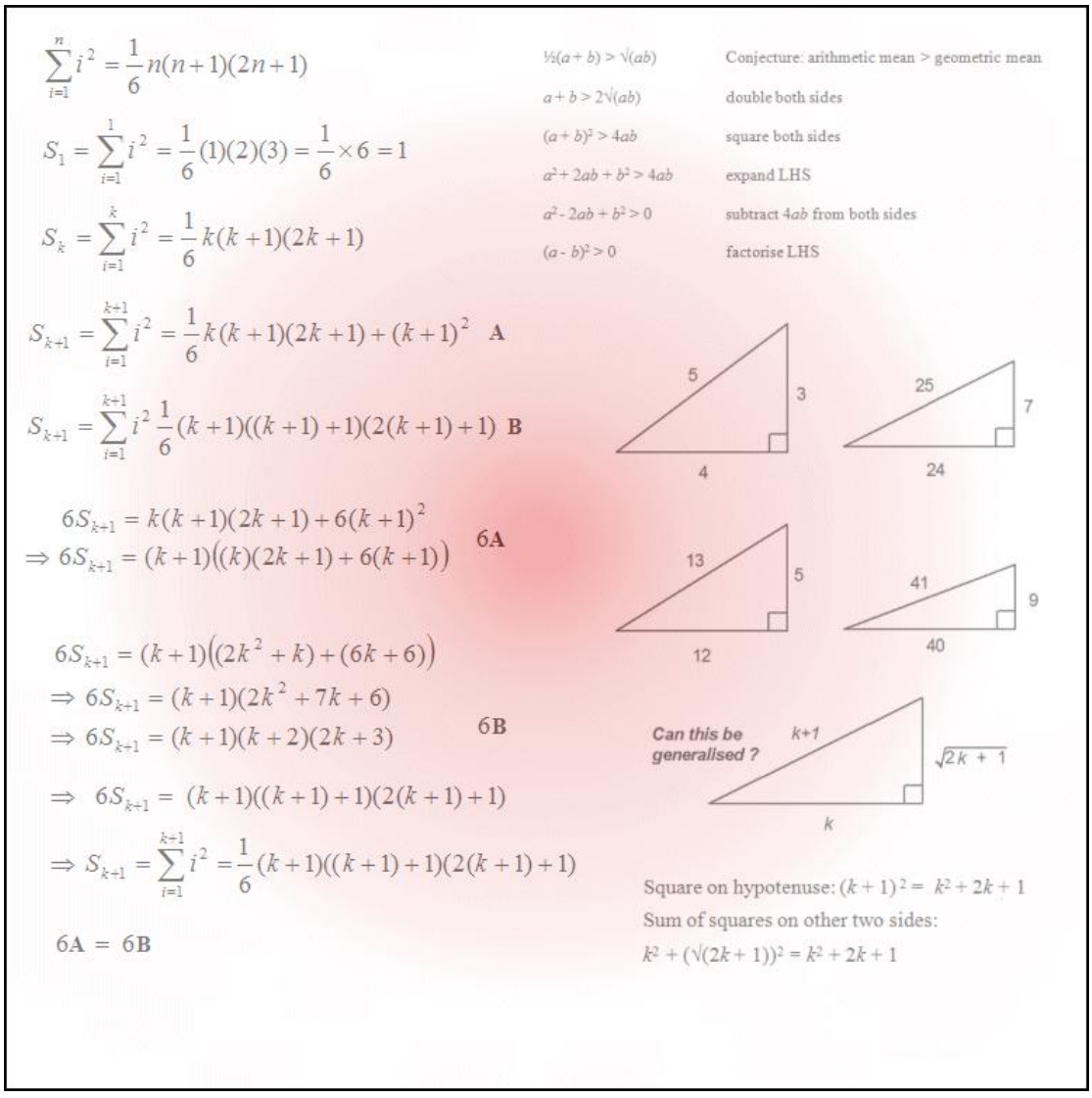
M.K. HOME TUITION

Mathematics Revision Guides

Level: A-Level Year 1 / AS

INTRODUCTION TO MATHEMATICAL PROOF



Version : 2.2 Date: 16-08-2007

Introduction to Mathematical Proof.

We have already met various theorems and proofs in Mathematics, at GCSE and higher levels.
This section will go into more detail about how to prove mathematical theorems and conjectures.

There are various methods of carrying out proofs, namely

- Proof by mathematical reasoning
- Proof by exhaustion
- Proof by contradiction
- Proof by induction
- Disproof by counterexample

The important thing about proving a conjecture is that 'every step must be justified'.

Example (1) : Prove that the product of three consecutive positive integers is a multiple of 6.

i) We can take sequences of three consecutive positive integers such as 1-2-3, 2-3-4 and 3-4-5 and see that at least one of them must be even and that one is a multiple of 3.

ii) The product must therefore have a factor of both 2 and 3. The L.C.M. of 2 and 3 is 6, since 2 and 3 have no common factor.

$\therefore$ The product of three consecutive positive integers is a multiple of 6.

Is this proof ? No, as far as statement i) is concerned. Looking at the number sequences and observing a pattern is not rigorous enough to justify the argument. Statement ii) is rigorous and concise, and thus can be left as it is when rewriting the 'proof'.

True proof:

To prove that the product of three consecutive positive integers is a multiple of 6 we must choose the general case of three consecutive positive integers: k, $k+1$ and $k+2$ and use the properties of division of integers.

First we check for the presence of even integers. The integer k can either be even (have no remainder) or odd (have remainder of 1).

If k is even, then the product is even (has a multiple of 2). If k is odd , then $k + 1$ will be even because the sum of two odd numbers is even, and so the product will be even due to the $k+1$ term.

By similar logic, the integer k can have three possible remainders when it is divided by 3.
It can be a multiple of 3 (no remainder), or will have a remainder of 1 or 2.

If dividing k by 3 leaves a remainder of 2, then $k + 1$ will be a multiple of 3; if dividing k by 3 leaves a remainder of 1, then $k + 2$ will be a multiple of 3.

Therefore there will always be one number of the sequence divisible by 3.

The product must therefore have factors of both 2 and 3. The L.C.M. of 2 and 3 is 6, since 2 and 3 have no common factor.

$\therefore$ The product of three consecutive positive integers is a multiple of 6 (the L.C.M. of 2 and 3).

The proof in Example 1 used a combination of exhaustion and mathematical reasoning. Here are a few more examples with full working:

Proof by mathematical reasoning.

This uses mathematical logic and uses well-established results to prove a conjecture or a theorem.

Example (2). Prove that the arithmetic mean of two different positive numbers a and b is greater than their geometric mean.

The arithmetic mean of two numbers a and b is equal to half their sum, i.e $\frac{1}{2}(a + b)$.
The geometric mean of two (positive) numbers is equal to the (positive) square root of their product, $\sqrt{(ab)}$.

Thus the arithmetic mean of 2 and 8 is $\frac{1}{2}(2 + 8)$ or 5; their geometric mean is $\sqrt{(2 \times 8)}$ or 4.
The arithmetic mean of 0.1 and 0.9 is $\frac{1}{2}(0.1 + 0.9)$ or 0.5; their geometric mean is $\sqrt{(0.1 \times 0.9)}$ or 0.3.

It looks as if the conjecture holds true, but since there are an infinite number of cases to test, these two examples do not make a proof. For that, we need to use the algebra of quadratic equations.

$\frac{1}{2}(a + b) > \sqrt{(ab)}$	Conjecture: arithmetic mean > geometric mean
$a + b > 2\sqrt{(ab)}$	double both sides
$(a + b)^2 > 4ab$	square both sides
$a^2 + 2ab + b^2 > 4ab$	expand LHS
$a^2 - 2ab + b^2 > 0$	subtract $4ab$ from both sides
$(a - b)^2 > 0$	factorise LHS

Since a and b are not equal, the square of their difference is always greater than 0, hence their arithmetic mean will always be greater than their geometric mean.

Example (3). If two integers are squared, and the resulting sum is doubled, then the result can also be expressed as the sum of the squares of two other integers.

For example, $2^2 + 3^2 = 4 + 9 = 13$, and doubling gives 26, which can be expressed as $1^2 + 5^2$.
Another example is , $4^2 + 9^2 = 16 + 81 = 97$. Double to obtain 194, which is 169 + 25, or $13^2 + 5^2$.

Prove that this holds true for all integers a and b, i.e. $2(a^2 + b^2) = p^2 + q^2$ where p and q are also integers.

Let $b = a + k$ for some integer k.

Then, $2(a^2 + b^2) = 2(a^2 + (a + k)^2)$, and expanding the RHS gives $2(a^2 + (a^2 + 2ak + k^2))$

$= 4a^2 + 4ak + 2k^2$.

This expression can then be rewritten as $(4a^2 + 4ak + k^2) + k^2$, the bracketed term factorising to give $(2a + k)^2 + k^2$.

Since we have set $b = a + k$, we can also replace $2a + k$ with $a + b$, and k with $b-a$
to obtain $(a + b)^2 + (b - a)^2$.

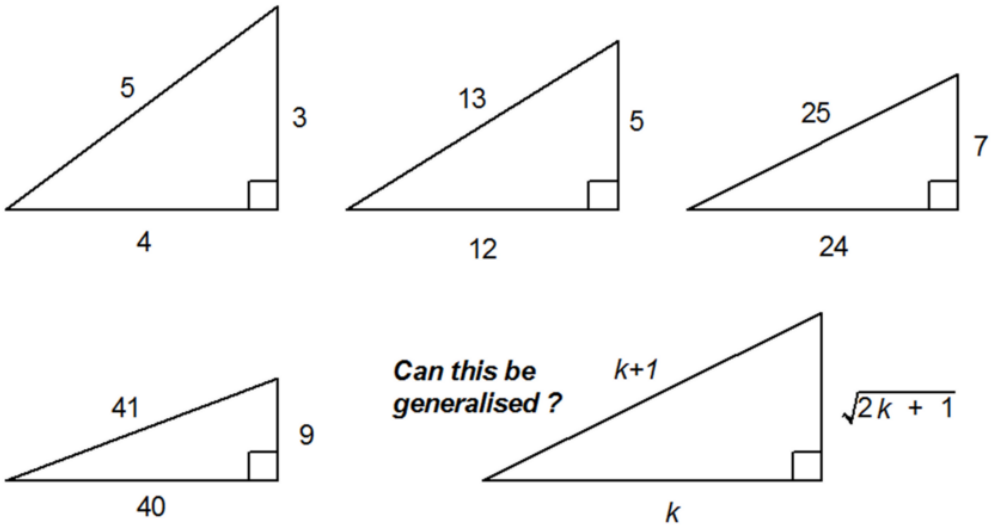
$\therefore$ This is the sum of the squares of two integers, as we set out to prove.

Thus if $a = 8$ and $b = 11$, then $a^2 + b^2 = 185$ and $2(a^2 + b^2) = 370$

$\Rightarrow$ $(a + b)^2 + (b - a)^2$, or $19^2 + 3^2 = 361 + 9 = 370$.

This result is also quoted in the form $2(a^2 + b^2) = (a + b)^2 + (a - b)^2$. (Note that $(b - a)^2 = (a - b)^2$.)

Example (4): The ratios between the sides of certain right-angled triangles were investigated:



In the triangles above, it was noticed that when the two longer sides differed by 1 unit in length, then the shortest side had a length equal to the square root of the sums of the two longer sides.

Thus $3 = \sqrt{(4 + 5)}$; $5 = \sqrt{(12 + 13)}$; $7 = \sqrt{(24 + 25)}$; $9 = \sqrt{(40 + 41)}$.

Does this pattern hold true for *all* right-angled triangles where the two longer sides differ in length by 1 unit ?

The hypotenuse has a length of $k + 1$ units, and therefore its square is $(k + 1)^2$ or $k^2 + 2k + 1$.

One of the remaining sides (not necessarily the longer one !) is k units long, and so its square is k^2.
The last side has a length of $\sqrt{(2k + 1)}$ units, and so its square is $2k + 1$.

These results satisfy Pythagoras' theorem that the square on the hypotenuse is equal to the sum of the squares on the other two sides.

This result can be generalised for all right-angled triangles where the hypotenuse is one unit longer than one of the remaining sides.

Other examples of right-angled triangles with sides quoted in order $k : k + 1 : \sqrt{(2k + 1)}$ are
$1 : 2 : \sqrt{3}$, $2 : 3 : \sqrt{5}$ and $3 : 4 : \sqrt{7}$.

The lengths of the sides do not have to be integers or even rational, thus triangles with sides in the ratios $1.5 : 2.5 : 2$ and $(\sqrt{2} - 0.5) : (\sqrt{2} + 0.5) : (\sqrt{(2\sqrt{2})})$ also satisfy the conjecture.

Example (5): Prove using the Binomial Theorem that the derivative of a power function x^n is given by nx^{n-1} i.e. 'multiply by the power, and then reduce the power by 1'.

Thus the derivative of x^2 is $2x$, that of x^3 is $3x^2$, that of x^4 is $4x^3$ and so on.
We just 'learnt the result', but here we are out to prove it.

In an earlier section, we differentiated $y = x^2$ from first principles.
Setting $y = x^2$, then a small change δx in x causes a corresponding change δy in y.
Since $y = x^2$, it follows that $y + \delta y = (x + \delta x)^2$.

$\therefore\ y + \delta y = x^2 + 2x\delta x + (\delta x)^2$.

Subtracting the original function gives $\delta y = 2x\delta x + (\delta x)^2$, and dividing throughout by δx, we have

$\frac{\delta y}{\delta x} = 2x + \delta x$. As δx tends to zero, $\frac{\delta y}{\delta x} \to \frac{dy}{dx} = 2x$ $\therefore$ $2x$ is the derivative of x^2.

To expand the method for higher powers of x we use the binomial theorem:

$$(a + b)^n = a^n + na^{n-1}b + \frac{n(n-1)}{2!}a^{n-2}b^2 + \frac{n(n-1)(n-2)}{3!}a^{n-3}b^3 + ... + b^n$$

Generalising to give $y = x^n$, there is again a relationship between a small change δx in x and the corresponding change δy in y.

Since $y = x^n$, it follows that $y + \delta y = (x + \delta x)^n$.

Replacing a in the general formula above with x and b with δx ,

$$y + \delta y = x^n + nx^{n-1}(\delta x) + \frac{n(n-1)}{2!}x^{n-2}(\delta x)^2 + \frac{n(n-1)(n-2)}{3!}x^{n-3}(\delta x)^3 + ... + (\delta x)^n$$

Subtracting the original function $y = x^n$ gives

$$\delta y = nx^{n-1}(\delta x) + \frac{n(n-1)}{2!}x^{n-2}(\delta x)^2 + \frac{n(n-1)(n-2)}{3!}x^{n-3}(\delta x)^3 + ... + (\delta x)^n$$

Dividing throughout by δx, we have

$$\frac{\delta y}{\delta x} = nx^{n-1} + \frac{n(n-1)}{2!}x^{n-2}(\delta x) + \frac{n(n-1)(n-2)}{3!}x^{n-3}(\delta x)^2 + ... + (\delta x)^{n-1}$$

This looks messy, but as δx tends to zero, all the terms except the first one tend to zero because of the existence of powers of δx. We can therefore discard all the terms in the expansion except the first.

As δx tends to zero, $\frac{\delta y}{\delta x} \to \frac{dy}{dx} = nx^{n-1}$.

$\therefore$ the derivative of a power function x^n is given by nx^{n-1}.

Proof by exhaustion.

This uses exhaustive testing when the set of results to be tested is finite. This is often used together with mathematical reasoning.

Example (6): Prove that $x^2 + x + 11$ is prime for all positive integers $x < 10$.

We calculate the value of $x^2 + x + 11$ for all integers between 1 and 9 and obtain the following:

x	$x^2 + x + 11$	x	$x^2 + x + 11$
1	13	6	53
2	17	7	67
3	23	8	83
4	31	9	101
5	41		

All of these results are prime, so the conjecture is true in this case.

Example (7): Prove that i) no square number ends in 2, 3, 7 or 8; ii) all square numbers ending in 5 must also end in 25.

We begin by taking the squares of the integers from 0 to 9; they are 0, 1, 4, 9, 16, 25, 36, 49, 64 and 81.
Next, we can express any integer greater than 10 as $10m + n$ where m and n are integers,
$m > 0$ and $0 \le n \le 9$.

Squaring $10m + n$ gives $100m^2 + 20mn + n^2 \rightarrow = 10m(10m + 2n) + n^2$.

The terms involving m are divisible by 10, and so the value of m will have no effect on the last ('units') digit in the square, i.e. $(10m + n)^2$ ends in the same digit as n^2.
(For example, the squares of 17, 27, 37,.... end in 9 because the square of 7 does so).

The squares of the integers from 0 to 9 have a 'units' digit of 0, 1, 4, 5, 6 and 9 – there are none ending in 2, 3, 7 or 8.

$\therefore$ no square number ends in 2, 3, 7 or 8.

Part ii) involves similar reasoning. 5 is the only integer between 0 and 9 whose square ends in 5.

Any positive integer ending in 5 can be expressed as $10m + 5$ where m is an integer and $m > 0$.
Squaring $10m + 5$ gives $100m^2 + 100m + 25 \implies = 100m(m + 1) + 25$.

The terms involving m are divisible by 100, and so the value of m will have no effect on the last two ('tens' and 'units') digits in the square, and thus all square numbers ending in 5 must also end in 25.

Proof by contradiction.

With this method, we are trying to prove the opposite of what we are actually proving, until the 'proof' throws up a falsehood or inconsistency.

Example (8): Prove that $\sqrt{5}$ is irrational.

We begin by trying to prove the opposite, namely that $\sqrt{5}$ is a rational number $\frac{a}{b}$ in its lowest terms, i.e. with a and b having no common factor.

If $\sqrt{5} = \frac{a}{b}$, then we can square both sides to give $5 = \frac{a^2}{b^2}$ and therefore $a^2 = 5b^2$.

From here we can establish that a^2 is a multiple of 5, and if a square number is a multiple of 5, so is its square root – i.e. 5 is a factor of a.

Hence we can set $a = 5k$ for some integer k.

Squaring a gives $a^2 = (5k)^2$ or $a^2 = 25k^2$
Substituting $5b^2$ for a^2 gives $5b^2 = 25k^2$.

Dividing the last by 5 gives $b^2 = 5k^2$, meaning that b^2 has a factor of 5.
Again, if a square number is a multiple of 5, so is its square root, so 5 is also a factor of b.

We have thus found that **both a and b have a common factor of 5**.

This result makes nonsense of our original assumption that $\sqrt{5}$ was a rational number $\frac{a}{b}$ in its lowest terms, i.e. with ***a* and *b* having no common factor**.

The absurdity of this contradiction therefore proves that $\sqrt{5}$ cannot be rational.

This argument can be applied to all numbers with irrational square roots, such as $\sqrt{2}$ (the most popular example in textbooks) , $\sqrt{3}$ and $\sqrt{10}$.

Example (9): Prove that there are infinitely many prime numbers.

We first assume the opposite, i.e. that the set of prime numbers is finite.

If the set of prime numbers were finite with n members, then we can label them $p_1 = 2$, $p_2 = 3$, $p_3 = 5$ and so on up to p_n.

This finite set of prime numbers would therefore have the product $\mathbf{\Pi} = p_1 \times p_2 \times p_3 \times ..... \times p_n$.

(The symbol $\mathbf{\Pi}$ here stands for 'product' and is quite unconnected with the familiar π used in circular measure).

If this product $\mathbf{\Pi}$ were increased by 1, then we would obtain a remainder of 1 when trying to divide $\mathbf{\Pi} + 1$ by each prime number in the finite set p_1, p_2, p_3 and so on up to p_n.

The result $\mathbf{\Pi} + 1$ would be itself prime **with respect to the numbers in the finite set** , therefore the set of prime numbers cannot be finite. (See note below).

$\therefore$ we have proved by contradiction that there are infinitely many prime numbers.

(Note) The result $\mathbf{\Pi}$ would not necessarily be prime. Assume for the sake of argument that the set of all prime numbers consisted of 2, 3, 5, 7, 11 and 13. The product, $(2 \times 3 \times 5 \times 7 \times 11 \times 13) + 1 = 30031$ would leave a remainder of 1 when divided by each of those primes, but it is not prime, as it is equal to 59×509 – two primes missing from the list.

Proof by induction.

This is generally used for proving results of sums of series, and is related to using an inductive definition for sequences.

Example(10): Prove that the sum of the first *n* natural numbers can be given by the formula

$\sum_{i=1}^{n} i = \frac{1}{2}n(n+1)$. (The expression in sigma notation is just shorthand for 1 + 2 + 3 + 4 +....+ *n*.)

Part (1): Show that the formula is true for a specific value of *n*.

We begin the proof by showing that the formula holds true for a particular value of *n*. Choosing the trivial case of *n* = 1, we have the result $S_1 = \sum_{i=1}^{1} i = \frac{1}{2}(1)(1+1) = \frac{1}{2}\times 1\times 2 = 1$.

$\therefore$ The formula holds for $n = 1$, i.e the 'sum' of the first 1 natural number is 1.

Part (2): Show that if the formula holds for *n = k*, it also holds for *n = k* + 1.

The next stage of the proof is showing that if the formula is true for a general value of *n = k*, then it is also true for the value *n* = *k*+1.

Substituting *n = k* into the formula gives $S_k = \sum_{i=1}^{k} i = \frac{1}{2}k(k+1)$.

If we were to add another term to the series, that term would be *k* + 1.
Thus, if *k* = 3, we would have the sum 1 + 2 + 3; adding *k* + 1 (here 4) would give 1 + 2 + 3 + 4.

The sum to *k*+1 terms will therefore be $S_{k+1} = \sum_{i=1}^{k+1} i = \frac{1}{2}k(k+1) + (k+1)$, since we have added the next term, *k* + 1, to the total. We will call this expression **A**.

We can however replace *k* by (*k* + 1) in the original formula to obtain
$S_{k+1} = \sum_{i=1}^{k+1} i = \frac{1}{2}(k+1)((k+1)+1)$. Call this expression **B**.

We therefore use algebra to show that the two expressions are equivalent.
Manipulation of expression **A** gives

$$S_{k+1} = \frac{1}{2}k(k+1) + (k+1) \Rightarrow 2S_{k+1} = k(k+1) + (2k+2)$$

$$\Rightarrow 2S_{k+1} = k^2 + 3k + 2 \Rightarrow 2S_{k+1} = (k+1)(k+2)$$

$$\Rightarrow S_{k+1} = \frac{1}{2}(k+1)(k+2) \Rightarrow S_{k+1} = \sum_{i=1}^{k+1} i = \frac{1}{2}(k+1)((k+1)+1).$$

We have manipulated expression **A** to obtain expression **B** $\therefore$ expressions **A** and **B** are equivalent.

$\therefore$ If the formula is true for *n = k*, then it is also true for *n = k*+1.

The first part of the proof shows that the formula holds for *n* = 1; the second part shows that if the formula is true for *k* = 1, it is also true for *k* = 2, and so on for all higher *k*.

Example(11): Prove that the sum of the squares of the first *n* natural numbers satisfies the formula

$$\sum_{i=1}^{n} i^2 = \frac{1}{6}n(n+1)(2n+1)$$ (Sigma notation shorthand for $1^2 + 2^2 + 3^2 + 4^2 + ... + n^2$.)

Part (1): Show that the formula is true for *n* = 1 (the trivial case).

$S_1 = \sum_{i=1}^{1} i^2 = \frac{1}{6}(1)(2)(3) = \frac{1}{6} \times 6 = 1.$ ∴ The formula holds for $n = 1$.

Part (2): Show that if the formula holds for *n* = *k*, it also holds for *n* = *k* + 1.

$$S_k = \sum_{i=1}^{k} i^2 = \frac{1}{6}k(k+1)(2k+1)$$

The sum to $k + 1$ terms will be the above total plus $(k+1)^2$.
Thus, if $k = 3$, we would have the sum $1^2 + 2^2 + 3^2$.
Adding $(k + 1)^2$ (here 4^2) would give $1^2 + 2^2 + 3^2 + 4^2$.

$S_{k+1} = \sum_{i=1}^{k+1} i^2 = \frac{1}{6}k(k+1)(2k+1) + (k+1)^2$. Call this expression **A**.

We can however replace k by $(k + 1)$ in the original formula to obtain

$S_{k+1} = \sum_{i=1}^{k+1} i^2 \frac{1}{6}(k+1)((k+1)+1)(2(k+1)+1)$. Call this expression **B**.

Next we must show that expressions **A** and **B** are equivalent.

By algebra, $S_{k+1} = \frac{1}{6}k(k+1)(2k+1) + (k+1)^2$

$\Rightarrow 6S_{k+1} = k(k+1)(2k+1) + 6(k+1)^2.$

Taking out the common factor of $k + 1$ we have

$6S_{k+1} = (k+1)\big((k)(2k+1) + 6(k+1)\big).$

Expanding and collecting the right-hand term we then have

$6S_{k+1} = (k+1)\big((2k^2 + k) + (6k+6)\big)$

$\Rightarrow 6S_{k+1} = (k+1)(2k^2 + 7k + 6)$

$\Rightarrow 6S_{k+1} = (k+1)(k+2)(2k+3)$

$\Rightarrow S_{k+1} = \sum_{i=1}^{k+1} i^2 = \frac{1}{6}(k+1)((k+1)+1)(2(k+1)+1)$

We have manipulated expression **A** to obtain expression **B** ∴ expressions **A** and **B** are equivalent.

∴ If the formula is true for $n = k$, then it is also true for $n = k+1$.

Disproof by counterexample.

This is used to counter a conjecture – just one counterexample is sufficient.

Example (12): Two points are selected on the circumference of a circle and a chord is drawn to connect them - this divides the circle into two regions.

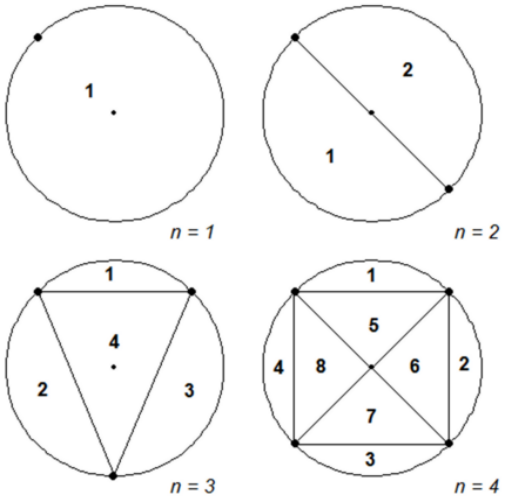
If we repeat this with three points, the circle is divided into four regions.

If four points are chosen and joined together to form all possible chords, then the same circle is divided into eight regions.

See the diagrams on the right, including the trivial case of one point (and no chord).

The number of regions, r, appears to follow the relationship $r = 2^{n-1}$.

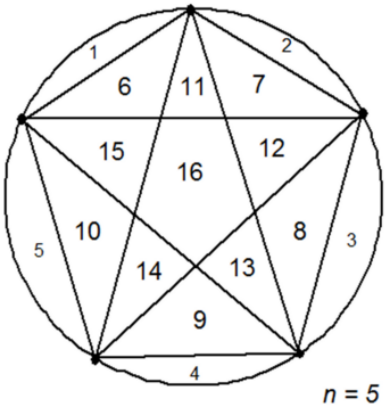
Can we prove if this is true for n =5 and n = 6 ?



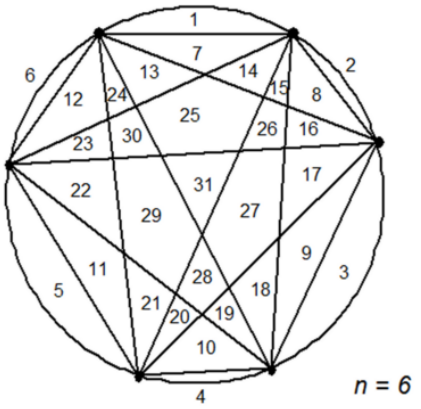
By selecting 5 points on the circumference and joining them to form all possible chords, we have 16 regions, which appears to confirm the soundness of the conjecture.

Unfortunately, the conjecture breaks down when n = 6. The maximum number of regions that can be produced is 31, not 32 as predicted.

(Had the six points been arranged in three diametrically opposite pairs rather than being offset as in the example, the number of regions would have been 30.)



16 regions - still seems to hold...



Alas... the conjecture breaks down !
31 regions, not 32 !

This counterexample therefore disproves the conjecture.

Example (13): Prove that $x^2 + x + 41$ is not necessarily prime for all positive integers x.

This is similar to Example (5), but here we are setting out to **disprove** a conjecture.

Substituting values $x = 0, 1, 2, 3, 4$ ... gives $x^2 + x + 41 = 41, 43, 47, 53, 61$ ... , which are all prime, and this does appear to hold for many higher values of x.

It is a little tedious to try testing by exhaustion, so we shall provide a counterexample algebraically.

If we set $x = 41$, the expression becomes $41^2 + 41 + 41$, which is **not** prime since 41 can be taken out as a factor:

$41^2 + 41 + 41 = 41(41 + 1 + 1) = 41 \times 43 = 1763$.

Setting $x = 40$ would also provide a counterexample, as $40^2 + 40 + 41 = 1681 = 41^2$, but any one counterexample is sufficient to disprove the conjecture.