2. NUMBERS AND DIVISIBILITY

§2.1. Numbers in Maths and Computing

The earliest numbers to be 'invented' were the positive whole numbers, and indeed these were the first numbers we encountered as children. Many early societies, but particularly the Greeks, developed the theory of numbers in quite a sophisticated way. Fundamental to this study is the notion of prime numbers, roughly speaking, numbers that have only 1 and themselves as factors.

For many, many centuries number theory was considered the purest of all parts of mathematics – purest in the sense of having no practical applications. The early 20th century number-theorist G.H. Hardy was proud that his subject had no practical applications. But then came the computer age with its digital foundations. The need for security in data transmission gave rise to the need for secure codes and the techniques for this were discovered to be lying dormant in the theory of prime numbers.

Throughout the history of mathematics this story has been repeated many times. Mathematics, rather than being created 'on demand', often arises out of natural curiosity as mathematicians have developed their subject purely as an academic enquiry. Then, often decades or even centuries later, someone has found an important application. If mathematicians had been too concerned about their research being useful much useful mathematics might never have arisen.

Zero and negative numbers came onto the scene long after their positive counterparts. We include these and operate within the system of integers. Including the negative numbers doesn't greatly alter the theory, but it does make it easier in places. With negative numbers included we must modify our definition of prime number – we must allow a prime number p to be divisible by -1 and $-p$ as well as 1 and p. But they must have no other divisors.

§2.2. The System of Integers

The system that we are studying in this chapter is the system of integers:

$$\ldots, -3, -2, -1, 0, 1, 2, 3, \ldots$$

We denote the set of integers by $\mathbb{Z}$ (from the German word '*zahlen*' which means 'numbers'). Since these are the only numbers we'll be considering here, we'll often use the more informal word 'number' instead of 'whole number' or 'integer'.

The system $\mathbb{Z}$ has two basic operations of addition and multiplication and these operations satisfy the following properties:

(1) (Closure Law for Addition):
For all $a, b \in \mathbb{Z}$, $a + b \in \mathbb{Z}$.
(2) (Associative Law for Addition):
For all $a, b, c \in \mathbb{Z}$, $(a + b) + c = a + (b + c)$.
(3) (Commutative Law for Addition):
For all $a, b \in \mathbb{Z}$, $a + b = b + a$.
(4) (Identity for Addition):
There exists $0 \in \mathbb{Z}$ such that for all $a \in \mathbb{Z}$, $0 + a = a$.
(5) (Inverses under Addition):
For all $a \in \mathbb{Z}$ there exists $-a \in \mathbb{Z}$ such that:

$$a + (-a) = 0.$$

(6) (Closure Law for Multiplication):
For all $a, b \in \mathbb{Z}$, $ab \in \mathbb{Z}$.
(7) (Associative Law for Multiplication):
For all $a, b, c \in \mathbb{Z}$, $(ab)c = a(bc)$.
(8) (Commutative Law for Multiplication):
For all $a, b \in \mathbb{Z}$, $ab = ba$.
(9) (Identity for Multiplication):
There exists $1 \in \mathbb{Z}$ such that $1 \neq 0$ and, for all $a \in \mathbb{Z}$,

$$1a = a.$$

The properties for multiplication mirror those for addition, except that $\mathbb{Z}$ does not have inverses under multiplication.

Tying the additive structure to the multiplicative structure we have the following property.

(10) (Distributive Law):
For all $a, b, c \in \mathbb{Z}$, $a(b + c) = ab + ac$.

In the system of real numbers we can cancel by a non-zero number. That is, if $ab = ac$ and $a \neq 0$ then we can multiply both sides by a^{-1} to conclude that $b = c$. In the system $\mathbb{Z}$ we don't have inverses a^{-1}. However cancellation is still valid.

(11) (Cancellation Law):
For all $a, b, c \in \mathbb{Z}$, $ab = 0$ implies that $a = 0$ or $b = 0$.

The reason why (11) is called the cancellation law is that it leads directly to the theorem that permits cancellation by any non-zero number.

Theorem 1: If $ab = ac$ and $a \neq 0$ then $b = c$.
Proof: Suppose $ab = ac$ and $a \neq 0$.
Then $a(b - c) = 0$.
By (11), either $a = 0$ or $b = c$.
But $a \neq 0$. ✋☺

Any system that has two operations of addition and multiplication that satisfies all 11 properties is called an **integral domain**. We say that these are the **axioms** for an

integral domain. There are other integral domains that you have already met, such as the system of polynomials in one variable with real coefficients.

In addition to the two binary operations the system $\mathbb{Z}$ has a subset $\mathbb{N}$ satisfying the following properties. This is the set $\{0, 1, 2, 3, \ldots\}$ and it is called the set of **natural numbers**.

(12) For all $a, b \in \mathbb{N}$, $ab \in \mathbb{N}$.
(13) For all $a \in \mathbb{Z}$, exactly one of a and $-a$ belongs to $\mathbb{N}$.
(14) For all $a \in \mathbb{N}$, $a + 1 \in \mathbb{N}$.
(15) If S is a subset of $\mathbb{N}$ and:
(i) $0 \in S$ and
(ii) $a \in S$ implies that $a + 1 \in S$
then $S = \mathbb{N}$.

We call the non-zero elements of $\mathbb{N}$ **positive**. All other numbers, except for zero, are called **negative**. So there are three basic sets of numbers according to this classification.

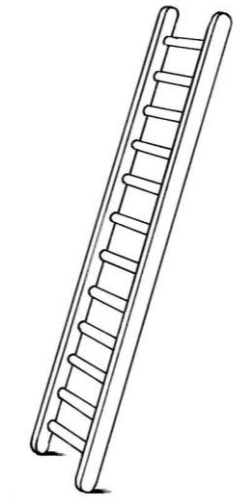
negative numbers	0	positive numbers

§2.3. Induction

When a scientist carries out certain experiments he or she assumes that if a certain outcome occurs under certain circumstances this outcome will *always* occur

under those circumstances. In most cases this turns out to be the case, but from time to time some unknown factor occurs that was not allowed for in the experiment and the scientific theory has to be modified later. All scientific truth is tentative in this sense. Light travels in a straight line. No, it bends when travelling in strong magnetic fields. Atoms are the smallest particles. No, they're not – they are made up of electrons, neutrons and protons.

In mathematics we prove theorems that state that certain things will always hold. We don't simply test it in certain cases and, like a scientist, infer that it will always hold. Unless our logic is faulty we will never have to revise our theory – just add to it.



There was an hypothesis that 'for all numbers n, $n^2 + n + 41$ is a prime number'. The first 10 values are 41, 43, 47, 53, 61, 71, 83, 97, 113, 131 and they're all prime. As a good scientist we'd infer that probably they must always be prime.

Testing from $n = 10$ up to 20 we continue to find that $n^2 + n + 41$ is a prime. Continued testing just reinforces this conclusion. Furthermore it *is* true that $n^2 + n + 41$ remains prime up to $n = 39$. But when $n = 40$, $n^2 + n + 41$ will be:

$$40^2 + 40 + 41 = 40(40 + 1) + 41,$$

quite clearly divisible by 41. And even more clearly it won't be prime for $n = 41$. Are these isolated examples? Not at all. From $n = 42$, $n^2 + n + 41$ is often prime and often not.

But how can we prove that something will *always* work? We can't check every instance! The answer is that we can often use an argument that works in every case. Sometimes we can only do it by climbing up a ladder, going from one instance to another. This is the **Principle of Induction**.

We prove that if it's true for n, then it's true for $n + 1$, by some argument. So, if it's true for $n = 1$ then it's true for $n = 2$. But then, being true for $n = 2$ it's true for $n = 3$, and then $n = 4$ and so on. What we would have done is to provide a method of getting from each n to the next, like some giant infinite ladder. But, like a real ladder, it isn't much use if the ladder isn't resting on the ground. With induction we must check the statement for $n = 0$ or $n = 1$, or whatever value we want to begin with.

Theorem 2: (PRINCIPLE OF INDUCTION)
Suppose $S(n)$ is a statement depending on some parameter $n \in \mathbb{N}$.
If (1) $S(0)$ is true and
(2) for all n, $S(n)$ implies $S(n + 1)$
then $S(n)$ is true for all n.
Proof: Let $S = \{n \in \mathbb{N} \mid S(n) \text{ is true}\}$.

The assumptions show that $0 \in \mathbb{N}$ and, if $n \in \mathbb{N}$ then $n + 1 \in \mathbb{N}$. So by property (15) above S = $\mathbb{N}$, in other words S(n) is true for all n. ✋☺

A good type of induction problem, but by no means the only one, is verifying a formula for the sum of the first n terms of a series.

We abbreviate $a_1 + a_2 + ... + a_n$ to $\sum_{r=1}^{n} a_n$.

So, for example, $\sum_{r=1}^{n} n^3 = 1^3 + 2^3 + 3^3 = 1 + 8 + 27 = 36.$

Example 1: Prove that $\sum_{r=1}^{n} n^3 = \frac{1}{4} n^2(n + 1)^2$.

Solution: For $n = 1$, LHS = $1^3 = ¼.1^2.2^2$ = RHS.
Now for the inductive step.

Suppose $\sum_{r=1}^{n} n^3 = ¼\ n^2(n + 1)^2$.

Then $\sum_{r=1}^{n+1} n^3 = ¼\ n^2(n + 1)^2 + (n + 1)^3$

$= ¼\ (n + 1)^2\ [n^2 + 4(n + 1)]$
$= ¼\ (n + 1)^2\ [n^2 + 4n + 4]$
$= ¼\ (n + 1)^2\ (n + 2)^2$.

So the result is true for $n + 1$.
Hence by induction it holds for all n.

Sometimes it's not feasible to go from n to $n + 1$. A stronger form of the Induction Principle is the following.

Theorem 3 (STRONG INDUCTION PRINCIPLE):
Suppose S(n) is a statement depending on some parameter $n \in \mathbb{N}$.
If for all n, S(m) is true for all $m < n$ implies that S(n) is true then S(n) is true for all n.
Proof: Let T(n) be the statement S(m) is true for all $m < n$.
In symbols we would write T(n) as $\forall m[m < n \rightarrow S(m)]$.

T(0) holds vacuously because $m < 0$ is always false. Remember here that our universe is the set of natural numbers and $p \rightarrow q$ is true whenever p is false.

Suppose T(n) holds. Hence S(m) holds for all $m < n$. By the assumption in the statement of the theorem this implies that S(n) is true.
Hence S(m) holds for all $m \leq n$, in other words:

for all $m < n + 1$.

Thus T($n + 1$) holds and so by Theorem 2, T(n) is true, and hence S(n) holds for all $n \in \mathbb{N}$. ✋☺

Example 2: Prove by induction that for all $n > 1$, n is a product of prime numbers.
Solution: We allow the notion of a prime number being a 'product' of one prime, so prime numbers are automatically covered.

Suppose all numbers less than n are products of prime numbers. (This is called the **induction hypothesis**.)
If n is prime it is a product of primes.
If it is not then $n = ab$ for some numbers a, b with:

$$1 < a, b < n.$$

By the induction hypothesis a, b are each a product of primes, so $n = ab$ is a product of primes. ✌☺

Notice that we couldn't go from n to $n + 1$ here. The factors a, b will be much smaller than n.

§2.4. The Peano Axioms

The 15 properties given in §2.2 were not proved. They represent facts about the integers and the natural numbers that "everyone knows". Now we can't prove everything out of nothing. In mathematics we must start with some fundamental axioms. But it would be nice to assume as little as possible.
The following four axioms define the system of natural numbers $\mathbb{N}$.

Peano Axioms: The set of **natural numbers** is a set, $\mathbb{N}$,together with a function $n \to n^+$. The value of n^+ is called the **successor** of n. The following axioms are assumed.

(P0) 0 is a natural number.
(P1) 0 has no predecessor, that is, it is not a successor of any natural number.

(P2) Two natural numbers with the same successor are equal.
(P3) If S is a subset of $\mathbb{N}$ that contains 0, and contains the successor of all of its elements, then S = $\mathbb{N}$.

Of course we may think of n^+ as being $n + 1$, but as yet there is no such operation as addition. We must define it. Firstly we can define individual numbers. For example we define 1 as 0^+, 2 is 0^{++}, 3 = 0^{+++} and so on.

We define addition and multiplication inductively as follows. For simplicity we write S(n) as n^+.

Addition:	**Multiplication:**
(A0) $\boldsymbol{n + 0 = n}$**.**	**(M0)** $\boldsymbol{n.0 = 0}$**.**
(A1) $\boldsymbol{n + m^+ = (n + m)^+}$**.**	**(M1)** $\boldsymbol{n.m^+ = nm + n}$**.**

Example 3: Prove that 2 + 2 = 4.
Solution: 1 is defined as 0^+, $2 = 1^+$, $3 = 2^+$ and $4 = 3^+$.
$2 + 0 = 2$ by definition.
$2 + 1 = 2 + 0^+ = (2 + 0)^+ = 2^+ = 3$.
Hence $2 + 2 = 2 + 1^+ = (2 + 1)^+ = 3^+ = 4$.

Make sure you check that every step follows from the definitions.

For all n, $n + 0 = n$ by (A0).
It is natural to expect that $0 + n = n$. After all, the addition of numbers is commutative. But we haven't yet proved

this. So we must prove that 0 behaves as we expect on the left as well as on the right.

Theorem 4: $0 + n = n$ for all $n \in \mathbb{N}$.
Proof: We prove this by induction on n.
Let $S = \{n \mid 0 + n = n\}$.
$0 + 0 = 0$ by (A0) so $0 \in S$.

Suppose that $n \in S$. Then $0 + n = n$.
$0 + n^+ = (0 + n)^+$ by A1
$= n^+$ by the induction hypothesis.
Hence $n^+ \in S$. By (P3), $S = \mathbb{N}$.

We can build up all the usual properties of the natural numbers from just the Peano axioms. You can find the details in my notes on Set Theory.

§ 2.5. Congruences

An integer m **divides** an integer n if $n = mq$ for some integer q. We write this as $\boldsymbol{m \mid n}$.
Equivalently we can say that n is a **multiple** of m.

Example 4: 3 divides 12, −17 divides 34, both 1 and −1 divide every number. Despite the maxim "you can't divide by 0" it is true that 0 divides 0, because $0 = 0q$ for all integers q. So $0 \mid 0$, even though $0 \div 0$ is undefined. Make sure you do not confuse $m \mid n$ with m/n or $m \div n$. The symbol $m \mid n$ is a statement. It can only be true or false. But m/n (equivalently $m \div n$) is a number.

If the 6th of July is a Monday in some year then 20th July is also a Monday. That's because 6th and 20th differ by 14 days, and this is exactly two weeks. Dates in the same month fall on the same day of the week if they differ by a multiple of 7.

When two numbers differ by a multiple of m they will leave the same remainder when you divide by m and we say that they are **congruent modulo m**. The number m is called the **modulus**. If two numbers are congruent modulo m, they are the same in some sense, even if they are not exactly the same. So we use a variation on the 'equals' sign. We write $a \equiv b$. But the modulus is important so we write $\boldsymbol{a \equiv b \pmod{m}}$.

Numbers which are congruent modulo 2 are said to have the same parity. Numbers which are congruent to zero are called even and those that are congruent to 1 are called *odd*.

We therefore have lots of different ways of saying the same thing:

- $a \equiv b \pmod{m}$,
- $a = b + mq$ for some $q \in \mathbb{Z}$,
- $m \mid (a - b)$,
- a, b leave the same remainder when divided by m.

Example 5: Since 42 – 12 = 30, and this is a multiple of 10 we can say that $42 \equiv 12 (\text{mod } 10)$.

Like equality, the relation of equivalence modulo m is an equivalence relation. That is, it is **reflexive**, **symmetric** and **transitive**.

Reflexive: Every number is congruent to itself.

Symmetric:
If a is congruent to b then b is congruent to a.

Transitive: If a is congruent to b and b is congruent to c then a is congruent to c.

Equivalence relations can be found all the way throughout mathematics. For example, in geometry there is the relation of lines being parallel and triangles being congruent.

Congruence shares other properties with equality when it comes to addition and multiplication.

Theorem 5: If $a \equiv b (\text{mod } m)$ and $c \equiv d (\text{mod } m)$ then

$$a + c \equiv b + d (\text{mod } m) \text{ and}$$
$$ac \equiv bd (\text{mod } m).$$

Proof: Suppose $a \equiv b (\text{mod } m)$ and $c \equiv d (\text{mod } m)$.
Then $m \mid (a - b)$ and $m \mid (c - d)$.
Since $(a + c) - (b + \text{d}) = (a - b) + (c - d)$ and

$ac - bd = a(c - d) + d(a - b)$, these are all multiples of m. ✋☺

Example 6: If today is Tuesday, on what day of the week will it be in 1000 days time?

Solution: Working modulo 7 we can divide 1000 by 7. We throw away the quotient and hang on to the remainder. With a little calculation we see that the remainder is 6.

Alternatively, if we wanted to do the calculation in our head we could reason as follows. Throw away 700 days. That's a whole number of weeks. That leaves 300. Throw away 280 and we're left with 20. Throw away 14 and we are left with 6.

The day of the week in 1000 days time will be the same as in 6 days time. Before we start counting 6 days forward we realise that $6 \equiv -1 \pmod 7$ so the day will be the same as yesterday, that is, Monday.

§2.6. Greatest Common Divisors

A fundamental property of the integers is the fact that we can divide one number by another, getting a quotient and a remainder.

Theorem 6: If m, n are integers, where $m \neq 0$, then $n = mq + r$ for some r with $0 \leq r < |m|$.
Proof: Let r be the smallest non-negative integer in the set $S = \{n - mq \mid q \in \mathbb{Z}\}$.
Suppose $r = n - mq \geq |m|$.

If $m > 0$ then this means that $r \geq m$.
But $0 \leq r - m = n - m(q + 1) \in S$, contradicting the fact that r is the least.

If $m < 0$ then $|m| = -m$ and so $r \geq -m$.
But $0 \leq r + m = n - m(q - 1) \in S$, again contradicting the fact that r is the least.

If the remainder is zero then m divides n.

We denote the set of divisors of n by $\mathbf{D(}n\mathbf{)}$ and the set of multiples of n by $n\mathbb{Z}$.

Example 7:
$D(12) = \{\pm1, \pm2, \pm3, \pm4, \pm6, \pm12\}$,
$12\mathbb{Z} = \{0, \pm12, \pm24, \pm36, \ldots\}$.

$D(1) = \{\pm1\}$,
$1\mathbb{Z} = \mathbb{Z}$.

$D(0) = \mathbb{Z}$ (because $n = n.0$ for all n).
$0\mathbb{Z} = \{0\}$.

D(n) is finite for all n, except when $n = 0$.
$n\mathbb{Z}$ is infinite for all n, except when $n = 0$.

The set of **common divisors** of m, n is simply:

$$D(m) \cap D(n).$$

Associated with this is $m\mathbb{Z} + n\mathbb{Z}$ which is the set of all numbers of the form $mh + nk$ where $h, k \in \mathbb{Z}$.

Theorem 7: For all integers m, n:

$$m\mathbb{Z} + n\mathbb{Z} = d\mathbb{Z} \text{ for some } d \in \mathbb{Z}.$$

Proof: Let d be the smallest positive element of $m\mathbb{Z} + n\mathbb{Z}$. Then $d = mh + nk$ for some $h, k \in \mathbb{Z}$.

Clearly any multiple of d will belong to $m\mathbb{Z} + n\mathbb{Z}$.
Now let $N = ma + nb \in m\mathbb{Z} + n\mathbb{Z}$.
Let r be the remainder on dividing N by d.
That is, $N = ma + nb = dq + r$ for some $q \in \mathbb{Z}$ and:

$$0 \leq r < d.$$

Now $r = ma + nb - (mh + nk)q$
$= m(a - hq) + n(b - kq) \in m\mathbb{Z} + n\mathbb{Z}$.
But d is the smallest positive element of $m\mathbb{Z} + n\mathbb{Z}$, so it must be that $r = 0$.

Hence $N = dq \in d\mathbb{Z}$ and so $m\mathbb{Z} + n\mathbb{Z}$ is a subset of $d\mathbb{Z}$. ✋☺

Suppose m, n are non-zero integers. Then $D(m) \cap D(n)$ is finite. An element of this set of largest absolute value is called a **greatest common divisor** of m, n.

Example 8: $D(15) = \{\pm 1, \pm 3, \pm 5, \pm 15\}$ and
$D(51) = \{\pm 1, \pm 3, \pm 17, \pm 51\}$ so
$D(15) \cap D(51) = \{\pm 1, \pm 3\}$.
The elements with largest absolute value are ±3, so these are both greatest common divisors of 15 and 51.

Theorem 8: If $m\mathbb{Z} + n\mathbb{Z} = d\mathbb{Z}$ then d is a greatest common divisor.
Proof: Let $d = mh + nk$. If e is a common divisor of m, n then $e \mid d$ and so d is a greatest common divisor. ✋☺
Corollary: A GCD of m, n can be expressed in the form $mh + nk$.

Clearly every pair of non-zero integers has exactly 2 greatest common divisors, $\pm d$.. However, when we refer to *the* greatest common divisor we mean the positive one. We denote this by **GCD(m, n)**.
By Theorem 5, GCD(m, n) = $mh + nk$ for some $h, k \in \mathbb{Z}$.

Example 9: GCD(91, 230) = 13, GCD(56, 27) = 1.

Two non-zero numbers m, n are defined to be **coprime** if GCD(m, n) = 1. Loosely speaking we might say that they have "no common factors", but what we'd really mean is that the only common factors are ± 1.

If we divide two numbers by their GCD the quotients will be coprime because we have removed all common factors.

Theorem 9: If $d = \text{GCD}(a, b)$ then:

a/d and b/d are coprime.

Proof: Let $a = a_0 d$ and $b = b_0 d$ and let $e = \text{GCD}(a_0, b_0)$.
Let $a_0 = a_1 e$ and $b_0 = b_1 e$.
Then $a = a_1 ed$ and $b = b_1 ed$ and so ed is a common divisor of a, b. Since d is the greatest common divisor it must be that $e = 1$. ✋☺

Theorem 10: If $m \mid ab$ and $\text{GCD}(a, m) = 1$ then $m \mid b$.
Proof: By Theorem 5, $1 = ah + mk$ for some $h, k \in \mathbb{Z}$ and so $b = abh + mkb$.
Since $m \mid ab$, $m \mid b$. ✋☺

There most obvious way of finding the greatest common divisor of two numbers is to factorise each of them. This, however, is highly inefficient. Factorising numbers is extremely time consuming, even with the help of a computer, unless the numbers are small. But long before computer the ancient Greeks had devised a very efficient method of finding GCDs.

§2.7. The Euclidean Algorithm

Long before computers the ancient Greeks had devised a very efficient method of finding Greatest Common Divisors.

THE EUCLIDEAN ALGORITHM:
To find the GCD of two positive numbers:

(1) Divide the smaller into the larger getting a quotient and remainder.
(2) Replace the larger number by this remainder.
(3) While the smaller number is positive go to step (1) and continue.
(4) When the smaller number becomes zero, the larger is the required GCD.

Often we don't just want to find the GCD, but also want to express it in the form *ah* + *bk*. We can do both simultaneously by what is called the Reverse Euclidean Algorithm.

THE REVERSE EUCLIDEAN ALGORITHM:
We perform the calculation in a table with three columns. We begin as follows:

A	**Q**	**B**
a		0
b	q = INT(*a*,*b*)	1

Continue as follows:

A	**Q**	**B**
…….	…….	…….
A′	…….	B′
A	q = INT(A′/A)	B
A′ – Aq		B′ – qB

Here INT(x) is the integer part function, so:
q = INT(A′/A) is the quotient when dividing A′ by A and A′ – Aq is the remainder.

We end as follows:

…….	…….	…….
GCD	q	**k**
0	← STOP	

The first column contains the successive remainders and the last non-zero remainder will be the GCD. In the third column, opposite the GCD will be a suitable value of k. Having found k the corresponding value of h is simply:

$$h = \frac{\text{GCD} - bk}{a} .$$

If we merely want to find the GCD we can omit the third column.

Example 10: Find GCD(2977,1131) and express it in the form 2977h + 1131k.
Solution:

A	**Q**	**B**
2977		0
1131	2	1
715	1	–2
416	1	3
299	1	–5
117	2	8
65	1	–21

52	1	29
13	4	**–50**
0		

Hence GCD(2977,1131) = 13,

$k = -50$ and $h = \dfrac{13 - 1131(-50)}{2977} = \dfrac{56563}{2977} = 19.$

So $13 = 2977.19 - 1131.50$.

We omit the proof that this algorithm works. A proof, by induction, can be found in my notes on Number Theory.

§2.8. Prime Numbers

We define a positive number to be **prime** if it has exactly 2 positive divisors. Note that this rules out 1. You might think that the number 1 should be called a prime, because it can't factorise into smaller numbers, but there are good technical reasons for excluding it.

When we come to positive and negative integers we have to modify this definition to 'a number is prime if it has exactly four divisors'. For a prime p these are 1, –1, p and $-p$.

Example 11: The prime numbers are ±2, ±3, ±5, ±7, ±11, ±13, ±17, ±19, ±23, ±31, …

Numbers that aren't prime, other than the three special numbers –1, 0, and 1, are called **composite**. There are four basic sets of numbers according to this classification.

0	**units**	**prime numbers**	**composite numbers**
0	± 1	$\pm 2, \pm 3, \pm 5, \pm 7,$ $\pm 11, \pm 13, \pm 17, \ldots$	$\pm 4, \pm 6, \pm 8, \pm 9, \pm 10,$ $\pm 12, \pm 14, \pm 15, \ldots$

The reason for classifying ± 1 separately to 0 is because they are the only integers that have integer inverses under multiplication.

Theorem 11: If p is prime and $p \mid ab$ then $p \mid a$ or $p \mid b$.
Proof: Suppose that p is prime and suppose that p does not divide a.
Then GCD(a, p) = 1 and so, by Theorem 6, $p \mid b$. ☝☺

It is a very useful fact that every number can be factorised uniquely into primes. Well, that isn't strictly true. Zero cannot be factorised into primes. The number 1 could be factorised into primes if we allowed products with zero factors, evaluating to 1. But then this wouldn't work for –1. Let's keep to numbers whose absolute value is bigger than 1. Is it true that "every number whose absolute value is bigger than 1 can be factorised uniquely into primes"? That depends on what we would consider to be a different factorisation.

Example 12: There are 4 factorisations of 6 into primes: $6 = 2.3 = 3.2 = (-2)(-3) = (-3)(-2)$. We consider all four factorisations to be the same.

If we allowed 1 and –1 to be primes we'd have infinitely many prime factorisations of 6.
For example, $6 = (-2).3.(-1).1.1.1.(-1)(-1)$.

Theorem 12: (FUNDAMENTAL THEOREM OF ARITHMETIC)
(1) If $|n| > 1$ then $n = p_1p_2 \dots p_h$ for some h and some primes $p_1, p_2, \dots, p_h$.
(2) If $n = p_1p_2 \dots p_h = q_1q_2 \dots q_k$ then $h = k$ and, after suitable rearrangement of the factors, $p_i = \pm q_i$ for each i.
Proof: We have already proved the first part by induction on $|n|$.
We prove the second part by induction on the number of prime factors, h of one factorisation.
Suppose that $N = p_1p_2 \dots p_h = q_1q_2 \dots q_k$.
Then p_1 divides $q_1q_2 \dots q_k$ and so p_1 divides q_j for some j, by Theorem 4.
Since q_j is prime and $p_1 \neq \pm 1$, this means that $p_1 = \pm q_j$.
Rearranging the factors and cancelling by p_1 we get:

$$p_2 \dots p_h = (\pm q_1)q_2 \dots q_k.$$

By induction $h - 1 = k - 1$ and for each $i \geq 2$, $p_i = \pm q_j$ for some $j \geq 2$.
Hence these two factorisations of N are the same (apart from rearrangements and multiplication by units.) ☺

§2.9. Generating Prime Numbers

There's no known formula for the n'th prime number. At least there are formulae that are so impractical to use they are worse than no formula at all. There is virtually no improvement on the simple-minded approach of testing all factors.

One obvious improvement is the fact that we only need to test for factors of a positive number n by primes up to $\sqrt{n}$.

Theorem 13: If p has no factors n for $2 \le n \le \sqrt{p}$ then p is prime.
Proof: If $p = ab$ where $1 < a, b < p$ then one of a, b must be less than or equal to $\sqrt{p}$ (If they were both bigger than $\sqrt{p}$ then ab would be bigger than p. ✋☺

It's useful to be able to recognise multiples of 2, 3 and 5.
Multiples of 2 are those that end in 0, 2, 4, 6 or 8.
Multiples of 5 are those that end in 0 or 5.
Multiples of 3 are those numbers where the sum of the digits is a multiple of 3.

Example 13: Is 3197 prime?
Solution: $\sqrt{3197} = 56.542\ldots$ so we only need to test by numbers up to 56. But 56, 55 and 54 are clearly composite so in fact we need only go up to 53.
Now 3197 is clearly not divisible by 2, 3 or 5. So, using our calculator we test for 7, 11, 13, 17, 19, 23, 29, 31, 37, 41, 43, 47, 53.

We discover that 23 is a factor and that 3197 = 23.139.

Example 14: Is 5113 prime?
Solution: $\sqrt{5113} = 71.50\ldots$ so we only need to test by numbers up to 71.
Clearly 5113 is not divisible by 2, 3 or 5. So, using our calculator we test for 7, 11, 13, 17, 19, 23, 29, 31, 37, 41, 43, 47, 53, 59, 61, 67, 71. Since 5113 is not divisible by any of these it must be prime.

§2.10. The Sieve of Eratosthenes

Eratosthenes was a Greek philosopher who was born in Cyrene in 276BC. He was also a mathematician, astronomer, poet and geographer but his employment was as head librarian of the famous library of Alexandria.

Among other things he calculated the circumference of the earth with remarkable accuracy. He travelled to a place about 800 kilometres south east of Alexandria, now known as Aswan, and noted that at the summer solstice the sun was directly overhead at noon, But his colleague back in Alexandria reported that at that same moment in Alexandria the sun's rays fell at an angle of 7.2 degrees from the vertical. Of course degrees hadn't been invented at that time – he

actually said ‘one fiftieth of a full circle’ He estimated the distance from Alexandria to Aswan to be 5,040 stadia, which converts to 787.5 kilometres. The circumference of the earth would then be 252000 stadia, or 39,690 kilometres. The accepted figure today is 40,075 so Aritosthenes was correct to within 1%.

He may have fudged a little since these figures allow for easy calculation. It seems remarkable that his angle should be exactly one fiftieth of a revolution. And 5040 is remarkable, as every bell ringer knows, is the number of changes in a full peal of bells, that is it is 7!

If he did, he wouldn’t be the only one who has fudged geographical measurements. The surveyor Andrew Waugh who was the first to measure the height of Mount Everest, came up with a figure of exactly 29,000 feet. He thought that if he reported it as such it would throw doubt on his accuracy because it would be thought that he had rounded it to arrive at 29,000 feet. So he reported it as 29,002 to suggest that his measurements were very precise. So some wits say that he was the first person to put two feet on top of Mount Everest!

Eratosthenes also invented what is now known as the **Sieve of Eratosthenes**. It is a particularly suitable method for producing primes if you happen to live in an ancient civilization without calculators. You write down a list of

all numbers, in order from 2 to some large number. You circle the 2 and then cross out every 2nd number after that.

At each stage you circle the first number that has not been crossed out. That will be a prime number. If is *p* then cross out every p^{th} number after that. Continue until every number has been circled or crossed out. The circled numbers will be prime and the crossed out ones will be composite.

Example 15: Use the sieve of Eratosthenes to find all the primes up to 100.

Solution:

	(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

Notice that as numbers get larger, primes become rarer. In successive groups of 10 the percentage of primes is 40%, 40%, 20%, 20%, 30%, 20%, 20%, 30%, 20%, 10%, giving 25% over the first 100. The percentage of primes up to 1000 drops to 16.8%. In the first 10,000 it is only

about 12% and in the first million it is less than 8%. Could it be that primes become so rare that they finish altogether? Is there in fact a largest prime?

Of course there are infinitely many numbers altogether, but even if there were only finitely many primes there would still be infinitely many numbers. After all there are infinitely many powers of 2 and that uses just one prime. This question was asked, answered, a long time ago by the ancient Greeks.

Theorem 14: (EUCLID) There are infinitely many primes.

Proof: The simple method of showing that there are infinitely many numbers is to say, "if there is a biggest number just add 1 and you get a bigger one". This does not work because adding 1, or even 2 to a prime does not always give a prime. But we can do something a little bit similar.

Suppose there is a largest prime N. Now take N! = N(N – 1)(N – 2) … 3.2.1. Every prime divides N! because every prime will appear as one of its factors. Now consider N! + 1. No prime number will divide it because they all divide N! and no number bigger than 1 can divide two successive numbers. But every number bigger than 1 is divisible by a prime number, so we get a contradiction. Hence there are infinitely many prime numbers.

§2.11. Solving Linear Congruences

Example 16: Find a multiple of 123 that is 231 more than a multiple of 312.

Solution: Expressed algebraically, the problem is to find numbers m, n so that

$$123m = 231 + 312n.$$

We could work through various values of n and divide by 123 until we find a value of n for which $231 + 312n$ is a multiple of 123. But this might take some time, if indeed there is a solution. We need some better technique than trial and error.

The problem is equivalent to solving the congruence $123m \equiv 231 (\text{mod } 312)$, which has the form $ax \equiv b (\text{mod } m)$. We can work with congruence equations pretty much like ordinary ones.

The important difference between the congruence $ax \equiv b (\text{mod } m)$ and the equation $ax = b$ is that with the equation, provided $a \neq 0$, we can divide and get the solution $x = a/b$. Things are a little trickier with congruence equations. For a start there may be no solutions.

Example 17: Solve the congruence equation
$15x \equiv 7 (\text{mod } 105)$.

Solution: Written as an equation this becomes
$15x = 7 + 105y$. Since 15 and 105 are both divisible by 5 and 7 is not there can be no solutions.

Theorem 15: The congruence $ax \equiv b \pmod{m}$ has a solution if and only if $\text{GCD}(a, m) \mid b$.

Proof: Let $d = \text{GCD}(a, m)$ and suppose that the congruence has a solution x. Then $ax = b + my$ for some y. Since $d \mid a$ and $d \mid m$ it must be that $d \mid b$.

Conversely suppose that $d \mid b$. Let $b = dq$.
By the corollary to Theorem 5 we may write $d = ah + mk$ for some integers h, k.

Then $b = dq = ahq + mkq$ so $a(hq) = b + m(-kq)$. Consequently $x = hq$ is a solution to the congruence.

Example 16 (continued): We wish to solve the congruence $123m \equiv 231 \pmod{312}$.
Now $123 = 3.41$ and $312 = 3.8.13$ so:

$$\text{GCD}(123, 312) = 3.$$

Since $3 \mid 231$ there is a solution. But what is it?
We calculate GCD(123, 312) by Euclid's Algorithm, even though we know the answer to be 3.

A	Q	B
312		0
123	2	1
66	1	– 2
57	1	3
9	6	– 5
3	3	33
0		

So GCD(312, 123) = 3 and this divides 231 so there are solutions.
Hence $3 = 312h + 123k$ where $k = 33$.
This gives $3 \equiv (123)(33) \pmod{312}$.
Since $\frac{231}{3} = 77$ we multiply both sides to get:

$$231 \equiv (123)(33)(77) \pmod{312}.$$

Hence $m \equiv (33)(77) \equiv 2541 \equiv 45 \pmod{312}$ is a solution.
However it is not the complete solution.

Theorem 16:
Let $d = \text{GCD}(a, m)$ and let $a = a_0 d$ and $m = m_0 d$.
If x_0 is a solution to the congruence equation

$$ax \equiv b \pmod{m}$$

then the complete solution is $x = x_0 + m_0 t$ for some t.
Proof: Let $a = a_0 d$ and $m = m_0 d$.
Suppose $ax_0 \equiv b \pmod{m}$ and let $ax_0 = b + mq$.
Let $x = x_0 + m_0 t$.
Then $ax = ax_0 + am_0 t$
$= b + mq + am_0 t$
$= mt$ so $ax \equiv b \pmod{m}$.

Conversely suppose $ax \equiv b \pmod{m}$.
Then $ax \equiv ax_0 \pmod{m}$ and so $x \equiv x_0 \pmod{m_0}$.

Example 16 (continued):
The complete solution is:

$$m = 2541 + 104\text{t} \text{ and } n = 1001 + 41\text{t}.$$

Theorem 17: $ax \equiv ay \pmod{m}$ if and only if:

$$x \equiv y \left(\mod \frac{m}{\mathrm{GCD}(a,m)} \right).$$

Proof: Let $d = \mathrm{GCD}(a, m)$ and let $a = a_0 d$ and $m = m_0 d$.
Suppose $ax \equiv ay \pmod{m}$. Then $ax = ay + mq$ for some number q.
Hence $a_0 dx = a_0 dx + m_0 dq$.
Dividing by d we get $a_0 x = a_0 y + m_0 q$.
That is m_0 divides $a_0(x - y)$.
Since $\mathrm{GCD}(a_0, m_0) = 1$, m_0 divides $x - y$ and so

$$x \equiv y \pmod{m_0}.$$

Conversely if $x \equiv y \pmod{m_0}$ then m_0 divides $x - y$ and so $m = m_0 d$ divides $d(x - y)$ and hence it divides

$$a_0 d(x - y) = ax - ay.$$

The moral of the story is that we are permitted to divide both sides of a congruence by a common factor provided we divide the modulus by the GCD of the modulus and the common factor.

Example 16 (again):
We wish find all integers m, n such that:

$$123m = 231 + 312n.$$

Instead of writing this as $123m \equiv 231 \pmod{312}$, we can write it as $312n \equiv -231 \pmod{123}$. Clearly we can reduce the numbers 312 and 231 modulo 123, giving $66n \equiv -108 \pmod{123}$.

But $-108 \equiv 15 \pmod{123}$ so we can write the equation as

$$66n \equiv 15 \pmod{123}.$$

Dividing by 3 this becomes $22n \equiv 5 \pmod{41}$

$$\equiv 46 \pmod{41}.$$

Dividing by 2 (this time the modulus does not change since 2 and 41 are coprime) we get:

$11n \equiv 23 \pmod{41}$

$\equiv 64 \pmod{41}$

$\equiv 105 \pmod{41}$

$\equiv 146 \pmod{41}$.

We are continuing to add the modulus until we get a multiple of 11.

$11n \equiv 146 \pmod{41}$

$\equiv 187 \pmod{41}$ so

$n \equiv 17 \pmod{41}$.

If we take $n = 17$ we get $123m = 231 + 312.17 = 5535$ so $m = 45$. This agrees with the previous solution if we take $t = -24$.

The complete solution is $n = 17 + 41t$, giving:

$123m = 231 + 312(17 + 41t)$

$= 5535 + 12792t$

so $m = 45 + 104t$.

This technique of dividing by factors of the coefficient can be quite useful if the coefficient has small factors. But if the coefficient is a large prime it would be very inefficient.

EXERCISES FOR CHAPTER 2

Exercise 1: Factorise 2926 into prime factors.

Exercise 2: Factorise 713 into primes.

Exercise 3: Show that 659 is prime.

Exercise 4: Find the first prime after 1000.

Exercise 5: Find the GCD of 11111 and 3403 and express it in the form $11111h + 3403k$.

Exercise 6: Find the GCD of 10101 and 5019 and express it in the form $10101h + 5019k$.

Exercise 7: Solve the congruence equation:

$$100x \equiv 26 \pmod{42}.$$

Exercise 8: Solve the congruence equation:

$$101x \equiv 26 \pmod{142}.$$

Exercise 9: Solve the congruence equation:

$$2018x \equiv 4 \pmod{5000}.$$

SOLUTIONS FOR CHAPTER 2

Exercise 1: 2926 = 2.1463.
We now try dividing 1463 by 3, 5, 7, 11, …and discover that it is exactly divisible by 7.
So 2926 = 2.7.209 = 2.7.11.19.

Exercise 2: We try dividing by the primes 3, 5, 7, … and eventually discover that 713 = 23.31.

Exercise 3: $\sqrt{659} = 25.6\ldots$ so we only need to check for divisibility by primes up to 23. Since none of these primes divide 659 we can conclude that 659 is prime.

Exercise 4: $\sqrt{1000} = 31.6$ so we will only need to check for prime divisors up to 31 (unless it turned out that there are no primes between 1000 and $33^2 = 1089$).
1001 = 7.143
1003 = 17.59
1007 = 19.53
1009 is prime.

Exercise 5:

A	Q	B
11111		0
3403	3	1
902	3	–3
697	1	10
205	3	–13

82	2	49
41	2	–111
0		

The last non-zero remainder is 41. Hence the GCD of 11111 and 3403 is 41.

$41 = 11111h - (3403)(111)$ where $h = \dfrac{41 + 3403.111}{11111}$

$= 34.$

So $41 = (11111)(34) - (3403)(111)$.

Exercise 6:

A	Q	B
10101		0
5019	2	1
63	79	–2
42	1	159
21	2	–161
0		

So GCD(10101, 5019) = 21 and

$21 = 10101h - (5019)(161)$.

Hence $h = \dfrac{21 + (5019)(161)}{10101} = 80$ so

$21 = (10101)(80) - (5019)(161)$.

Exercise 7: Suppose $100x \equiv 26 \pmod{42}$.

$\therefore\ 16x \equiv 26 \pmod{42}$, since $100 \equiv 16 \pmod{42}$

$\therefore\ 8x \equiv 13 \pmod{21}$

$\equiv 34 \pmod{21}$

$\therefore\ 4x \equiv 17 \pmod{21}$

$\equiv 38 \pmod{21}$

$\therefore\ 2x \equiv 19 \pmod{21}$

$\equiv 40 \pmod{21}$

$\therefore\ x \equiv 20 \pmod{21}$

Exercise 8: The method used in exercise 7 is not suitable because 101 has no small divisors – in fact it is prime. In this case we use the general method, which is to find GCD(101, 142). Of course, since 101 is prime, it will be 1, but we carry out the calculations anyway because we need the details.

A	**Q**	**B**
142		0
101	1	1
41	2	–1
19	2	3
3	6	–7
1	3	45
0		

So $(101)(45) \equiv 1 \pmod{142}$.

Hence the solution is $x \equiv 45.26 \pmod{142}$

$\equiv 1170 \pmod{142}$

$\equiv 34 \pmod{142}$.

Exercise 9: Suppose $2018x \equiv 4 \pmod{5000}$.
Then $1009x \equiv 2 \pmod{2500}$.

A	Q	B
2500		0
1009	2	1
482	2	–2
45	10	5
32	1	–52
13	2	57
6	2	–166
1	6	389
0		

$1 \equiv (1009)(389) \pmod{2500}$
Hence the solution to $1009x \equiv 2 \pmod{2500}$ is:

$$x \equiv (389)(2) \pmod{2500}$$
$$\equiv 778 \pmod{2500}.$$