addition, if m is a positive integer, then:

5. $a^m \equiv_n b^m$.

However, similar to equality of integers, we are not able to divide both sides of the equivalence with any integers. For example we know that if $n = 9$, the integers 6 and 24 are congruent to each other, namely $6 \equiv_9 24$. However, if we were able to divide both sides, dividing with 3 gives us $2 \equiv_9 8$ which is false! 2 and 8 do not lie in the same class since their difference is not a multiple of 12.

However, we still can do this for some cases.

Proposition 2.4. Let $n > 0$ be the modulus and a, b, c are integers such that $ca \equiv_n cb$. If c is such that $\mathrm{GCD}(n, c) = 1$, then $a \equiv_n b$.

So we can divide both sides with some integer provided that this integer is coprime to the modulus. Going back to the example above, if $n = 9$, we would have $6 \equiv_9 24$. Since 2 is coprime to 9, we can divide both sides with 2 to get $3 \equiv_9 12$.

Example 2.5. Solve for x the following congruence:

$$(x-2)(x+4) \equiv_5 (x+2)(x+1).$$

To solve this, let us expand the blackets first:

$$(x-2)(x+4) \equiv_5 (x+2)(x+1) \;\Rightarrow\; x^2+2x-8 \equiv_5 x^2+3x+2.$$

Since x^2 and 2 are integers, we can subtract x^2 and 2 from both sides to get:

$$\begin{aligned} x^2+2x-8 \equiv_5 x^2+3x+2 \;&\Rightarrow\; x^2+2x-8-x^2-2 \equiv_5 x^2+3x+2-x^2-2 \\ &\Rightarrow\; 2x-10 \equiv_5 3x. \end{aligned}$$

However, in modulo 5, $10 \equiv_5 0$, so if we substitute this in the congruence, we would get: $2x \equiv_5 3x$. Finally, subtracting $2x$ from both sides gives us $x \equiv_5 0$.

This means that the solution to the congruence $(x-2)(x+4) \equiv_5 (x+2)(x+1)$ is any integer x which is congruent to 0 in modulo 5, namely x must be in the same class as 0 in modulo 5. So the solution is $x = 5k$ for any integer k.

Now we have seen the techniques in modular arithmetic, we shall see some applications of it in real life.

Example 2.6. Our clock system uses a modulo 12 arithmetic. If you look at the face of a clock, there are only 12 numbers and after 12 o'clock, the cycle goes back to 1 o'clock. The numbers form the representative of the classes of time. This also helps us to compute time efficiently.

Suppose that it is 7am now. We want to find the time 400 hours from now. We work in modulo 12, so we want to find $7 + 400 \pmod{12}$. To find which class 407 lies in, we find the remainder 407 leaves upon division with 12. The remainder is 11, so we have $407 \equiv_{12} 11$, which means that it will be 11 o'clock after 400 hours. But will it be 11am or 11pm?

In order to determine this, we work with the 24-hour system, namely in mod 24. So now we want to find the remainder 407 leaves upon division with 24. The remainder is 23, so we have $407 \equiv_{24} 23$, which means that it will be 11pm after 400 hours.

We can also find the time backwards: if it is now 7am, what was the time 700 hours ago? So we want to find $7 - 700 \pmod{24}$, or equivalently $-693 \pmod{24}$. If the time is x, this problem is exactly:

$$x \equiv_{24} -693 \tag{9}$$

However, we note that $0 \equiv_{24} 24$, and multiplying this with 30 on both sides, we have $0 = 0 \times 30 \equiv_{24} 24 \times 30 = 720$. Adding this to the congruence (9), we have:

$$x + 0 \equiv_{24} -693 + 720 = 27 \;\Rightarrow\; x \equiv_{24} 27 \equiv_{24} 3,$$

so it was 3am 700 hours ago.

Similarly, the days of the week follows a 7-day cycle, so using the same argument but in modulo 7, we can determine the day of some event in a similar fashion. Another application would be to find the last digit of a large number.

Example 2.7. We want to find the last digit of the number 4567^{678}. Finding the last digit of a number is the same as finding the equivalence class of the number in modulo 10. This is because in decimal representation an integer is represented as the sum of multiples of powers of 10^k for $k \geq 0$. For example, the decimal expansion of the number 4567 is $(4 \times 10^3) + (5 \times 10^2) + (6 \times 10) + 7$. When we consider modulo 10, all multiples of 10 are equivalent to 0 since $10 \equiv_{10} 0$, leaving only the last digit behind.

So, to find the last digit of 4567^{678}, we fix the modulus to be 10 and aim to find the equivalence class this number is in:

$$4567 \equiv_{10} 7 \;\Rightarrow\; 4567^{678} \equiv_{10} 7^{678}. \tag{10}$$

To find 7^{678} modulo 10, let us try some small cases for powers of 7 in mod 10.

$$\begin{aligned}
&7^1 \equiv_{10} 7,\\
&7^2 = 49 \equiv_{10} 9,\\
&7^3 = 49 \times 7 \equiv_{10} 9 \times 7 = 63 \equiv_{10} 3,\\
&7^4 = 63 \times 7 \equiv_{10} 3 \times 7 = 21 \equiv_{10} 1.
\end{aligned}$$

So 7^4 is equivalent to 1 in modulo 10. We can use this information in congruence (10), so that we have:

$$4567^{678} \equiv_{10} 7^{678} = (7^4)^{169} \times 7^2 \equiv_{10} 1^{169} \times 7^2 = 49 \equiv_{10} 9.$$

This implies that the last digit of 4567^{678} is 9.

Finally, let us look at a type of problem in mathematics called the Diophantine equation. A Diophantine equation is an equation in two or more variables which can only be integers. Namely, we have an equation in two or more variables and we want to find the integer solutions to this equation.

This problem is widely studied in number theory and can be very difficult to solve. One way of finding the solutions or showing that there are no solutions to an equation is via modular arithmetic.

Example 2.8. Consider the Diophantine equation:

$$x^2 + y^2 = 123. \tag{11}$$

We want to show that there are no solutions to this problem. One way to do this is to check this for the various integers x and y from 0 to 11, but this is a tedious task because we have so many of them. A slick way of doing this is to consider modulo 4. We can make a table of squares in modulo 4 as follows:

$a \pmod 4$	0	1	2	3
$a^2 \pmod 4$	0	1	0	1

Thus any square can only be equivalent to 0 or 1 in modulo 4. Hence for integers x and y, we must have $x^2 + y^2 \equiv_4 0, 1, 2$ only. However, $123 \equiv_4 3$, so the two expressions are not congruent to each other in modulo 4. Thus there are no integers x and y that satisfy the equation (11).

Usually it is tricky to find the modulus that would give us the desired result. However, for squares it is always worth working with modulo 3,4,5, and 8, cubes with modulo 7 and 9, and fourth and fifth powers with modulo 5.

2.1 Exercise

1. Find the remainder when:

   (a) $123 + 234 + 32 + 56 + 22 + 12 + 78$ is divided by 3.

   (b) $2222^{5555} + 5555^{2222}$ is divided by 7.

2. If today is Sunday, what day will it be in 100 days time?

3. Find the last digit of 17^{17}.

4. Find the last two digits of 7^{7^7}.

5. Prove that $n^5 + 4n$ is divisible by 5 for any positive integer $n \geq 1$.

6. Two positive integers a and b are given such that $a^2 + b^2$ is divisible by 3. Prove that a and b are also divisible by 3.

7. Show that there are no integer solutions to the equation $x^3 + y^3 + z^3 = 400$.

8. Find all the integer solutions to $2^x - 1 = 3^y$.

9. Given that a and x are positive integers greater than or equal to 2. If $a^x \equiv a - 2 \pmod{a - 1}$, find the value of a.

3 Circular Geometry

We first describe the most important axiom in plane geometry, namely the parallel postulate. First, we must accept that the angle on a straight line is 180°. Now suppose that we have a pair of parallel lines and a third line transversal to these two line. This is described in Figure 1 where the lines AB and CD are parallel with the line EF transversal to them, intersecting at X and Y respectively.

Then the parallel postulate says that the sum of the interior angles to one side of the transversal line is 180°, namely $\angle BXF + \angle DYE = 180°$. As a direct result, using the fact that the angle on a straight line is 180°, we have the equality of angles $\angle BXF = \angle CYE = \angle FYD$.

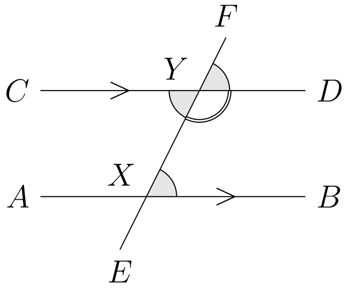


Figure 1: Parallel postulate.

In fact, starting from this fact, we can build up the whole of plane geometry and show, among others, the fact that the sum of the angles in a triangle is 180°, the angles at the foot of an isosceles triangle are equal, and so on. We first state an important result on similar triangles, which is very useful when studying angles and lengths.

Definition 3.1 (Similar triangles)**.** Two triangles ΔABC and ΔDEF are similar if every angle in ΔABC has the same measure with a corresponding angle in ΔDEF, namely $\angle ABC = \angle DEF$, $\angle BCA = \angle EFD$, and $\angle CAB = \angle FDE$. We denote this as $\Delta ABC \sim \Delta DEF$.

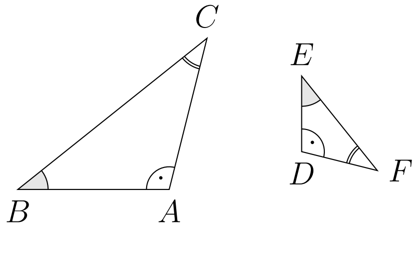


Figure 2: Similar (but not congruent) triangles $\Delta ABC \sim \Delta DEF$.

Similar triangles are nice because they are in direct proportion to each other. Suppose that two triangles are similar, namely $\Delta ABC \sim \Delta DEF$, then the lengths of the sides satisfy the following ratios:

$$\frac{AB}{DE} = \frac{BC}{EF} = \frac{CA}{FD}.$$

In order to check that two triangles are similar, it is enough to check:

1. one pair of internal angles of two triangles have the same measure as each other, and another pair also have the same measure as each other, or

2. one pair of corresponding sides of two triangles are in the same proportion as are another pair of corresponding sides, and their included angles have the same measure, or

3. three pairs of corresponding sides of two triangles are all in the same proportion.

Definition 3.2 (Congruent triangles)**.** Two triangles ΔABC and ΔDEF are congruent if they are similar ($\Delta ABC \sim \Delta DEF$) and their corresponding sides are of the same length, namely $AB = DE$, $BC = EF$, and $CA = FD$.

Congruent triangles is a stronger relationship compared to similar triangles as we require not only the angles are the same, but the size of the triangles are also the same. Therefore, we need more information to show that two triangles are congruent. The following are the things we can check in order to conclude that two triangles are congruent. We compare the two triangles according to the following rules:

1. SSS: all three sides are the same for both triangles.

2. SAS: two sides and an angle between them are the same for both triangles.

3. ASA: two angles and a side between the two angles are the same for both triangles.

4. AAS: two angles and a side not between the two angles are the same for both triangles.

The mnemonic SSS, SAS, ASA, and AAS in the list above are very useful for summarising the things you need to check: the A's stand for angles and the S's stand for sides.

3.1 Anatomy of a Circle

In this note, we are going to look at the geometric properties of a circle. We first describe the anatomy of a circle.

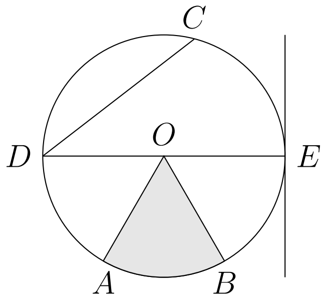


Figure 3: Anatomy of a circle.

A circle is described by two quantities: the center O and the radius $r > 0$. In Figure 3, the center is denoted as O and the circle are points which are of the same distance r from O, we call this distance the radius of the circle. In Figure 3, the line segments OA, OB, OD, and OE are also called the radius of the circle because they join the center of the circle with points on the circle and hence have lengths r. The shaded region is called the minor sector OAB The rest of the region is called the major sector OAB. It is important to distinguish the minor and major sectors as they subtend different angles at the center of the circle.

Along with the minor and major sectors, we have the minor and major arcs $\widehat{AB}$. The minor arc $\widehat{AB}$ is the smaller part of the circle which joins the points A and B. The major arc is the larger part of the circle which joins the points A and B. Together, these arcs make up the circumference of the circle.

If we pick two points on the circle C and D and draw a straight line segment joining them, we would get a chord CD. If the chord drawn passes through the center, we call this chord the diameter of the circle, and it has length $2r$. In Figure 3 above, the line segment DE is a chord that passes through the center O, hence it is a diameter.

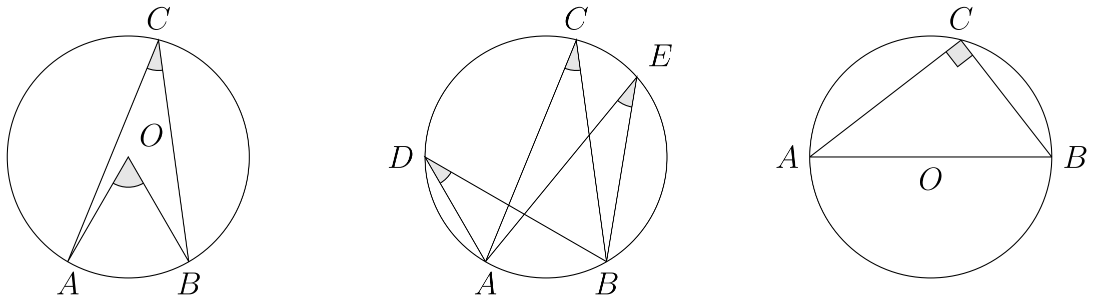
Finally, if we were to draw any line in addition to the circle, they will intersect at exactly either $0, 1$, or 2 points. If this line intersects the circle at exactly 1 point, say E, on the circle, we call this line the tangent line, or more specifically the line tangent to the circle at the point E.

3.2 Basic Properties of a Circle

Suppose that we have a circle with centre O. Suppose further that A, B, C are three distinct points on the circle. Then the angle $\angle AOB$ is twice the angle $\angle ACB$ no matter where the point C is on the circle. In other words, the angle subtended by an arc at the centre of the circle is twice the angle subtended by the same arc on the circle. This is shown in Figure 4a.

As a direct result, two angles subtended by the same arc has the same value, as depicted in Figure 4b. If we have two additional points D, E on the circle, we would have

$\angle ADB = \angle ACB = \angle AEB$. In fact, by rotational symmetry on the circle, two angles on the circle subtended by arcs of the same length have equal angles. Another direct result is that the angle subtended by the semicircle arc $\widehat{AB}$ is 90° since the angle subtended at the center by this arc is 180°.



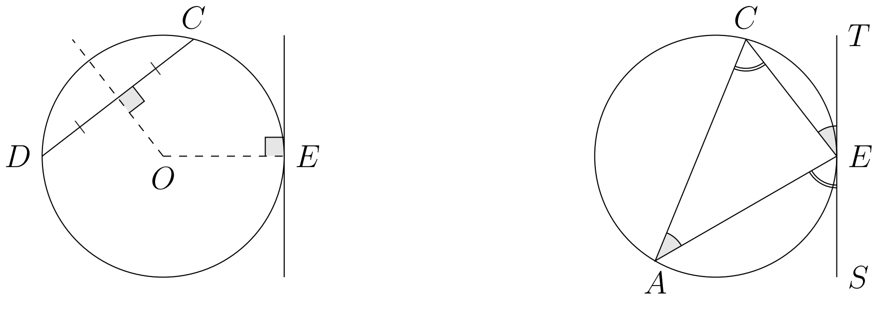
(a) $\angle AOB = 2\angle ACB$.

(b) $\angle ADB = \angle ACB = \angle AEB$.

(c) $\angle ACB = 90°$.

Figure 4: Angles at the centre and on the circle subtended by the arc $\widehat{AB}$.

Next, let us look at the chord of a circle. If we were to draw a perpendicular bisector to the chord (a line perpendicular to the chord that splits the chord into two equal lengths), this perpendicular bisector would pass through the center O. On the other hand, if we draw a line perpendicular to the tangent line at E from the point of tangency E, it also passes through the center O. This is illustrated in Figure 5a.



(a)

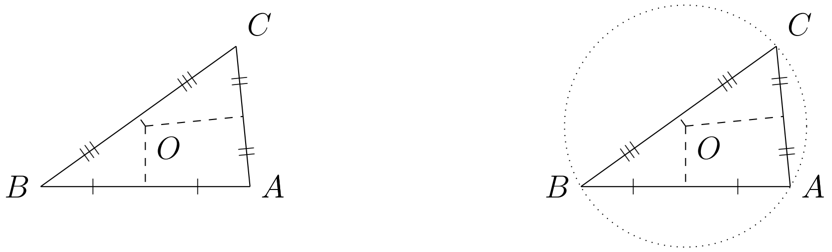
(b) $\angle CET = \angle CAE$ and $\angle AES = \angle ACE$.

Figure 5: Properties of chord and tangent.

Finally, suppose that we have a tangent line to a circle at the point E and A, C are any other two distinct points on the circle. Suppose that the ends of the tangent line is labeled T and S respectively as in Figure 5b. Then we would have two pairs of equal angles, namely $\angle CET = \angle CAE$ and $\angle AES = \angle ACE$. This is called the alternate segment theorem.

3.3 Circumcircle and Circumcenter

Given a triangle ΔABC, we can always find a circle that passes through all the three vertices of the triangle. How do we find this circle? The idea lies in the property of the chord of a circle. For each side of the triangle, we construct its perpendicular bisector. It can be proven using similar triangles that all three of the perpendicular bisectors intersect at a common point O (you will prove this later in the exercise). This common point will be the center of our desired circle and the radius is just the distance from this point to any of the vertices A, B, or C.



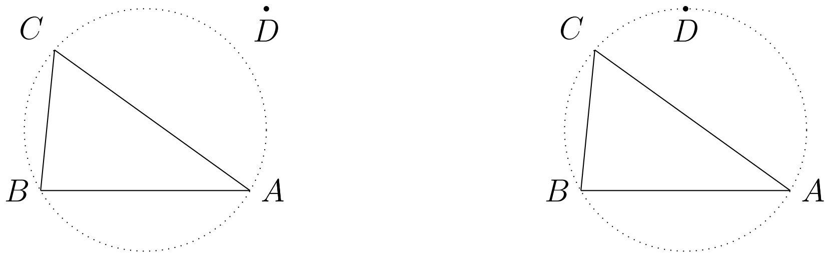
(a) Perpendicular bisectors of the sides. (b) The circle can then be drawn.

Figure 6: Drawing a circle passing through the vertices of ΔABC.

This circle and center has a name. The circle is called the circumcircle of the triangle ΔABC and the center is called the circumcenter of the triangle ΔABC. For any given triangle, this circumcircle is unique: there is only one such circle that passes through the vertices of the given triangle.

3.4 Cyclic Quadrilateral

We have seen above that there is a unique circle that passes through the vertices of a triangle. S given any three distinct points which do not all lie in a straight line, we can find a circle passing through these points. However, can the same be said if we are given four points? Not always.



(a) Four points not on the same circle. (b) Four points on the same circle.

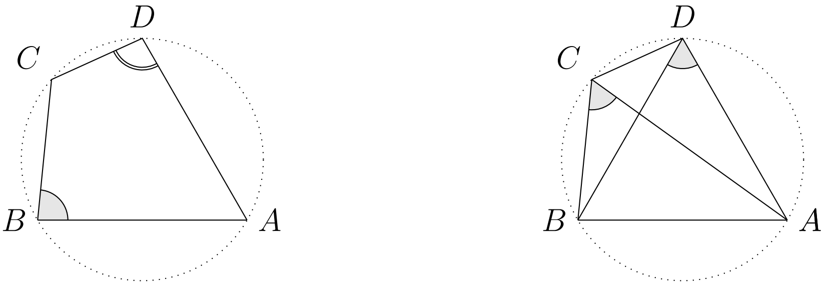
Figure 7: Four points A, B, C, D might not lie on the same circle.

However we have a condition to determine whether four points lie on the same circle. These four points are called cyclic if there is a circle that passes through all of them.

Proposition 3.3. Four vertices of a quadrilateral $ABCD$ are cyclic if either:

1. the sum of their opposite angles of the quadrilateral $ABCD$ adds up to 180°, or
2. the angle between a side and a diagonal is the same as the angle between the opposite side and the other diagonal.

If either condition holds, then the quadrilateral is called a cyclic quadrilateral.



(a) $\angle CBA + \angle CDA = 180°$.

(b) $\angle BCA = \angle BDA$.

Figure 8: Checking if four points A, B, C, D are cyclic.

In fact, the converse also holds true: if the quadrilateral $ABCD$ is cyclic, both of the conditions in the above proposition are true.

3.5 Exercise

1. Triangle ΔABC has a right angle at C. Let H be a point on the side AB so that $\angle CHA = 90°$. Prove that $AC^2 = AB \cdot AH$ and $CH^2 = AH \cdot BH$.
2. Circles Γ_1 and Γ_2 intersect at A and B. Let C and D lie on Γ_1. Let lines CB and DB intersect Γ_2 again at E and F respectively. Prove $\Delta ACD \sim \Delta AEF$.
3. In a cyclic quadrilateral $ABCD$, we have the ratio $\angle DAB : \angle ABC : \angle BCD = 9 : 10 : 11$. Find the angle $\angle CDA$.
4. Let ΔABC be a triangle with circumcircle Γ. Let D, E be points on AB, AC such that DE is parallel to the tangent to Γ at A. Prove that the quadrilateral $BDEC$ is cyclic.
5. Let ΔABC be a triangle. Prove that the perpendicular bisectors of the sides all intersect at a unique point O.