MAS121/MAS221

Number Systems and the Foundations of Analysis

Semester 1, 2005/2006

Lecturer: Dr A Duncan

This module is an introduction to Pure Mathematics. The central theme of the course is the notion of proof. Often we believe things to be true because of numerical calculations by hand, or by computer. These methods are valuable because they suggest possible truths. However, we do not know if a plausible statement is true until it has been proved. We shall see how proofs are used to build mathematical theories starting from simple assumptions and definitions. We study various common methods of proof and some of the techniques of argument that make them up. In particular we consider proof by induction and contradiction. The module also introduces two principal branches of pure mathematics: Algebra via number systems in Semester 1, and Analysis which depends on the notion of a limit, in Semester 2. In both of these areas we shall be interested in making precise statements and deciding whether or not they are true.

These notes are intended to supplement the notes you make during the lectures: material given on slides in the lectures is covered here, what is written on the blackboard during lectures may not be. The notes and other course information can be found on the web at

`www.mas.ncl.ac.uk/~najd2/teaching/mas121/`

from where they can be viewed or printed out. The module page is at

`http://www.ncl.ac.uk/math/undergrad/modules/mas121.htm`

and gives the official course description, syllabus and reading list. In addition, for the first semester I recommend *A cascade of numbers* by R P Burn and A Chetwynd (Arnold 1996) and *Introduction to geometry* by H S M Coxeter.

AJ Duncan September 2005

Contents

Chapter 1

Background

In this Chapter we shall establish and/or revise some of the basic ideas and notation that we need in this and other courses. Much of the material will be familiar and you should use the section as reference when you need it. In lectures I shall refer to Sections of this Chapter as and when they're needed and only go through parts of the Chapter that are less familiar or cause difficulty. Most of the Chapter is about Sets but we start by discussing some terminology.

1.1 Definitions, Lemmas and so on

In mathematics and statistics we sometimes need words to have precise, unambiguous, technical meanings. To give a word such a meaning we make what is called a *definition* of the word. The definition acts like a dictionary definition and the words mean precisely what the definition says and nothing else. For example in Section 1.6 we define the word *integer* to mean the set of whole numbers. From this point on, as far as this course goes, the word "integer" has this meaning and means absolutely nothing else, at all, ever. Some words may have the same meaning in everyday life as in their definition, but others may not. The word "integer", as far as I'm aware, has no meaning other than the one above. On the other hand in Definition 2.5 the word "divides" is given a meaning which may differ from the common usage. For instance we might like to say that if we divide 5 by 2 we get $2\frac{1}{2}$, which seems perfectly sensible. However in the sense given in Definition 2.5 we find that 2 does **not** divide 5. We use our definition for the meaning of "divide" so as far as we are concerned 2 doesn't divide 5.

Definitions record the basic terms and describe the fundamental structures which we work with. Reasoning from the definitions we attempt to understand such things as numbers, sequences, functions etc. The conclusions we draw are recorded and may be referenced later. Important conclusions are called *Theorems*. Less important results may be called *Lemmas*. (Some authors use *Proposition* as a label for a result of medium importance.) *Corollary* is a term used to mean "result which follows more or less obviously from a previous theorem". Conclusions are set out as statements of fact in the Theorems, Lemmas, Corollaries etc.. The reasoning leading to a conclusion is usually set out as a *proof* following the statement.

Examples cover not only illustrative calculations and standard techniques of problem solution but sometimes also results so minor that we don't wish to dignify them with a label like Lemma

or Theorem. (See for instance Example 2.8 in Section 2.2.)

Once a Lemma, Theorem or Corollary has been established by some line of reasoning it can be referred to in subsequent arguments. By recording our results as we go we allow ourselves to build up gradually to surprising or well–hidden conclusions. If we prove the right Theorems on the way we will be able to quote them in appropriate places to make our arguments look concise and elegant.

1.2 Sets

In widespread and in common everyday use there are numerous words for collections: when we refer to such things as a

family, flock, team or pack

we are, in each case, referring to several

people, sheep, players or wolves

as one single entity. This idea of regarding a collection of things as a single object is fundamental to mathematics and statistics where the single entity is usually a set. It may seem somewhat surprising then that we can't make a short, easily understood and unambiguous description of exactly what a set is. Luckily it doesn't usually matter and we can be content with the the following. A **set** is a collection of objects together with some method of (in principle) identifying which objects belong to the collection and which do not. Sets will be studied further in the module MAS131, "Introduction to Probability and Statistics". (There are some more unusual words for sets at www.ojohaven.com/collectives/).

1.3 Membership

If S is a set and x is an object which belongs to S then we say that x is an **element** of S or a **member** of S. The symbol $\in$ is used as an abbreviation for "is a member of", so $x \in S$ reads "x is an element of S". Similarly, the symbol $\notin$ is used as an abbreviation for "is not a member of", so $y \notin S$ reads "y is not an element of S".

One way of describing a set is to enclose a list of its members in curly braces, separated by commas. Thus the set with elements $1, 2, 3, 4, 5$ can be denoted by

$$\{1, 2, 3, 4, 5\}.$$

Judicious use of $\ldots$ allows us to use this notation when the list of elements of the set is infinite. For example the set of positive whole numbers $\mathbb{N}$ can be written as

$$\mathbb{N} = \{1, 2, 3, \ldots\}$$

and the set of all whole numbers $\mathbb{Z}$ as

$$\mathbb{Z} = \{\ldots, -3, -2, -1, 0, 1, 2, 3, \ldots\}.$$

1.4 Subsets

A set S is a **subset** of a set T if every element of S is also an element of T. For example $\{a, b\}$ is a subset of the set $\{a, b, c\}$. The symbol $\subset$ is used as an abbreviation for "is a subset

of". Thus
$$\{1, 2, 3, \ldots\} \subset \{\ldots, -3, -2, -1, 0, 1, 2, 3, \ldots\}.$$
The symbol $\not\subset$ is used as an abbreviation for "is a not a subset of". Thus
$$\{\ldots, -3, -2, -1, 0, 1, 2, 3, \ldots\} \not\subset \{1, 2, 3, \ldots\}.$$
Note that every set is a subset of itself, that is $S \subset S$, for all sets S so, for example,
$$\{a, b, c\} \subset \{a, b, c\}.$$

We also use the symbol $\supset$ as an abbreviation for "contains the subset". For example
$$\{78, 69, 45, 32\} \supset \{78, 45\},$$
$$\{78, 69, 45, 32\} \supset \{78, 32, 69, 45\}$$
and
$$\{78, 69, 45, 32\} \supset \{78, 45\}.$$
The symbol $\not\supset$ has the obvious meaning, that is
$$\{78, 69\} \not\supset \{78, 32, 69, 45\}$$
and
$$\{78, 69, 45, 32\} \not\supset \{78, 31, 64, 49\}.$$

1.5 The empty set

The set with no elements is called the **empty set** denoted $\emptyset$. It follows from the definitions we have already made that the empty set $\emptyset$ is a subset of S, for all sets S. To see this observe that, given our definition of subset, we need to test whether or not every element of $\emptyset$ belongs to S, where S is a set (in fact we need to do this for all sets S). However there are no elements in $\emptyset$ so no element of $\emptyset$ fails the test. Hence $\emptyset$ is a subset of S (no matter what set S we choose).

1.6 Some sets of numbers

We have standard names for some sets of numbers.

(1) The positive whole numbers are called the **natural numbers** and the set $\{1, 2, 3, \ldots\}$ of natural numbers is denoted $\mathbb{N}$.

(2) The elements of the set $\{\ldots -3, -2, -1, 0, 1, 2, 3, \ldots\}$ of all whole numbers, positive, negative and zero are called the **integers** and the set of integers is denoted $\mathbb{Z}$.

(3) A number which can be expressed as a fraction p/q, where p and q are integers and $q \neq 0$ is called a **rational** number and the set of all rational numbers is denoted $\mathbb{Q}$.

(4) A number which has a decimal expansion is called a **real** number and the set of all real numbers is denoted $\mathbb{R}$.

Note that $\mathbb{N} \subset \mathbb{Z} \subset \mathbb{Q} \subset \mathbb{R}$. However $\mathbb{Z} \not\subset \mathbb{N}$, $\mathbb{Q} \not\subset \mathbb{Z}$ and $\mathbb{R} \not\subset \mathbb{Q}$. (Do you know why?)

1.7 Specification of new sets from old

Using the symbol ":" to denote "with the property that" or "such that" we can use curly braces to specify subsets. For example consider the set $\mathbb{N}$ of all positive whole numbers. Then
$$\{n \in \mathbb{N} : n \text{ is even }\}$$
is read as "the set of elements n of $\mathbb{N}$ such that n is even". That is
$$\{2, 4, 6, 8, \ldots\}.$$
The new description is more precise as it removes the necessity for the "...", which are possibly ambiguous. Further examples of this notation are:
$$\{n \in \mathbb{N} : n > 9\} = \{10, 11, 12, \ldots\},$$
and
$$\{n \in \mathbb{N} : n \geq 11 \text{ and } n < 16\} = \{11, 12, 13, 14, 15\}.$$
Sometimes "|" is used instead of ":" as in
$$\{n \in \mathbb{N} \,|\, n \text{ is a multiple of } 10\} = \{10, 20, 30, \ldots\},$$
$$\{n \in \mathbb{N} \,|\, n \text{ is a multiple of 10 and of 3}\} = \{30, 60, 90, \ldots\},$$
$$\{n \in \mathbb{N} \,|\, n \text{ is a multiple of 3 and } n+1 \text{ is a multiple of } 7\} = \{6, 27, 48, \ldots\}.$$

1.8 Unions, intersections, complements and differences

The **union** of two sets S and T, denoted $S \cup T$ is the set consisting of all those elements which either belong to S or belong to T. For example
$$\{A, B, C\} \cup \{X, Y, Z\} = \{A, B, C, X, Y, Z\}$$
and
$$\{A, B, C, Y, Z\} \cup \{A, X, Y, Z\} = \{A, B, C, X, Y, Z\}.$$

The **intersection** of two sets S and T, denoted $S \cap T$ is the set consisting of only those elements which belong to both S and T. For example
$$\{A, B, C, L, M\} \cap \{L, M, X, Y, Z\} = \{L, M\}$$
and
$$\{A, B, C\} \cap \{X, Y, Z\} = \emptyset.$$

If S is a subset of a set E then the **complement** of S **in** E, denoted S', is the set consisting of those elements of E which do not belong to S. That is $S' = \{x \in E : x \notin S\}$. For example if $E = \{a, b, c, d, e, f\}$ and $S = \{a, b, c\}$ then $S' = \{d, e, f\}$.

The **difference** of two sets S and T (in that order), denoted $S \backslash T$, is the set of elements of S which do not belong to T. For example if $S = \{A, B, C, D, E, F\}$ and $T = \{D, E, F, G, H, I\}$ then $S \backslash T = \{A, B, C\}$.

1.9 Objectives

The material in this chapter is mainly for reference but you should become familiar with it as the course goes on. Once you have covered this chapter you should be able to:

(i) understand the use of terms such as Definition, Lemma, Theorem,...

(ii) read and use the symbols $\in$, $\{\ldots\}$, $\subset$, $\not\subset$, $\supset$, $\not\supset$ and $\emptyset$;

(iii) know which sets of numbers $\mathbb{N}$, $\mathbb{Z}$, $\mathbb{Q}$ and $\mathbb{R}$ refer to;

(iv) understand notation of the form $\{n \in \mathbb{Z} : n > 10\}$;

(v) know what unions, intersections, complements and differences of sets are and understand the meaning of $X \cup Y$, $X \cap Y$, $X\backslash Y$ and X', where X and Y are sets.

1.10 Exercises

Use these questions to test your set theory. If you can't do them you should read the Chapter.

1.1 Go to the library and find the Mathematics and Statistics books. You are allocated a range of shelf marks below. In a book with your shelf mark find a piece of technical mathematical or statistical terminology (that is a word like *definition*, *theorem*, *lemma* or *corollary*) which is not mentioned in Section 1.1 of this course. Write out

(a) the name of the book, its author, its publisher and date of publication;

(b) the word that you have found and the page it occurs on;

(c) the sentence containing the word you have found (or enough of its context to show how it is used) and

(d) describe, in not more than 3 lines, what the word means and how it is used.

Your shelf mark is as follows, depending on the first letter of your surname.

Name	Shelf mark	Name	Shelfmark	Name	Shelfmark
A–B	511–511.52	**C–D**	512.52–512.8	**E–F**	515.354–515.7
G–H	511.6–512.02	**I–J**	512.9–514.744	**K–L**	515.72–515.9
M–N	512.1–512.22	**O–P**	515–515.15	**Q–R**	515.93–516.7
S–T	512.23–512.507	**U–V**	515.2–515.353	**W–Z**	516.8–519

1.2 List the elements of the following sets:

(a) $\{n \in \mathbb{N} \ : \ 10 < n^2 + n < 42\}$;

(b) $\{x \in \mathbb{R} \ : \ x^2 + 6x + 9 = 0\}$;

(c) $\{n \in \mathbb{N} \ : \ n$ and $n + 2$ are prime with $n < 30\}$;

1.3 List the elements of the following sets:

(a) $\{n \in \mathbb{N} \ : \ 2 < n^2 < 75\}$;

(b) $\{x \in \mathbb{R} \ : \ x^2 + 3x + 2 = 0\}$;

(c) $\{n \in \mathbb{N} \ : \ n$ is a 2 digit prime $\}$;

1.4 TRUE or FALSE

(a) $6 \notin \{x \in \mathbb{N} \ : \ x = 3n + 1,$ for some $n \in \mathbb{N}\}$;

(b) $2 \in \{x \in \mathbb{R} \ : \ x^2 = 4\}$;

(c) $-2 \in \{x \in \mathbb{R} \ : \ x^2 = 4$ and $x > 0\}$;

(d) $7 \notin \{x \in \mathbb{Q} \ : \ x^2 \geq 7$ and $x^3 < 343\}$.

1.5 TRUE or FALSE:

(a) $\emptyset \subset \mathbb{N} \subset \mathbb{N}$

(b) $\{x \in \mathbb{R} : x = 3n + 1,$ where $n \in \mathbb{N}\} \subset \{x \in \mathbb{Z} : x > 3\}$

(c) $\{x \in \mathbb{Z} : x > 3\} \subset \{x \in \mathbb{R} : x = 3n + 1,$ where $n \in \mathbb{N}\}$

(d) $\{x \in \mathbb{N} : x$ is even $\} \subset \{x \in \mathbb{R} : x^2$ is even$\}$

Chapter 2

Division and Greatest Common Divisors

A professor decides to reward the class by handing out toffees. There are 24 toffees in a packet and the professor buys several packets. On the way to the lecture the prof eats 6 toffees. There are 30 students in the lecture, each receives the same number of toffees and then there are no toffees left. What's the least number of packets the prof could have bought and how many toffees would each student then get?

We can solve this problem algebraically.

Suppose that
 the number of packets of toffees bought $= x$
 the number of toffees each student gets $= y$

We can easily work out:
 Total number of toffees bought: $= 24x$
 Number of toffees handed out to class $= 24x - 6$

Since each student gets y toffees and there are 30 students

$$24x - 6 = 30y.$$

What can x be? We must solve the equation above to find whole numbers x and y which are both positive (if possible). To simplify matters notice we can divide through by 6 and the equation becomes

$$4x - 1 = 5y.$$

We can solve this by trying values of x until we find one which works. We start with $x = 1$, since we're looking for the smallest number of packets the prof could have bought, and increase x by one each time:

x	1	2	3	4
$4x-1$	3	7	11	15
y?	???	???	???	3

When x is 4 and y is 3 we have $4x - 1 = 5y$. No smaller value of x makes $4x - 1$ equal to a multiple of 5. We now know that the prof could have got away with buying just $x = 4$ packets of toffees. Each of the students would then have received 3 toffees.

There are two features of this problem that I'd like to draw attention to.

- We are only interested in solutions to this problem which are natural numbers (defined in Section 1.6). Solutions would be very easy to find if we allowed ourselves to use rational numbers or real numbers (see Section 1.6). For example if we set $x = 1$ then we can take $y = 3/5$. On the other hand finding integer solutions is just as difficult as finding natural number solutions (integers are also defined in Section 1.6).

- To simplify the equation I divided through by 6. I could have divided by 2 or by 3 but the resulting equation would have had bigger numbers in it. However 6 is as big as I can go without making some number in the equation into a fraction. Put another way, 24, 30 and 6 are all multiples of 6 but they're not all multiples of anything bigger than 6.

This chapter looks into some of the properties of natural numbers and integers that, among other things, prove useful in solving problems such as the toffees above. We'll look at a a step by step recipe which would give us the number 6 to divide our equation by in this problem and then investigate, in some detail, why it works.

2.1 The Euclidean Algorithm

To solve the equation $24x-6 = 30y$ I first divided throughout by 6. I chose 6 because it is the biggest positive number that divides all 3 of $24, 6$ and 30. How do I know? Because I'm familiar with the positive divisors of all these numbers and I mentally list them and pick the biggest that appears on all 3 lists, which in this case happens to be 6. Let's see how this process works for some other numbers. For simplicity suppose I want the biggest positive number that divides both 24 and 30. I make two lists.

Positive divisors of 24 : $1, 2, 3, 4, 6, 8, 12, 24$

Positive divisors of 30 : $1, 2, 3, 5, 6, 10, 15, 30$

Now I pick the largest number which appears on both of the lists, which is 6, and this is my answer.

Example 2.1. Find the biggest number which divides both 2028 and 2600.
Positive divisors of

2028 : 1, 2, 3, 4, 6, 12, 13, 26, 39, 52, 78, 156, 169, 338, 507, 676, 1014, 2028

2600 : 1, 2, 4, 5, 8, 10, 13, 20, 25, 26, 40, 50, 52, 65,100, 104, 130, 200, 260, 325,520, 650, 1300, 2600

By examining these lists we see that the biggest number dividing both 2028 and 2600 is 52.

The last example involved alot of calculation and required us to factorise both 2028 and 2600. Without some systematic method it would be very easy to leave out some divisor of either 2028 or 2600. The following is a method which in many cases involves much less work and is easier to validate.

The algorithm

The biggest natural number which divides both natural numbers a and b is called the **greatest common divisor** of a and b. Given natural numbers a and b we wish to find their greatest common divisor. The recipe works as follows.

EA1. Input the pair (b, a), with $0 < a < b$.

EA2. Write $b = aq + r$, where q and r are integers with $0 \leq r < a$.

EA3. If $r = 0$ then **output** $\gcd(a, b) = a$ and **stop**.

EA4. Replace the ordered pair (b, a) with (a, r). Repeat from (2).

Before going into why this algorithm works we look at some examples.

Example 2.2. Find the greatest common divisor d of 12 and 63. Find $x, y \in \mathbb{Z}$ such that $12x + 63y = d$.

As shown in the above example we can use the Euclidean Algorithm not only to find the greatest common divisor d of two natural numbers a and b but also to express d as sum of multiples of a and b. This can be useful in solving equations as we'll see later. (Note that x and y are not always natural numbers: they may be negative.)

Example 2.3. Find the greatest common divisor d of 2600 and 2028. Find integers x and y such that $d = 2600x + 2028y$.

First we find $\gcd(2028, 2600)$. The input to the Euclidean Algorithm is $(2600, 2028)$. We write out the results of Step EA2 as the algorithm runs:

$$\begin{array}{lll}
(2600,2028) & 2600 = 2028 \cdot 1 + 572 & (2.1)\\
(2028,572) & 2028 = 572 \cdot 3 + 312 & (2.2)\\
(572,312) & 572 = 312 \cdot 1 + 260 & (2.3)\\
(312,260) & 312 = 260 \cdot 1 + 52 & (2.4)\\
(260,52) & 260 = 52 \cdot 5 + 0. & (2.5)
\end{array}$$

This gives $\gcd(2600, 2028) = 52$, as we found in Example 2.1.

To find the integers x, y we work back from (2.4) to (2.1).

$$\begin{aligned}
52 &= 312 - 260 \cdot 1 && \text{from (2.4)}\\
&= 312 - (572 - 312 \cdot 1) = 312 \cdot 2 - 572 && \text{from (2.3)}\\
&= (2028 - 572 \cdot 3) \cdot 2 - 572 = 2028 \cdot 2 - 572 \cdot 7 && \text{from (2.2)}\\
&= 2028 \cdot 2 - (2600 - 2028 \cdot 1) \cdot 7 = 2028 \cdot 9 - 2600 \cdot 7 && \text{from (2.1).}
\end{aligned}$$

Thus $52 = 2600 \cdot (-7) + 2028 \cdot 9$ so we may take $x = -7$ and $y = 9$.

Example 2.4. Find the greatest common divisor d of 2028 and 626. Find $x, y \in \mathbb{Z}$ such that $2028x - 626y = d$.

First we find $\gcd(2028, 626)$. The input to the Euclidean Algorithm is $(2028, 626)$. We write out the results of Step EA2 as the algorithm runs:

$$\begin{array}{lll}
(2028,626) & 2028 = 626 \cdot 3 + 150 & (2.6)\\
(626,150) & 626 = 150 \cdot 4 + 26 & (2.7)\\
(150,26) & 150 = 26 \cdot 5 + 20 & (2.8)\\
(26,20) & 26 = 20 \cdot 1 + 6 & (2.9)\\
(20,6) & 20 = 6 \cdot 3 + 2 & (2.10)\\
(6,2) & 6 = 2 \cdot 3 + 0. & (2.11)
\end{array}$$

This gives $\gcd(2028, 626) = 2$.

To find the integers x, y we work back from (2.10) to (2.6) to find an expression for 2.

$$\begin{aligned}
2 &= 20 \cdot 1 - 6 \cdot 3 && \text{from (2.10)}\\
&= 20 \cdot 1 - 3 \cdot (26 \cdot 1 - 20 \cdot 1) = 20 \cdot 4 - 26 \cdot 3 && \text{from (2.9)}\\
&= (150 \cdot 1 - 26 \cdot 5) \cdot 4 - 26 \cdot 3 = 150 \cdot 4 - 26 \cdot 23 && \text{from (2.8)}\\
&= 150 \cdot 4 - (626 - 150 \cdot 4) \cdot 23 = 150 \cdot 96 - 626 \cdot 23 && \text{from (2.7)}\\
&= (2028 - 626 \cdot 3) \cdot 96 - 626 \cdot 23 = 2028 \cdot 96 - 626 \cdot 311 && \text{from (2.6).}
\end{aligned}$$

Thus $2 = 2028 \cdot 96 - 626 \cdot 311$ so we may take $x = 96$ and $y = 311$.

2.2 Divisibility in the integers

From the evidence of the examples above it appears that the Euclidean Algorithm really does return the greatest common divisor of two natural numbers. I'd like to understand why this is so. We shall consider integer arithmetic and hopefully this will allow us to see exactly how the algorithm performs and why it works. We shall take for granted the basic properties of arithmetic with numbers. By arithmetic is meant addition and multiplication. For example we consider it a basic law that $x + y = y + x$, where x and y are natural numbers, integers or real numbers[1]. Among other properties that hold for numbers x, y and z are that

$$\begin{gathered}
0 + x = x\\
1 \cdot x = x\\
x(y + z) = xy + xz\\
(-x)(-y) = xy\\
\text{if } x > 0 \text{ and } y < 0 \text{ then } xy < 0.
\end{gathered}$$

We've already used the terminolgy "a divides b" for integers a and b but let's be absolutely clear of what we mean by this.

Definition 2.5. Let a and b be integers. If there exists an integer q such that $b = qa$ then we say that a **divides** [2] b, which we write as $a|b$.

(*A definition establishes once and for all the meaning of a word. From now on whenever we say "divides" we mean what it says above, nothing more, nothing less.*)

Other ways of saying $a|b$ are that a is a **factor** of b, a is a **divisor** of b or b is a **multiple** of a. We write $a \nmid b$ to denote "a does not divide b".

Example 2.6. From the definition we can easily check that $6|18$ because $18 = 6 \cdot 3$. In the same way we see that 6 divides $24, 12, 6, 0$ and -6. It's also fairly obvious that $7 \nmid 16$ and $-15 \nmid 25$, although explaining exactly why may take a little thought.

In the next few examples we'll use Definition 2.5 as a starting point and from it prove some very simple facts, just to get used to the terminology for integer arithmetic.

Example 2.7. We shall prove that $6|(6n + 6)$, for all integers n.

[1] The real numbers are defined in Section 1.6

[2] Bold face is used for definitions. Some authors use italics. On the blackboard underlining is used instead.

Example 2.8. Prove that $4|[(2n+1)^2-1]$, for all integers n.

What we need to settle the question of explaining why, for example $6 \nmid 13$ is something like: if we form the fraction $13/6$ it's equal to $2+1/6$ which is not an integer. Alternatively, to verify that $32 \nmid 121$ we could try to divide 121 by 31 and we'd find a non–zero remainder. In fact we can express 121 as

$$121 = 32 \times 3 + 25.$$

(In this expression 3 is called the *quotient* and 25 the *remainder*.) This is the content of the Theorem we come to next.

Before stating the Theorem we need to recall some notation.

Definition 2.9. The **modulus** or **absolute value** of a real number x is denoted $|x|$ and is given by the formula

$$|x| = \begin{cases} x, & \text{if } x \geq 0 \\ -x, & \text{if } x < 0. \end{cases}$$

All integers are real numbers so it makes perfect sense to talk of the modulus of an integer. For example

$$|-6| = 6 = |6|,$$
$$102 = |102| = |-102| \text{ and}$$
$$|0| = 0 = -0 = |-0|.$$

Theorem 2.10 (The Division Algorithm). *Let a and b be integers with $a \neq 0$. Then there exist unique integers q and r such that $b = aq + r$ and $0 \leq r < |a|$.*

We could prove this: but it is intuitively obvious, rather mundane and up to now we just accepted it as an obvious fact: so we'll continue to accept it for now. If you're unhappy with this, more detail of why and how it should be proved can be found in any book on elementary number theory; and later on we'll prove a similar statement in a setting where it's not obviously true. Instead let's take stock.

(1) The condition that $a \neq 0$ is necessary. It's the same as saying that we can't have fractions like $3/0$.

(2) There are two parts to the conclusion of the Theorem. Firstly it says that q and r do exist, with the properties described. Secondly it says that q and r are ***unique***. In terms of the example above this means that if we have q and r with $0 \leq r < 32$ such that $121 = 32q + r$ then q **must** be 3 and r **must** be 25. This is not surprising: we'd be dismayed if $121/32$ had some value other than $3 + 25/32$.

(3) One way if assessing whether the Theorem is worth stating or not is to see how it might work in other settings. Suppose for example we were to work with rational numbers instead of integers. If b and a are rational with $a > 0$ then I can pick any r I like, in the given range $0 \leq r < |a|$, and obtain $b = aq + r$ by setting $q = (b-r)/a$. Thus q and r are not unique and the Division Algorithm does not hold. More dramatic failure of the Division Algorithm is exhibited in some other situations. For example in the set of polynomials in two variables x and y with integer coefficients it's easy to find polynomials f and g for which there is no way of writing $f = g \cdot q + r$ with r in any meaningful way "less than" g.

Here are some examples of the Division Algorithm in action.

Example 2.11. Every integer n can be written as $n = 2q + r$, with $0 \leq r < 2$. If $r = 0$ we say n is **even** and if $r = 1$ we say n is **odd**.

Here we've used the Division Algorithm (Theorem 2.10) to partition of integers into odd and even.

Example 2.12.

Example 2.13. Show that $3|n^3 - n$, for all integers n.

Example 2.14. Show that if n is an integer then n^3 has the form $4k$, $4k + 1$ or $4k + 3$, for some $k \in \mathbb{Z}$.

2.3 Why the Euclidean Algorithm works

Example 2.15. Consider the equality $112 = 20 \cdot 5 + 12$.

Lemma 2.16. *Let s, t and u be integers, which are not all zero, such that*

$$s = tq + u.$$

Then $\gcd(s, t) = \gcd(t, u)$.

(*A lemma is a lesser result: one which is not important enough to be given the grand title of theorem. Lemmas are often small steps made on the way to establishing a theorem.*)

Proof. Strategy: show that any integer that divides both s and t must also divide u. Then show that any integer that divides both t and u must also divide s. Having done this it's clear that the set of common divisors of s and t is exactly the same as the set of common divisors of t and u and their greatest commond divisors are thus equal.

$\square$

Example 2.17. We can write $337 = 11 \cdot 30 + 7$.

The lemma above is the key to the Euclidean Algorithm. We shall not *prove* that the Euclidean algorithm works, being content to see that it must do on some fairly general examples. A proof

using what we have done so far is set out in Appendix A. Before going any further we record some very basic consequences of the definition of division; as a lemma.

Lemma 2.18.

1. *$a|a$, for all integers a.*

2. *$a|0$, for all integers a.*

3. *If a and b are integers such that $a|b$ and $b > 0$ then $a \leq b$.*

4. *If a and b are positive integers such that $a|b$ then $\gcd(a, b) = a$.*

Proof.

□

Example 2.19. Consider the Equations (2.6)–(2.11).

Stringing all these facts together we have

$$2 = \gcd(6,2) = \gcd(20,6) = \gcd(26,20) = \gcd(150,26) = \gcd(626,150) = \gcd(2028,626),$$

that is $\gcd(2028,626) = 2$. This is what the Euclidean Algorithm told us. Lemma 2.16 and Equations (2.6)–(2.11) show why the algorithm comes up with the correct answer.

Example 2.20. Consider the Equations (2.1)–(2.5). As in the example above we have

$$\begin{aligned}
\gcd(2600,2028) &= \gcd(2028,572), \text{ using Equation (2.1)}\\
\gcd(2028,572) &= \gcd(572,312), \text{ using Equation (2.2)}\\
\gcd(572,312) &= \gcd(312,260), \text{ using Equation (2.3)}\\
\gcd(312,260) &= \gcd(260,52), \text{ using Equation (2.4).}
\end{aligned}$$

From Equation (2.5) we see that $52|260$ and so we have $\gcd(260,52) = 52$:

Therefore

$$\begin{gathered}
52 = \gcd(260,52) = \gcd(312,260) = \\
\gcd(572,312) = \gcd(2028,572) = \gcd(2600,2028),
\end{gathered}$$

that is $\gcd(2600,2028) = 52$. Again we've seen why the answer given by the Euclidean Algorithm was the correct one.

In addition to finding the greatest common divisor of two integers a and b we can work back through the output of the Euclidean algorithm, as we did in Examples 2.2, 2.3 and 2.4, to find integers x and y such that $ax + by = \gcd(a,b)$. This give us the following Theorem.

Theorem 2.21. *Let a and b be integers, not both zero, and let $d = \gcd(a,b)$. Then there exist integers u and v such that $d = au + bv$.*

Note that we restricted the input of the Euclidean algorithm to pairs of positive integers, so we might worry that if a or b is non-positive then the Theorem does not work. However it's easy to see that $\gcd(a,b) = \gcd(-a,b) = \gcd(-a,-b) = \gcd(a,-b)$ and from this it follows that the Theorem holds in all cases.

2.4 An application

We began this Chapter by looking at the problem of distribution of toffees. This problem was resolved by solving the equation $24x - 6 = 30y$. An equation of this form, where the coefficients are integers and only x's and y's occur (nothing like x^2, x^3, xy or xy^2 occurs) and for which we seek integer solutions, are called **linear Diophantine equations**. Here we look at some linear Diophantine equations.

Example 2.22. Find integers x and y such that $2600x + 2028y = 104$.

In Example 2.3 we ran the Euclidean Algorithm and found $\gcd(2600,2028) = 52$. Once we'd done so we were able to use the equations generated to find integers x and y such that

$$2600 \cdot (-7) + 2028 \cdot 9 = 52. \tag{2.12}$$

Example 2.23. Find integers x and y such that $-72 = 12378x - 3054y$.

First we run the Euclidean Algorithm to find $\gcd(12378,3054)$.

$$\begin{aligned}
&(12378,3054) & 12378 &= 3054 \cdot 4 + 162 & (2.13)\\
&(3054,162) & 3054 &= 162 \cdot 18 + 138 & (2.14)\\
&(162,138) & 162 &= 138 \cdot 1 + 24 & (2.15)\\
&(138,24) & 138 &= 24 \cdot 5 + 18 & (2.16)\\
&(24,18) & 24 &= 18 \cdot 1 + 6 & (2.17)\\
&(18,6) & 18 &= 3 \cdot 6 + 0. & (2.18)
\end{aligned}$$

This gives $\gcd(12378,3054) = 6$.

Next we work back from (2.17) to (2.13) to find integers u, v such that $6 = 123738u + 3054v$.

$$\begin{aligned} 6 &= 24 - 18 \cdot 1 && \text{from (2.17)} \\ &= 24 - (138 - 24 \cdot 5) = 24 \cdot 6 - 138 && \text{from (2.16)} \\ &= (162 - 138) \cdot 6 - 138 = 162 \cdot 6 - 138 \cdot 7 && \text{from (2.15)} \\ &= 162 \cdot 6 - (3054 - 162 \cdot 18) \cdot 7 = 162 \cdot 132 - 3054 \cdot 7 && \text{from (2.14)} \\ &= (12738 - 3054 \cdot 4) \cdot 132 - 3054 \cdot 7 = 12378 \cdot 132 - 3054 \cdot 535 && \text{from (2.13).} \end{aligned}$$

Thus

$$6 = 12378 \cdot 132 + 3054 \cdot (-535) \tag{2.19}$$

so we may take $u = 132$ and $v = -535$.

The method above of finding integer solutions can be extended to find all such solutions to equations of this kind. Here we establish conditions which determine whether or not there exists a solution. Later on we'll see how to describe all solutions.

Lemma 2.24. *Let a, b and c be integers (a, b not both zero). The equation*

$$ax + by = c \tag{2.20}$$

has integer solutions x, y if and only if $\gcd(a, b)|c$.

Proof.

$\square$

Example 2.25. Are there integers x and y such that $2600x + 2028y = 130$?

Example 2.26. For which c does the equation $72x + 49y = c$ have a solution? $\gcd(72, 49) = 1$ so the equation $72x + 49y = c$ has a solution for every choice of c.

2.5 Objectives

After covering this chapter of the course you should be able to:

(i) use terms such as *Definition*, *Lemma* and *proof* with confidence;

(ii) read and understand simple proofs;

(iii) remember Definition 2.5 of a *divides* b, for integers a and b;

(iv) apply this definition to prove simple divisibility properties;

(v) state the Division Algorithm and be able to use it to demonstrate properties of integers;

(vi) remember the definition of greatest common divisor of two integers;

(vii) apply this definition to prove results;

(viii) apply the Euclidean algorithm and explain why it works;

(ix) find solutions to equations of the kind given in Section 2.4.

2.6 Exercises

2.1 For each of the following pairs a, b of integers find $\gcd(a, b)$ and integers r and s such that $\gcd(a, b) = ra + sb$.

(a) $a = 13, b = 1000$; (c) $a = 1729, b = 703$; (e) $a = 5213, b = 2867$.
(b) $a = 306, b = 657$; (d) $a = 1147, b = 851$;

2.2 Prove the following using only the definition of division (Definition 2.5). In each case indicate where in your proof you have used the definition.

(a) $13|169$, $13|1859$ and $143|1859$. (c) $5|(5n^2 + 4)^2 - 1$, for all $n \in \mathbb{Z}$.
(b) $5|(5n^2+25n+75n)$, for all integers n.

2.3 Use the Division Algorithm to show that, if n is an integer then

(a) n^2 is either of the form $3k$ or $3k + 1$;
(b) n^2 is either of the form $4k$ or $4k + 1$;
(c) n^3 has one of the forms $9k$, $9k + 1$ or $9k + 8$;
(d) n^4 is of the form either $5k$ or $5k + 1$.

2.4 Show that $5|n^5 - n$, for all integers n.

2.5 Use the Division Algorithm to prove that for any integer a one of the integers a, $a + 2$, $a + 4$ is divisible by 3. Indicate where and how you use the Division Algorithm in your proof.

2.6 Use the Division Algorithm to prove that for any integer a one of the integers a, $a + 2$, $a + 4$, $a + 6$ or $a + 8$ is divisible by 5. Indicate where and how you use the Division Algorithm in your proof.

2.7 Use only the definition of division, Definition 2.5, to prove the following facts. Do **not** mention the Division Algorithm, Theorem 2.10. Let a, b and c be integers.

(a) Prove that if $c|a$ then $-c|a$ and $c|(-a)$.
(b) Prove that if $a|b$ and $b|c$ then $a|c$.

2.8 Let a and b be integers.

(a) Prove that $\gcd(a, b) = \gcd(-a, b) = \gcd(-a, -b)$.
(b) If $a > 0$ show that $\gcd(a, 0) = a$. What is $\gcd(a, 0)$ if $a < 0$?

2.9 Determine integer solutions x, y to the following equations.

(a) $56x + 72y = 40$; (d) $5x + 17y = 22$;
(b) $24x + 138y = 18$; (e) $63x + 45y = 783$;
(c) $221x + 35y = 11$; (f) $119x - 6y = 7$.

2.10 Which of the following equations have integer solutions? (Justify your answers but do not find the solutions.)

(a) $56x + 72y = 88$; (d) $5x + 17y = 88$;
(b) $24x + 138y = 88$; (e) $63x + 45y = 88$;
(c) $221x + 35y = 88$; (f) $119x - 6y = 88$.

Chapter 3

Logic and Proof

First we look at some of the forms that our results commonly take. Then we discuss two common methods of proof, namely Contradiction and Induction.

3.1 Menagerie

"There exists ..."

Many of the Lemmas and Examples in Chapter 2 assert the existence of something. For instance Example 2.4 asked for integers x and y such that $2028x - 626y = \gcd(2028, 626)$. One such pair $x = 96$, $y = 311$, was found by applying the Euclidean Algorithm. Once such a pair has been found we have *proved* the truth of the statement

"There exist integers x and y such that $2028x - 626y = \gcd(2028, 626)$."

It is only necessary to find *one* pair x, y to prove that this statement is true. (There are lots of other pairs besides the one given, $x = 409$, $y = 1325$, for example, but this doesn't matter. The assertion can be seen to be true once we've found our first solution.)

Notation: the symbol "$\exists$" is read "there exists".

Example 3.1. Prove that $\exists q \in \mathbb{Z}$ such that $7q = 28$.

Example 3.2. Prove that $\exists x \in \mathbb{R}$ such that $x \cdot 0 = 0$.

"For all..."

Similarly in Examples 2.8, 2.13 and 2.14 we show that something holds for all integers. In each case we do this by using a letter n to represent an arbitrary integer. Again, it is easy to verify these results for particular values of n but this does not prove that the statements hold *for all* integers.

Counter–example and disproof

Is the following statement true or false?

$$3|n^2 + 2n, \text{ for all } n \in \mathbb{Z}.$$

Notation: the symbol "$\forall$" is read "for all".

Example 3.3. Show, by finding a counter–example that the statement

"n^2 is even, $\forall n \in \mathbb{Z}$"

is false.

Example 3.4. Disprove the assertion that

"$\exists n \in \mathbb{Z}$ such that n^3 can be written as $4k + 2$, with $k \in \mathbb{Z}$".

Example 3.5. Consider the statement

$$\text{“}\exists x \in \mathbb{R} \text{ such that } x^2 = -10.$$

I believe this is false. To prove it's false I must show it fails for all $x \in \mathbb{R}$ (infinitely many). I can use a basic property of real number arithmetic to do this. Namely, if $x \in \mathbb{R}$ then $x^2 \geq 0$. Thus, no matter what value b takes the statement is false. Note that a counter–example is no use here as I must check all possible values of x.

"If ... then ..."

Example 3.6. Consider the assertion,

$$\text{“if } x > 2 \text{ then } x^2 + x - 6 > 0\text{”.}$$

In statements of the form "if A then B" it is crucial that "A" occurs between "if" and "then" and that "B' occurs after "then". If we swap A and B around we end up with something that has a different meaning. This is easy to understand on the level of everyday language. For example

"If I am a frog then I can swim"

is a plausible enough statement which for arguments sake we can assume is true. The A part is "I am a frog" and the B part is "I can swim". Switching the order of A and B we have

"If I can swim then I am a frog".

This can't be true, unless lots of people we know are in fact frogs!

Example 3.7. If we switch the order of A and B in Example 3.6 we obtain the statement

$$\text{“If } x^2 + x - 6 > 0 \text{ then } x > 2.\text{ ”}$$

Switching A and B always gives a new statement (as long as we don't consider statements where A and B are the same). The switched statement is called the **converse** of the original.

Example 3.8. The converse of

$$\text{“If } x^2 > 0 \text{ then } x > 0\text{”}$$

is

$$\text{“If } x > 0 \text{ then } x^2 > 0\text{”.}$$

This time, if $x \in \mathbb{R}$, the original statement is false but its converse is true.

As in the above examples, even if the original statement is true its converse may not be, and vice–versa. In some circumstances it may turn out however that both statements are true: as in the next example.

"... if and only if ..."

Example 3.9. Let $a, b, c \in \mathbb{R}$ with $a > 0$. Consider the statement

"If $b^2 - 4ac \geq 0$ then $ax^2 + bx + c = 0$ has a real solution."

We know that this is true.

What we have seen in the previous example is that

"[if $b^2 - 4ac \geq 0$ then $ax^2 + bx + c = 0$ has a real solution]
AND
[if $ax^2 + bx + c = 0$ has a real solution then $b^2 - 4ac \geq 0$]"

is a true statement. We have a shorthand for statements of this form: we say

"$ax^2 + bx + c = 0$ has a real solution *if and only if* $b^2 - 4ac \geq 0$"

instead. Sometimes "if and only if" is shortened to "iff". In general a statement of the form

"A if and only if B"

means

"[if A then B] AND [if B then A]".

Here is an "if and only if" version of Lemma 2.18.3.

Corollary 3.10. *Assume that a and b are positive integers. Then $a|b$ if and only if $\gcd(a, b) = a$.*

Proof. The statement of the Corollary uses shorthand and when written out in full becomes
"[if $a|b$ then $\gcd(b, a) = a$] AND [if $\gcd(b, a) = a$ then $a|b$]".
The general rule in a proof of such a statement is *prove each part separately*.

We have proved both statements are true so we have completed the proof of the Lemma. □

In general terms to show that

"A if and only if B"

is true we must establish the truth of both

"if A then B"

and

"if B then A".

Synonyms

There are several different ways of saying things like "if ... then ..." and "... if and only if ...". The symbol $\Rightarrow$ is read "implies". All the entries on a given line of the following table mean the same thing.

if A then B	A $\Rightarrow$ B	B if A
if B then A	A $\Leftarrow$ B	A if B
A if and only if B	A $\Leftrightarrow$ B	A iff B

3.2 Contradiction

Most of the proofs we have seen so far are direct. Look for example at Lemma 2.16. Here we prove that if s, t and u are integers and $s = tq + u$, for some $q \in \mathbb{Z}$, then $\gcd(s, t) = \gcd(t, u)$. The proof starts with the assumption that $s = tq + u$ and makes deductions until the required result is reached. Here is a mathematical example of the second kind of, indirect, argument.

Example 3.11. Show that $x^2 = -1$ has no real solution.

Step(1) **Assume the opposite of what is to be proved.** Let us suppose that there is a real number r such that $r^2 = -1$ and see where this leads us.

Step(2) **Derive some consequences of the assumption.** As $r \in \mathbb{R}$ we have $0 \leq r^2$.

Step(3) **Show that something we've derived is false.** Combining the fact above with the assumption that $r^2 = -1$ we obtain $0 \leq -1$, which is clearly false.

Step(4) **Conclude that the assumption is false and so prove the required result.** The false statement in Step(3) was a direct consequence of the assumption that a solution $x = r$ to $x^2 = -1$ exists. We are forced to conclude that there is no such solution.

This is a technique of argument known as **contradiction**. We start by assuming that whatever we wish to prove is false. This assumption is then used to make deductions. We hope that these deductions lead to something which we know is false: that is to a contradiction. We conclude that our assumption is wrong so what we want to prove is true.

3.3 Examples: proof by contradiction

The proof that $q > 0$ in the proof of Lemma 2.18.3 is a proof by contradiction.

Theorem 3.12. *There are no natural numbers x and y such that $x^2 - 2y^2 = 0$.*

Proof.

$\square$

We can use this to prove something that may seem more familiar, namely that $\sqrt{2}$ is not a rational number. As this follows easily from the Theorem we call it a Corollary. (*A corollary is a consequence of another result which is (usually) easy to prove given the other result.*) Again we use proof by contradiction.

Corollary 3.13. *There is no rational number r such that $r^2 = 2$. That is $\sqrt{2} \notin \mathbb{Q}$.*

Proof.

Step(1) Suppose that there is a rational number r such that $r^2 = 2$.

Step(2) As $r \in \mathbb{Q}$ we have $r = p/q$, where $p, q \in \mathbb{Z}$ and $q \neq 0$. We have

$$\begin{aligned} & \left(\frac{p}{q}\right)^2 = 2 \\ \Rightarrow \quad & \frac{p^2}{q^2} = 2 \\ \Rightarrow \quad & p^2 = 2q^2, \text{ as } q \neq 0, \\ \Rightarrow \quad & |p|^2 = 2|q|^2 \\ \Rightarrow \quad & |p|^2 - 2|q|^2 = 0. \end{aligned}$$

The introduction of $|\cdot|$ is justified because $(-x)^2 = x^2 = |x|^2$, for all $x \in \mathbb{R}$.

Step(3) As $r^2 = 2$ it cannot be the case that $p = 0$, because then we'd have $2 = 0$. Thus p and q are non–zero. Therefore $|p|$ and $|q|$ are natural numbers and we have deduced, in Step(2), a contradiction to Theorem 3.12. It follows that there is no such rational number r.

Note that $\sqrt{2}$ by definition has square equal to 2: so we've shown it can't be in $\mathbb{Q}$. $\square$

3.4 Objectives

After covering this chapter of the course you should be able to:

(i) recognise and use the symbols $\exists$, $\forall$, $\Rightarrow$, $\Leftarrow$ and $\Leftrightarrow$;

(ii) apply appropriate arguments to show whether or not statements of the form
"$\exists$ ...",
"$\forall$ ..."
"if ... then ... "
and
"... if and only if ..."
are true.

(iii) explain what a *Corollary* is;

(iv) understand and use proof by contradiction.

3.5 Exercises

3.1 TRUE or FALSE?

(a) If $x > 10$ then $2x > 15$.
(b) If $n \in \mathbb{N}$ then $n+1 \in \mathbb{N}$.
(c) $\exists n \in \mathbb{N}$ such that $n+1 \notin \mathbb{N}$.
(d) $\exists n \in \mathbb{N}$ such that $n-1 \notin \mathbb{N}$.
(e) $n+1 \in \mathbb{N}, \forall n \in \mathbb{N}$.
(f) $n-1 \notin \mathbb{N}, \forall n \in \mathbb{N}$.
(g) $\forall x \in \mathbb{R}, x > 0 \Rightarrow 1/x > 0$.
(h) $\exists x \in \mathbb{R}, x^2 = 4$.
(i) $\exists x \in \mathbb{R}, x^2 = -1$.

3.2 Disprove the following by finding a counterexample.

(a) If $x^2 > 16$ then $x > 4$.
(b) $\forall m \in \mathbb{N}$, $\exists n \in \mathbb{N}$ such that $n+1 = m$.
(c) $\forall m \in \mathbb{Z}$, $\exists n \in \mathbb{Z}$ such that $mn = 1$.
(d) $\forall m \in \mathbb{Q}$, $\exists n \in \mathbb{Q}$ such that $mn = 1$.
(e) For all real numbers $x \geq 1$, there is a real number $\delta > 0$ such that $x - \delta \geq 1$.

3.3 A lecturer rashly claims that:

(a) if $a|b$ and $c|d$ then $(a+c)|(b+d)$ and
(b) if $ac|bc$ then $a|b$.

Give counter–examples to show that these beliefs are ill–founded.

3.4 Disprove the following assertions. Use Questions 2.3 and 3.8 – that is assume that the results of these questions have been established – but indicate where you use them. You should also indicate where you use the Division Algorithm (if you do).

(a) $\exists n \in \mathbb{Z}$ such that $3 \nmid n(n+1)(n+2)$.
(b) $\exists n \in \mathbb{Z}$ such that $3 \nmid n(2n^2+7)$.
(c) $\exists n \in \mathbb{Z}$ such that n^2 has the form $3k+2$, for some integer k.
(d) $\exists n \in \mathbb{Z}$ such that n^3 has the form $9k+2$, for some integer k.

3.5 Are the statements below true or false? Write down the converse of each. Is the converse true or false?

(a) If $a^2 - b^2 = 0$ then $a = b = 0$.
(b) If $a \neq 0$ then $2a \neq 0$.
(c) If $a = b$ then $a^2 = (-b)^2$.
(d) If $a^2 = 1$ then $a = -1$.

3.6 What, if anything, is wrong with the following.

(a) If I am a dog then I have a nose. I have a nose. Therefore I am a dog.

(b) If you are not a reptile then you are not an alligator. I am an alligator so I am also a reptile.
(c) If you are not a fish then you cannot be a haddock. I am a fish so I must be a haddock.

3.7 Prove each statement below using only the definition of division (and basic laws of arithmetic). Point out where in your proof you use the definition of division. Let a, b, c, d be integers. The following hold.

(a) $a|a^2$.
(b) If $a|b$ then $a|bc$ and $ac|bc$.
(c) If $a|b$ and $c|d$ then $ac|bd$.
(d) If $0|a$ then $a = 0$.
(e) $a|1$ if and only if $a = \pm 1$. [**Hint**: Consider cases $a > 0$ and $a < 0$ separately. If $a > 0$ use the previous part of the question. If $a < 0$ apply the result for $a > 0$ to $-a$. Can $a = 0$?]
(f) If $a|b$ and $b|a$ then $b = \pm a$.

3.8 Use the Division Algorithm and Question 3.7 to prove that for an arbitrary integer a

(a) $2|a(a+1)$;
(b) $3|a(a+1)(a+2)$;
(c) $3|a(2a^2+7)$;
(d) if a is odd then $32|(a^2+3)(a^2+7)$.

In each case indicate where the Division Algorithm and results of Question 3.7 are used and how.

3.9 Show that there do not exist integers x, y such that $x^2 - 4y = 3$. [**Hint:** first prove that there are no such numbers with x even, then that there no such with x odd.]

3.10 Show that there is no pair of natural numbers x, y such that $x^2 - 3y^2 = 0$. Use this to show that there is no rational number r such that $r^2 = 3$.

3.11 Show that there is no pair of natural numbers x, y such that $x^2 - 5y^2 = 0$. Use this to show that there is no rational number r such that $r^2 = 5$.

Chapter 4

Proof by Induction

4.1 Induction

Some properties of sets and numbers are so obvious that we treat them as natural laws which do not require proof. We call such a property an *axiom*. For instance all the properties of numbers listed at the beginning of Section 2.2 are axioms for numbers. The method of proof by induction is based on the following property which is really an axiom for the natural numbers $\mathbb{N}$.

The Principle of proof by induction

Assume that $P(n)$ is a statement, for all $n \in \mathbb{N}$. Assume further that it can be shown that

(1) $P(1)$ is true and

(2) if $P(k)$ is true then $P(k+1)$ is true, for $k \geq 1$.

Then $P(n)$ is true for all $n \in \mathbb{N}$.

In the following example we use "sigma" notation for sums, that is we define

$$\sum_{j=1}^{n} a_j = a_1 + \cdots + a_n.$$

Example 4.1. Suppose that we wish to prove that

$$\sum_{j=1}^{n} \frac{1}{j(j+1)} = 1 - \frac{1}{n+1}, \text{ for all } n \in \mathbb{N}.$$

Here $P(n)$ is the statement

$$\sum_{j=1}^{n} \frac{1}{j(j+1)} = 1 - \frac{1}{n+1},$$

and we wish to prove $P(1), P(2), P(3), \ldots$.

Proof by induction takes the following form.

Example 4.2 (Bernoulli's Inequality). Prove that

$$(1+x)^n \geq 1+nx, \text{ for all } n \in \mathbb{N} \text{ and for all } x \in \mathbb{R}, x > 0.$$

Example 4.3 (Summing a geometric progression). Prove that

$$\sum_{j=0}^{n-1} ar^j = \frac{a(r^n-1)}{r-1}, \text{ for all } a \in \mathbb{R} \text{ and } r \in \mathbb{R}, r \neq 1, \text{ and for all } n \in \mathbb{N}.$$

Example 4.4 (Special cases of summing geometric progressions).

(1) $a = 1$, $r = x$ ($\neq 1$):

From Example 4.3
$$1 + x + x^2 + \cdots + x^{n-1} = \frac{x^n - 1}{x - 1}.$$
Multiplying through by $x - 1$ gives
$$(1 + x + x^2 + \cdots + x^{n-1})(x - 1) = x^n - 1.$$

If we defined division for polynomials as we've done for integers, in Definition 2.5, we could say that this shows that
$$(x - 1)|(x^n - 1)$$
and that
$$(1 + x + x^2 + \cdots + x^{n-1})|(x^n - 1).$$
For example
$$(1 + x)(x - 1) = x^2 - 1,$$
$$(1 + x + x^2)(x - 1) = x^3 - 1,$$
$$(1 + x + x^2 + x^3)(x - 1) = x^4 - 1.$$

(2) $a = 1$, $r = -x$ ($x \neq -1$), $n = 2m + 1$, $m \in \mathbb{N}$:

The lefthand side of the equality of Example 4.3 becomes
$$\begin{aligned}\sum_{j=0}^{2m} ar^j &= \sum_{j=0}^{2m} (-x)^j \\ &= 1 - x + x^2 - \cdots + (-1)^{2m}x^{2m} \\ &= 1 - x + x^2 - \cdots + x^{2m}.\end{aligned}$$
The righthand side is
$$\begin{aligned}\frac{a(r^n - 1)}{r - 1} &= \frac{(-x)^{2m+1} - 1}{-x - 1} \\ &= \frac{x^{2m+1} + 1}{x + 1}.\end{aligned}$$
From Example 4.3
$$1 - x + x^2 - \cdots + x^{2m} = \frac{x^{2m+1} + 1}{x + 1}.$$
Multiplying by $x + 1$ gives
$$(1 - x + x^2 - \cdots + x^{2m})(x + 1) = x^{2m+1} + 1.$$
For example
$$(1 - x + x^2)(x + 1) = x^3 + 1,$$
$$(1 - x + x^2 - x^3 + x^4)(x + 1) = x^5 + 1,$$
$$(1 - x + x^2 - x^3 + x^4 - x^5 + x^6)(x + 1) = x^7 + 1.$$
We can say
$$(x + 1)|(x^{2m+1} + 1)$$
and
$$(1 - x + x^2 - \cdots + x^{2m})|(x^{2m+1} + 1).$$

4.2 Change of basis

It is sometimes useful to be able to start the induction at some point other than $n = 1$. In this case we use the following alternative statement of the Principle of Induction.

Let $s \in \mathbb{Z}$. Assume that $P(n)$ is a statement, for all $n \geq s$. Assume further that it can be shown that

(1′) $P(s)$ is true and

(2′) if $P(k)$ is true then $P(k + 1)$ is true, for $k \geq s$.

Then $P(n)$ is true for all $n \geq s$.

Example 4.5. Show that $2^n > n^3$, for all $n \geq 10$.

Note that $2^9 = 512 < 729 = 9^3$, so the result does not hold when $n = 9$.

4.3 Pascal's triangle and Fibonacci numbers

The **binomial coefficient** or **choice number** $\binom{n}{k}$ is given by the formula

$$\binom{n}{k} = \frac{n!}{(n-k)!k!},$$

for non-negative integers n and k, with $0 \le k \le n$. We define $0! = 1$ so that $\binom{n}{0} = \binom{n}{n} = 1$, for all n. As you can verify

$$\binom{n}{k} = \binom{n-1}{k} + \binom{n-1}{k-1}.$$

We can use this fact to generate binomial coefficients, as follows. Start with $\binom{0}{0}$ and write out succesive rows starting with $1 = \binom{n}{0}$ and ending with $\binom{n}{n} = 1$. Fill the rows making the kth entry on the nth row the sum of the $(k-1)$th and kth entries from the row above.

$$\begin{array}{ccccccccccccc}
 & & & & & & \binom{0}{0} & & & & & & \\
 & & & & & \swarrow & & \searrow & & & & & \\
 & & & & \binom{1}{0} & & & & \binom{1}{1} & & & & \\
 & & & \swarrow & & \searrow & & \swarrow & & \searrow & & & \\
 & & \binom{2}{0} & & & & \binom{2}{1} & & & & \binom{2}{2} & & \\
 & \swarrow & & \searrow & & \swarrow & & \searrow & & \swarrow & & \searrow & \\
\binom{3}{0} & & & & \binom{3}{1} & & & & \binom{3}{2} & & & & \binom{3}{3}
\end{array}$$

Then the $(n+1)$st row will contain the binomial coefficients $\binom{n}{k}$, for $k = 0, \dots, n$. This array is known as **Pascal's triangle** and is more familiar as

$$\begin{array}{ccccccccccccc}
 & & & & & & 1 & & & & & & \\
 & & & & & \swarrow & & \searrow & & & & & \\
 & & & & 1 & & & & 1 & & & & \\
 & & & \swarrow & & \searrow & & \swarrow & & \searrow & & & \\
 & & 1 & & & & 2 & & & & 1 & & \\
 & \swarrow & & \searrow & & \swarrow & & \searrow & & \swarrow & & \searrow & \\
1 & & & & 3 & & & & 3 & & & & 1
\end{array}$$

Write out Pascal's triangle with the left hand "1"s aligned in a column, as follows.

$$\begin{array}{cccccccc}
1 \\
1 & 1 \\
1 & 2 & 1 \\
1 & 3 & 3 & 1 \\
1 & 4 & 6 & 4 & 1 \\
1 & 5 & 10 & 10 & 5 & 1 \\
1 & 6 & 15 & 20 & 15 & 6 & 1 \\
1 & 7 & 21 & 35 & 35 & 21 & 7 & 1
\end{array}$$

Now add numbers on the diagonals running from lower left to upper right:

$$\begin{aligned}
&1\\
&1\\
1+1 &= 2\\
1+2 &= 3\\
1+3+1 &= 5\\
1+4+3 &= 8\\
1+5+6+1 &= 13\\
1+6+10+4 &= 21.
\end{aligned}$$

These are the first 8 of the **Fibonacci** numbers, which are generated by the rules

$$\begin{aligned}
f_1 &= 1\\
f_2 &= 1\\
f_{n+1} &= f_n + f_{n-1}, \text{ for } n \ge 2.
\end{aligned}$$

Thus the Fibonacci numbers are

$$1, 1, 2, 3, 5, 8, 13, 21, 34, 55, 89, 144, 233, 377, 610, \dots$$

Do the diagonals of Pascal's triangle sum to the Fibonacci numbers after the first 8? They do because each entry on a diagonal is the sum of one number from the diagonal one row above it and a second number from the diagonal two rows above it. Thus each diagonal is the sum of the two diagonals above it: as on the following diagram.

We could write out an algebraic proof based on the idea above using induction.

Example 4.6. Consider the following.

$$\begin{aligned}
f_2 &= 1\\
f_3 &= 2\\
f_4 &= 3\\
f_2 + f_4 &= 4\\
f_5 &= 5\\
f_2 + f_5 &= 6\\
f_3 + f_5 &= 7\\
f_4 + f_5 &= 8\\
f_2 + f_5 + f_9 &= 1 + 5 + 34 = 40\\
f_3 + f_7 + f_{10} &= 2 + 13 + 55 = 70.
\end{aligned}$$

Each of these numbers has been written as a sum of different Fibonacci numbers (no Fibonacci number appears twice in any sum). We'll prove by induction that any natural number can be written as a sum of different Fibonacci numbers.

Example 4.7. If we take every third Fibonacci number we obtain a new sequence of numbers,

$$f_3, f_6, f_9, f_{12}, \ldots$$

with values

$$2, 8, 34, 144, 610, 2584, 10946, 46368, 196418, \ldots$$

We shall prove, by induction that f_{3n} is even, for all $n \geq 1$.

Example 4.8 (The binomial theorem). *This example is not examinable*

$$(x+y)^n = \sum_{k=0}^{n} \binom{n}{k} x^{n-k} y^k, \text{ for all } n \in \mathbb{N} \text{ and all } x, y \in \mathbb{R}.$$

We shall prove this by induction.

Basis: $P(1)$ is

$$(x+y) = \sum_{k=0}^{1} \binom{1}{k} x^{1-k} y^k$$

and, as

$$\sum_{k=0}^{1}\binom{1}{k}x^{1-k}y^k=\binom{1}{0}x+\binom{1}{1}y=x+y,$$

$P(1)$ holds, for all $x,y\in\mathbb{R}$.

Inductive Hypothesis: Assume $P(k)$ holds for some $m\geq 1$. That is

$$(x+y)^m=\sum_{k=0}^{m}\binom{m}{k}x^{m-k}y^k,\ \text{for all } x,y\in\mathbb{R}.$$

Inductive Step: Given the inductive hypothesis we wish to show that $P(m+1)$ holds. That is

$$(x+y)^{m+1}=\sum_{k=0}^{m+1}\binom{m+1}{k}x^{m+1-k}y^k,\ \text{for all } x,y\in\mathbb{R}.$$

We have

$$\begin{aligned}(x+y)^{m+1}&=(x+y)^m(x+y)\\&=\left[\sum_{k=0}^{m}\binom{m}{k}x^{m-k}y^k\right](x+y),\ \text{using the inductive hypothesis,}\\&=\left[\sum_{k=0}^{m}\binom{m}{k}x^{m+1-k}y^k\right]+\left[\sum_{k=0}^{m}\binom{m}{k}x^{m-k}y^{k+1}\right].\end{aligned}$$

Now setting $s=k+1$ we can write

$$\binom{m}{k}x^{m-k}y^{k+1}=\binom{m}{s-1}x^{m+1-s}y^s,$$

for $k=0,\ldots m$. Therefore

$$\sum_{k=0}^{m}\binom{m}{k}x^{m-k}y^{k+1}=\sum_{s=1}^{m+1}\binom{m}{s-1}x^{m+1-s}y^s=\sum_{k=1}^{m+1}\binom{m}{k-1}x^{m+1-k}y^k.$$

Hence

$$\begin{aligned}(x+y)^{m+1}&=\left[\sum_{k=0}^{m}\binom{m}{k}x^{m+1-k}y^k\right]+\left[\sum_{k=1}^{m+1}\binom{m}{k-1}x^{m+1-k}y^k\right]\\&=\binom{m}{0}x^{m+1}+\sum_{k=1}^{m}\left[\binom{m}{k}+\binom{m}{k-1}\right]x^{m+1-k}y^k+\binom{m}{m}y^{m+1}.\end{aligned}$$

We have

$$\binom{m}{0}=\binom{m}{m}=\binom{m+1}{0}=\binom{m+1}{m+1}=1$$

and, for $1\leq k\leq m$,

$$\begin{aligned}\binom{m}{k}+\binom{m}{k-1}&=\frac{m!}{k!(m-k)!}+\frac{m!}{(k-1)!(m+1-k)!}\\&=\frac{m!(m+1-k)+m!k}{k!(m-k)!(m+1-k)}\\&=\frac{m!(m+1)}{k!(m+1-k)!}\\&=\frac{(m+1)!}{k!(m+1-k)!}\\&=\binom{m+1}{k}.\end{aligned}$$

Thus

$$\begin{aligned}(x+y)^{m+1}&=\binom{m+1}{0}x^{m+1}+\sum_{k=1}^{m}\binom{m+1}{k}x^{m+1-k}y^k+\binom{m+1}{m+1}y^{m+1}\\&=\sum_{k=0}^{m+1}\binom{m+1}{k}x^{m+1-k}y^k.\end{aligned}$$

That is, $P(m+1)$ holds.

Conclusion: Therefore, by induction, $P(n)$ holds for all $n\in\mathbb{N}$.

4.4 Objectives

After covering this chapter of the course you should be able to:

(i) understand the principle of proof by induction;

(ii) carry out proof by induction, both starting with the integer 1 and starting with an integer other than 1;

(iii) remember the definition of binomial coefficients;

(iv) remember the definition of the Fibonacci numbers.

4.5 Exercises

4.1 A infinite sequence $x_1, x_2, x_3, \ldots$ of integers is defined by the rules $x_1 = 2$ and $x_{n+1} = x_n + 2(n+1)$, for all $n \geq 1$. Show by induction that $x_n = n(n+1)$, for all $n \in \mathbb{N}$.

4.2 Prove that $n! > 2^n$ for all $n \in \mathbb{N}$ with $n \geq 4$.

4.3 Prove by induction that:

$$(1+x)^n \geq 1 + nx + \frac{1}{2}n(n-1)x^2,$$

for all $n \in \mathbb{N}$ and $x \in \mathbb{R}, x \geq 0$.

4.4 Prove by induction that:

$$\sum_{k=1}^{n} k^3 = \left[\frac{1}{2}n(n+1)\right]^2$$

for all $n \in \mathbb{N}$.

4.5 Prove by induction that:

$$\sum_{k=1}^{n} k(k+1) = \frac{1}{3}n(n+1)(n+2)$$

for all $n \in \mathbb{N}$.

4.6 Prove by induction that:

$$\sum_{k=1}^{n} k(k+1)\ldots(k+a) = \frac{1}{(a+2)}n(n+1)(n+2)\ldots(n+a+1)$$

for all $n \in \mathbb{N}$ and all $a \in \mathbb{N}$.

4.7 Use proof by induction to show that each of the following hold, for all $n \geq 1$.

(a) $8|5^{2n} + 7$; [**Hint:** $5^{2(k+1)} + 7 = 5^2(5^{2k} + 7) + (7 - 5^2 \cdot 7)$]

(b) $15|2^{4n} - 1$;

(c) $5|3^{3n+1} + 2^{n+1}$;

(d) $21|4^{n+1} + 5^{2n-1}$;

(e) $24|2 \cdot 7^n + 3 \cdot 5^n - 5$.

4.8 *Geography made simple.* What is wrong with the following "proof by induction" of the fact that all British towns have the same name. Prove, by induction, that any collection of n towns have the same name. This is true when $n = 1$. Assume the truth of the statement for any collection of k towns, where $k \geq 1$. Now take a collection of $k+1$ towns. Exclude 1 town from the collection to leave a collection of k towns, which by the inductive hypothesis, all have the same name. Now take the $k+1$ towns and exclude a different one. The remaining k towns all have the same name and this time include the one that was left out before. Therefore all $k+1$ towns have the same name and the statement holds for all $n \geq 1$.

4.9 Prove the following.

(a) Every 4th Fibonacci number is divisible by 3, that is $3|f_{4n}$, for all $n \geq 1$.

(b) Every 5th Fibonacci number is divisible by 5, that is $5|f_{5n}$, for all $n \geq 1$.

4.10 In Maple type the command

```
with(combinat, fibonacci);
```

Now Maple will return the nth Fibonacci number in response to the command

```
fibonacci(n);
```

We can write a loop to generate and print Fibonacci numbers:

```
for i from 1 to 20 do
print("f",i,"=",fibonacci(i));
od;
```

The output can be restricted to every 6th Fibonacci number and then divided by 4:

```
for i from 1 to 20 do
print("f",6*i,"=",fibonacci(6*i), "and ", fibonacci(6*i)/4);
od;
```

What does this suggest? Can you prove it? Try to some other numbers to see if you can detect nth Fibonacci numbers which they divide.

Chapter 5

Primes and Coprimes

A central concept of number theory is that of the prime number which is introduced in this chapter. These numbers form the basic building blocks out of which the integers are formed and into which they can be decomposed. We shall barely scratch the surface of the theory of prime numbers here. We shall establish the Fundamental Theorem of Arithmetic, which shows that every integer factors uniquely as a product of primes, and we shall see that there are infinitely many primes. We begin by considering a property of pairs of integers.

5.1 Greatest common divisors again

First we establish a few more properties of the greatest common divisor. Recall that whenever we ran the Euclidean Algorithm, on natural numbers a and b, we obtained not only $\gcd(a, b)$ but also integers u and v such that

$$\gcd(a, b) = au + bv,$$

and from this fact we obtained Theorem 2.21. We'll now give an alternative proof of this Theorem.

Second proof of Theorem 2.21

Suppose that we have positive integers a and b. (The cases where a or b are non-positive follow easily from this case, and are left to the reader.) This proof depends on analysis of the set

$$S = \{ak + bl \in \mathbb{Z} : ak + bl > 0 \text{ and } k, l \in \mathbb{Z}\}.$$

This is clearly a set of positive integers. We shall prove the theorem by showing that it's smallest element is $\gcd(a, b)$. First of all we need to show that it does have a smallest element. It is a fundamental property of numbers that every non-empty set of positive integers has a smallest element. Then, as S contains only positive integers it must have a smallest element unless it's empty. It's easy to see S is non-empty as it contains, for example $a + b$. Therefore S has a smallest element, s say. The fact that $s \in S$ means

$$s = ak + bl, \text{ for some } k, l \in \mathbb{Z}. \tag{5.1}$$

Now, using the Division Algorithm, we can write

$$a = sq + r, \text{ where } 0 \le r < s.$$

Substituting for s using (5.1) this becomes

$$\begin{aligned} a &= (ak + bl)q + r \\ &= a(kq) + b(lq) + r, \end{aligned}$$

so

$$r = a(1 - kq) + b(-lq), \text{ with } 0 \le r < s.$$

If $r \ne 0$ then we have $r \in S$ and $r < s$, a contradiction. Therefore $r = 0$ and $a = sq$. That is, $s|a$. Similarly $s|b$.

Now suppose that $c|a$ and $c|b$. Then $a = cu$ and $b = cv$, for some $u, v \in \mathbb{Z}$. Substitution in (5.1) gives

$$s = c(uk) + c(vl) = c(uk + vl).$$

Therefore $c|s$ and from Lemma 2.18.3 we have $c \le s$. This completes the proof that $s = \gcd(a, b)$ and we've already found k, l such that $s = ak + bl$, so Theorem 2.21 follows.

5.2 Coprimes and Euclid's Lemma

Pairs of integers have greatest common divisor 1 have particularly nice properties and it's useful to have a name for them.

Definition 5.1. If a and b are integers with $\gcd(a, b) = 1$ then we say that a and b are **coprime**.

Example 5.2. It is easy to see that 6 and 35 are coprime, for example. Now from Theorem 2.21 it follows that there are integers u and v such that $6u + 35v = 1$. For instance we may set $u = 6$ and $v = -1$. (There are other possibilities: see the exercises.)

On the other hand suppose that for some integers a and b we happen to know that, say, $5a - 2b = 1$. Does this mean that $\gcd(a, b) = 1$?

Corollary 5.3. *Integers a and b are coprime if and only if there exist integers u and v such that $au + bv = 1$.*

Proof. This is an if and only if proof so has two halves.

Step(1) Prove that if a and b are coprime then there exist integers u and v such that $au+bv=1$. If a and b are coprime then it follows directly from Theorem 2.21 that such u and v exist.

Step(2) Prove that if there exist integers u and v such that $au+bv=1$ then $\gcd(a,b)=1$. Assume that there are integers u and v such that $au+bv=1$. Let $d=\gcd(a,b)$. Then $d|a$ and $d|b$ so $d|(au+bv)$:

Therefore $d|1$. As $d>0$ (why?) it follows, that $d \leq 1$:

Thus $d=1$, so a and b are coprime, as required.

□

Corollary 5.3 allows us to prove a result known as Euclid's Lemma.

Lemma 5.4 (Euclid's Lemma). *Let a, b and c be integers with $\gcd(a,b)=1$. If $a|bc$ then $a|c$.*

Proof.

□

5.3 Application to solving equations

We've already seen (Lemma 2.24) that a linear Diophantine equation, that is an equation of the form $ax+by=c$, where a,b and c are integers, has integer solution x and y if and only if $c|\gcd(a,b)$. We can now use Euclid's lemma to find all solutions to such equations.

Theorem 5.5. *Let a,b,c be integers and let $d=\gcd(a,b)$. The equation*

$$ax+by=c \tag{5.2}$$

has an integer solution if and only if $d|c$. If $d|c$ then equation (5.2) has infinitely many solutions and if $x=u_0$, $y=v_0$ is one solution then $x=u_1$, $y=v_1$ is a solution if and only if

$$u_1=u_0+(b/d)t \text{ and } v_1=v_0-(a/d)t, \text{ for some } t\in\mathbb{Z}.$$

Proof.

□

Example 5.6. In Example 2.22 we saw that $\gcd(2600, 2028) = 52$ and that the equation $2600x + 2028y = 104$ has a solution $x = -14, y = 18$. As $2600/52 = 50$ and $2028/52 = 39$ the solutions to this equation are

$$x = -14 + 39t, y = 18 - 50t, \text{ for } t \in \mathbb{Z}.$$

For each integer t we have a solution, some of which are shown below.

t	x	y
-2	-92	-118
-1	-53	68
0	-14	18
1	25	-32
2	64	-82

5.4 Prime Numbers

It follows from the definition of division that every integer n is divisible by ± 1 and by $\pm n$. Amongst the positive integers a special case is the integer 1 which has only one positive divisor, namely 1. All other positive integers n have at least 2 positive divisors, 1 and n, and may have more.

Definition 5.7. A positive integer $p > 1$ is called a **prime** if the only positive divisors of p are 1 and p. An integer which is not prime is called **composite**.

For example $2, 5, 7, 11, 13, 17$ and 19 are prime whilst the first few composite integers are:

4	which is divisible by	2
6	which is divisible by	2 and 3
8	which is divisible by	2 and 4
9	which is divisible by	3
10	which is divisible by	2 and 5.

A fundamental property of prime numbers is the following.

Theorem 5.8 (The prime divisor property). *If p is a prime and $p|ab$ then $p|a$ or $p|b$.*

Proof. If $p|a$ then we have nothing to prove. If $p \nmid a$ then the common divisors of a and p are ± 1 (since the only divisors of p are ± 1 and $\pm p$). Hence $\gcd(a, p) = 1$. From Lemma 5.4 (Euclid's Lemma) it follows that $p|b$, as required. ☐

Example 5.9. If $3|bc$ then either $3|b$ or $3|c$. The same goes for 29: if $29|bc$ then $29|b$ or $29|c$. This does not hold for all integers. For instance $6|24$ and $24 = 8 \cdot 3$, so $6|8 \cdot 3$ but $6 \nmid 8$ and $6 \nmid 3$. Once we've discussed prime factorisation it will be easy to see why this property doesn't hold for any composite integers.

The Theorem above can easily be extended to products of more than 2 integers. For example, if $3|abc$ then, from the Theorem either $3|ab$ or $3|c$. If $3|ab$ then, from the Theorem again, $3|a$ or $3|b$. Therefore, if $3|abc$ then $3|a$ or $3|b$ or $3|c$.

Corollary 5.10. *If p is prime and $p|a_1 \cdots a_n$ then $p|a_i$, for some i.*

Proof. The proof is by induction on n, starting with $n = 2$.

Basis: $P(2)$ follows from Theorem 5.8.

Inductive Hypothesis: If $n \geq 2$ and $p|a_1 \cdots a_n$ then $p|a_i$, for some i.

Inductive Step: Suppose that $p|a_1 \cdots a_{n+1}$. Let

$$a = a_1 \cdots a_n \text{ and } b = a_{n+1}.$$

Then $p|ab$ so, from Theorem 5.8, $p|a$ or $p|b$. If $p|a$ the inductive hypothesis implies that $p|a_i$, for some i with $1 \leq i \leq n$. If $p|b$ then $p|a_{n+1}$. Hence $p|a_i$, for some i, as required. ☐

5.5 Prime Factorisation

We now come to the main result of this chapter: the Fundamental Theorem of Arithmetic. It may seem that this theorem does not say anything very much or that what it does say is obvious. However there are number systems in which the theorem does not hold: examples are left to the exercises. During the nineteenth century there were attempts to prove Fermat's last theorem using so called "algebraic" number systems. It escaped the attention of mathematicians for some time that these proofs were incorrect precisely because of the failure of the Fundamental Theorem of Arithmetic in the algebraic number systems concerned.

An expression of an integer n as a product of primes is called a **prime factorisation** of n. For example 12 and 25 have prime factorisations $12 = 2 \cdot 2 \cdot 3$ and $25 = 5 \cdot 5$, respectively. We aim to show that every positive integer greater than one has a prime factorisation and that this prime factorisation is unique, up to the order in which the prime factors occur. For instance

$$\begin{gathered} 2 \cdot 5 \cdot 2 \cdot 7, \\ 2 \cdot 7 \cdot 2 \cdot 5, \\ 7 \cdot 2 \cdot 2 \cdot 5 \end{gathered}$$

are all prime factorisations of 140 but are regarded as the same because the number of 2's, 5's and 7's is the same in each.

Example 5.11. It's easy enough to see that 7 cannot be written as a product of primes other than by writing it as ... well ... 7. What about a larger prime like 6991 say? Can I write this as a product of primes: other than the length one product 6991?

By listing all possible factorisations it's easy to see that small integers have unique prime factorisation. In the proof of the next theorem we'll show that this is true for all integers $n > 1$.

Theorem 5.12 (The Fundamental Theorem of Arithmetic). *Every integer $n > 1$ is a product of one or more primes. This product is unique apart from the order in which the primes occur.*

Proof. Step(1) Prove that every $n > 1$ has a prime factorisation.

Step(2) Prove that prime factorisations are unique.

$\square$

It is often convenient to write the prime factorisation of an integer with all like primes collected together, in ascending order, and with exponential notation. For example we could write the prime factorisations of 140 and 2200 as

$$140 = 2^2 \cdot 5 \cdot 7 \text{ and}$$
$$2200 = 2^3 \cdot 5^2 \cdot 11.$$

We call this the **collected prime factorisation** of an integer n or say that we've written n in **standard form**. From the Fundamental Theorem of Arithmetic it follows that collected prime factorisations are unique. We record this fact in the following corollary.

Corollary 5.13. *Let $n > 1$ be an integer. Then n may be written uniquely as*

$$n = p_1^{a_1} \cdots p_k^{a_k},$$

where $k \geq 1$, $p_1 < \cdots < p_k$, p_i is prime and $a_i \geq 1$.

Example 5.14. It is easy to multiply together integers in standard form: we just add corresponding superscripts. For example $3388 = 2^2 \cdot 7 \cdot 11^2$ and $2200 = 2^3 \cdot 5^2 \cdot 11$ so $3388 \cdot 2200 = 2^5 \cdot 5^2 \cdot 7 \cdot 11^3$. In general if integers a and b have standard forms

$$a = p_1^{\alpha_1} \cdots p_n^{\alpha_n} \text{ and}$$
$$b = p_1^{\beta_1} \cdots p_n^{\beta_n}$$

then ab has standard form

$$ab = p_1^{\alpha_1+\beta_1} \cdots p_n^{\alpha_n+\beta_n}.$$

Here we've padded out the collected prime factorisations (with p_i^0 where necessary) to make them the same length: as in the following example.

$$2200 = 2^3 \cdot 5^2 \cdot 11 = 2^3 \cdot 5^2 \cdot 7^0 \cdot 11^1 \cdot 13^0 \text{ and}$$
$$572572 = 2^2 \cdot 7 \cdot 11^2 \cdot 13^2 = 2^2 \cdot 5^0 \cdot 7^1 \cdot 11^2 \cdot 13^2$$

so

$$2200 \cdot 572572 = 2^5 \cdot 5^2 \cdot 7^1 \cdot 11^3 \cdot 13^2.$$

Example 5.15. Reversing the idea of the previous example, it's easy to find the divisors of an integer given in standard form. For instance if $a|3388$ then

$$3388 = 2^2 \cdot 7 \cdot 11^2 = ab,$$

for some integer b.

Example 5.16. As 2200 has standard form $2^3 \cdot 5^2 \cdot 11$ the positive divisor of 2200 are of the form $2^a 5^b 11^c$, where $0 \le a \le 3$, $0 \le b \le 2$ and $0 \le c \le 1$. First list all such triples (a, b, c):

$$\begin{array}{cccccc}
(0,0,0) & (0,0,1) & (0,1,0) & (0,1,1) & (0,2,0) & (0,2,1) \\
(1,0,0) & (1,0,1) & (1,1,0) & (1,1,1) & (1,2,0) & (1,2,1) \\
(2,0,0) & (2,0,1) & (2,1,0) & (2,1,1) & (2,2,0) & (2,2,1) \\
(3,0,0) & (3,0,1) & (3,1,0) & (3,1,1) & (3,2,0) & (3,2,1)
\end{array}$$

The positive divisors of 2200 are therefore:

$$\begin{array}{cccccc}
1 & 11 & 5 & 5 \cdot 11 & 5^2 & 5^2 \cdot 11 \\
2 & 2 \cdot 11 & 2 \cdot 5 & 2 \cdot 5 \cdot 11 & 2 \cdot 5^2 & 2 \cdot 5^2 \cdot 11 \\
2^2 & 2^2 \cdot 11 & 2^2 \cdot 5 & 2^2 \cdot 5 \cdot 11 & 2^2 \cdot 5^2 & 2^2 \cdot 5^2 \cdot 11 \\
2^3 & 2^3 \cdot 11 & 2^3 \cdot 5 & 2^3 \cdot 5 \cdot 11 & 2^3 \cdot 5^2 & 2^3 \cdot 5^2 \cdot 11
\end{array}$$

Example 5.17. If two numbers are expressed in standard form its easy to find their greatest common divisor. The standard form of 572572 is $2^2 \cdot 7 \cdot 11^2 \cdot 13^2$ so any divisor of 572572 has the form $2^e 7^f 11^g 13^h$, with $0 \le e \le 2$, $0 \le f \le 1$, $0 \le g \le 2$ and $0 \le h \le 2$. Hence common divisors of 2200 and 572572 have the form $2^u 11^v$, with $0 \le u \le 2$ and $0 \le v \le 1$. Therefore $\gcd(2200, 572572) = 2^2 \cdot 11 = 44$.

Example 5.18. Find $\gcd(11990979, 637637)$.

5.6 Fermat's Method of Factorisation

Factoring an integer $n > 1$ means finding a pair of positive integers $a > 1$ and $b > 1$ such that $ab = n$. If n is given as a collected prime factorisation then we've seen that it's easy to do this.

However if all we are given is n then to find a factorisation $n = ab$ is generally much harder than to multiply a and b to give n. In fact many commonly used methods of sending coded messages (from an automatic cash machine to your bank for example) rely on the relative difficulty of factoring to multiplying. Consequently there is currently alot of attention focused on methods of factorisation and there are cash prizes (from "RSA laboratories") available for factoring certain large integers. Here we'll look at one method of factoring, discovered by Fermat, which works well in some cases.

Example 5.19. Use Fermat's method of factorisation to find factors of 266004389. We have $16309 < \sqrt{266004389} < 16310$. Therefore we start with $u = 16310$:

$$\begin{aligned}
16310^2 - 266004389 &= 11711\\
16311^2 - 266004389 &= 44332\\
16312^2 - 266004389 &= 76955\\
16313^2 - 266004389 &= 109580\\
16314^2 - 266004389 &= 142207\\
16315^2 - 266004389 &= 174836\\
16316^2 - 266004389 &= 207467\\
16317^2 - 266004389 &= 240100 = 490^2.
\end{aligned}$$

Therefore $266004389 = 16317^2 - 490^2 = (16317+490)(16317-490)$. As $16317+490 = 16807$ and $16317 - 490 = 15827$ we've found the factorisation

$$266004389 = 16807 \cdot 15827.$$

Unfortunately, if n does not have 2 factors of similar size then this method of factoring can be very slow. (It does however form the basis of some more powerful methods.)

5.7 Primality testing

One way to see whether or not an integer $n > 1$ is prime is to test it for divisibility by all prime numbers p such that $1 < p < n$. If none of these primes divide n then the Fundamental Theorem of Arithmetic implies that n is prime. This is very time consuming but does allow us to build up a list of primes. The process can be speeded up significantly by using the observation that if n is composite then it has a prime divisor $p \leq \sqrt{n}$. This is the content of the following lemma.

Lemma 5.20. *An integer $n > 1$ is composite if and only if it has a prime divisor p such that $p < \sqrt{n}$.*

Proof.

□

Example 5.21. To find all primes in the range 1 to 45:

$$2, 3, 5, 7, 11, 13, 17, 19, 23, 29, 31, 37, 41, 43.$$

This is now a complete list of primes between 1 and 45. This method of constructing lists of primes is known as the *Sieve of Eratosthenes*. In fact it is still too inefficient to use in practice to determine if a large number is prime.

5.8 A Theorem of Euclid

The following theorem appears in Book IX of the *Elements*, a mathematical textbook written by Euclid: a Greek mathematician who lived around 300 bc.

Theorem 5.22. *There are infinitely many primes.*

Proof. The proof is by contradiction.

$\square$

5.9 Objectives

After covering this chapter of the course you should be able to:

(i) recall Theorem 2.21 and understand its proof;

(ii) define a coprime pair of integers;

(iii) recall Corollary 5.3 and Euclid's Lemma and understand their proofs;

(iv) define prime and composite numbers;

(v) recall the prime divisor property, Theorem 5.8, and understand its proof;

(vi) recall the Fundamental Theorem of Arithmetic, Theorem 5.12, and understand its proof;

(vii) recognise and write down the prime factorisation and standard form or collected prime factorisation of an integer;

(viii) use prime factorisation to find divisors and greatest common divisors;

(ix) recall the statement of Theorem 5.22 and understand its proof.

5.10 Exercises

5.1 Let a, b and c be integers such that $\gcd(a, b) = 1$ and $a|c$ and $b|c$. Prove that $ab|c$. [**Hint:** Use Theorem 2.21 and multiply by c.]

5.2 Let a, b and n be integers such that $\gcd(a, n) = 1 = \gcd(b, n)$. Prove that $\gcd(ab, n) = 1$. [**Hint:** Use Corollary 5.3.]

5.3 Let a and b be integers, not both zero.

(a) Show that if $k > 0$ and $\gcd(a, b) = d$ then $\gcd(ka, kb) = kd$. [**Hint:** Use an appropriate result to express d as $d = ax + by$. Multiply both sides by k.]

(b) Prove that if a and b be integers with $\gcd(a, b) = d$ then

$$\gcd\left(\frac{a}{d}, \frac{b}{d}\right) = 1.$$

[**Hint:** Use the previous part of the question.]

5.4 Write down the collected prime factorisation of 4725, 17460, 1234 and 36000. Hence find $\gcd(4725, 17460)$.

5.5 Write down the collected prime factorisation of $a = 252$, $b = 1470$ and $c = 525$. Hence find $\gcd(a, b)$, $\gcd(a, c)$ and $\gcd(b, c)$ and list all divisors of 252.

5.6 (a) Suppose that $n_1, \ldots, n_t$ are integers and that $n_i = 3q_i + r_i$, with $r_i = 0$ or 1, for $i = 1, \ldots, t$. Show that $n_1 \cdots n_t$ has the form $3q + r$, with $r = 0$ or 1.

(b) Show that an integer of the form $3n + 2$ has a prime factor of the same form.

5.7 (a) Show that, if $2^n - 1$ is a prime then n must also be a prime. [**Hint:** $a^n - 1 = (a-1)(a^{n-1} + \cdots + 1)$.] Primes of this form are called Mersenne primes. Show that $2^{11} - 1$ is not a prime.

(b) Show that, if $2^n + 1$ is a prime then n must be a power of 2. [**Hint:** $a^5 + 1 = (a+1)(a^4 - a^3 + a^2 - a^1 + 1)$.] Primes of this form are called Fermat primes.

5.8 Let p, q_1 and q_2 be prime and suppose that $p|q_1q_2$. Show, without using the Fundamental Theorem of Arithmetic, that $p = q_1$ or $p = q_2$.

5.9 Let n be an integer $n > 1$. Assume that n has the property that

"if $n|ab$ then $n|a$ or $n|b$".

Show that n is prime. Conclude, by quoting an appropriate result, that p is prime if and only if p has the prime divisor property.

5.10 (a) Let $a_1, \ldots, a_m$ and b be integers such that a_i and b are coprime, for all i. Let $c = a_1 \cdots a_m$. Prove by induction that b and c are coprime. (Use the result of question 5.2.)

(b) Let $a_1, \ldots, a_n$ be integers such that a_i and a_j are coprime whenever $i \neq j$. Show by induction that if $a_i | b$, for $i = 1, \ldots, n$, then $a_1 \cdots a_n | b$. (Use the result of question 5.1.)

5.11 Use Fermat Factorisation to factorise
(i) 143; (ii) 2279; (iii) 43; (iv) 11413.

5.12 Use Fermat Factorisation to factorise
(i) 8051; (ii) 73; (iii) 45009; (iv) 11021.

5.13 Write out the odd integers from 3 to 100 and then use the sieve of Eratosthenes to reduce this list to a list of primes between 3 and 100.

5.14 Using the solutions to Question 2.9, determine the general form of the solution x, y to the following equations.

(a) $56x + 72y = 40$;

(b) $24x + 138y = 18$;

(c) $221x + 35y = 11$;

(d) $5x + 17y = 22$;

(e) $63x + 45y = 783$;

(f) $119x - 6y = 7$.

Chapter 6

Finite Arithmetic

In this chapter we introduce some new number systems and study their arithmetic. These number systems are based on the idea of *congruence* in the integers. Congruence arithmetic was developed by one of the greatest of all mathematicians, Carl Friedrich Gauss, in the 19th Century. It is an important and useful part of mathematics which has many applications both theoretical and practical. We'll look at one application at the end of the Chapter: there are many more. We begin with some curiosities which can be understood once we've developed the theory.

6.1 Casting Out Nines

This is a method of testing integers for divisibility by 9. In fact it outputs the unique remainder obtained (by the Division Algorithm) on expressing a positive integer as $9q + r$, with $0 \leq r < 9$. The procedure is the following.

Procedure 6.1 (Casting Out Nines). Given a non–negative integer n (written in base 10) repeat the following steps (in any order) until a number less than 9 is obtained.

1 Cross out any digits that sum to 9 or a multiple of 9.

2 Add the remaining digits.

The result is the remainder of division of n by 9.

Example 6.2. Cast out Nines from 215763401.

Example 6.3. Cast out Nines from 51422211.

The casting out nines procedure can be used to check the results of numerical calculations.

Example 6.4. Check the computation

$$215763401 \times 51422216 = 11095032211116616.$$

Example 6.5. Check

$$5^7 + 3 = 78128 = 304 \times 257$$

for arithmetic mistakes.

These examples do not *guarantee* the results of calculations. All that can be said is that if we cast out nines and get different answers then we've made a mistake.

We can also use casting out nines to check for divisibility by 9. A number is divisible by 9 if and only if the result is 0.

Example 6.6. Decide which of 215763401, 51422216 and 3254787 is divisible by 9.

The Telephone Number Trick

1 Write down your telephone number.

2 Write down your telephone number with digits reversed.

3 Subtract the smaller of these two numbers from the larger.

4 By casting out nines from the result decide whether or not it is divisible by 9.

6.2 The "Odd & Even" Number System

6.3 Red, white and blue arithmetic

6.4 Congruence

In the Red, White and Blue number system we collected together all integers which left remainder 1, after attempting division by 3, and called them blue. Notice that if a and b are blue then $3|b-a$.

Conversely, given any two integers a and b such that $3|b-a$ we can write

$$b-a=3k, \text{ for some } k\in\mathbb{Z}.$$

Using the division algorithm we can also write

$$b=3q+r, \text{ for } r=0,1 \text{ or } 2.$$

Therefore

$$a=b-3k=3(q-k)+r.$$

That is a and b are both the same colour in the Red, White and Blue number system.

Our analysis shows that a and b are the same colour if and only if $3|b-a$. Generalising this from 3 to an arbitrary integer n leads us to the definition of congruence.

Definition 6.7. Let n be a positive integer and let $a,b\in\mathbb{Z}$. If $n|b-a$ then we say that a is **congruent** to b **modulo** n, and write

$$a\equiv b \pmod{n}.$$

For instance $17\equiv 5 \pmod{12}$ and $216\equiv 6 \pmod{7}$. As in the case $n=3$ above, $a\equiv b \pmod{n}$ if and only if a and b both leave the same remainder after attempting division by n. In fact, if

$$a=nq+r \text{ and } b=np+r, \text{ where } 0\le r<n \tag{6.1}$$

then

$$b-a=n(p-q),$$

so $n|b-a$: that is $a\equiv b \pmod{n}$.

On the other hand if we know that $a\equiv b \pmod{n}$ then $n|b-a$ so, using the argument above, with n instead of 3, we'll find that there is some r such that (6.1) holds.

Example 6.8. Congruence modulo 2 gives rise to the Odd and Even number system.

Example 6.9. Congruence modulo 3 gives rise to the Red, White and Blue number system.

Example 6.10. Suppose $n=10$. Then $0\equiv 10 \pmod{10}$, $10\equiv 101090 \pmod{10}$, $11\equiv 121 \pmod{10}$ and $27\equiv 253427 \pmod{10}$. Every positive integer is congruent to its last digit (written to base 10). In particular integers congruent to 0 all end in the digit 0. These are exactly the integers divisible by 10.

Congruence is not the same as equality but it does share some of the properties of equality. If we have any integers a, b and c and n is a positive integer then

1. $a\equiv a \pmod{n}$,
2. if $a\equiv b \pmod{n}$ then $b\equiv a \pmod{n}$ and
3. if $a\equiv b \pmod{n}$ and $b\equiv c \pmod{n}$ then $a\equiv c \pmod{n}$.

These are all properties of equality. Let's check them for congruence. The first one is easy since $n|0=a-a$, for all integers a. We'll check the last one here and leave the second as an exercise.

6.5 Modular arithmetic

Arithmetic with congruences is called *modular* arithmetic. We've already seen a couple of examples: Odd & Even arithmetic and Red, White and Blue arithmetic. The idea is to add and multiply integers in the usual way but to regard two numbers as the same if they are congruent. There is a possible problem with this. Suppose we work modulo 10, that is $n = 10$. Now take two integers which are congruent modulo 10, say 23 and 3. We are to regard these as the same. This means that if we do something to one, say add 6, then we should get the same answer as if we add 6 to the other. Here "the same answer" means the same answer modulo 10. Let's see:

$$23 + 6 = 29 \text{ and } 3 + 6 = 9.$$

This is alright because $29 \equiv 9 \pmod{10}$ and so we regard 29 and 9 as the same. Does this always work? The purpose of the next Lemma is to reassure us that it does.

Lemma 6.11. *Let n be a positive integer. Suppose that a, b, u and v are integers such that*

$$a \equiv u \pmod{n}$$

and

$$b \equiv v \pmod{n}.$$

Then

(i) $-a \equiv -u \pmod{n}$*;*

(ii) $a + b \equiv u + v \pmod{n}$ *and*

(iii) $ab \equiv uv \pmod{n}$.

Proof. We prove parts (i) and (iii) here, leaving part (ii) as an exercise.

□

Lemma 6.12. *Every integer is congruent modulo n to one and only one of the integers in the list* $0, 1, \ldots, n-1$.

Proof. This follows from the division algorithm because if $a \in \mathbb{Z}$ then we can write $a = nq + r$, with $0 \le r < n$. Then $n|a - r$ so $a \equiv r \pmod{n}$ and r is in the given list. If $a \equiv r \pmod{n}$ and $a \equiv s \pmod{n}$ then, from the above, $r \equiv s$ with $0 \le r < n$ and $0 \le s < n$. Assuming that $r > s$ then $n|r - s$ and $n > r \ge r - s$, contradicting Lemma 2.18.3. Thus a is congruent to only one integer in the list. □

Example 6.13. In Modular arithmetic we can always avoid computation with large numbers. For example working modulo 10 we have

$$7459898790352045324 \equiv 4 \pmod{10}$$

and

$$9874558754423 \equiv 3 \pmod{10}.$$

Therefore

$$7459898790352045324 \cdot 9874558754423 \equiv 4 \cdot 3 = 12 \equiv 2 \pmod{10}.$$

Similarly, working modulo 7 we have

$$4543362 \equiv 5 \pmod{7}.$$

Therefore

$$4543362^2 \equiv 5^2 \equiv 25 \equiv 4 \pmod{7}$$

and

$$4543362^3 = 4543362 \cdot 4543362^2 \equiv 5 \cdot 4 \equiv 20 \equiv 6 \pmod{7}.$$

6.6 Divisibility Tests

Divisibility by 9

When we write a number like 20195 to base 10 we are expressing the number

$$2 \times 10^4 + 0 \times 10^3 + 1 \times 10^2 + 9 \times 10^1 + 5$$

in shorthand (there's a 1 in the 100's column etc.).

Applying this argument in general we write

$$a_m a_{m-1} \cdots a_1 a_0$$

for the number

$$a_m \times 10^m + a_{m-1} \times 10^{m-1} + \cdots + a_1 \times 10 + a_0.$$

As $10^k \equiv 1 \pmod{9}$, for $k = 1, \ldots, m$, we have

$$a_m a_{m-1} \cdots a_1 a_0 \equiv a_m + a_{m-1} + \cdots + a_1 + a_0 \pmod{9}. \tag{6.2}$$

Now consider Casting out Nines, Procedure 6.1. Suppose we cast out nines from an integer m. In Step 1 we cross out any digits which sum to a multiple of 9. The sum of these digits is congruent to zero modulo 9 so, from (6.2), the result is an integer congruent to m modulo 9. In Step 2 we add the digits and again, from (6.2), the result is an integer congruent to m modulo 9. Thus the casting out nines procedure results at every stage in an integer congruent to m modulo 9. The procedure ends with a number r such that $0 \le r < 9$ and $r \equiv m \pmod{9}$. Therefore $9|m - r$, from which it follows that $m = 9q + r$, for some $q \in \mathbb{Z}$ and $0 \le r < 9$. That is, the output from Casting out Nines is the unique remainder guaranteed by the division algorithm, on attempting division by 9.

The following lemma follows from (6.2).

Lemma 6.14. *An integer is divisible by* 9 *if and only if the sum of its digits is divisible by* 9.

Example 6.15. Are 31357989921 or 5179183229478 divisible by 9?

Divisibility by 4

Now $10^2 \equiv 0 \pmod 4$. Thus, for example,

$$1932526 = (19325 \times 100) + 26 \equiv 26 \pmod 4$$

and

$$\begin{gathered}939756564890843577455655687386 75 = \\ (9397565648908435774556556873 86 \times 100) + 75 \equiv 75 \pmod 4.\end{gathered}$$

More generally, if $a_m \cdots a_1 a_0$ is an integer written to base 10 then

$$a_m \cdots a_1 a_0 = (a_m \cdots a_2 \times 100) + a_1 a_0 \equiv a_1 a_0 \pmod 4.$$

Therefore

$$a_m \cdots a_1 a_0 \equiv 0 \pmod 4 \quad \text{if and only if} \quad a_1 a_0 \equiv 0 \pmod 4.$$

That is

$$4 | a_m \cdots a_1 a_0 \Leftrightarrow 4 | a_1 a_0.$$

Example 6.16. Does 4 divide 937475900345 or 80345003732?

6.7 Inverses in modular arithmetic

If we work in the rational numbers $\mathbb{Q}$ we can find a multiplicative inverse for any non-zero element. For example the inverse of $11/201$ is $201/11$. The same is true in $\mathbb{R}$ where the inverse of $x \neq 0$ is $1/x$. In general if x is a number and y has the property that $xy = 1$ then we say that x has **inverse** y. Most elements of $\mathbb{Z}$ don't have inverses in $\mathbb{Z}$. For example 2 has no inverse. In fact ± 1 are the only elements of $\mathbb{Z}$ which have inverses. What about arithmetic modulo n.

Example 6.17. Try to find the inverse of 2 modulo 6.

Example 6.18. Do either 3 or 7 have inverses modulo 10?

Example 6.19. Which numbers have inverses modulo 8?

Lemma 6.20. *An integer a has an inverse modulo n if and only if $\gcd(a, n) = 1$.*

Proof. $\square$

What happens if we do arithmetic modulo a prime number p? In this case, for every integer a either

1 $p \nmid a$ in which case $\gcd(a,p)=1$ or

2 $p|a$ in which case $a \equiv 0 \pmod p$.

Thus every integer which is not congruent to zero modulo p has an inverse. This means that arithmetic modulo p resembles arithmetic in $\mathbb{Q}$ more closely that arithmetic in $\mathbb{Z}$.

Example 6.21. Write out the multiplication table for arithmetic modulo 5 with the integers $0,1,2,3$ and 4. Hence find the inverse of every integer which is not congruent to zero modulo 5.

6.8 Solving Congruences

Example 6.22. Find all integers x such that

$$2x \equiv 4 \pmod 6. \tag{6.3}$$

We call such equations **congruences** and this is an example of a **linear** congruence. Note that if $x=a$ is a solution and $a \equiv b$ then $x=b$ is also a solution: so if there's one solution there are infinitely many. Every integer is congruent to one of

$$0,1,\ldots,n-1 \text{ modulo } n$$

so we seek solutions to congruences in this range. Once we know the solutions in this range then, given the preceeding remark, we know all solutions. One method of solving the congruence above is to construct a table:

x	0	1	2	3	4	5
$2x \pmod 6$						

From the table we see that the only solutions are $x=2$ and $x=5$.

This method certainly works but it require alot of work. A more efficient method is to use the results of Section 5.3. Suppose we wish to find solutions to the congruence

$$ax \equiv b \pmod n. \tag{6.4}$$

By definition of congruence x is a solution to (6.4) if and only if $n|(ax-b)$: that is if and only if $ax-b=ny$, for some integer y. Rearranging the last equation, x is a solution if and only if $ax-ny=b$, for some $y \in \mathbb{Z}$. This is an equation of the form solved in Section 5.3 and we know from Theorem 5.5 that it has a solution if and only if $\gcd(a,n)|b$. If $\gcd(a,n)|b$ then, as in Section 5.3, we can use the Euclidean algorithm to find a particular solution to the equation. Also, writing $\gcd(a, n) = d$, if $d|b$ and $x = u$, $y = v$ is a solution then the list of solutions to this equation consists of all the pairs

$$x = u - (n/d)t,\ \ y = v - (a/d)t,\ \text{for } t \in \mathbb{Z}.$$

Therefore, if $d|b$ and $x = u$ is one solution to the congruence (6.4) then the list of solutions to (6.4) consists of the integers of the form $u - (n/d)t$, for $t \in \mathbb{Z}$.

Applying this to congruence (6.3) above,

In the general case (of congruence (6.4)) the only remaining question is which of the solutions we have found are congruent?

We summarise our findings in a Theorem.

Theorem 6.23. *Let a, b and n be integers with $n > 0$ and let $d = \gcd(a, n)$. Then the congruence* (6.4) *has a solution if and only if $d|n$. If $d|n$ then there are exactly d pairwise incongruent solutions to* (6.4).

Example 6.24. Find all solutions to the congruence

$$2x \equiv 3 \pmod 6.$$

Example 6.25. Find all solutions to the congruence $6x \equiv 9 \pmod{15}$.

Example 6.26. Compare the solutions to the congruences

$$2x \equiv 4 \pmod 6 \text{ and } x \equiv 2 \pmod 6.$$

6.9 Random numbers: an application

A sequence of numbers in which each new term is selected independently of the previous term is called a sequence of **random** numbers. Such sequences can be obtained mechanically; by rolling a dice, spinning a roulette wheel, or running the lottery. However if the sequence is to be used in a scientific experiment then it is often desirable to be able to repeat the experiment. This means producing a sequence which *looks* random but which can be reconstructed when we wish to verify our experimental results. Such sequences cannot be truly random and are called **pseudo-random**. Pseudo-random numbers are often generated by computer but this means that we need to find good algorithms to produce them. The art and science of pseudo-random number generation is highly developed and very sophisticated: look at the web page Random number generators – The pLab Project Home Page at http://random.mat.sbg.ac.at/.

Here we present a pseudo-random number generator, first proposed by D.H. Lehmer in 1949, that is easy to understand and for many purposes does a good enough job. To generate a sequence of pseudo-random integers $a_0, a_1, a_2, \ldots$ perform the following process.

1 Fix a positive number n and two integers m and c, with $2 \leq m < n$ and $0 \leq c < n$.

2 Choose a start value a_0, such that $0 \leq a_0 \leq n$.

3 Generate elements of the sequence successively using the formula

$$a_{k+1} = ma_k + c \pmod n, \text{ where } 0 \leq a_{k+1} < n.$$

If a large value of n is chosen the sequence appears random, at least to start with.

Example 6.27. With $n = 800$, $m = 71$, $c = 57$, and $a_0 = 2$ the first ten elements of the sequence are

$$2, 199, 586, 63, 530, 87, 634, 271, 98, 615.$$

Now altering a_0 to 551 the sequence produced is

$$551, 778, 95, 402, 599, 186, 463, 130, 487, 234.$$

Keeping everything fixed except $n = 8000$ we obtain

$$551, 7178, 5695, 4402, 599, 2586, 7663, 130, 1287, 3434.$$

With $n = 40$, $m = 22$, $c = 20$ and $a_0 = 13$ we obtain

$$13, 26, 32, 4, 28, 36, 12, 4, 28, 36, 12.$$

Of course such sequences are not random (by definition) and we have a formula for the terms.

Theorem 6.28. *The kth term of the sequence generated by the process above is*

$$a_k = \left(m^k a_0 + \frac{c(m^k - 1)}{(m-1)} \right) \pmod{n},$$

with $0 \leq a_k < n$.

Analysis of "how random" a pseudo-random sequence is involves applying statistical tests to the sequence. For instance the frequency of occurence of a particular integers in the sequence can be tested; as can the frequency of occurence of pairs of integers.

6.10 Objectives

After covering this chapter of the course you should be able to:

(i) recall the definition of congruence;

(ii) recall the statement of Lemma 6.11 and understand its proof;

(iii) do arithmetic modulo n;

(iv) understand how various divisibility tests work and be able to apply them;

(v) decide whether or not an integer has an inverse modulo n;

(vi) generate a sequence of pseudo-random numbers.

6.11 Exercises

6.1 Perform the following calculations in arithmetic modulo n for $n = 2$, 10 and 9. In each case give your answer as an integer in the range 0 to $n-1$.
(a) $1+2$; (b) $2 \cdot 3$; (c) $4 \cdot (3+5)$; (d) $6 \cdot 7$; (e) $(6+5) \cdot (5+7)$.

6.2 Perform the following calculations in arithmetic modulo n for $n = 2$, 10 and 9. In each case give your answer as an integer in the range 0 to $n-1$.
(a) $1+1$; (b) $0 \cdot 1$; (c) $3 \cdot (4+5)$; (d) $2 \cdot 5$; (e) $(4+5) \cdot (6+7)$.

6.3 Construct tables for addition and multiplication modulo 4. Which integers if any have inverses modulo 4?

6.4 Complete the following tables which give the rules for addition and multiplication modulo 10

$+$	0	1	2	3	4	5	6	7	8	9
0	0	1	2	3	4	5	6	7	8	9
1	1	2	3	4	5	6	7	8	9	0
2	2	3	4	5	6	7	8	9	0	1
3	3									
4	4									
5	5									
6	6									
7	7									
8	8									
9	9									

$\cdot$	0	1	2	3	4	5	6	7	8	9
0	0	0	0	0	0	0	0	0	0	0
1	0	1	2	3	4	5	6	7	8	9
2	0	2	4	6	8	0	2	4	6	8
3	0	3	6	9	2	5				
4	0		8	2	6					
5	0			5						
6	0									
7	0									
8	0									
9	0									

Which integers have inverse modulo 10?

6.5 Construct tables, similar to those in Question 6.4, for addition and multiplication in modulo 9. Which integers have inverse modulo 9?

6.6 Let n be a natural number and let $a, b \in \mathbb{Z}$. Use the definition of congruence to show that if

$$a \equiv b \pmod{n} \quad \text{then} \quad b \equiv a \pmod{n}.$$

6.7 Let n be a natural number and let $a, b \in \mathbb{Z}$. Use the definition of congruence, Lemma 6.11 and induction to show that if $a \equiv b \pmod{n}$ then

$$a^k \equiv b^k \pmod{n}, \quad \text{for all integers } k \geq 0.$$

6.8 Find all solutions of the following congruences modulo 5 and modulo 8.

(a) $3x \equiv 7$; (b) $4x + 6 \equiv 3$; (c) $x + 3 \equiv 3x + 11$; (d) $6x + 1 \equiv x - 2$; (e) $-x + 2 \equiv 3$; (f) $-4x - 3 \equiv -3x + 2$.

6.9 Find all solutions of the following congruences.

(a) $3x \equiv 5 \pmod{11}$;
(b) $10x + 9 \equiv 9 \pmod{15}$;
(c) $18x \equiv 18 \pmod{27}$;
(d) $182x + 21 \equiv 112 \pmod{1001}$;
(e) $42x + 100 \equiv 53 \pmod{105}$;
(f) $-63x \equiv 0 \pmod{99}$.

6.10 We say that a is a *square root* of b in arithmetic modulo n if

$$a^2 \equiv b \pmod{n}.$$

Show that 3 is a square root of (-1) in arithmetic modulo 10. Find all of the square roots of (-1) in arithmetic modulo 10: that is find all solutions of the congruence

$$x^2 \equiv -1 \pmod{10}.$$

6.11 Show that $x = 7$ is a solution of the quadratic equation $x^2 - 5x + 6 \equiv 0 \pmod{10}$. Find all the solutions of this quadratic equation modulo 10.

6.12 Find all solutions to the following simultaneous congruences modulo 6 and 11.

(a) $\begin{aligned} 7x + 10 &\equiv 2 \\ 3x + 9 &\equiv 4 \end{aligned}$; (b) $\begin{aligned} 2x + 3y &\equiv 8 \\ 5x + 4y &\equiv 8 \end{aligned}$;

(c) $\begin{aligned} 4x + 15y &\equiv 3 \\ 3x + 2y &\equiv 5 \end{aligned}$; (d) $\begin{aligned} 5x + 3y &\equiv 7 \\ 7x + 2y &\equiv 1 \end{aligned}$.

6.13 (a) Show that an integer is divisible by 3 if and only if the sum of its digits is divisible by 3.

(b) Show that an integer is divisible by 5 if and only if its last digit is divisible by 5.

(c) Show that the integer

$$a_m a_{m-1} \cdots a_1 a_0$$

is divisible by 11 if and only if the alternating sum

$$a_0 - a_1 + \cdots + (-1)^{m-1} a_{m-1} + (-1)^m a_m$$

is divisible by 11.

(d) Test the following for divisibility by 3, 5 and 11: the numbers 13451, 800834, 23422345, 234221054 and 2987090.

6.14 Use induction on k to prove Theorem 6.28.

Appendix A

Proof that the Euclidean Algorithm works

This appendix is included for information only: the material it contains is not examinable.

From the examples of Chapter 2 we can see that with the input of Examples 2.3 and 2.4 the Euclidean Algorithm does give the correct output. As we can always replace an integer by its absolute value, without changing the set of its positive divisors, the algorithm is only ever needed to find the greatest common divisor of a pair of positive integers. We may therefore assume that the input to the Euclidean Algorithm is a pair of natural numbers a and b with $a < b$.

Suppose then that we are given a and b with $0 < a < b$ and that we wish to explain why the output from the Euclidean Algorithm is $\gcd(b, a)$.

EA1. We input the pair (b, a).

EA2. Express b as $b = aq_0 + r_0$, for some integers q_0 and r_0, with $0 \leq r_0 < a$. We know that we can always do this because the Division Algorithm, Theorem 2.10, tells us so.

EA3. Do nothing if $r_0 \neq 0$. We'll come back to what happens if $r_0 = 0$ later.

EA4. If we reach this step then we must have had $r_0 > 0$ in Step EA3. In this case we replace (b, a) with (a, r_0). Then we go back to Step EA1 and begin again.

Next time we reach Step EA2 we express $a = r_0q_1 + r_1$, for some integers q_1 and r_1 with $0 \leq r_1 < r_0$. Assuming that $r_1 > 0$ we'll reach Step EA4 again and replace (a, r_0) with the pair (r_0, r_1). We'll then start again at Step EA1. This process continues: we replace (r_0, r_1) with (r_1, r_2) where $r_0 = r_1q_2 + r_2$ and $0 \leq r_2 < r_1$ and so on, as long as none of the r_i's is zero. The result is a sequence of positive integers

$$b > a > r_0 > r_1 > \cdots > r_n > 0,$$

with $r_{i-1} = r_iq_{i+1} + r_{i+1}$, for $i = 1, \ldots, n-1$. These are equations are Equations 2.1–2.5 in Example 2.3 and the r_i's are the remainders which occur there. The algorithm continues adding to this sequence if the remainder r_n is non–zero. This cannot continue indefinitely as b is a fixed positive integer. Therefore, at some stage we'll input (r_n, r_{n+1}) at Step EA1 and when we reach

Step EA3 find that we have $r_n = r_{n+1}q_{n+2} + 0$, for some integer q_{n+2}. As in the examples above, at this point we have

$$\gcd(b, a) = \gcd(a, r_0) = \gcd(r_0, r_1) = \cdots = \gcd(r_{n-1}, r_n) = \gcd(r_n, 0) = r_n$$

(using Lemma 2.16). Now Step EA3 outputs r_n and stops. Thus the Euclidean Algorithm does indeed give the correct answer.

Appendix B

Glossary of notation

$\{a, b, c\}$	the set with elements a, b, c
$\in$	is a member of
$\notin$	is not a member of
$\emptyset$	the empty set
$X \subset Y$	X is a subset of Y
$X \not\subset Y$	X is not a subset of Y
$X \supset Y$	Y is a subset of X
$X \not\supset Y$	Y is a not a subset of X
: or $\vert$	such that
$\mathbb{N}$	the set of natural numbers
$\mathbb{Z}$	the set of integers
$\mathbb{Q}$	the set of rational numbers
$\mathbb{R}$	the set of real numbers
$\{x \in S : x \text{ has property } P\}$	the set of elements of the set S which have property P
$X \cup Y$	the union of X and Y
$X \cap Y$	the intersection of X and Y
$X \backslash Y$	the difference of X and Y
X'	the complement of X (in a given set E)
$\exists$	there exists
$\forall$	for all
$A \Rightarrow B$	A implies B (or if A then B)
$A \Leftarrow B$	B implies A (or if A then B)
$A \Leftrightarrow B$	A if and only if B (or A iff B)
$a \vert b$	a divides b (or a is a factor of b, or a is a divisor of b)
$a \nmid b$	a does not divide b
$\vert x \vert$	the modulus (or absolute value) of x
$\gcd(a, b)$	greatest common divisor of a and b
$\text{hcf}(a, b)$	highest common factor of a and b ($\gcd(a, b) = \text{hcf}(a, b)$)
$\sum_{j=1}^{n} a_j$	$a_1 + \cdots + a_n$
$a \equiv b \pmod{n}$	a is congruent to b modulo n