SECTION H **Further Mathematical Induction**

By the end of this section you will be able to
- apply induction to prove divisibility propositions
- apply induction to prove other mathematical results

In the last section we used the principle of mathematical induction to prove results concerning finite sums of natural numbers. However this technique of proof can also be used to prove more widespread results as you will see in this section.

Remember the procedure for proof by mathematical induction of a proposition $P(n)$ is:

1. We check the result for $n=1$. Check $P(1)$.
2. Assume it is true for $n=k$. Assume $P(k)$. [Induction hypothesis]
3. Prove the result for $n=k+1$ by assuming it holds for $n=k$. Prove
$$P(k) \quad \Rightarrow \quad P(k+1)$$

Remember the procedure for mathematical induction is we check the result is true for $n=1$ and we assume it is true for any arbitrary number k and then prove it is true for the next number $k+1$. From this we know the result is true for all natural numbers *n*. Checking $P(1)$ is analogous to the 1st domino being knocked over. Proving $P(k) \Rightarrow P(k+1)$ is analogous to ensuring the k^{th} domino is close enough to the $(k+1)^{\text{th}}$ domino to knock it over.

Recall that to prove propositions of the type:

$P(n)$ is true for *all* natural numbers *n*

We should first consider 'proof by induction'.

H1 Divisibility

Remember we can write a divides b by the following notation $a \mid b$ where the vertical line represents division. Recall a divides b means that there is an integer m such that $am=b$ or b is a multiple of a. In mathematical notation we write

$$a \mid b \quad \Leftrightarrow \text{ there is an integer } m \text{ such that } am=b$$

This was definition (1.5) given earlier in the chapter.

In the next example we prove a result concerning the divisibility of the natural number n^2-n. In fact we prove n^2-n is an even number.

Example 4

Show that for every natural number n; n^2-n is divisible by 2, or in notation form $2 \mid (n^2-n)$.

How do we prove the given proposition?

The proposition involves natural numbers n therefore we can try using mathematical induction. We apply the principle of mathematical induction to show

$$2 \mid \left(n^2 - n\right)$$

That is 2 divides $n^2 - n$ exactly, there is NO remainder (or $n^2 - n$ is even).

Proof

First we check the proposition is true for $n = 1$:

$$1^2 - 1 = 0 \qquad \surd$$

Clearly 2 divides 0 because $2 \times 0 = 0$. (Actually every number (apart from 0) divides 0).

Hence the given proposition is true for $n = 1$.

Next we assume the proposition is true for $n = k$, that is 2 divides $k^2 - k$. This can be written in symbolic form as

$$2 \mid \left(k^2 - k\right)$$

which means there is an integer m such that

$$2m = k^2 - k \qquad (*)$$

The challenge in applying mathematical induction is to prove the given proposition for the next number $k+1$. *What do we need to prove?*

We need to show that 2 divides $(k+1)^2 - (k+1)$ or $(k+1)^2 - (k+1)$ is a multiple of 2. Well let's examine this expression, $(k+1)^2 - (k+1)$, and see if it is a multiple of 2:

$$\begin{aligned}(k+1)^2 - (k+1) &= k^2 + 2k + 1 - k - 1 && [\text{Expanding Brackets}]\\ &= k^2 - k + 2k + 1 - 1 && [\text{Rearranging}]\\ &= \underbrace{k^2 - k}_{=2m \text{ by } (*)} + 2k\\ &= 2m + 2k \ = 2(m + k)\end{aligned}$$

Hence $(k+1)^2 - (k+1)$ is multiple of 2 because

$$(k+1)^2 - (k+1) = 2(m+k) \qquad [2\times(\text{Integer})]$$

Therefore 2 divides $(k+1)^2 - (k+1)$. We have proven the given proposition for $n = k+1$.

Thus by induction, 2 divides $n^2 - n$, our required result.

■

In example 4 we proved that $n^2 - n$ is an even number or $2 \mid \left(n^2 - n\right)$. We first checked it was correct for $n = 1$ then we assumed it was true for $n = k$ and finally we showed the result holds for $n = k+1$ - the k^{th} domino knocks over the $(k+1)^{\text{th}}$ domino which means *all* the dominos have fallen.

Example 5

For every natural number *n* prove the proposition $P(n)$ given by

$$3 \mid \left(2^{2n-1} + 1\right)$$

What does $3 \mid \left(2^{2n-1} + 1\right)$ *mean?*

$2^{2n-1} + 1$ is divisible by 3 exactly

or there is an integer m such that

$$2^{2n-1}+1=3m$$

That is $2^{2n-1}+1$ is a multiple of 3 for every natural number n.

Proof

How do we prove $3\left|\left(2^{2n-1}+1\right)\right.$*?*

We apply mathematical induction. *Why?*

Because we need to prove the given proposition $P(n)$ holds for every natural number n.

First we check the proposition is true for $n=1$, that is $P(1)$, by substituting this into $2^{2n-1}+1$:

$$2^{2-1}+1=2^1+1=3 \qquad \surd$$

Clearly 3 divides 3 and this is denoted by $3\left|\left(2^{2-1}+1\right)\right.$. Hence the proposition is true for $P(1)$.

Next we assume the given proposition is true for $n=k$ that is 3 divides $2^{2k-1}+1$. This means there is an integer q such that

$$3q=2^{2k-1}+1 \qquad (\dagger)$$

Challenge is to prove the result for the next number $k+1$ by using (†). *How do we write down* $P(k+1)$*?*

By substituting $n=k+1$ into the given proposition $3\left|\left(2^{2n-1}+1\right)\right.$:

$$3\left|\left(2^{2(k+1)-1}+1\right)\right.$$

That is we *need* to prove

$$3 \text{ divides } 2^{2(k+1)-1}+1$$

Let's examine the right hand term, $2^{2(k+1)-1}+1$:

$$\begin{aligned}
2^{2(k+1)-1}+1 &= 2^{2k-1+2}+1 && \left[\text{Rewriting the index of 2}\right]\\
&= 2^{2k-1}2^2+1 && \left[\text{Applying the rules of indices } a^{m+n}=a^m a^n\right]\\
&= (4)2^{2k-1}+1 && \left[\text{Rewriting } 2^2=4\right]\\
&= (3+1)2^{2k-1}+1 && \left[\text{Rewriting } 4=3+1\right]\\
&= (3)2^{2k-1}+2^{2k-1}+1 && \left[\text{Expanding } (3+1)2^{2k-1}\right]
\end{aligned}$$

By (†) we know the last two terms on the right hand side , $2^{2k-1}+1$, are equal to $3q$.

Therefore we have

$$\begin{aligned}
2^{2(k+1)-1}+1 &= (3)2^{2k-1}+\underbrace{2^{2k-1}+1}_{=3q \text{ by } (\dagger)}\\
&= (3)2^{2k-1}+3q\\
&= 3\left(2^{2k-1}+q\right) && \left[\text{Taking out a common factor of 3}\right]
\end{aligned}$$

Hence the left hand term $2^{2(k+1)-1}+1=3(\text{Integer})$ which means it is a multiple of 3 or 3 divides $2^{2(k+1)-1}+1$. We have proven $P(k) \Rightarrow P(k+1)$. Therefore our result follows by induction.

■

H2 Using Mathematical Induction to Prove Other Results

We can apply the principle of mathematical induction to prove general results concerning natural numbers. For example we can use induction to prove the binomial theorem for positive integers (natural numbers) which you are asked to show in Exercise 1(h).
There is a great deal of algebraic manipulation in proving the binomial theorem but the procedure of mathematical induction is the same as in sections G and H1.
Let's first prove a result regarding the factoring of $a^n - b^n$ where a and b are real numbers and n is a natural number. This is a particularly useful result because it can be employed to factor polynomials of the form $a^n - b^n$. The difficulty lies in trying to prove the result for $n = k+1$ so we use the 'trick' of writing 0 as $x - x$, or in our Example 6 below $-a^k b + a^k b (= 0)$.

Up to now we have been proving results by mathematical induction for all natural numbers 1, 2, 3, 4,…, *n*, …
Clearly some results may *not* be valid for the first few natural numbers. That is the initial value given in the proposition may not be 1 but some other natural number such as n_0 say. In the next example the result is valid for 1, 2, 3, 4, 5,…, *n*, … but the starting point is $n = 2$ and *not* $n = 1$. In general the process of mathematical induction is the same apart from the starting point. If the starting point is n_0 then the process of mathematical induction is:

1. We check the result for $n = n_0$ (starting point). Check $P(n_0)$.
2. Assume it is true for $n = k$. Assume $P(k)$. [Induction hypothesis]
3. Prove the result for $n = k+1$ by assuming it holds for $n = k$. Prove
$$P(k) \quad \Rightarrow \quad P(k+1)$$

Example 6

Let a and b be real numbers then for the natural numbers $n \geq 2$ we have the proposition $P(n)$ given by

$$a^n - b^n = (a-b)\left(a^{n-1} + a^{n-2}b + a^{n-3}b^2 + \cdots + b^{n-1}\right)$$

Prove $P(n)$.

What does this proposition mean?

It says that if you have a polynomial of the form $a^n - b^n$ then it can be factorized into

$$(a-b)\left(a^{n-1} + a^{n-2}b + a^{n-3}b^2 + \cdots + b^{n-1}\right)$$

We can use this result to solve equations of the type $a^n - b^n = 0$. *In any case how do we prove this result?*

It is a result concerning natural numbers n therefore we can use induction.

Proof

We first show this result for $n = 2$ (Our starting point is $n = 2$). *How?*

By substituting $n = 2$ into the given proposition:

$$a^2 - b^2 = (a-b)\underbrace{\left(a^{2-1} + b^{2-1}\right)}_{=a^1+b^1}$$

$$a^2 - b^2 = (a-b)(a+b)$$

Of course this is a fundamental identity in algebra, do you remember what it is called?

It is the difference of two squares'. Thus $P(2)$ is true.

Assume the proposition is true for $n=k$ that is $P(k)$. *How do we write* $P(k)$*?*

By substituting $n=k$ into the given proposition:

$$a^k-b^k=(a-b)\left(a^{k-1}+a^{k-2}b+a^{k-3}b^2+\cdots+b^{k-1}\right) \qquad (*)$$

The difficulty in the process of induction is to prove the result for $n=k+1$ by employing (*). *What do we need to prove?*

Required to prove $P(k+1)$ which is

$$a^{k+1}-b^{k+1}=(a-b)\left(a^{k+1-1}+a^{k+1-2}b+a^{k+1-3}b^2+\cdots+b^{k+1-1}\right)$$

$$=(a-b)\left(a^k+a^{k-1}b+a^{k-2}b^2+\cdots+b^k\right) \qquad (**)$$

We need to show the left hand side is equal to the right hand side of (**). Let's consider the left hand side:

$$a^{k+1}-b^{k+1}=a^{k+1}-a^kb+a^kb-b^{k+1} \qquad \left[\begin{array}{l}\text{Using the above stated trick}\\ \text{of writing } 0=-a^kb+a^kb\end{array}\right]$$

$$=a^ka-a^kb+a^kb-b^kb \qquad \left[\text{Using the rules of indices } a^{m+n}=a^ma^n\right]$$

$$=a^k(a-b)+b\left(a^k-b^k\right) \qquad [\text{Factorizing out common terms}]$$

$$=a^k(a-b)+b\underbrace{(a-b)\left(a^{k-1}+a^{k-2}b+a^{k-3}b^2+\cdots+b^{k-1}\right)}_{\text{by (*)}}$$

$$=(a-b)\left[a^k+b\left(a^{k-1}+a^{k-2}b+a^{k-3}b^2+\cdots+b^{k-1}\right)\right] \qquad \left[\text{Factorizing out } (a-b)\right]$$

$$=(a-b)\left[a^k+a^{k-1}b+a^{k-2}b^2+a^{k-3}b^3+\cdots+b^k\right] \qquad \left[\begin{array}{l}\text{Multiplying by } b\\ \text{in the second bracket}\end{array}\right]$$

The last line is the right hand side of (**) so we have shown (**). Hence we have our result,

$$a^n-b^n=(a-b)\left(a^{n-1}+a^{n-2}b+a^{n-3}b^2+\cdots+b^{n-1}\right)$$

■

Example 6 was a challenging problem but the procedure for mathematical induction remained the same, apart from the starting point which was $n=2$.

H3 Principle of Strong Mathematical Induction

Up to now we have always used an induction hypothesis $P(k)$ to prove the proposition for the next number, $P(k+1)$. Sometimes it is difficult to derive $P(k+1)$ from the previous $P(k)$. However you may see a connection between $P(k+1)$ and $P(m)$ where m is greater than or equal to 1 and less than k. *Can we use* $P(m)$ *where* $1\le m<k$ *to prove* $P(k+1)$*?*

Yes of course. Recall the domino effect – all the dominos before the $(k+1)^{\text{th}}$ domino have fallen so the proposition is true for *m* where $1\le m<k$. Actually

$$P(1),\ P(2),\ \cdots,\ P(m),\ \cdots,\ P(k) \text{ are all true}$$

The difference between strong mathematical induction and just mathematical induction is that to show $P(k+1)$ we can use any of the previous propositions, that is we can use

$$P(1),\ P(2),\ \cdots,\ P(m),\ \cdots,\ P(k)$$

and *not* just $P(k)$.

For the next example we demonstrate a strong induction process.

Example 7

Prove that every integer $n \geq 2$ is a product of primes.

Proof

Clearly the result holds for $n = 2$ because 2 is a prime.

Assume that result is true for all the natural numbers between 2 and *k*. This means that the numbers

$$2,\ 3,\ 4,\ \cdots,\ k \text{ can be written as a product of primes} \qquad (*)$$

We are required to prove that the next number, $k+1$, can also be written as a product of primes.

If $k+1$ is prime then we are done because we have a product of primes.

If $k+1$ is composite then there are natural numbers p and q such that

$$pq = k+1$$

Note that *p* and *q* lie between 2 and *k*, that is $2 \leq p \leq k$ and $2 \leq q \leq k$. By the induction hypothesis (*) we know that *p* and *q* can be written as a product of primes.

Since $k+1 = pq$ so we can write $k+1$ as a product of primes.

By the principle of strong induction we have our result.

■

H4 de Moivre's Theorem

The following example requires a basic knowledge of complex numbers. If you have not covered the basic properties of complex numbers then you may find the next example problematic. However try following it through.

The complex identity we will use is $i^2 = -1$.

This is one of the fundamental theorems of complex numbers called de Moivre's theorem, which we will prove by applying mathematical induction.

We prove an important theorem on complex numbers called de Moivre's theorem by applying mathematical induction.

Figure 3
Abraham de Moivre
1667 to 1754

Abraham de Movire was born in France in 1667 but moved to England in 1688 because of religious intolerance in France. He lived in London for the rest of his life, becoming a private tutor in

mathematics. He wrote a book on probability theory titled 'Doctrine of Chances' which was one of the areas he worked in. He also occupied himself in the fields of trigonometry and algebra. However, to most undergraduate students he is better known for de Moivre's theorem, which converts a complex numbers problem to a trigonometry problem. You can use de Moivre's theorem to derive some of the most elegant trigonometric identities.

We need to use the following trigonometric identities to prove de Moivre's theorem.

$$\cos(A+B)=\cos(A)\cos(B)-\sin(A)\sin(B) \qquad (\dagger)$$

$$\sin(A+B)=\sin(A)\cos(B)+\cos(A)\sin(B) \qquad (\dagger\dagger)$$

Example 8

Prove de Moivre's theorem, that is prove that

$$\left[\cos(\_)+i\sin(\_)\right]^n=\cos(n\_)+i\sin(n\_)$$

where n is a natural number.

Proof

Check that the theorem is correct for $n=1$:

$$\left[\cos(\_)+i\sin(\_)\right]^1=\cos(\_)+i\sin(\_) \qquad \surd$$

Hence the theorem is true for $n=1$. Next we assume the theorem is true for $n=k$, that is

$$\left[\cos(\_)+i\sin(\_)\right]^k=\cos(k\_)+i\sin(k\_) \qquad (*)$$

What is our next step?

We are Required to show that the theorem for the next number, $n=k+1$, is true *How do we write down de Moivre's theorem for* $n=k+1$*?*

By substituting $n=k+1$ into the given proposition

$$\left[\cos(\_)+i\sin(\_)\right]^n=\cos(n\_)+i\sin(n\_)$$

which gives

$$\left[\cos(\_)+i\sin(\_)\right]^{k+1}=\cos\left((k+1)\_\right)+i\sin\left((k+1)\_\right) \qquad (**)$$

We need to prove (**).

Examining the left hand side of (**) we have

$$\begin{aligned}
\left[\cos(_)+i\sin(_)\right]^{k+1} &= \left[\cos(_)+i\sin(_)\right]^{k}\left[\cos(_)+i\sin(_)\right]^{1} \quad \left[\text{By } a^{m+n}=a^m a^n\right] \\
&= \underbrace{\left[\cos(k_)+i\sin(k_)\right]}_{\text{by (*)}}\left[\cos(_)+i\sin(_)\right] \quad \left[\text{Remember } a^1=a\right] \\
&= \cos(k_)\cos(_)+i\left[\sin(_)\cos(k_)\right] \\
&\quad +i\left[\sin(k_)\cos(_)\right]+i^2\left[\sin(k_)\sin(_)\right] \quad \left[\text{Expanding brackets}\right] \\
&= \cos(k_)\cos(_)+i\left[\sin(_)\cos(k_)+\sin(k_)\cos(_)\right]-\sin(k_)\sin(_) \\
&\qquad \left[\text{Collecting } i \text{ terms and using } i^2=-1\right] \\
&= \underbrace{\cos(k_)\cos(_)-\sin(k_)\sin(_)}_{=\cos(k_+_)\text{ by (†)}}+i\underbrace{\left[\sin(_)\cos(k_)+\cos(_)\sin(k_)\right]}_{=\sin(k_+_)\text{ by (††)}} \\
&\qquad \left[\text{Applying the above trigonometric identities}\right] \\
&= \cos(k_+_)+i\left[\sin(k_+_)\right] \\
&= \cos\left((k+1)_\right)+i\left[\sin\left((k+1)_\right)\right] \qquad \left[\text{Factorizing } \; k_+_=(k+1)_\right]
\end{aligned}$$

The last line is the same as the right hand side of (**). We have established (**), which means the required result has been proven:

$$\left[\cos(\_)+i\sin(\_)\right]^{k+1}=\cos\left((k+1)\_\right)+i\sin\left((k+1)\_\right)$$

Hence by mathematical induction we have proven de Movire's theorem for any natural number n.

■

Comment: de Movire's theorem is actually true for *all* real values of n but we have just proved it for all natural numbers n. In fact de Moivre derived it for natural numbers n but Euler, the Swiss mathematician, derived it for all real values of n in 1749.

SUMMARY

The general procedure in the case of proving a proposition $P(n)$ by induction is

1. Check the result for $P(n_0)$.
2. Assume it is true for $P(k)$.
3. Prove $P(k) \;\Rightarrow\; P(k+1)$.