AMSI
AUSTRALIAN MATHEMATICAL
SCIENCES INSTITUTE

INTERNATIONAL CENTRE
OF EXCELLENCE FOR
EDUCATION IN
MATHEMATICS

The Improving Mathematics Education in Schools (TIMES) Project

PRIMES AND PRIME FACTORISATION

A guide for teachers - Years 7–8

NUMBER AND ALGEBRA :
Module 16

June 2011

YEARS 7 8

Primes and prime factorisation

(Number and Algebra : Module 16)

For teachers of Primary and Secondary Mathematics

510

Cover design, Layout design and Typesetting by Claire Ho

The Improving Mathematics Education in Schools (TIMES) Project 2009-2011 was funded by the Australian Government Department of Education, Employment and Workplace Relations.

The views expressed here are those of the author and do not necessarily represent the views of the Australian Government Department of Education, Employment and Workplace Relations.

The Improving Mathematics Education in Schools (TIMES) Project

PRIMES AND PRIME FACTORISATION

A guide for teachers - Years 7–8

NUMBER AND ALGEBRA
Module 16

June 2011

Peter Brown
Michael Evans
David Hunt
Janine McIntosh
Bill Pender
Jacqui Ramagge

YEARS
7
8

PRIMES AND PRIME FACTORISATION

ASSUMED KNOWLEDGE

- Fluency in multiplication and division are essential.
- Divisibility tests, particularly by 2, 3, 5 and 11, are useful.
- Index notation with whole-number indices, and square roots, are required.
- The Highest Common Factor (HCF) and The Lowest Common Multiple (LCM), and cube and possibly higher roots, are required for the last two content items, which are often studied a little later than prime factorisation.

MOTIVATION

A fundamental technique in mathematics is to break something down into its component parts, and rebuild it from those parts. Thus we can factor any whole number into a product of *prime numbers*, for example

$$60 = 2^2 \times 3 \times 5$$

and this prime factorisation is unique, apart from the order of the factors. Conversely, if we are given the prime factors of a number, we can reconstruct the original whole number by multiplying the prime factors together,

$$(2 \times 2) \times (3 \times 5) = 4 \times 15 = 60 \qquad \text{or} \qquad (2 \times 5) \times (2 \times 3) = 10 \times 6 = 60$$

and we will always get the same original number, whatever order we choose for multiplying the prime factors.

In other situations, however, such processes do not work nearly as straightforwardly, as can be illustrated using the analogy of chemistry. Every *compound* can be broken down uniquely into its elements, but if we are given the *elements*, there are often a great many different compounds that can be formed from them.

Prime factorisation is a very useful tool when working with whole numbers, and will be used in mental arithmetic, in fractions, for finding square roots, and in calculating the HCF and LCM.

CONTENT

THE DEFINITION OF PRIME NUMBERS

The discussion above shows that for the purposes of prime factorisation, we need to distinguish three types of whole numbers. We leave aside the numbers 0 and 1, and then organise the remaining whole numbers 2, 3, 4, 5, ... into:

- the prime numbers 2, 3, 5, 7, 11, ..., which cannot be factored into smaller numbers,
- the composite numbers 4, 6, 8, 9, 10, ..., which can be factored into the product of two smaller numbers.

Prime numbers and composite numbers need to be defined rather carefully:

- A **prime number** is a whole number greater than 1 whose only whole number factors are itself and 1.'
- A **composite number** is a whole number greater than 1 that is not a prime number.

The phrase 'greater than 1' is needed in the definition of prime numbers to exclude 1. We do not want 1 to be a prime number, otherwise the factorisation of numbers into primes would not be unique. For example, we could write

$$60 = 2^2 \times 3 \times 5 = 1 \times 2^2 \times 3 \times 5 = 1^2 \times 2^2 \times 3 \times 5 = \ldots$$

The phrase 'greater than 1' is needed in the definition of composite numbers to exclude 1, which has no prime factors and so is not the product of two or more prime numbers. The phrase also excludes 0, which is divisible by every whole number and so has no sensible prime factorisation.

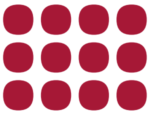
The number system we are talking about is the set of whole numbers 0, 1, 2, 3, ..., and the phrase 'whole number factor' makes the restriction in the definitions quite clear. Students often realise that a prime number like 5 has other factors if larger number systems are considered, for example,

$$5 = (-5) \times (-1) \qquad \text{and} \qquad 5 = 2 \times 2\tfrac{1}{2}.$$

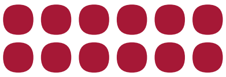
It is better to be precise than to invite arguments about what may be implied, but unsaid.

PRIMES AND RECTANGULAR ARRAYS

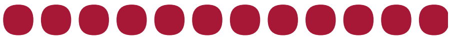
A composite number can be represented by at least two different rectangular arrays. For example, 12 can be represented by rectangular arrays in three ways:



12 = 3 × 4

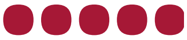


12 = 2 × 6



12 = 1 × 12

A prime number like 5, however, can only be represented by a rectangular array with just one row.



5 = 1 × 5

PRIME FACTORISATION AND ITS UNIQUENESS

The two basic facts about prime factorisation are:

1 Every whole number greater than 1 is either prime or can be written as a product of prime numbers.

2 This prime factorisation is unique, apart from the order in which we write the prime factors.

The first part is easy to prove. If the number is not prime, keep factoring it into smaller factors. The process must stop because the factors get smaller at every step, but each factor is bigger than 1. When the process can't be continued any further, the factors are all primes.

The proof of the uniqueness statement involves mathematics that is beyond the K-10 Syllabus. The proof is included in an appendix at the end if this module.

This theorem is known as **The Fundamental Theorem of Arithmetic**

THERE ARE INFINITELY MANY PRIMES

Euclid's *Elements* has a wonderful and simple proof by contradiction of the fact that there are infinitely many prime numbers.

Take any finite collection of primes, say 2, 5, 7 and 11. Multiply them together and add 1 to give

$$2 \times 5 \times 7 \times 11 + 1 = 770 + 1 = 771.$$

The resulting number 771 is not divisible by 2, or by 5, or by 7, or 11, because the remainder will be 1 after division by each of these primes. Hence either 771 is a prime different from 2, 5, 7 and 11, or its prime factorisation involves primes different from 2, 5, 7 and 11. (In this case, 771 happens to have prime factorisation 771 = 3 × 257.)

If there were only finitely many primes, we could multiply them all together and add 1, and the resulting number would have a prime factorisation that did not involve any primes on our finite list. This, of course, would be a contradiction.

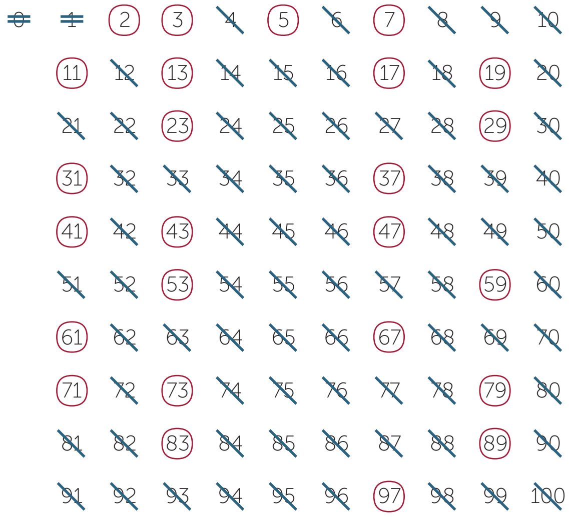
PROOF BY CONTRADICTION

The previous section used a proof by contradiction. This is a very dramatic way of proving theorems, because it starts off by assuming that the theorem is false, and then argues logically from this assumption to a contradiction. Proof by contradiction is probably best introduced to students by using it to prove that there are infinitely many whole numbers.

Suppose by way of contradiction that there were only finitely many whole numbers. If this were the case, we could sort through them and find the largest whole number N. Then $N + 1$ would be a whole number greater than N. This is a contradiction, because N was chosen to be the greatest whole number. Hence there are infinitely many whole numbers.

THE SIEVE OF ERATOSTHENES

Here is a systematic way of writing down all the prime numbers, and all the composite numbers, up to 100.



~~0~~	~~1~~	2	3	~~4~~	5	~~6~~	7	~~8~~	~~9~~	~~10~~
	11	~~12~~	13	~~14~~	~~15~~	~~16~~	17	~~18~~	19	~~20~~
	~~21~~	~~22~~	23	~~24~~	~~25~~	~~26~~	~~27~~	~~28~~	29	~~30~~
	31	~~32~~	~~33~~	~~34~~	~~35~~	~~36~~	37	~~38~~	~~39~~	~~40~~
	41	~~42~~	43	~~44~~	~~45~~	~~46~~	47	~~48~~	~~49~~	~~50~~
	~~51~~	~~52~~	53	~~54~~	~~55~~	~~56~~	~~57~~	~~58~~	59	~~60~~
	61	~~62~~	~~63~~	~~64~~	~~65~~	~~66~~	67	~~68~~	~~69~~	~~70~~
	71	~~72~~	73	~~74~~	~~75~~	~~76~~	~~77~~	~~78~~	79	~~80~~
	~~81~~	~~82~~	83	~~84~~	~~85~~	~~86~~	~~87~~	~~88~~	89	~~90~~
	~~91~~	~~92~~	~~93~~	~~94~~	~~95~~	~~96~~	97	~~98~~	~~99~~	~~100~~

1 Write down all the whole numbers up to 100.

2 Cross out 0 and 1 — they are exceptions.

3 Circle the next number 2, and then cross out every multiple of 2

4 Circle the next number not crossed out (which is 3), and then cross out multiples of 3.

5 Continue until all numbers are either circled or crossed out.

The 25 circled numbers are the primes up to 100, and the 74 crossed-out numbers (not including 0 and 1) are the composite numbers up to 100.

The patterns within the sequence of prime numbers are notoriously complicated, and have generated some of the most famous solved and unsolved problems in mathematics. Apart from the obvious fact that all primes end in 1, 3, 7 or 9, except for 2 and 5, there are no other obvious patterns.

The table does give some hint that the primes become more widely spaced on average as the numbers get bigger. This is intuitively clear once one observes that more and more prime numbers are used in the sieving process as the numbers get bigger.

EXERCISE 1

a Imagine the sieving process extended to all numbers up to 200. Identify all the composite numbers from 100 to 200 that are sieved by 11 and 13, but were not sieved by 2, 3, 5 or 7.

b Identify the first times there are gaps of exactly 4, 6 and 8 between successive prime numbers.

PRIME TESTING AND FACTORISING A NUMBER

Testing whether a reasonably large number is prime is a massive computing problem. One important insight, however, greatly reduces the amount of computation required.

Students will have noticed from the Sieve of Eratosthenes that when finding all primes up to 100, it was only necessary to sieve by the primes 2, 3, 5 and 7. When they sieved by the next prime 11, they would have found that all the multiples of 11 were already crossed out, because the first multiple of 11 not crossed out already would be $11 \times 11 = 121$, which is greater than 100. The general principle is:

- When testing whether a whole number n is prime, it is sufficient to test divisibility by all the primes up to $\sqrt{n}$.

Any number n that is to be tested in school mathematics should thus yield to the following plan of attack:

- Use the standard divisibility tests to test n for divisibility by the primes 2, 3, 5 and 11. These divisions tests are presented in the module, *Multiples, Factors and Powers*.
- Then use division to test divisibility by the remaining primes 7, 13, 17, 19, ... up to $\sqrt{n}$.

It is usual to write the prime factorisation in index form with the primes in increasing order,

$$60 = 2^2 \times 3 \times 5.$$

EXERCISE 2

List the primes that are needed when the Sieve of Eratosthenes is applied to find all the primes up to 1000.

EXERCISE 3

How many final zeroes are there in the number $30! = 30 \times 29 \times 28 \times \ldots \times 2 \times 1$?

PRIMES AND MENTAL ARITHMETIC

Awareness of prime divisors can greatly simplify mental arithmetic problems. Combining factors of 2 and 5 together is always useful:

$15 \times 14 = 30 \times 7 = 210$ and $825 \div 25 = 1650 \div 50 = 3300 \div 100 = 33$.

In other situations, dealing separately with different prime divisors can be helpful:

$17 \times 33 = 51 \times 11 = 561$ and $616 \div 28 = 308 \div 14 = 154 \div 7 = 22$.

Powers of 2 and powers of 5 are particularly easy to work with:

$8 \times 17 = 4 \times 34 = 2 \times 68 = 136$ (double, double, double 17)

$496 \div 8 = 248 \div 4 = 124 \div 2 = 62$ (halve, halve, halve 496)

$112 \times 125 = 56 \times 250 = 28 \times 500 = 14 \times 1000 = 14000$ (halve, halve, halve 112)

EXERCISE 4

Calculate mentally using primes:

75×12, $714 \div 21$, 17×55, $1325 \div 25$, $1072 \div 16$.

LISTING FACTORS OF A NUMBER

Once the prime factorisation of a number has been obtained, all its factors can quickly be written down. For example,

$60 = 2^2 \times 3 \times 5$;

so the complete list of factors of 60 is

$2^2 \times 3 \times 5 = 60$ $2^1 \times 3 \times 5 = 30$ $1 \times 3 \times 5 = 15$

$2^2 \times 1 \times 5 = 20$ $2^1 \times 1 \times 5 = 10$ $1 \times 1 \times 5 = 5$

$2^2 \times 3 \times 1 = 12$ $2^1 \times 3 \times 1 = 6$ $1 \times 3 \times 1 = 3$

$2^2 \times 1 \times 1 = 4$ $2^1 \times 1 \times 1 = 2$ $1 \times 1 \times 1 = 1$

and the total number of factors is

$(2 + 1) \times (1 + 1) \times (1 + 1) = 12$,

because the power of 2 in the factor can be 1, 2 or 2^2 (3 choices), the power of 3 can be 1 or 3 (2 choices), and the power of 5 can be 1 or 5 (2 choices).

EXERCISE 5

a List all the factors of 256 and 210.

b Prove that a number is a square if and only if it has an odd number of factors.

c Find a site to play Kenken online. This puzzle requires one to think about all the ways to factor a given number.

PRIME FACTORISATION AND SQUARE ROOTS

Once the index laws have been established for whole-number indices, whole-number square roots can be found from the prime factorisation of a number by halving the indices, provided that all the indices are even. For example,

$$784 = 2^4 \times 7^2, \qquad \text{so } \sqrt{784} = 2^2 \times 7^1 = 28.$$

Cube roots can be found by dividing the indices by 3:

$$216 = 2^3 \times 3^3, \qquad \text{so } \sqrt[3]{216} = 2 \times 3 = 6,$$

and *n*th roots by dividing the indices by *n*.

In later years, surds can be simplified in a similar way,

$$360 = 2^3 \times 3^2 \times 5^1; \text{ so } \sqrt{360} = 2^1 \times 3^1 \times \sqrt{2 \times 5} = 6\sqrt{10}.$$

EXERCISE 6

List in index form all the whole number square roots, cube roots and higher roots of 2^{30}.

PRIME FACTORISATION AND THE HCF AND LCM

The HCF and LCM of two whole numbers can be found from their prime factorisations. The method is easier once the zero index has been introduced. For example,

$$784 = 2^4 \times 3^0 \times 5^0 \times 7^2 \qquad \text{and} \qquad 210 = 2^1 \times 3^1 \times 5^1 \times 7^1.$$

The HCF is found by taking the smaller index of each prime, and the LCM by taking the larger index of each prime, so

$$\text{HCF}(784, 210) = 2^1 \times 3^0 \times 5^0 \times 7^1 = 14$$

$$\text{LCM}(784, 210) = 2^4 \times 3^1 \times 5^1 \times 7^2 = 11\,760.$$

If the zero index has not been introduced when students study this material, then the situation where a prime is missing from one of the prime factorisations will need to be explained separately:

> 'When a prime is missing from one prime factorisation, exclude the prime power from the HCF, but include the prime power in the LCM.'

THREE GENERAL RESULTS ABOUT THE HCF AND LCM OF TWO WHOLE NUMBERS

The last three parts of the next exercise are true for any two whole numbers. The calculations below can quickly be adapted for any pair of numbers, once their prime factorisations have been found.

EXERCISE 7

a Find the prime factorisations of 540 and 792

b Hence find the LCM and HCF of 540 and 792.

c Show that every common multiple is a multiple of the LCM.

d Show that every common factor is a factor of the HCF.

e Show that HCF × LCM = 540 × 720.

A CONCISE LAYOUT FOR FINDING THE HCF AND LCM AND BOTH PRIME FACTORISATIONS

The working on the right below shows a concise way to lay out the working for find the HCF and LCM of two numbers, using the same numbers 336 and 840 as in the example above:

	336	840
2	168	420
2	84	210
2	42	105
3	14	35
7	2	5

- At each step divide by a common prime factor, placed on the left.
- Stop when the two quotients are relatively prime.
- The product $2^3 \times 3 \times 7 = 168$ of the primes on the left is the HCF.
- The product $168 \times 2 \times 5 = 1680$ of the HCF and the numbers along the bottom is the LCM.

We have also incidentally found the prime factorisations of 336 and 840,

$$336 = 2^4 \times 3 \times 7 \qquad \text{and} \qquad 840 = 2^3 \times 3 \times 5 \times 7.$$

EXERCISE 8

Repeat the method with the numbers 7920 and 2376, including the prime factorisations.

LINKS FORWARD

IRREDUCIBLE POLYNOMIALS

In Years 9–10, we begin to factor polynomials into irreducible polynomials. Irreducible polynomials play a role in algebra analogous to the role of prime numbers in arithmetic. For example,

$$x^2 - 9 = (x + 3)(x - 3).$$

Moreover, factoring of polynomials can be used to factor numbers. For example, 91 can be factored using the identity above,

$$91 = 10^2 - 3^2 = (10 + 3)(10 - 3) = 13 \times 7,$$

PRIMES IN THE SET OF INTEGERS

The word 'prime' in school syllabuses is very definitely restricted to whole numbers. Students often ask, however, whether opposites of primes, like –5, can sensibly be called 'primes'. It is quite possible to construct such a definition—a prime in the set of integers is an integer other than 0, 1 and –1 whose only integer factors are itself, its opposite, 1 and –1.

With this definition, every integer can be factored into prime integers, but the factorisation is only unique if primes in the factorisation are allowed to be replaced by their opposites. For example,

$$-60 = 2 \times 2 \times 3 \times (-5) \qquad \text{and} \qquad -60 = 2 \times (-2) \times (-3) \times (-5).$$

PRIMES AND THE COMPLEX NUMBERS

The following factorisation of the prime 5 involving the imaginary number *i* shows that primes have to be defined quite differently when working with complex numbers:

$$5 = 4 + 1 = 2^2 - i^2 = (2 + i)(2 - i).$$

HISTORY AND APPLICATIONS

Although primes were probably known to the Egyptians, the first known study of them occurs in the *Elements* of the Greek mathematician Euclid about 300BC. Euclid proved that every number can be factored uniquely into primes, and also proved that there are infinitely many prime numbers.

Eratosthenes described his sieve some 50 years later.

TWO UNSOLVED PROBLEMS — GOLDBACH'S CONJECTURE AND TWIN PRIMES

In 1742, Goldbach famously conjectured that every even number greater than 2 is the sum of two prime numbers. For example,

$$4 = 2 + 2, \qquad 14 = 11 + 3, \qquad 104 = 97 + 7.$$

No mathematician has been able to establish whether or not this conjecture is true, making it one of the world's longest-standing unsolved mathematical problems.

A *prime pair* consists of two primes with a difference of 2, like 3 & 5, 11 & 13, 71 & 73. Prime pairs stand out in the list of primes up to 100. Although the problem has been around for nearly 200 years, nobody has yet been able to establish whether there are infinitely many prime pairs, or whether the prime pairs form a finite list that terminates with a 'largest prime pair'.

Mathematics is full of unsolved problems. Wikipedia is a good place to find links to the present state of these and other outstanding problems. Both the Goldback Conjecture and the twin prime *conjecture* are thought to be true

THE LARGEST KNOWN PRIME

There is no known algorithm for generating arbitrarily large prime numbers. Thus at any point in mathematical history, there has always been a 'largest known prime'. In recent years, massive computing power has been used to find very large prime numbers, and at the time of writing, the largest known prime is $2^{43\,112\,609} - 1$, discovered on 23rd August, 2008, but see Wikipedia for further details and updates. Prime numbers of this type are called *Mersenne primes*, and the index of 2 in such a prime must be a prime number.

EXERCISE 9

a Find the first number in the series $2^2 - 1$, $2^3 - 1$, $2^5 - 1$, $2^7 - 1$, ... that is not a prime number, where the indices in the sequence are the primes in order.

b Use the difference of squares identity to prove that $2^n - 1$ is not prime when n is an even number greater than 2. (Slightly harder arguments are needed to prove that $2^n - 1$ is not prime when n is an odd composite number.)

APPLICATIONS OF PRIMES IN SECURITY CODES

One of the most important problems in everyday life is the secure transmission of information. Prime numbers are used in computing as a means of *encoding* information so that it can be kept secure. Although in theory, every whole number is a product of primes, in practice it is very hard to find the actual factorisation of a very large number, even using high speed modern computers.

For example, if you were given the number 410 000 137 and told to factor it, it would take you some time, even with a calculator, to find that it is in fact 4549 × 9013. Computer scientists exploit this fact to build codes that are very hard to break, using very large prime numbers.

PRIMES IN SEQUENCE — AUSTRALIA'S FIELDS MEDAL

The primes 3, 7, 11 form an arithmetic sequence of three primes. (An *arithmetic sequence* is a sequence that increases at each step by a *common difference*, which in this case is 4.) The primes 5, 11, 17, 23, 29 form an arithmetic sequence of five primes — in this case the common difference is 6. In 2004, Terence Tao from Australia and Ben Green from the UK proved that there are arithmetic sequences of primes of *any given length*. For this and other work, Tao in 2006 became the first Australian to be awarded a Fields Medal, which is considered to be equivalent to a Nobel Prize in Mathematics..

EXERCISE 10

Find an arithmetic sequence of six or more primes. The record at the time of writing is a sequence of 25 primes found in 2008, but see Wikipedia for more details.

SEQUENCES OF SUCCESSIVE COMPOSITE NUMBERS

In contrast to these difficult questions about primes, the following exercise easily shows that there are sequences of arbitrary length consisting only of successive composite numbers.

EXERCISE 11

For any whole number n greater than 1, prove that the following is a sequence of $n - 1$ successive composite numbers:

$$n! + 2, n! + 3, \ldots, n! + n.$$

Describe a million successive composite numbers.

APPENDIX — PROVING THE FUNDAMENTAL THEOREM OF ARITHMETIC

Here is a proof of the prime factorisation theorem. As noted in the module, it is the uniqueness that is difficult to prove. Three initial lemmas are needed, each of which is important in its own right.

SUBTRACTING BEFORE FINDING THE HCF

When finding the HCF of two numbers, it is often useful to subtract them. For example, when asked to find the HCF of 30 and 26, it is natural to subtract the two numbers and find instead the HCF of 26 and 4. The HCF of 26 and 4 is 2, and this is also the HCF of 30 and 26.

The following lemma justifies this procedure.

Lemma 1: Let a and b be whole numbers, not both zero, with $a \leq b$. Then

$$\text{HCF}(a, b - a) = \text{HCF}(a, b).$$

Proof: First, if d is a divisor of a and of b, then d is a divisor of $b - a$.
Secondly, if d is a divisor of a and of $b - a$, then d is a divisor of b because $a = b - (b - a)$.

THE EUCLIDEAN ALGORITHM

Euclid shows in his *Elements* how to continue this subtraction procedure, with the numbers getting smaller at each step, until one of the numbers is zero. Then the other number is the HCF.

For example, applying this process to 30 and 26:

$30 - 26 = 4$, so $\text{HCF}(30, 26) = \text{HCF}(26, 4)$.

$26 - 6 \times 4 = 2$, so $\text{HCF}(26, 4) = \text{HCF}(4, 2)$.

$4 - 2 \times 2 = 0$, so $\text{HCF}(4, 2) = \text{HCF}(2, 0)$.

Hence the HCF of 26 and 30 is 2. Notice that the second step can be interpreted as subtracting 4 from 26 six times, or as dividing 26 by 4 and getting quotient 6 and remainder 2 – the two processes are, of course, identical. Similarly the third step is either two subtractions of 2, or a single division.

Starting from the second-last step and working upwards, we can express 2 as a sum of integer multiples of the original numbers 30 and 26:

$$2 = 26 - 6 \times 4 = 26 - 6(30 - 26) = 7 \times 26 - 6 \times 30.$$

This process is formalised in the following lemma to prove that it can be carried out in every case.

The lemma is only stated in the case where the HCF of the two numbers is 1, because that is all that is needed on the later proof, but the exercise following the lemma quickly extends it to the general case.

Lemma 2: Let HCF$(a, b) = 1$, where a and b are whole numbers, not both zero, with $a < b$. Then there exist integers x and y so that

$$ax + by = 1.$$

Proof: We prove the result using mathematical induction on b, the result being trivial if $b = 1$ because then

$$a \times 0 + b \times 1 = 1.$$

Thus we may assume that $b \geq 2$, and since HCF$(a, b) = 1$, it follows that $0 < a < b$. Hence a and $b - a$ are non-zero whole numbers less than b, with HCF$(a, b - a) = 1$ by Lemma 1. Thus by the induction hypothesis we can choose integers x and y so that

$$ax + (b - a)y = 1.$$

Hence $a(x - y) + by = 1$, as required.

EXERCISE 12

Let a and b be two whole numbers, not both zero, with HCF d.

a Prove that the HCF of $\frac{a}{d}$ and $\frac{b}{d}$ is 1.

b Use part **a** and Lemma 2 to prove that there exist integers x and y so that $ax + by = d$.

EXERCISE 13

a Use the Euclidean algorithm to find the HCF of 21 and 13, and explain why the algorithm, when applied to two successive numbers in the Fibonacci sequence, runs backwards through the Fibonacci sequence.

b Use your calculations to find integers x and y so that $21x + 13y = 1$, and explain the position of x and y in the Fibonacci sequence.

PRIME DIVISORS OF A PRODUCT

The prime number 5 is a divisor of 210. Our experiences of factoring numbers should convince us that whenever 210 is factored as a product, the prime 5 will be a divisor of one of the factors. For example, 5 is a divisor of one the factors in each factoring below:

$$210 = 21 \times 10, \qquad 210 = 35 \times 6, \qquad 210 = 2 \times 105, \qquad 210 = 15 \times 14.$$

The formal statement of this result is Lemma 3 below, which will provide us with the key step in proving the uniqueness of prime factorisation. Its proof requires Lemma 2.

Lemma 3: Let p be a prime divisor of ab, where a and b are non-zero whole numbers. Then

p is a divisor of a or p is a divisor of b.

Proof: Suppose that p is not a divisor of a. Then HCF(a, p) = 1 because p is prime, so by Lemma 2 we can choose integers x and y so that

$$ax + py = 1.$$

Multiplying both sides by b gives

$$abx + pby = b.$$

Hence p is a divisor of b, because p is a divisor of both ab and pby.

EXERCISE 14

Let p be whole number greater than 1. Prove that p is a prime number if and only if p is a divisor of either a or b, for all whole numbers a and b such that ab is a multiple of p.

PROVING THE THEOREM

We now have the machinery necessary to prove both parts of the The Fundamental Theorem of Arithmetic.

Part 1

Every whole number n greater than 1 can be written as a product of primes.

Proof: We prove the result using mathematical induction on n, if n is prime there is nothing to prove. Thus we can assume n is composite, so we can factor n as

$n = a \times b$, where a and b are whole numbers greater than 1 and less than n.

Since a and b are less than n, it follows by the induction hypothesis that each is a product of primes. The product of these is a factorisation of n into primes, as required.

Part 2

This prime factorisation is unique, apart from the order of the prime factors.

Proof: We proceed by contradiction and mathematical induction, the result being clear for all prime numbers.

1 Let n be the smallest number that has two distinct prime factorisations

$n = p_1 \dots p_r$ and $n = q_1 \dots q_s$, 2 where $p_1, \ldots, p_r$ are primes (not necessarily distinct), and $q_1, \ldots, q_s$ are primes (not necessarily distinct).

We can write n as a product

$n = p_1 \times (p_2 \ldots p_r)$,

where $p_2 \ldots p_r$ has a unique prime factorisation by the induction hypothesis, because $p_2 \ldots p_r < n$. Since p_1 is a prime divisor of $n = p_1 \times (p_2 \ldots p_r)$, it follows by Lemma 3 that either

q_1 is a divisor of p_1 or q_1 is a divisor of $p_2 \ldots p_r$.

If q_1 is a divisor of p_1, then $q_1 = p_1$. If, on the other hand, q_1 is a divisor of $p_2 \ldots p_r$, then q_1 is one of the primes $p_2, \ldots, p_r$, because $p_2 \ldots p_r$ has a unique prime factorisation.

3 In either case, q_1 is one of the primes $p_1, \ldots, p_r$, and after reordering, we may assume that $q_1 = p_1$. Hence $\frac{n}{p_1} = \frac{n}{q_1}$ has two distinct prime factorisations

$\frac{n}{p_1} = p_2 \ldots p_r$ and $\frac{n}{q_1} = q_2 \ldots q_s$,

which is a contradiction because $\frac{n}{p_1} < n$.

PRIMES AND PRIME FACTORISATION ANSWERS

EXERCISE 1

a 121, 143, 169, 187

b 79, 83, 89, 97

EXERCISE 2

2, 3, 5, 7, 11, 13, 17, 19, 23, 29, 31

EXERCISE 3

7 zeroes

EXERCISE 4

900, 34, 935, 53, 67

EXERCISE 5

a Factors of 256 are $2^0 = 1$, $2^1 = 1$, 2^2, 2^3, 2^4, 2^5, 2^6, 2^7, $2^8 = 256$
factors of 210 are 1, 2, 3, 5, 7, 2 × 3, 2 × 5, 2 × 7, 3 × 5, 3 × 7, 5 × 7, 2 × 3 × 5, 2 × 3 × 7, 3 × 5 × 7, 2 × 5 × 7, 2 × 3 × 5 × 7

b Each factor of a number is paired with another number. If the number is a square, the square root of the number is paired with itself.

EXERCISE 6

$\sqrt{2^{30}} = 2^{15}$, $\sqrt[3]{2^{30}} = 2^{10}$, $\sqrt[5]{2^{30}} = 2^{6}$, $\sqrt[6]{2^{30}} = 2^{5}$, $\sqrt[10]{2^{30}} = 2^{3}$, $\sqrt[15]{2^{30}} = 2^{2}$, $\sqrt[30]{2^{30}} = 2$

EXERCISE 7

a $540 = 2^2 \times 3^3 \times 5$ and $792 = 2^3 \times 3^2 \times 11$.

b $\text{LCM} = 2^3 \times 3^3 \times 5 \times 11 = 11\,880$ and $\text{HCF} = 2^2 \times 3^2 = 36$.

c A common multiple must be a multiple of 2^3, of 3^3, of 5, and of 11. Hence it is a multiple of their product, which is the LCM.

d A common factor cannot have as a factor any power of 2 greater than 2^2, or any power of 3 greater than 3^2, or any other prime. Hence it is a factor of $2^2 \times 3^2$, which is the HCF.

e $\text{LCM} \times \text{HCF} = (2^3 \times 3^3 \times 5 \times 11) \times (2^2 \times 3^2)$

$$= 2^5 \times 3^5 \times 5 \times 11$$

$$= 540 \times 720$$

EXERCISE 8

a

	7920	2376
2	3960	1188
2	1980	594
2	990	297
3	330	99
3	110	33
11	10	3

Hence $\text{HCF} = 2^3 \times 3^2 \times 11$

$= 792$

and $\text{LCM} = 792 \times 10 \times 3$

$= 23\,760.$

Also $7920 = 2^4 \times 3^2 \times 5 \times 11$

and $2376 = 2^3 \times 3^3 \times 11.$

$$\begin{aligned} \text{Hence} \quad \text{HCF} &= 2^3 \times 3^2 \times 11 \\ &= 792 \\ \text{and} \quad \text{LCM} &= 792 \times 10 \times 3 \\ &= 23\,760. \\ \text{Also} \quad 7920 &= 2^4 \times 3^2 \times 5 \times 11 \\ \text{and} \quad 2376 &= 2^2 \times 3^2 \times 11. \end{aligned}$$

EXERCISE 9

a $2^{11} - 1 = 23 \times 89$

b $2^{2n} - 1 = (2^n + 1)(2^n - 1)$

EXERCISE 10

7, 37, 67, 97, 127, 157

EXERCISE 11

$n! + 2$ is divisible by 2, $n! + 3$ is divisible by 3, ..., $n! + n$ is divisible by n. The sequence has length $n - 1$.

EXERCISE 12

a Assume $m \div \frac{a}{d}$ and m divides $\frac{b}{d}$.

So, there exists k_1 and k_2 such that $\frac{a}{d} = mk_1$ and $\frac{b}{d} = mk_2$.

Hence a $= mk_1d$ and $b = mk_2d$.

Therefore md divides both a and b. But $md \geq d$.

b $\frac{a}{d}x + \frac{b}{d}y = 1$ and so $ax + by = d$.

EXERCISE 13

a $21 = 13 \times 1 + 8$

$13 = 8 \times 1 + 5$

$8 = 5 \times 1 + 3$

$3 = 2 \times 1 + 1$

$2 = 1 \times 1 + 1$

The Fibonacci sequence is obtained by adding the two previous terms.

b $21 \times 5 - 13 \times 8 = 1$; $x = 5$ and $y = 8$

These are the two preceding terms.

EXERCISE 14

The converse of Lemma 3 needs to be proved.

Suppose $p \mid ab$ implies $p \mid a$ or $p \mid b$

If p is not prime, it has prime factors, p_i. Therefore p must divide one of these prime factors which is a contradiction.

INTERNATIONAL CENTRE
OF EXCELLENCE FOR
EDUCATION IN
MATHEMATICS

The aim of the International Centre of Excellence for Education in Mathematics (ICE-EM) is to strengthen education in the mathematical sciences at all levels- from school to advanced research and contemporary applications in industry and commerce.

ICE-EM is the education division of the Australian Mathematical Sciences Institute, a consortium of 27 university mathematics departments, CSIRO Mathematical and Information Sciences, the Australian Bureau of Statistics, the Australian Mathematical Society and the Australian Mathematics Trust.

AUSTRALIAN MATHEMATICS TRUST

AMSI
AUSTRALIAN MATHEMATICAL
SCIENCES INSTITUTE

The ICE-EM modules are part of *The Improving Mathematics Education in Schools* (TIMES) *Project*.

The modules are organised under the strand titles of the Australian Curriculum:

- Number and Algebra
- Measurement and Geometry
- Statistics and Probability

The modules are written for teachers. Each module contains a discussion of a component of the mathematics curriculum up to the end of Year 10.

www.amsi.org.au