1. INTEGERS AND DIVISIBILITY

§1.1. The System of Integers

Number Theory is basically about the counting numbers 1, 2, 3, ... though we soon feel the need to include zero and the negative integers. So the system that we are studying in these notes is the system of integers: … , –3, –2, –1, 0, 1, 2, 3, …

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 in this chapter 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 $\mathbb{Z}$ doesn't have inverses under multiplication. Although there exists a number b such that $2b = 1$, it's not an integer.

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}, but cancellation is still valid.

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

A restatement of the cancellation law is:
If $ab = ac$ and $a \neq 0$ then $b = c$, since ab = ac is equivalent to $a(b - c) = 0$.

Any system, with operations of addition and multiplication, that satisfies all these 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've already met, such as the system of polynomials in one variable with real coefficients.

An important subset of the integers is the set of **natural numbers**, $\mathbb{N}$ consisting of the numbers:

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

[Some number-theorists exclude zero and start with 1.] This is closed under addition and multiplication and contains the additive and multiplicative identities. But it doesn't have inverses, either under addition or multiplication.

In terms of the natural numbers we can define an order relation on $\mathbb{Z}$, with $m \leq n$ defined to mean that $n = m + k$ for $k \in \mathbb{N}$. We define $\geq$, $<$ and $>$ in the usual way.

A set with an ordering $\leq$ is said to be **well-ordered** if every non-empty subset has a least. The set $\mathbb{R}$ of real numbers is not well-ordered since there is no smallest positive real number. However $\wp(S)$, the set all subsets is well-ordered by the subset relation (just write '$\leq$' for subset instead of '$\subseteq$'). The least subset in any non-empty set of subsets is clearly their intersection. An important property of the set of natural numbers is that it is well-ordered by $\leq$.

Theorem 1 (Well-Ordering Principle): Every non-empty subset of the natural numbers has a least.
Proof: It's tempting to say that it's obvious. Or, like many 'obvious things in mathematics' we could take it as an axiom. But it is possible to prove it, but to do so would require a formal definition of natural number, which takes us away from Number Theory. I prove the well-ordering principle in my notes on Sets.

An important consequence of the Well-Ordering Principle is the Principle of Mathematical Induction.

Theorem 1 (PRINCIPLE OF INDUCTION):
Suppose S(n) is a statement depending on some parameter $n \in \mathbb{N}$.
If S(0) is true and if, for all n, S(n) implies S($n + 1$), then S(n) is true for all n.
Proof: Let $F = \{n \in \mathbb{N} \mid S(n) \text{ is false}\}$. Suppose that F is non-empty. It therefore has a least.
Let $m \in F$ be the least element of F. Since S(0) is true, $m > 0$ and so $m - 1 \in \mathbb{N}$.
Since $m - 1 < m$ we conclude that $m - 1 \notin F$.
But this means that S($m - 1$) must be true.
By our assumption this implies that $S(m)$ is true which means that $m \notin F$, a contradiction.
So this F is empty and so S(n) must be true for all $n \in \mathbb{N}$.

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

Solution: For $n = 1$, LHS = 1 = RHS.

Suppose $\sum_{r=1}^{n} r^3 = \frac{1}{4} n^2(n + 1)^2$.

Then $\sum_{r=1}^{n+1} r^3 = \frac{1}{4} n^2(n + 1)^2 + (n + 1)^3$

$$= \frac{1}{4} (n + 1)^2 [n^2 + 4(n + 1)]$$

$$= \frac{1}{4} (n + 1)^2 [n^2 + 4n + 4]$$

$$= \frac{1}{4} (n + 1)^2 (n + 2)^2.$$

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

However it's just as easy to use the Principle of Well-Ordering itself, using a technique called the **minimal counterexample technique**. To prove something is true for all n we suppose that there's a counter-example. Then the set of counter-examples will be non-empty and so there must be a minimal counter-example. Hence the theorem must be true for everything smaller. But then we proceed to prove that the theorem is true for the minimal counter-example itself, which is clearly a contradiction. Hence there can be no counter-

example at all – the theorem is always true. Here is how we can prove Example 1 by using the minimal counter-example technique.

Example 1 revisited: Prove that $\sum_{r=1}^{n} r^3 = \frac{1}{4} n^2(n + 1)^2$ for all $n \in \mathbb{N}$.

Solution: Suppose the theorem is false and let N be a minimal counter-example.

For $n = 1$, LHS = 1 = RHS, so N > 1.

Then $\sum_{r=1}^{N-1} r^3 = \frac{1}{4} (N - 1)^2 N^2$.

Then $\sum_{r=1}^{N} r^3 = \frac{1}{4} (N - 1)^2 N^2 + N^3$

$$= \frac{1}{4} N^2 [(N - 1)^2 + 4N]$$

$$= \frac{1}{4} N^2 [N^2 - 2N + 1 + 4N]$$

$$= \frac{1}{4} N^2 (N + 1)^2.$$

So the result is true for N, contradicting the fact that N is a minimal counter-example,

Hence the statement holds for all n.

It's actually no more work. But there are many situations where we can't go from n to $n + 1$ and the

Principle of Induction fails. Often one gets around this by developing what's called the Strong Principle of Induction. But this isn't necessary because in those situations we can still use the minimal counter-example technique.

We are about to introduce the notions of prime and composite numbers. Integers, n, with $|n| > 1$ are either prime (can't be factorised into factors with smaller absolute value), or composite (not prime). In the next example we allow the notion of a prime being the 'product' of one prime.

Theorem 2: Prove every integer $n > 1$, n is a product of prime numbers.

Solution:

[Suppose the theorem is false.]

Suppose $N > 0$ is a minimal counter-example.

If N is prime it is the 'product' of 1 prime so N must be composite.

Then $N = ab$ for some numbers a, b with $1 < a, b < N$.

Now a, b are products of primes (they are smaller than the minimal counter-example).

Hence $N = ab$ is itself a product of primes, contradicting the fact that it is a counter-example.

[Hence there is no counter-example and the theorem is true for all n.]

Corollary: Every integer n with $|n| > 1$ is a product of primes.

Proof: This follows from the fact that p is prime if and only if –p is prime.

In practice we'd leave out the first and last lines of the theorem. They're included here to for emphasis. As I said, most people would use the so-called Strong Principle of Induction. However there are many branches of mathematics where even the Strong Principle is not strong enough, while the minimal counter-example technique still works!

§1.2. Divisibility

A fundamental property of the integers is the fact that we can divide one number by another, getting a quotient and a remainder. Here, again, we appeal to the Well-Ordering Principle.

If m, n are integers and $m > 0$, the **remainder** on dividing n by m is the smallest element of the set $\{n - mq \mid q \in \mathbb{Z}\} \cap \mathbb{N}$ and the **quotient** is the corresponding q.
This set is non-empty because $n - mq \geq 0$ for $q = -|n|$ (Prove this as an exercise.)

Example 2:
Let $n = 17$ and $m = 3$.
$\{n - mq \mid q \in \mathbb{Z}\} = \{\ldots, 23, 20, 17, 14, 11, 8, 5, 2, -1, -4, -7, \ldots\}$.
$\{n - mq \mid q \in \mathbb{Z}\} \cap \mathbb{N} = \{\ldots, 23, 20, 17, 14, 11, 8, 5, 2\}$.

The least element of this set is 2, so this is the remainder, and since $2 = 17 - 3.5$, the quotient is 5.

Let $n = -17$ and $m = 5$.
$\{n - mq \mid q \in \mathbb{Z}\} = \{\ldots, -27, -22, -17, -12, -7, -2, 3, 8, 11, \ldots\}$.
$\{n - mq \mid q \in \mathbb{Z}\} \cap \mathbb{N} = \{3, 8, 11, \ldots\}$.
The least element of this set is 3, so this is the remainder, and since $3 = -17 - 5.(-4)$, the quotient is -4.

Theorem 3 (DIVISION ALGORITHM):
If m, n are integers, where $m > 0$, then $n = mq + r$ for some r with $0 \leq r < m$.
Proof: Let $S = \{n - mq \mid q \in \mathbb{Z}\} \cap \mathbb{N}$ and let r be the remainder on dividing n by m, that is the smallest element of S.
Then $n = mq + r$, and $r \geq 0$, by the definition of remainder.
It remains to show that $r < m$.
Suppose $r \geq m$. Then $0 \leq r - m = n - m(q + 1) \in S$, contradicting the fact that r is the least element of S.

NOTES: (1) It is always called the Division Algorithm but strictly speaking an algorithm is a computational process. I suppose it is called this because it justifies the algorithm of long division that we all learnt in primary school.

(2) Usually the Division Algorithm includes the case $m < 0$, replacing $r < m$ by $r < |m|$. But rarely do we have occasion to divide by a negative number in Number Theory and it strikes me that to include that case is unnecessary. I have left it as an exercise.
(3) When you are called on to find the quotient and remainder in practice don't attempt to set up the set $\{n - mq \mid q \in \mathbb{Z}\} \cap \mathbb{N}$. Continue to use long division as you always have.

If the remainder is zero, that is if $m = nq$ for some $q \in \mathbb{Z}$, we say that m **divides** n. We write this as $\boldsymbol{m \mid n}$. Equivalently we can say that n is a **multiple** of m.

Clearly $1 \mid n$ for all n And, surprisingly, $0 \mid 0$ is also true! You've always learnt that you can't divide by 0 but it *is* true that 0 divides 0, because $0 = 0q$ for all integers q. So $0 \mid 0$ is true even though $0/0$ is undefined. Make sure you don't confuse $m \mid n$ with m/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*.

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

Example 3:
$D(12) = \{\pm1, \pm2, \pm3, \pm4, \pm6, \pm12\}$, $12\mathbb{Z} = \{0, \pm12, \pm24, \pm36, \ldots\}$.
$D(1) = \{\pm1\}$, $1\mathbb{Z} = \mathbb{Z}$.
$D(0) = \mathbb{Z}$ (because $n = n.0$ for all n).
$0\mathbb{Z} = \{0\}$.
$D(n)$ is finite for all n, except where $n = 0$.
$n\mathbb{Z}$ is infinite for all n, except where $n = 0$.

The set of **common divisors** of m, n is simply $D(m) \cap D(n)$. Associated with this is $\boldsymbol{m}\mathbb{Z} + \boldsymbol{n}\mathbb{Z}$ which is the set of all numbers of the form $mh + nk$ where $h, k \in \mathbb{Z}$.

Theorem 4: For all integers m, n we have $m\mathbb{Z} + n\mathbb{Z} = d\mathbb{Z}$ for some $d \in \mathbb{Z}$.
Proof: Let d be the smallest positive element of $m\mathbb{Z} + n\mathbb{Z}$. (Well-ordering comes in here.)
Then $d = mh + nk$ for some $h, k \in \mathbb{Z}$.
Clearly any multiple of d will belong to $m\mathbb{Z} + n\mathbb{Z}$ and so $d\mathbb{Z} \subseteq m\mathbb{Z} + n\mathbb{Z}$.

Now let $k = ma + nb \in m\mathbb{Z} + n\mathbb{Z}$. Let r be the remainder on dividing k by d.
That is, $k = ma + nb = dq + r$ 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 $k = dq \in d\mathbb{Z}$ and so $m\mathbb{Z} + n\mathbb{Z} \subseteq d\mathbb{Z}$.

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 4: $D(15) = \{\pm1, \pm3, \pm5, \pm 15\}$ and $D(51) = \{\pm1, \pm3, \pm17, \pm51\}$ so
$D(15) \cap D(51) = \{\pm1, \pm3\}$. The elements with largest absolute value are ±3, so these are both greatest common divisors of 15 and 51.

Theorem 5: 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 4, $GCD(m, n) = mh + nk$ for some $h, k \in \mathbb{Z}$.

Example 5: GCD(91, 130) = 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 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’d have removed all common factors.

Theorem 6: If d = 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 = 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 $e = 1$.

§1.3. The Euclidean Algorithm

The 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 computers the ancient Greeks had devised a very efficient method of finding GCDs.

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.

Example 6: Find GCD(1131, 2977).
Solution: $2977 = 1131.2 + 715$
$1131 = 715.1 + 416$
$715 = 416.1 + 299$
$416 = 299.1 + 117$
$299 = 117.2 + 65$
$117 = 65.1 + 52$
$65 = 52.1 + 13$
$52 = 13.4 + 0$
The last non-zero remainder is 13 and so GCD(1131, 2977).

By the Corollary to Theorem 4 we can express 13 in the form $1131h + 2977k$ for some numbers h, k.

Example 7: Find integers h, k such that $13 = 1131h + 2977k$.
Solution: We work back through the above calculations.
$13 = 65 – 52$

$= 65 – (117 – 65) = 65.2 – 117$
$= (299 – 117.2).2 – 117 = 299.2 – 117.5$
$= 299.2 – (416 – 299).5 = 299.7 – 416.5$
$= (715 – 416).7 – 416.5 = 715.7 – 416.12$
$= 715.7 – (1131 – 715).12 = 715.19 – 1131.12$
$= (2977 – 1131.2).19 – 1131.12 = 2977.19 – 1131.50$

So $h = –50$, $k = 19$ is one solution.

You must resist the temptation to simplify, except as a check. Keep the two current numbers intact at all times. However at the end you should check that the expression simplifies to the GCD.

Theorem 7: Euclid's algorithm finds the GCD of two positive integers.

Proof: Let m, n be positive integers. Suppose $m = nq + r$ where $0 \leq r < m$.

Then $D(m) \cap D(n) = D(n) \cap D(r)$ since any k that divides both m, n will divide r and any k that divides both n, r divides m. At each stage the set of common divisors of the two numbers we are dealing with is the original $D(m) \cap D(n)$. Suppose at the final stage, when $r = 0$, the other number is d. Then $D(m) \cap D(n) = D(d) \cap D(0) = D(d)$ since $D(0) = \mathbb{Z}$. [Remember that every integer is a multiple of 0.] So the greatest common divisor of m and n is the largest divisor of d, which is d itself.

Theorem 8: If $m \mid ab$ and a, m are coprime then $m \mid b$.
Proof: By Theorem 4, $1 = ah + mk$ for some $h, k \in \mathbb{Z}$ and so $b = abh + mkb$.
Since $m \mid ab$, $m \mid b$.

§1.4. The One-Way Euclidean Algorithm

The reverse algorithm is unpleasant to perform and is error prone, yet it's important for a number of applications, such as finding inverses modulo m. The following tabular version involves about half the arithmetic and about a quarter of the writing as the usual method and proceeds in a single direction by computing the ingredients for the inverse as we go instead of having to work backwards. We'll prove that this works in the next chapter.

To find the GCD of a, b and to express it in the form $ah + bk$:
Generate three recurrence sequences:

$$\begin{cases} A_0 = a \quad B_0 = 0 \\ A_1 = b \quad B_1 = 1 \\ q_{n+1} = \mathrm{INT}(A_n/A_{n+1}) \\ B_{n+2} = B_n - B_{n+1}q_{n+1} \\ A_{n+2} = A_n - A_{n+1}q_{n+1} \end{cases}.$$

We perform the calculation in a table with three columns.

A	**Q**	**B**
a		0
b		1
…	…	…
A′	…….	B′
A	q = INT(A′/A)	B
A′ – Aq		B′ – qB
…	…	…
GCD	q	**k**
0	← STOP	

The pattern for each of the outside columns is “up two minus down times across”

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

Examples 5 and 6 revisited: 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 $h = \frac{13 - 1131(-50)}{2977} = \frac{56563}{2977} = 19$.

So 13 = 2977.19 – 1131.50.

Example 7: Find the inverse of 30 modulo 143. This means 'find b such that 30b = 1 plus a multiple of 143.

A	Q	B
143		0
30	4	1
23	1	–4
7	3	5
2	3	–19
1		**62**
0		

The fact that we get 1 as the last non-zero entry in the first column ensures that an inverse exists. The inverse is the entry in the B column opposite to this 1.
Hence $30^{-1} \equiv 62 (\text{mod } 143)$. This means that $30.62 = 1$ plus a multiple of 143, as you can check.

§1.5. Prime Numbers

We define a number to be **prime** if it has exactly 2 positive divisors. Note that this rules out ±1 from being prime. The usual definition of 'prime' says that 'p is prime if $p \neq \pm 1$ and the only divisors of p are ± 1 and $\pm p$', which is equivalent.

Why don't we allow 1 or −1 to be called prime? There is no logical reason why they couldn't be included. It's just a matter of convenience. The numbers ± 1 have special properties and if we included them as primes we'd repeatedly have to often say 'prime number except ± 1' in our theorems. We call ± 1 **units** because they are the integers that have inverses under multiplication within $\mathbb{Z}$.

Example 8: The prime numbers are ±2, ±3, ±5, ±7, ±11, ±13, ±17, ±19, ±23, ±29, ±31, …

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

0	**units**	**prime numbers**	**composite numbers**

Theorem 9: 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 7, $p \mid b$.

It's a very useful fact that every number can be factorised uniquely into primes. Well, that is not strictly true. Zero can't be factorised into primes. Let's keep to numbers whose absolute value is bigger than 1, that is, numbers that are not 0 or ±1. Is it true that every such number can be factorised uniquely into primes? That depends on our definition of 'uniquely'.

Example 9: There are 4 factorisations of 6 into primes: $6 = 2.3 = 3.2 = (-2)(-3) = (-3)(-2)$. However we consider all four factorisations to be the one factorisation. Note that if we allowed 1 and −1 to be primes we would have infinitely many prime factorisations of 6. For example, $6 = (-2).3.(-1).1.1.1.(-1)(-1)$.

The following theorem describes exactly what we mean by ‘unique’ in the context of unique factorisation.

Theorem 10 (FUNDAMENTAL THEOREM OF ARITHMETIC):
If $|n| > 1$ then $n = p_1p_2 \ldots p_h$ for some h and some primes $p_1, p_2, \ldots, p_h$.
Moreover if $n = p_1p_2 \ldots p_h = q_1q_2 \ldots q_k$ then $h = k$ and, after suitable rearrangement of the factors,
$p_i = \pm q_i$ for each i.
Proof: We proved in Theorem 2.
We prove the second part by induction on the number of prime factors.
Suppose that $p_1p_2 \ldots p_h = q_1q_2 \ldots q_k$ where the p_i and q_i are primes.
Then p_1 divides $q_1q_2 \ldots q_k$ and so p_1 divides q_j for some j, by Theorem 9.
Since q_j is prime $p_1 = \pm q_j$.
Renumbering the q_i’s so that q_j becomes q_1 and dividing by p_1 we get $p_2 \ldots p_h = q_2 \ldots q_k$.
By induction $h - 1 = k - 1$ and for each $i \geq 2$, $p_i = \pm q_j$ for some $j \geq 2$.

§1.6. Generating Prime Numbers

There’s no known formula for the n’th prime number. At least there *are* formulae but they’re so impractical to use that they’re 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 in testing n we only need to test for factors up to $\sqrt{n}$.

Theorem 11: If p has no factors n for $2 \leq n \leq \sqrt{p}$ 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.)

Another improvement is that if we're generating all primes, by the time we got to p we would have a list of all primes less than p. So we never need to test for divisibility by numbers that are composite. If we're just testing a single number p, and don't have a list of primes less than p then at least we should not be testing divisibility by numbers that are clearly composite, such as even numbers and multiples of 3 or 5.

It's useful to be able to recognise multiples of 2, 3 and 5.

- Multiples of 2 are those numbers that end in 0, 2, 4, 6 or 8.
- Multiples of 5 are those numbers that end in 0 or 5.
- Multiples of 3 are those numbers where the sum of the digits is a multiple of 3.

Example 10: 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.
3197 is clearly not divisible by 2, 3 or 5. So, using our calculator we test for divisibility by 7, 11, 13, 17, 19, 23, 29, 31, 37, 41, 43, 47, 53, and we discover that 23 is a factor and that 3197 = 23.139.

Example 11: Is 5113 prime?
Solution: $\sqrt{5113} = 71.50\ldots$ so we only need to test by numbers up to 71.
5113 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, 59, 61, 67, 71. Since 5113 is not divisible by any of these it must be prime.

An ancient method for generating primes is known as the Sieve of Eratosthenes. It's particularly suitable 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 2^{nd} number after that.

At each stage you circle the first number that hasn't been crossed out. That will be a prime number. If this is p then you cross out every p^{th} number after that. Continue until every number on your clay tablet has

been circled or crossed out. The circled numbers will be prime and the crossed out ones will be composite.

Example 12: 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 percentages of primes are 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's only about 12% and in the first million it's 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 they could still generate infinitely many

numbers. After all there are infinitely many powers of 2 and that uses just one prime. This question was asked, and answered, a long time ago by Euclid. There are, indeed, infinitely many primes, though they become gradually rarer as the numbers get larger. We shall prove this in chapter 5.

EXERCISES FOR CHAPTER 1

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 5777 and express it in the form $10101h + 5777k$.

SOLUTIONS FOR CHAPTER 1

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, 11, …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:

3	3	1	3
3403)11111	902)3403	697)902	205)697
10209	2706	697	615
902	697	205	82

2	2
82)205	41)82
164	82
41	0

The last non-zero remainder is 41. Hence the GCD of 11111 and 3403 is 41.
$41 = 205 - 82\times2$
$= 205 - (697 - 205\times3)\times2 = 205\times7 - 697\times2$
$= (902 - 697)\times7 - 697\times2 = 902\times7 - 697\times9$
$= 902\times7 - (3403 - 902\times3)\times9 = 902\times34 - 3403\times9$
$= (11111 - 3403\times3)\times34 - 3403\times9$
$= 11111\times34 - 3403\times111$

Using the One-Way Algorithm instead:
(Remember for the outside columns the pattern is **UP 2 MINUS DOWN TIMES ACROSS**.

A	**Q**	**B**
11111		0
3403	3	1
902	3	–3
697	1	10
205	3	–13
82	2	49
41	2	**–111**
0		

So the GCD = 41 = 11111*h* – 3403*111.
Hence *h* = 34, so 41 = 11111×34 – 3403×111.

Exercise 6:

A	**Q**	**B**
10101		0
5777	1	1
4324	1	–1
1453	2	2
1418	1	–5
35	40	7
18	1	–285
17	1	292
1	17	**–577**

Clearly the last non-zero remainder is 1.
So GCD = 1 = 10101h – 5777*577 so h = 350.