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:

\[ \ldots, -3, -2, -1, 0, 1, 2, 3, \ldots \]

We denote the set of integers by \( \mathbb{Z} \) (from the German word “Zahlen” which means “numbers”). Since these are the only numbers we will be considering in this chapter we will 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. Although there exists a number \( b \) such that \( 2b = 1 \), it is 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 \( a^{-1} \). However cancellation is still valid.

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

Any system, with 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.

An important subset of the integers is the set of natural numbers, \( \mathbb{N} \) consisting of the numbers 0, 1, 2, 3, …. [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 does not 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.

An important property of the natural numbers is the fact that every non-empty subset $S$ of $\mathbb{N}$ has a least, that is an element $m \in S$ such that $m \leq n$ for all $n \in S$. This is the basis for the Principle of 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 $F = \{ n \in \mathbb{N} \mid S(n)$ 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 $\sum_{r=1}^{n} r^3 = \frac{1}{4} n^2(n + 1)^2$.

**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 $n$.

Sometimes we can’t go from $n$ to $n + 1$ or from $n - 1$ to $n$. For example, in proving that every number $n > 1$ can be factorised into primes, we suppose that $n$ can be factorised into primes and then we would have to consider $n + 1$. If $n + 1$ is composite then $n + 1 = ab$ where $0 < a, b < n$, but neither $a$ nor $b$ would be equal to $n$ and so we can’t use the induction hypothesis.

**Theorem 2 (STRONG INDUCTION):**
Suppose $S(n)$ is a statement depending on some parameter $n \in \mathbb{N}$.
If for all $n$, $S(m)$ being 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 $T(n) = \forall m[m < n \rightarrow S(m)]$.
$T(0)$ holds vacuously because $m < 0$ is always false. Remember here that our universe is the set of all natural numbers and also recall that $p \rightarrow q$ 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 1, $T(n)$, 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 “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. Otherwise \( n = ab \) 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 \( n + 1 \), or \( n - 1 \) to \( n \) here. The factors \( a, b \) will be much smaller than \( n \).

§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.

**Theorem 2 (DIVISION ALGORITHM):**

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 natural number in the set \( S = \{ n - mq \mid q \in \mathbb{Z} \} \cap \mathbb{N} \).

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 element of \( S \).

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 element of \( S \).

Hence \( 0 \leq r < |m| \).

We call \( r \) the remainder on dividing \( n \) by \( m \). 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 \( m \mid n \). Equivalently we can say that \( n \) is a multiple of \( m \).

**Example 2:** 3 divides 12, \(-17\) divides 34 and 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 | 0 is true even though 0 \( \div \) 0 is undefined. Make sure you do not confuse \( m \mid n \) with \( m \div n \) or \( m \divides n \). The symbol \( m \mid n \) is a statement. It can only be true or false. But \( m/n \) (equivalently \( m \divides n \)) is a number.

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

**Example 3:**

\[
D(12) = \{ \pm 1, \pm 2, \pm 3, \pm 4, \pm 6, \pm 12 \}, \quad 12\mathbb{Z} = \{ 0, \pm 12, \pm 24, \pm 36, \ldots \}.
\]

\[
D(1) = \{ \pm 1 \}, \quad 1\mathbb{Z} = \mathbb{Z}.
\]

\[
D(0) = \mathbb{Z} \quad (\text{because} \ n = n.0 \text{ for all} \ n).
\]

\[
0\mathbb{Z} = \{ 0 \}.
\]

\( D(n) \) 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 \( m\mathbb{Z} + n\mathbb{Z} \) which is the set of all numbers of the form \( mh + nk \) where \( h, k \in \mathbb{Z} \).
Theorem 3: 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 \( m\mathbb{Z} + n\mathbb{Z} \).
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: \( D(15) = \{\pm 1, \pm 3, \pm 5, \pm 15\} \) 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 \( \pm 3 \), so these are both greatest common divisors of 15 and 51.

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

Example 5: \( \text{GCD}(91, 130) = 13, \text{GCD}(56, 27) = 1. \)

Two non-zero numbers \( m, n \) are defined to be coprime if \( \text{GCD}(m, n) = 1 \). Loosely speaking we might say that they have “no common factors”, but we would really mean is that the only common factors are \( \pm 1 \).

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

Theorem 5: If \( d = \text{GCD}(a, b) \) then \( a/d \) and \( b/d \) are coprime.

Proof: Let \( a = a_0d \) and \( b = b_0d \) and let \( e = \text{GCD}(a_0, b_0) \). Let \( a_0 = a_1e \) and \( b_0 = b_1e \).
Then \( a = a_1ed \) and \( b = b_1ed \) 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

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 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 \times 2 + 715
1131 = 715 \times 1 + 416
715 = 416 \times 1 + 299
416 = 299 \times 1 + 117
299 = 117 \times 2 + 65
117 = 65 \times 1 + 52
65 = 52 \times 1 + 13
52 = 13 \times 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
= (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 6: Euclid’s algorithm finds the GCD of two positive integers.
Proof: Let m, n be positive integers. Suppose m = nq + r where 0 ≤ r < m.
Then D(m) ∩ D(n) = D(n) ∩ 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) ∩ D(n). Suppose at the final stage, when r = 0, the other number is d. Then D(m) ∩ D(n) = D(d) ∩ 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 7: 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 will 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:

\[
\begin{align*}
A_0 &= a & B_0 &= 0 \\
A_1 &= b & B_1 &= 1 \\
q_{n+1} &= \text{INT}(A_n/A_{n+1}) \\
B_{n+2} &= B_n - B_{n+1}q_{n+1} \\
A_{n+2} &= A_n - A_{n+1}q_{n+1}
\end{align*}
\]

We perform the calculation in a table with three columns. We begin as follows:

<p>| | | |</p>
<table>
<thead>
<tr>
<th></th>
<th></th>
<th></th>
</tr>
</thead>
<tbody>
<tr>
<td>$a$</td>
<td>$0$</td>
<td></td>
</tr>
<tr>
<td>$b$</td>
<td>$q = \text{INT}(a,b)$</td>
<td>$1$</td>
</tr>
</tbody>
</table>

Continue as follows:

<p>| | | |</p>
<table>
<thead>
<tr>
<th></th>
<th></th>
<th></th>
</tr>
</thead>
<tbody>
<tr>
<td>$A$</td>
<td>$Q$</td>
<td>$B$</td>
</tr>
<tr>
<td>$\ldots$</td>
<td>$\ldots$</td>
<td>$\ldots$</td>
</tr>
<tr>
<td>$A'$</td>
<td>$\ldots$</td>
<td>$B'$</td>
</tr>
<tr>
<td>$A$</td>
<td>$q = \text{INT}(A'/A)$</td>
<td>$B$</td>
</tr>
<tr>
<td>$A' - Aq$</td>
<td>$B' - qB$</td>
<td></td>
</tr>
</tbody>
</table>

Here $\text{INT}(x)$ is the integer part function, so $q = \text{INT}(A'/A)$ is the quotient when dividing $A'$ by $A$ and $A' - Aq$ is the remainder.

We end as follows:

<p>| | | |</p>
<table>
<thead>
<tr>
<th></th>
<th></th>
<th></th>
</tr>
</thead>
<tbody>
<tr>
<td>$\ldots$</td>
<td>$\ldots$</td>
<td>$\ldots$</td>
</tr>
<tr>
<td>$\text{GCD}$</td>
<td>$q$</td>
<td>$k$</td>
</tr>
<tr>
<td>$0$</td>
<td>$\leftarrow$</td>
<td>\text{STOP}</td>
</tr>
</tbody>
</table>

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

**Examples 6 and 7 revisited:** Find $\text{GCD}(2977,1131)$ and express it in the form $2977h + 1131k$.

**Solution:**

<p>| | | |</p>
<table>
<thead>
<tr>
<th></th>
<th></th>
<th></th>
</tr>
</thead>
<tbody>
<tr>
<td>$A$</td>
<td>$Q$</td>
<td>$B$</td>
</tr>
<tr>
<td>$2977$</td>
<td>$0$</td>
<td></td>
</tr>
<tr>
<td>$1131$</td>
<td>$2$</td>
<td>$1$</td>
</tr>
<tr>
<td>$715$</td>
<td>$1$</td>
<td>$-2$</td>
</tr>
<tr>
<td>$416$</td>
<td>$1$</td>
<td>$3$</td>
</tr>
<tr>
<td>$299$</td>
<td>$1$</td>
<td>$-5$</td>
</tr>
<tr>
<td>$117$</td>
<td>$2$</td>
<td>$8$</td>
</tr>
<tr>
<td>$65$</td>
<td>$1$</td>
<td>$-21$</td>
</tr>
<tr>
<td>$52$</td>
<td>$1$</td>
<td>$29$</td>
</tr>
<tr>
<td>$13$</td>
<td>$4$</td>
<td>$-50$</td>
</tr>
<tr>
<td>$0$</td>
<td></td>
<td></td>
</tr>
</tbody>
</table>
Hence \(\text{GCD}(2977, 1131) = 13\), \(k = -50\) and \(h = \frac{13 - 1131(-50)}{2977} = \frac{56563}{2977} = 19\).

So \(13 = 2977.19 - 1131.50\).

**Example 8:** Find the inverse of 30 modulo 143.

\[
\begin{array}{c|c|c}
 A & Q & B \\
143 & 0 & \\
30 & 4 & 1 \\
23 & 1 & -4 \\
7 & 3 & 5 \\
2 & 3 & -19 \\
1 & 62 & \\
0 & & \\
\end{array}
\]

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 \(30^{-1} \equiv 62\) (mod 143).

**§1.5. Prime Numbers**

We define a number to be **prime** if it has exactly 2 positive divisors. Note that this rules out \(\pm 1\) 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 \(\pm 1\) 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 is just a matter of convenience. The numbers \(\pm 1\) have special properties and if we included them as primes we would repeatedly have to often say “prime number except \(\pm 1\)” in our theorems. We call \(\pm 1\) units because they are the integers that have inverses under multiplication within \(\mathbb{Z}\).

**Example 9:** The prime numbers are \(\pm 2, \pm 3, \pm 5, \pm 7, \pm 11, \pm 13, \pm 17, \pm 19, \pm 23, \pm 29, \pm 31, \ldots\)

Numbers that are not 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.

<table>
<thead>
<tr>
<th>(0)</th>
<th>units</th>
<th>prime numbers</th>
<th>composite numbers</th>
</tr>
</thead>
</table>

**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 \(\text{GCD}(a, p) = 1\) 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 \(\pm 1\). Is it true that every such number can be factorised uniquely into primes? That depends on our definition of “uniquely”.

**Example 10:** There are 4 factorisations of 6 into primes:
\[6 = 2.3 = (-2)(-3) = (-3)(-2).\] 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, $p_i = \pm q_j$ for each $i$.

Proof: We prove the first part by induction on |n|. Suppose that $n$ is an integer such that |n| > 1 and suppose that numbers whose absolute value is smaller than |n| can be factorised into primes.
If $n$ is prime then $h = 1$ and $p_1 = n$.
If $n$ is composite then $n = ab$ for some numbers $a, b$ where |a| and |b| are bigger than 1.
Since |a| and |b| are smaller than |n| it follows by the strong principle of induction that each of $a, b$ can be factorised into primes and hence so can $n$.
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 and $p_1 \neq \pm 1$, this means that $p_1 = \pm q_j$. 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 $i \geq 2$, $p_i = q_j$ for some $j \geq 2$.

§1.6. Generating Prime Numbers
There is no known formula for the $n$’th prime number. At least there are formulae but they 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 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 are 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 is 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 11: 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 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 12: 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 is 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\textsuperscript{nd} number after that.

At each stage you circle the first number that has not 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 has been circled or crossed out. The circled numbers will be prime and the crossed out ones will be composite.

Example 13: Use the sieve of Eratosthenes to find all the primes up to 100.
Solution:

<table>
<thead>
<tr>
<th></th>
<th>2</th>
<th>3</th>
<th>5</th>
<th>7</th>
<th>11</th>
<th>13</th>
<th>17</th>
<th>19</th>
<th>23</th>
<th>29</th>
<th>31</th>
<th>37</th>
<th>41</th>
<th>43</th>
<th>47</th>
<th>53</th>
<th>59</th>
<th>61</th>
<th>67</th>
<th>71</th>
<th>73</th>
<th>79</th>
<th>83</th>
<th>89</th>
<th>97</th>
<th>100</th>
</tr>
</thead>
<tbody>
<tr>
<td>11</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>31</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>41</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>61</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>71</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

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, and answered, a long time ago by Euclid. There are 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.

Exercise 6: Find the GCD of 10101 and 5019.

SOLUTIONS FOR CHAPTER 2

Exercise 1: $2926 = 2 \times 1463$. We now try dividing 1463 by 3, 5, 7, 11, … and discover that it is exactly divisible by 7. So $2926 = 2 \times 7 \times 209 = 2 \times 7 \times 11 \times 19$.

Exercise 2: We try dividing by the primes 3, 5, 7, 11, … and eventually discover that $713 = 23 \times 31$.

Exercise 3: $\sqrt{659} = 25.6…$ 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 $33^2 = 1089$).

$1001 = 7 \times 143$

$1003 = 17 \times 59$

$1007 = 19 \times 53$

$1009$ is prime.

Exercise 5:

<table>
<thead>
<tr>
<th>3403</th>
<th>902</th>
<th>3403</th>
<th>697</th>
<th>902</th>
<th>205</th>
<th>697</th>
<th>82</th>
<th>205</th>
<th>41</th>
<th>205</th>
</tr>
</thead>
<tbody>
<tr>
<td>10209</td>
<td>2706</td>
<td>697</td>
<td>205</td>
<td>82</td>
<td>41</td>
<td>0</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

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

Exercise 6: $10101 = 5019 \times 2 + 63$

$5019 = 63 \times 79 + 42$

$79 = 42 + 37$

$42 = 37 + 5$

$37 = 5 \times 7 + 2$

$5 = 2 \times 2 + 1$

So GCD(10101, 5019) = 1.