SECTION H **Further Mathematical Induction**

By the end of this section you will be able to

- apply proof by induction to prove divisibility results
- apply proof by induction to prove other mathematical results such as factorization and de Moivre's theorem

So far we have 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 $P(k)$.
3. Prove the result for $n=k+1$ by assuming it holds for $n=k$. Prove $P(k) \Rightarrow P(k+1)$.

First we apply mathematical induction to prove a certain term is divisible by an integer.

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

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

This was definition (1.5) 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 46

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

Comment

How do we prove the given proposition?

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

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

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 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

$$2\,|\,(k^2-k)$$

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 $n=k+1$ by using (*). *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:

$$\begin{aligned}(k+1)^2-(k+1)&=k^2+2k+1-k-1 && [\text{Expanding Brackets}]\\ &=k^2-k+2k+\underbrace{1-1}_{=0} && [\text{Rearranging}]\\ &=\underbrace{k^2-k}_{=2m \text{ by (*)}}+2k\\ &=2m+2k \ =2(m+k)\end{aligned}$$

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

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

therefore 2 divides $(k+1)^2-(k+1)$ and in symbolic form $2\,|\,(k+1)^2-(k+1)$. We have proven the given proposition for $n=k+1$. Thus we have by induction that 2 divides n^2-n the required result.

■

In example 46 we proved that n^2-n is an even number or $2\,|\,(n^2-n)$. 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 $n=k+1$.

Example 47

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

$$3\,|\,(2^{2n-1}+1)$$

Comment

What does $3\,|\,(2^{2n-1}+1)$ *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 $3\,|\,(2^{2n-1}+1)$*?*

We apply mathematical induction. *Why?*
Because 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 $3 \mid (2^{2-1}+1)$**.** Hence the proposition is true for $P(1)$. Next we assume the given proposition is true for $n=k$ that is 3 divides $2^{2k-1}+1$ or in notation form $3 \mid (2^{2k-1}+1)$. This means there is an integer q such that

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

Challenge is to prove the result for $n=k+1$ by using (\$). *How do we write down* $P(k+1)$*?*
By substituting $n=k+1$ into the given proposition $3 \mid (2^{2n-1}+1)$:

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

That is we **need to prove**

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

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

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

By (\$) we know the last two terms on the Right Hand Side, $2^{2k-1}+1$, are equal to $3q$. Therefore we have

$$\begin{aligned}
2^{2(k+1)-1}+1 &= (3)2^{2k-1}+\underbrace{2^{2k-1}+1}_{=3q \text{ by } (\$)} \\
&= (3)2^{2k-1}+3q \\
&= 3(2^{2k-1}+q) && [\text{Taking Out a Common Factor of 3}]
\end{aligned}$$

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). 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. You are asked to show the binomial theorem in Exercise 1(h).
Let's first prove a result regarding factorizing 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 factorize polynomials of the form $a^n - b^n$. The difficulty is trying to prove the result for $n = k+1$ and we use the 'trick' of writing 0 as $x - x$ or in our Example 48 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 starting point may not be 1 but some other natural number such as n_0 say. In the next example the result is valid for 2, 3, 4, 5,…, *n*, … so 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 $P(k)$.
3. Prove the result for $n = k+1$ by assuming it holds for $n = k$. Prove $P(k) \Rightarrow P(k+1)$.

In the next example the starting point is $n = 2$.

Example 48

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

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

Prove $P(n)$.

Comment

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

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

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

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:

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

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 $P(k+1)$. *How do we write* $P(k+1)$*?*

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

$$\begin{aligned} a^{k+1}-b^{k+1} &= (a-b)\left(a^{k+1-1}+a^{k+1-2}b+a^{k+1-3}b^2+\ldots+b^{k+1-1}\right) \\ &= (a-b)\left(a^k+a^{k-1}b+a^{k-2}b^2+\ldots+b^k\right) \qquad (**) \end{aligned}$$

We need to show the Left Hand Side is equal to the Right Hand Side of (**). Let's consider the Left Hand Side on its own:

$$\begin{aligned} a^{k+1}-b^{k+1} &= a^{k+1}-a^kb+a^kb-b^{k+1} && \left[\begin{array}{l}\text{Using the above stated trick}\\ \text{of writing } 0=-a^kb+a^kb\end{array}\right] \\ &= a^ka-a^kb+a^kb-b^kb && \left[\text{Using the rules of indices } a^{m+n}=a^ma^n\right] \\ &= a^k(a-b)+b\left(a^k-b^k\right) && \left[\text{Factorizing out common terms}\right] \\ &= a^k(a-b)+b\underbrace{(a-b)\left(a^{k-1}+a^{k-2}b+a^{k-3}b^2+\ldots+b^{k-1}\right)}_{\text{by (*)}} \\ &= (a-b)\left(a^k+b\left(a^{k-1}+a^{k-2}b+a^{k-3}b^2+\ldots+b^{k-1}\right)\right) && \left[\text{Factorizing out } (a-b)\right] \\ &= (a-b)\left(a^k+a^{k-1}b+a^{k-2}b^2+a^{k-3}b^3+\ldots+b^k\right) && \left[\begin{array}{l}\text{Multiplying by } b\\ \text{in the Second Bracket}\end{array}\right] \end{aligned}$$

Since the last line is the Right Hand Side of (**) we have shown (**). Hence we have our result, $a^n-b^n=(a-b)\left(a^{n-1}+a^{n-2}b+a^{n-3}b^2+\ldots+b^{n-1}\right)$.

■

Example 48 was a challenging problem but the procedure for mathematical induction is the same apart from the starting point which was $n=2$.

H3 de Moivre's Theorem

The following example requires you to know basic concepts of complex numbers. If you have not covered basic properties of complex numbers then you will find the next example problematic. However try following it through. The result of complex numbers that you need to know is $i^2=-1$.

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

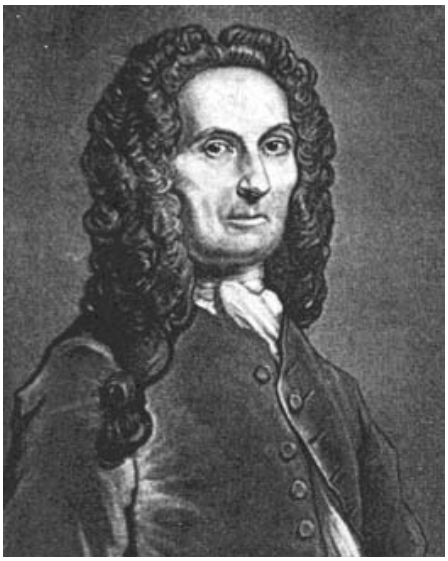

Figure 7
Abraham de Moivre
1667 to 1754

Abraham de Movire was born in France in 1667 and around 1688 he moved to England 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 transforms a problem from complex numbers to trigonometry. You can use de Moivre's theorem to derive 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 49

Prove de Moivre's theorem that is

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

where n is a natural number.
[Comment: This result is actually true for all real values of n but we will just prove 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].

Proof

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

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

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

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

What is our next step?
Required to show the theorem for $n=k+1$. *How do we write down de Moivre's theorem for* $n=k+1$ *?*

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

$$\left[\cos(\theta)+i\sin(\theta)\right]^{n} = \cos(n\theta)+i\sin(n\theta)$$

which gives

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

We need to prove ($\blacktriangle\blacktriangle$). *What do we need to show?*
The Left Hand Side is equal to the Right Hand Side of ($\blacktriangle\blacktriangle$). *How?*
We need to employ ($\blacktriangle$) in the derivation. Examining the Left Hand Side we have

$$\left[\cos(\theta)+i\sin(\theta)\right]^{k+1} = \left[\cos(\theta)+i\sin(\theta)\right]^{k}\left[\cos(\theta)+i\sin(\theta)\right]^{1} \qquad \left[\begin{array}{l}\text{Using the rules of}\\ \text{Indices } a^{m+n}=a^{m}a^{n}\end{array}\right]$$

$$= \underbrace{\left[\cos(k\theta)+i\sin(k\theta)\right]}_{\text{by }(\blacktriangle)}\left[\cos(\theta)+i\sin(\theta)\right] \qquad \left[\text{Remember } a^{1}=a\right]$$

$$= \cos(k\theta)\cos(\theta)+i\left[\sin(\theta)\cos(k\theta)\right]+i\left[\sin(k\theta)\cos(\theta)\right]+i^{2}\left[\sin(k\theta)\sin(\theta)\right]$$

$$\left[\text{Expanding Brackets}\right]$$

$$= \cos(k\theta)\cos(\theta)+i\left[\sin(\theta)\cos(k\theta)+\sin(k\theta)\cos(\theta)\right]-\sin(k\theta)\sin(\theta)$$

$$\left[\text{Collecting } i \text{ terms and using } i^{2}=-1\right]$$

$$= \underbrace{\cos(k\theta)\cos(\theta)-\sin(k\theta)\sin(\theta)}_{=\cos(k\theta+\theta)\text{ by }(\dagger)}+i\underbrace{\left[\sin(\theta)\cos(k\theta)+\sin(k\theta)\cos(\theta)\right]}_{=\sin(k\theta+\theta)\text{ by }(\dagger\dagger)}$$

$$\left[\text{Applying the above trigonometric identities}\right]$$

$$= \cos(k\theta+\theta)+i\left[\sin(k\theta+\theta)\right]$$

$$= \cos\left((k+1)\theta\right)+i\left[\sin\left((k+1)\theta\right)\right] \qquad \left[\text{Writing } k\theta+\theta=(k+1)\theta\right]$$

The last line is the same as the Right Hand Side of ($\blacktriangle\blacktriangle$). We have ($\blacktriangle\blacktriangle$), which means required result has been proven:

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

Hence we have proven de Movire's theorem for the natural number n.

■

SUMMARY

We can apply mathematical induction to prove results concerning divisibility and other areas of mathematics.

Starting point of mathematical induction may not be 1 but n_0 say. The procedure in this 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 $P(k) \Rightarrow P(k+1)$.