Chapter 2: Primes and their Factorization

SECTION A **Introduction to Primes**

By the end of this section you will be able to
- understand the importance of primes
- prove some properties of primes

A1 Importance of Primes

Prime numbers are central to number theory. We first define what is meant by a prime number and then state and prove some properties of prime numbers.

Definition (2.1).
An integer p greater than 1 is called a **prime number** or **prime** if its only divisors are 1 and p. An integer greater than 1 that is *not* prime is called **composite**.

This definition means that every integer greater than 1 is either a prime or composite.
Examples of prime numbers are 2, 3, 5, 7, 11, 13, 17, 19, 23, …
Examples of composite numbers are 4, 6, 8, 9, 10, 12, 14, 15, …
Note that the only even prime is 2.

Why are primes important?

For over two thousand years, number theory had no serious application. Then in the 1970's with the advent of the digital computer came lots of applications for number theory. One such application is encryption of messages – this is transmitting secret messages by codes. This is generally called cryptography.
Cryptography is the study of communication by stealth. It is the coding and decoding of messages. This is a growing area of number theory applications because agencies like the CIA use cryptography to encode and decode information.
We use cryptography all the time. For example emails, websites, ATM cards and passwords are all protected by encryption.

What has encryption got to do with prime numbers?

It is difficult and time consuming to factor a large number into its prime factors. So we use a large number to encrypt the message. Decrypting the message relies on factorizing the large number into prime factors.

Is there any other real life application of prime numbers?

Figure 1

Cicadas are insects which hibernate underground. Some scientist believe that their lifecycle has evolved in a way that allows them to minimize encounters with predators. They emerge every 13 or 17 years. Once out of hibernation they mate and die while the new born cicadas head for underground hibernation.
They have one shot at breeding and then they die. If the cicadas emerged every 8 years then the predators with a lifespan of 1, 2, 4 and 8 years will coincide with the availability of cicadas. This could drive the cicadas to extinction.

Having a prime number of years (13 or 17) of hibernation ensures predators are less likely to catch them.
A prime numbered life span means that predators such as birds cannot match their own life cycles to the availability of cicada prey.

A2 Fundamental Theorem of Arithmetic

The Fundamental Theorem of Arithmetic is an important result in mathematics and claims the following:

> Every integer greater than 1 is either a prime or a product of primes whose representation is unique apart from the order.

Examples of this are

$$3 = 3,\ 10 = 2\times 5,\ 20 = 2^2\times 5,\ 100 = 2^2\times 5^2,\ 101 = 101,\ \ldots$$

The Fundamental Theorem of Arithmetic says that the decomposition of an integer greater than 1 into primes is unique apart from the order. *What does this mean?*
If we consider $100 = 2^2\times 5^2$ then 2 and 5 are the *only* primes which when multiplied together a number of times gives 100. There are *no* other primes in the decomposition of 100. Of course we can write $100 = 2^2\times 5^2 = 2\times 2\times 5^2 = 5\times 5\times 2\times 2 = \ldots$ but this just changes the order of multiplication. The prime numbers 2 and 5 are the building blocks of 100.

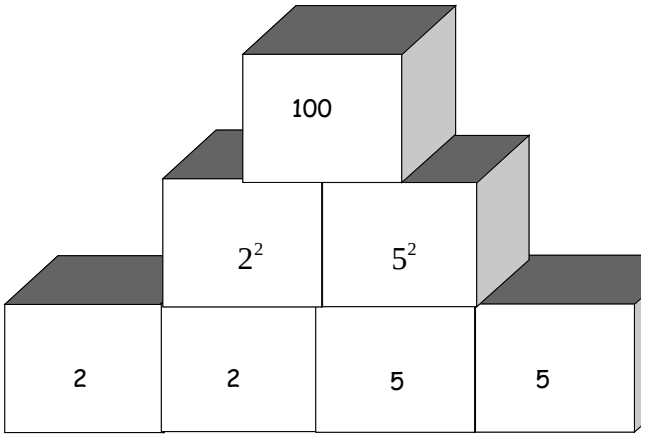

Figure 2
This figure shows the building block for 100.
This fundamental theorem says that every integer greater than 1 is either a prime number or can be made up by a product of primes. This means that primes are the building blocks of the positive integers.

A3 Properties of Primes

Now we examine the divisors or factors of a positive integer greater than 1. For example

$$2 \mid 20 \text{ implies that } 2 \mid 4\times 5 \text{ which implies } 2 \mid 4$$

Note that 2 is a prime number. Similarly

$$5 \mid 70 \ \Rightarrow\ 5 \mid 10\times 7 \ \Rightarrow\ 5 \mid 10$$

In general we have:

> Proposition (2.2).
> If p is prime and $p \mid a\times b$ then $p \mid a$ or $p \mid b$.

Proof.
Suppose prime p does *not* divide a. This implies $\gcd(a,\ p) = 1$. *Why?*

Let $\gcd(a,\ p)=g$ then $g \mid p$ but the only factors of *p* are 1 and *p* because *p* is prime. This implies that $g=p$ or $g=1$.

Also $g \mid a$ so $g \neq p$ [not equal] because we are supposing *p* does *not* divide *a*. Hence

$$g=\gcd(a,\ p)=1$$

We are given $p \mid a\times b$ and we need to show $p \mid b$ because our supposition is $p \not\mid a$.

How do we show this?
We use Euclid's Lemma of the last chapter (1.13):

If $x \mid yz$ and $\gcd(x,\ \ y)=1$ then $x \mid z$

Applying this to $p \mid a\times b$ with $\gcd(a,\ p)=1$ gives $p \mid b$.

Similarly if *p* does *not* divide *b* then applying Euclid's Lemma gives $p \mid a$.

Either way we have our result.

■

We can extend this proposition to a product of more than two terms:

Corollary (2.3).
If *p* is prime and $p \mid a_1\times a_2\times a_3\times\cdots\times a_n$ then $p \mid a_1$ or $p \mid a_2$ or … or $p \mid a_n$.

How do we prove this result?
We can prove this result by using induction. Remember the 3 steps of induction are:
Step 1 : Check the result holds for some base case $n=k_0$.
Step 2 : Assume the result is true for $n=k$.
Step 3 : Use steps 1 and 2 to prove the result for $n=k+1$.

Proof.
Step 1 : With $p \mid a_1\times a_2$ we get $p \mid a_1$ or $p \mid a_2$ by the previous Proposition (2.2).
Step 2 : Assume the result is true for $n=k$:

$$p \mid a_1\times a_2\times a_3\times\cdots\times a_k \text{ implies that } p \mid a_1 \text{ or } p \mid a_2 \text{ or … or } p \mid a_k$$

Step 3 : We are required to prove this result for $n=k+1$; that is we need to prove:

$$p \mid a_1\times a_2\times a_3\times\cdots\times a_{k+1} \text{ implies that } p \mid a_1 \text{ or } p \mid a_2 \text{ or … or } p \mid a_{k+1}$$

We have $p \mid a_1\times a_2\times a_3\times\cdots\times a_{k+1}$ which implies that

$$p \mid (a_1a_2a_3\cdots a_k)\times a_{k+1}$$

Applying the previous Proposition (2.2) to $p \mid (a_1a_2a_3\cdots a_k)\times a_{k+1}$ gives

$$p \mid (a_1a_2a_3\cdots a_k) \text{ or } p \mid a_{k+1}$$

Using step 2 on $p \mid (a_1a_2a_3\cdots a_k)$ gives $p \mid a_1$ or $p \mid a_2$ or … or $p \mid a_k$. Combining these results we have:

$$p \mid a_1\times a_2\times a_3\times\cdots\times a_{k+1} \text{ implies that } p \mid a_1 \text{ or } p \mid a_2 \text{ or … or } p \mid a_{k+1}$$

By mathematical induction we have our result.

■

If the *a*'s in this Corollary (2.3) are prime then *p* is equal to one of the *a*'s. For example

$$7 \mid 3\times5\times7\times11\times13 \quad \Rightarrow \quad 7=7$$
$$101 \mid 31\times101 \quad \Rightarrow \quad 101=101$$

This is always true as the next result states:

Corollary (2.4).
If $p,\ q_1,\ q_2,\ q_3,\ \cdots,\ q_n$ are *all* primes and $p \mid q_1\times q_2\times q_3\times\cdots\times q_n$ then $p=q_k$ where q_k is one of the primes amongst the list $q_1,\ q_2,\ q_3,\ \cdots,\ q_n$.

Proof.
We are given that $p \mid q_1\times q_2\times q_3\times\cdots\times q_n$ where *q*'s are prime. Applying the previous Corollary (2.3):

If *p* is prime and $p \mid a_1\times a_2\times a_3\times\cdots\times a_n$ then $p \mid a_1$ or $p \mid a_2$ or … or $p \mid a_n$.

To $p \mid q_1\times q_2\times q_3\times\cdots\times q_n$ implies that $p \mid q_k$ where q_k is one of the primes in the list $q_1,\ q_2,\ q_3,\ \cdots,\ q_n$. Since q_k is prime, the only divisors of this are 1 and q_k. Therefore from $p \mid q_k$ we have $p=q_k$ because *p* is prime.

■

Note that this result (2.4) is not valid for composite divisors. For example

$$6 \mid (2\times3\times7) \text{ but } 6\neq2,\ 6\neq3 \text{ and } 6\neq7$$

A4 The Fundamental Theorem of Arithmetic Proof

This is a powerful result in mathematics.

Fundamental Theorem of Arithmetic (2.5).
Every integer *n* greater than 1 is either a prime or can be written uniquely as a product of primes apart from the order.

How do we prove this result?
First we prove that *n* is a product of primes and then we show that this representation is unique apart from the order.

Proof.
Proof that *n* is a product of primes:
Either $n>1$ is prime or composite.
If *n* is a prime then we are done.
If *n* is composite then it has a divisor, say *d*, which means that $d \mid n$. Let *S* be the set of positive divisors greater than 1 of *n*. Then *S* is non-empty because *n* is in *S* as $n \mid n$.
Amongst this set *S* of divisors there must be a smallest divisor, call this p_1, of *n*. *Why?*
Because of the Well Ordering Principle:

Every non-empty subset of non-negative integers has a least element.

This p_1 must be prime otherwise we would have a smaller divisor of *n*. Since $p_1 \mid n$ we can write *n* as

$$n = p_1\times n_1 \text{ where } n_1 \text{ is an integer}$$

If n_1 is prime then we have shown that *n* is a product of primes and only need to prove uniqueness.
If n_1 is composite then we can repeat the above process.

Let p_2 be the smallest divisor of n_1 and as above p_2 must be prime. Hence $p_2 \mid n_1$ so

$$n_1 = p_2 \times n_2 \text{ where } n_2 \text{ is an integer}$$

Substituting this $n_1 = p_2 \times n_2$ into the above $n = p_1 \times n_1$ gives

$$n = p_1 \times p_2 \times n_2$$

If n_2 is prime then we have our product of primes. If n_2 is composite then repeating the above process we have

$$n = p_1 \times p_2 \times p_3 \times n_3$$

This *cannot* continue forever, there must be an integer n_k say, where n_k is prime, that is $n_k = p_k$. We have

$$n = p_1 \times p_2 \times p_3 \times \cdots \times n_k = p_1 \times p_2 \times p_3 \times \cdots \times p_k$$

Hence we have shown that *n* is a product of primes.

Uniqueness:

Suppose that

$$n = p_1 \times p_2 \times p_3 \times \cdots \times p_r = q_1 \times q_2 \times q_3 \times \cdots \times q_s \qquad (\dagger)$$

where the *p*'s and *q*'s are prime and they are in descending order, that is

$$p_1 \geq p_2 \geq p_3 \geq \cdots \geq p_r \text{ and } q_1 \geq q_2 \geq q_3 \geq \cdots \geq q_s \qquad (*)$$

Without loss of generality assume $s \geq r$.

By (†) we have $p_1 \times (p_2 \times p_3 \times \cdots \times p_r) = q_1 \times q_2 \times q_3 \times \cdots \times q_s$ which implies

$$p_1 \mid (q_1 \times q_2 \times q_3 \times \cdots \times q_s)$$

Applying the previous Corollary (2.4):

If $p,\ q_1,\ q_2,\ q_3,\ \cdots,\ q_n$ are *all* primes and $p \mid (q_1 \times q_2 \times q_3 \times \cdots \times q_n)$ then $p = q_k$.

To this $p_1 \mid (q_1 \times q_2 \times q_3 \times \cdots \times q_s)$ yields

$$p_1 = q_k \text{ where } q_k \text{ is one of primes in the list } q_1,\ q_2,\ q_3,\ \cdots,\ q_s$$

Since q_k is an element in the *ordered* list it follows from (*) that $q_1 \geq q_k$ (since q_1 was the *largest* element) and so $q_1 \geq p_1$ which we write as $p_1 \leq q_1$.

This $p_1 = q_k$ implies $p_1 \leq q_1$ because by (*) q_1 is the largest prime in the list $q_1, q_2, \cdots, q_s$.

Going other way; that is by (†) we have $q_1 \times (q_2 \times \cdots \times q_s) = p_1 \times p_2 \times \cdots \times p_r$ which implies

$$q_1 \mid (p_1 \times p_2 \times p_3 \times \cdots \times p_r)$$

Again by Corollary (2.4):

$$q_1 = p_m \text{ where } p_m \text{ is one of primes in the list } p_1,\ p_2,\ p_3,\ \cdots,\ p_r$$

This $q_1 = p_m$ implies that $q_1 \leq p_1$ because by (*), p_1 is the largest prime in the list $p_1,\ p_2,\ p_3,\ \cdots,\ p_r$.

The only way that both $p_1 \leq q_1$ and $q_1 \leq p_1$ are true is if

$$p_1 = q_1$$

Again repeating this process we obtain

$$p_2 = q_2,\ p_3 = q_3,\ p_4 = q_4, \ldots \text{ and } p_r = q_r$$

If $s > r$ then by cancelling out the common factors; p_1 with q_1, p_2 with q_2, $\cdots$ and p_r with q_r in the multiplication $p_1 \times p_2 \times p_3 \times \cdots \times p_r = q_1 \times q_2 \times q_3 \times \cdots \times q_s$ gives

$$1 = q_{r+1} \times q_{r+2} \times \cdots \times q_s$$

This is impossible because the *q*'s are primes and the smallest prime is 2. Therefore we have $s = r$ which means that

$$p_1 = q_1,\ p_2 = q_2,\ p_3 = q_3,\ p_4 = q_4,\ \ldots,\ p_r = q_r$$

The factorization of *n* is unique.
We have proven that any integer $n > 1$ can be expressed as a product of primes and the representation is unique apart from the order.

■

Note that the prime factors may repeat. For example

$$120 = 2 \times 2 \times 2 \times 3 \times 5 = 2^3 \times 3 \times 5$$

We can also write the Fundamental Theorem of Arithmetic as:

Corollary (2.6).
Every integer *n* greater than 1 is either a prime or can be written uniquely as a product of primes apart from the order in the following manner:

$$n = p_1^{k_1} p_2^{k_2} p_3^{k_3} \cdots p_r^{k_r}$$

For example

$$360 = 2 \times 2 \times 2 \times 3 \times 3 \times 5 = 2^3 3^2 5$$
$$1\,000\,000 = 2^6 5^6$$
$$1\,000\,001 = 101 \times 9901$$
$$2789865215 = 5 \times (557973043)$$

SUMMARY
A prime number is an integer greater than 1 with only factors of 1 and itself.
Every integer $n > 1$ can be written uniquely as a product of primes.