MAS1241/MAS2241

Number Systems

Semester 1, 2010/2011

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 is based on a principal branch of pure mathematics: algebra, via number systems. Investigation of number systems involves making precise statements and deciding whether or not they are true. It is crucial that statements and arguments are clearly set out and logically structured so that they can be understood by any reader with the appropriate background. This requires careful use of words, symbols and logic to express ideas and the relationships between them. An important aspect of this module is to develop your ability to write clear legible mathematics: partly by reading the notes and other sources but mainly by attempting the exercises.

These notes are intended to supplement the notes you make during the lectures: material given on slides in the lectures corresponds to what is written in the booklet. What is written on the board during lectures may not be, and there are gaps left in the notes for you to write this material in.

The notes and other course information can be found on the web at

`www.mas.ncl.ac.uk/~najd2/teaching/mas1241/`

from where they can be viewed or printed out. The module page can be accessed by following the links from this page and gives the official course description, syllabus and reading list.

AJ Duncan August 2010

Contents

Chapter 1

Division and Greatest Common Divisors

Move forward to a time after the collapse of the banking system when we have returned to bartering.

In the university 1 *loaf of bread can be exchanged for 11 apples and a chocolate cake can be exchanged for* 15 *apples. A professor has baked a batch of cakes and a student turns out to have a dozen loaves of bread and hundreds of apples. The professor wants just one apple, so would like to exchange some cakes for one apple and some loaves. Can this be done, and if so how?*

We can use the university loaves to apples conversion table:

Loaves	Apples										
1	1	2	3	4	5	6	7	8	9	10	11
2	12	13	14	15	16	17	18	19	20	21	22
3	23	24	25	26	27	28	29	30	31	32	33
4	34	35	36	37	38	39	40	41	42	43	44
5	45	46	47	48	49	50	51	52	53	54	55
6	56	57	58	59	60	61	62	63	64	65	66

Is there more than one solution?

We can describe the problem algebraically. Let a, b and c and stand for the value of an **a**pple, a **c**ake and a loaf of **b**read, respectively. Then $c = 15a$ and $b = 11a$.

Can we find another solution?

Are there any other solutions?

Now suppose that at bottle of French wine is worth 30 *apples and a bottle of English wine is worth* 24 *apples. A lecturer has a crate of french wine and some apples and the professor now wants* 6 *apples, but only has a crate of English wine. Can a fair transaction be made so that the prof ends up with* 6 *apples?*

We can describe the problem algebraically again. Let f and e stand for the values of **F**rench and **E**nglish wine, respectively.

The crucial feature of these problems is that we are only interested in solutions which are natural numbers (defined in Section A.6). Solutions would be very easy to find if we allowed ourselves to use rational numbers or real numbers (see Section A.6). For example if we set $x = 1$ in the second problem then we can take $y = 3/5$. On the other hand integer solutions are no easier to find than natural number solutions (integers are also defined in Section A.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 bartering ones above. We'll look at a a step by step recipe which would give us a number, like 6 in the second problem above, which can be used to simplify the problem and in fact determines whether or not there is a solution. We shall investigate, in some detail, how and why this works.

1.1 The Euclidean Algorithm

To solve the equation $6 + 30y = 24x$ 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. This is easy, because the numbers here are small, but let's make the process we go through absolutely clear, and then try it for some bigger numbers. For simplicity suppose I want the biggest positive number that divides both 24 and 30. I make two lists.

$$\begin{array}{lcl} \text{Positive divisors of } 24 & : & 1, 2, 3, 4, 6, 8, 12, 24 \\ \text{Positive divisors of } 30 & : & 1, 2, 3, 5, 6, 10, 15, 30 \end{array}$$

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

Example 1.1. Find the biggest number which divides both 2028 and 2600.
Positive divisors of

$$\begin{array}{lcl} 2028 & : & 1, 2, 3, 4, 6, 12, 13, 26, 39, 52, 78, 156, 169, 338, 507, 676, 1014, 2028 \\ 2600 & : & 1, 2, 4, 5, 8, 10, 13, 20, 25, 26, 40, 50, 52, 65{,}100, 104, 130, 200, 260, \\ & & 325{,}520, 650, 1300, 2600 \end{array}$$

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**[1] 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 1.2. Find the greatest common divisor d of 12 and 63. Find $x, y \in \mathbb{Z}$ such that $12x + 63y = d$.

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

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 1.3. 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:

$$(2600,2028) \qquad 2600 = 2028 \cdot 1 + 572 \tag{1.1}$$
$$(2028,572) \qquad 2028 = 572 \cdot 3 + 312 \tag{1.2}$$
$$(572,312) \qquad 572 = 312 \cdot 1 + 260 \tag{1.3}$$
$$(312,260) \qquad 312 = 260 \cdot 1 + 52 \tag{1.4}$$
$$(260,52) \qquad 260 = 52 \cdot 5 + 0. \tag{1.5}$$

This gives $\gcd(2600, 2028) = 52$, as we found in Example 1.1.

To find the integers x, y we work back from (1.4) to (1.1).

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

Example 1.4. 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:

$$\begin{aligned}
(2028,626) \quad & 2028 = 626 \cdot 3 + 150 && (1.6)\\
(626,150) \quad & 626 = 150 \cdot 4 + 26 && (1.7)\\
(150,26) \quad & 150 = 26 \cdot 5 + 20 && (1.8)\\
(26,20) \quad & 26 = 20 \cdot 1 + 6 && (1.9)\\
(20,6) \quad & 20 = 6 \cdot 3 + 2 && (1.10)\\
(6,2) \quad & 6 = 2 \cdot 3 + 0. && (1.11)
\end{aligned}$$

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

To find the integers x, y we work back from (1.10) to (1.6) to find an expression for 2.

$$\begin{aligned}
2 &= 20 \cdot 1 - 6 \cdot 3 && \text{from (1.10)}\\
&= 20 \cdot 1 - 3 \cdot (26 \cdot 1 - 20 \cdot 1) = 20 \cdot 4 - 26 \cdot 3 && \text{from (1.9)}\\
&= (150 \cdot 1 - 26 \cdot 5) \cdot 4 - 26 \cdot 3 = 150 \cdot 4 - 26 \cdot 23 && \text{from (1.8)}\\
&= 150 \cdot 4 - (626 - 150 \cdot 4) \cdot 23 = 150 \cdot 96 - 626 \cdot 23 && \text{from (1.7)}\\
&= (2028 - 626 \cdot 3) \cdot 96 - 626 \cdot 23 = 2028 \cdot 96 - 626 \cdot 311 && \text{from (1.6).}
\end{aligned}$$

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

1.2 Integer Arithmetic

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 study integer arithmetic which will show us 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. The basic laws governing such arithmetic are listed here **as background information only: you do not need to memorise these rules for examination**: although they should be second nature.

Laws of integer arithmetic (not examinable). Let x, y and z be integers.

1. $x + 0 = x = 0 + x$.
2. For every integer n there is an integer $-n$ such that $n + (-n) = 0$.
3. $(x + y) + z = x + (y + z)$.
4. $x + y = y + x$.
5. $x \cdot 1 = x = 1 \cdot x$.
6. $(xy)z = x(yz)$.
7. $xy = yx$.
8. $(x + y)z = xz + yz$.

Subtracting n from x is the same as adding $-n$ to x: so subtraction is a convenient operation but is not essential. The integers are **ordered** by a relation denoted $\leq$ which respects addition and multiplication: that is the following laws hold.

1. If $a \leq b$ and $c \leq d$ then $a + c \leq b + d$;
2. If $a \leq b$ and $0 < c$ then $ac \leq bc$.

Here "$a < b$" is shorthand for "$a \leq b$ and $a \neq b$".

In fact all these laws apply to arithmetic with rational and real numbers[2] as well as integers. From these basic laws we can derive all the other familiar properties of arithmetic such as (for integers x, y and z)

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

(Again these are **not examinable**.)

[2]The real numbers are defined in Section A.6

"If and only if". The notation $\Leftrightarrow$ above is shorthand for the phrase "if and only if". To say "$x + z = y + z$ *if and only if* $x = y$ means two things:

1. if $x + z = y + z$ then $x = y$ and
2. if $x = y$ then $x + z = y + z$.

The second statement is the *converse* of the first. (More generally, the converse of "If A is true then B is true" is "If B is true then A is true".)
We have to make both statements because it is possible that a true statement has a converse which is false. This is apparent in everyday life. For example it would be quite reasonable to say that the statement "If I am a frog then I can swim" is true. The converse is "If I can swim then I am a frog", and this is commonly regarded as false. More precise mathematical examples are not hard to find.

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: entries on different lines do not 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

There is one further important property of integer arithmetic which does **not** apply to rational or real numbers. To state this property we need to recall some notation.

Definition 1.5. The **modulus** or **absolute value** of a real number x is denoted $|x|$ and is given

by the formula

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

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

The definition of modulus above is what is known as a *definition by cases*.

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

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

Theorem 1.6 (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 from the properties listed above, but it seems intuitively obvious and 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.

Comments on the Division algorithm.

(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 if you believe in fractions:

(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.

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

Definition 1.7. Let a and b be integers. If there exists an integer q such that $b = qa$ then we say that a **divides** b, which we write as $a|b$.

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 1.8. 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 $7 \nmid 18$ and $-15 \nmid 25$, although explaining exactly why may take a little thought.

Notation.

The expression "$3|6$" means that there is an integer q such that $6 = 3q$.

The expression "$3/6$" denotes a rational number.

Another way of saying $a|b$ would be to say "b/a is an integer, or $a = b = 0$", but this is more complicated in at least two ways.

Take care not to confuse $a|b$ with a/b or b/a.

1.3 Examples of integer arithmetic

In the next few examples we'll use Definition 1.7 as a starting point and from it prove some very simple facts, using this definition and the Division Algorithm, just to get used to the terminology for integer arithmetic.

Example 1.9. We shall prove that $6|(6n + 6)$, for all integers n.

"For all" and "there exists". In Example 1.9 we have proved something is true *for all* integers. To prove this it is **not** enough to find an example of some integer n for which the statement is true. On the other hand if you are asked to prove that there *exist* integers x and y such that $2600x + 2028y = 52$ then it would be enough to find an example: say $x = -7$ and $y = 9$, as in Example 1.3.

Example 1.10. Prove that $4|[(2n + 1)^2 - 1]$, for all integers n.

Example 1.11. From the Division Algorithm, 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 1.6) to partition of integers into odd and even.

Example 1.12.

Example 1.13. Show that $3|n^3 - n$, for all integers n.

Example 1.14. Show that if n is an integer then n^3 has the form $4k$, $4k+1$ or $4k+3$, for some $k \in \mathbb{Z}$.

1.4 Common Divisors

Next we'll uncover some basic facts about common divisors which help to understand the workings of the Euclidean algorithm. First let's make the terminology precise. Greatest common divisors were defined on page 7 but now that we've got the definition of division we can make a better job.

Definition 1.15. Let a and b be integers. An integer c such that $c|a$ and $c|b$ is called a **common divisor** of a and b.

Definition 1.16. Let a and b be integers, not both 0. The **greatest common divisor** of a and b is the integer d such that

1. $d|a$ and $d|b$ and
2. if c is any common divisor of a and b then $d \geq c$.

We write $\gcd(a, b)$ for the greatest common divisor of a and b.

Example 1.17. Consider the equality $112 = 20 \cdot 5 + 12$.

Lemma 1.18. *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:

Step(1) Show that if c is a common divisor or s and t then c is a common divisor of t and u.

Step(2) Show that if c' is a common divisor or t and u then c' is a common divisor of s and t.

Step(3) From Steps (1) and (2) 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 common divisors are thus equal. Another way of putting this is to write $d = \gcd(s, t)$ and $d' = \gcd(t, u)$ and then say that Step(1) shows that d is a common divisor of t and u so $d \leq d'$. Moreover Step(2) shows that d' is a common divisor of s and t, so $d' \leq d$. As $d \leq d'$ and $d' \leq d$ we have $d = d'$.

□

Example 1.19. We can write $337 = 11 \cdot 30 + 7$, so

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 so on some fairly general examples. (Although a proof using what we have done could be constructed.) Before going any further we record some very basic consequences of the definition of division; as a lemma.

Lemma 1.20.

1. $n|n$, *for all integers* n.
2. $n|0$, *for all integers* n.
3. *If* m *and* n *are integers such that* $m|n$ *and* $n > 0$ *then* $m \leq n$.
4. *If* m *and* n *are positive integers such that* $m|n$ *then* $\gcd(m, n) = m$.

Proof.

□

The proof of the third part of the Lemma above is known as *proof by contradiction*. This always works as follows.

Step(1) **Start with some statement to be proved.** In the Lemma this is that "If $m|n$ and $n > 0$ then $m \leq n$."

Step(2) **Assume the negation of what is to be proved.** In the proof of the Lemma this is that there exist integers m, n such that $m|n$ and $n > 0$ and $m > n$.

Step(3) **Derive some consequences of the assumption.** As a result we find that $n = mq$, with $q \geq 1$.

Step(4) **Show that something we've derived is false.** This means that $n \geq m$, which together with $m > n$ makes $n > n$, which is *impossible*.

Step(5) **Conclude that the result holds.** It cannot happen that $m|n$ and $n > 0$ and $m > n$ because this forces $n > n$, which is impossible. The conclusion is that whenever $m|n$ and $n > 0$ then $m \leq n$.

1.5 Why the Euclidean Algorithm works

Example 1.21. Consider the Equations (1.6)–(1.11) on page 12.

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 1.18 and Equations (1.6)–(1.11) show why the algorithm comes up with the correct answer.

Example 1.22. Consider the Equations (1.1)–(1.5) on page 9. As in the example above we have

$$\begin{aligned}
\gcd(2600, 2028) &= \gcd(2028, 572), \text{ using Equation (1.1)} \\
\gcd(2028, 572) &= \gcd(572, 312), \text{ using Equation (1.2)} \\
\gcd(572, 312) &= \gcd(312, 260), \text{ using Equation (1.3)} \\
\gcd(312, 260) &= \gcd(260, 52), \text{ using Equation (1.4)}.
\end{aligned}$$

From Equation (1.5) we see that $52|260$ and so we have $\gcd(260, 52) = 52$. Therefore

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

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 1.2, 1.3 and 1.4, to find integers x and y such that $ax + by = \gcd(a, b)$. This gives us the following Theorem.

Theorem 1.23. *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.

1.6 An application

We began this Chapter by looking at the problem of batering with apples, cakes and loaves. This problem was resolved by finding integer solutions to the equation $1 + 11y = 15x$. Equations of this form, where we seek integer solutions (and the coefficients are integers) are called **Diophantine equations**. In our case and only x's and y's occur (nothing like x^2, x^3, xy or xy^2 occurs) and such equations are called **linear**. Here we shall see how to find solutions to some linear Diophantine equations.

Example 1.24. Find integers x and y such that $2600x + 2028y = 104$.

In Example 1.3 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

$$2600 \cdot (-7) + 2028 \cdot 9 = 52. \tag{1.12}$$

Example 1.25. Find integers x and y such that $-72 = 12378x - 3054y$.

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

$$\begin{aligned}
(12378,3054) \quad & 12378 = 3054 \cdot 4 + 162 && (1.13)\\
(3054,162) \quad & 3054 = 162 \cdot 18 + 138 && (1.14)\\
(162,138) \quad & 162 = 138 \cdot 1 + 24 && (1.15)\\
(138,24) \quad & 138 = 24 \cdot 5 + 18 && (1.16)\\
(24,18) \quad & 24 = 18 \cdot 1 + 6 && (1.17)\\
(18,6) \quad & 18 = 3 \cdot 6 + 0. && (1.18)
\end{aligned}$$

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

Next we work back from (1.17) to (1.13) to find integers u, v such that $6 = 12378u + 3054v$.

$$\begin{aligned}
6 &= 24 - 18 \cdot 1 && \text{from (1.17)}\\
&= 24 - (138 - 24 \cdot 5) = 24 \cdot 6 - 138 && \text{from (1.16)}\\
&= (162 - 138) \cdot 6 - 138 = 162 \cdot 6 - 138 \cdot 7 && \text{from (1.15)}\\
&= 162 \cdot 6 - (3054 - 162 \cdot 18) \cdot 7 = 162 \cdot 132 - 3054 \cdot 7 && \text{from (1.14)}\\
&= (12738 - 3054 \cdot 4) \cdot 132 - 3054 \cdot 7 = 12378 \cdot 132 - 3054 \cdot 535 && \text{from (1.13).}
\end{aligned}$$

Thus

$$6 = 12378 \cdot 132 + 3054 \cdot (-535) \tag{1.19}$$

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

$$ax + by = c \tag{1.20}$$

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

This is an example of an "if and only if" statement.

The Lemma says two things:

1. "If $ax + by = c$ has a solution then $\gcd(a, b)|c$" and
2. "If $\gcd(a, b)|c$ then the equation $ax + by = c$ has a solution."

Both must be proved, because it can happen that a true statement has a converse which is false ("e.g. "If you are a crocodile then you have big teeth and a long tail.")

Proof.

□

Example 1.27. Are there integers x and y such that $2600x + 2028y = 130$?

Example 1.28. For which c does the equation $72x + 49y = c$ have a solution?

We conclude this chapter with some remarks about Lemma 1.26. Fix a pair of integers a and b and let $d = \gcd(a, b)$. The lemma tells us that the equation $ax + by = c$ has a solution if and only if $d|c$. Now this means that

1. there is a solution if $d = c$ and
2. there is no solution if $0 < c < d$.

We can therefore conclude that d is the smallest positive integer that can be written in the form $ax + by$, with $x, y \in \mathbb{Z}$.

Now let's suppose that once we've fixed a and b we find there exist integers u and v such that $au + bv = 1$. For example this happens if we set $a = 25132$ and $b = 15079$, for then $3a - 5b = 1$. What can we say about $\gcd(a, b)$ in this case? We'll take up these threads again in the next chapter.

1.7 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 1.7 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 simple results;

(viii) understand the strategy of the proof of Lemma 1.18 and be able to apply it to other situations;

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

(x) find solutions to equations of the kind given in Section 1.6.

1.8 Exercises

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

1.2 Prove the following using only the definition of division (Definition 1.7). In each case indicate where in your proof you have used the definition.

(a) $13|169$, $13|1859$ and $143|1859$.
(b) $5|(5n^2+25n+75n)$, for all integers n.

1.3 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^4 is of the form either $5k$ or $5k+1$.

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

1.5 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.

1.6 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.

1.7 Use only the definition of division, Definition 1.7, to prove the following facts. Do **not** mention the Division Algorithm, Theorem 1.6. 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 $a|c$.

1.8 Let a and b be integers.

(a) Prove that $\gcd(a,b) = \gcd(-a,b) = \gcd(-a,-b)$. [**Hint.** Use a similar strategy to the proof of Lemma 1.18.]
(b) If $a > 0$ show that $\gcd(a,0) = a$. What is $\gcd(a,0)$ if $a < 0$?

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

(a) $56x + 72y = 40$;
(b) $24x + 138y = 18$;
(c) $221x + 35y = 11$.

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

(a) $51x - 7y = 88$;
(b) $33x + 44y = 88$;
(c) $11x - 66y = 0$;
(d) $33x + 27y = 88$;
(e) $33x + 44y = 1$.

1.11 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 $b = \pm a$.

1.12 Use the Division Algorithm and Question 1.11 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 1.11 are used and how.

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

1.14 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 $r^2 = 5$.

1.15 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.]

Chapter 2

Coprime Pairs of Numbers

The professor has been awarded a pay increase and decides to throw a party. He wants French wine for this party. Unfortunately in this department the pay is in bottles of English wine. Lecturers in Classics are paid in French wine and apples; so the professor wishes to trade English wine for apples and French wine. The prof still wants to eat six apples, as it happens. Can the professor buy sufficient wine to make a really memorable party?

In this section we'll develop enough of the theory of integers to enable us to write down a formula which tells us exactly which values of x and y are solutions to equations of this type for which we seek integer solutions (linear Diophantine equations).

2.1 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 1.23. We'll now give an alternative proof of this Theorem.

Second proof of Theorem 1.23

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

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

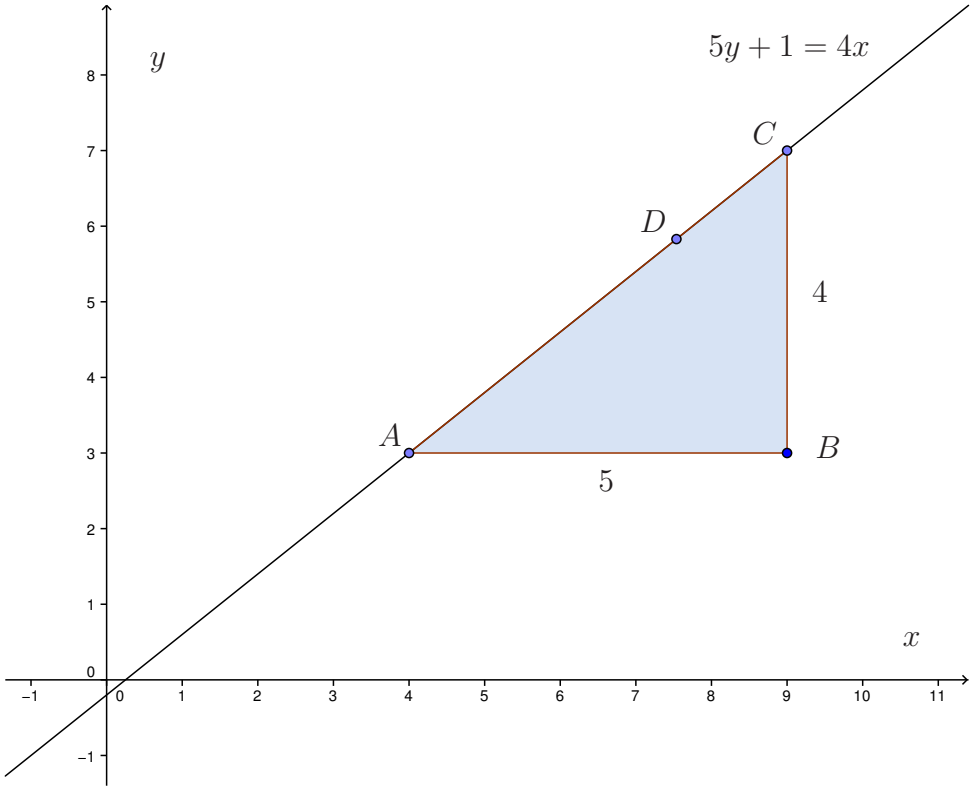

Figure 2.1: $A = (4, 3)$, $C = (9, 7)$, D may have non-integer coordinates.

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

$$s = ak + bl, \text{ for some } k, l \in \mathbb{Z}. \tag{2.1}$$

Now, using the Division Algorithm, we can write

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

Substituting for s using (2.1) this becomes

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

so

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

If $r \neq 0$ 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 (2.1) gives

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

Therefore $c|s$ and from Lemma 1.20.3 we have $c \leq s$. This completes the proof that $s = \gcd(a, b)$ and we've already found k, l such that $s = ak + bl$, so Theorem 1.23 follows.

2.2 Coprime pairs of integers

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

Definition 2.1. If a and b are integers with $\gcd(a, b) = 1$ then we say that a and b are **coprime**.

Example 2.2. It is easy to see that 6 and 35 are coprime, for example. Now from Theorem 1.23 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 2.3. *Integers a and b are coprime if and only if there exist integers u and v such that $au + bv = 1$.*

A *corollary* is something which follows easily from a previously proven fact.

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 1.23 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 $d = \gcd(a, b)$.

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

□

2.3 Euclid's Lemma

Corollary 2.3 allows us to prove a result known as Euclid's Lemma.

Lemma 2.4 (Euclid's Lemma). *Let a, b and c be integers with $\gcd(a, b) = 1$. If $a|bc$ then $a|c$.*

Proof.

□

2.4 Application to solving equations

Recall that a linear Diophantine equation is an equation of the form $ax + by = c$, where a, b and c are integers. We've already seen (Lemma 1.26) that a linear Diophantine equation has integer solution x and y if and only if $\gcd(a, b)|c$. We can now use Euclid's lemma to find all solutions to such equations.

Theorem 2.5. *Let a, b, c be integers and let $d = \gcd(a, b)$. The equation*

$$ax + by = c \tag{2.2}$$

has an integer solution if and only if $d|c$. If $d|c$ then equation (2.2) *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*

$$u_1 = u_0 + (b/d)t$$

and

$$v_1 = v_0 - (a/d)t,$$

for some $t \in \mathbb{Z}$.

Proof.

□

Example 2.6. In Example 1.24 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

Example 2.7. Find all integer solutions to the equation $63x + 12y = 18$. List all solutions with $x > -12$ and $y > 6$.

From Example 1.2 we have $\gcd(63, 12) = 3$ and as $3|18$ the equation has solutions. In Example 1.2 we also found that $63 \cdot 1 + 12 \cdot (-5) = 3$.

Example 2.8. Find the general form for integer solutions to the equation $12378x + 3054y = 42$. Find all solutions x, y with $x > 0$ and $y > -2000$. Find all solutions with $x > 0$ and $y > 0$.

In Example 1.25 we found that $\gcd(12378, 3054) = 6$ and since $6|42$ this equation has solutions. In the given example we also found $12378 \cdot 132 + 3054 \cdot (-535) = 6$. Multiplying through by 7 gives $12378 \cdot 132 \cdot 7 + 3054 \cdot (-535) \cdot 7 = 42$. This gives a particular solution

$$x = 132 \cdot 7 = 924 \text{ and } y = (-535) \cdot 7 = -3745.$$

For the general form of the solution, in this case we have $a/d = 12378/6 = 2063$ and $b/d =$

$3054/6 = 509$. The general form of the solution is therefore

$$x = 924 + 509t \text{ and } y = -3745 - 2063t,$$

for $t \in \mathbb{Z}$.

(We can check this is correct: with $t = 1$ we verify that $12378 \cdot 1433 + 3054(-5808) = 42$.)

For solutions with $x > 0$ we require $924 + 509t > 0$, that is $t > -924/509$. As t is an integer we therefore require $t \geq -1$.

We have solutions with $y > -2000$ if and only if $-3745 - 2063t > -2000$ if and only if $3745 + 2063t < 2000$ if and only if $t < -1745/2063$ if and only if $t \leq -1$.

Therefore there is a unique solution with $x > 0$ and $y < -2000$, which we obtain by setting $t = -1$, namely

$$x = 415, y = -1682.$$

We have solutions with $y > 0$ if and only if $3745 + 2063t < 0$ if and only if $t < -3745/2000$ if and only if $t \leq -2$. Thus to obtain a solution with $x, y > 0$ we need both $t \geq -1$ and $t \leq -2$. There are no such t so there are no solutions with $x, y > 0$.

2.5 Objectives

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

(i) recall Theorem 1.23 and understand its proof;

(ii) define a coprime pair of integers;

(iii) recall Corollary 2.3 and Euclid's Lemma and understand their proofs;

(iv) find the general form of the solution of a linear Diophantine equation in two variables.

2.6 Exercises

2.1 Let a, b and c be integers such that $c|a$ and $c|b$. Show that $c|(au + bv)$, for all integers u and v.

2.2 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 1.23 and multiply by c.]

2.3 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.]

2.4 Using the solutions to Question 1.9, determine the general form of the integer solutions x, y to the following equations.

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

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

(c) $24x + 138y = 18$.

2.5 Find the general form of integer solutions to the equation $348x + 152y = 32$. Find all solutions with $x > 0$ and $y < 0$. Also find all solutions with $x > 0$ and $y > -300$.

2.6 Find the general form of integer solutions to the equation $84x + 66y = -30$. Find all solutions with $x > 1$ and $y > 35$. Also find all solutions with $x < 15$ and $y < 35$.

Chapter 3

Proof by Induction

3.1 Proof by Induction

Proof by induction is a method of proving that a sequence of statements, one for each positive integer, are all true. We could use induction to prove for example that

$$3|(n^3 - n), \text{ for all integers } n \geq 1,$$

(which we already know because by Example 1.13) or that

$$1 + 3 + 5 + \cdots + (2n - 1) = n^2, \text{ for all integers } n \geq 1,$$

which is to say that the sum of the first n odd numbers is equal to n^2.

In the first case we have to prove something for all values of n, namely that

In Example 1.13 we used the Division Algorithm to prove all these to be true (as well as the corresponding statements for negative values of n). In this chapter we'll see a different method of proof.

In the second case above we have to prove that the entries in the second and third columns of the table below are equal, on every line.

n	sum of first n odd numbers	n^2
1	1	1×1
2	$1 + 3 = 4$	2×2
3	$1 + 3 + 5 = 9$	3×3
4	$1 + 3 + 5 + 7 = 16$	4×4
5	$1 + 3 + 5 + 7 + 9 = 25$	5×5
$\vdots$	$\vdots$	$\vdots$
100	$1 + \cdots + 199$	10000
$\vdots$	$\vdots$	$\vdots$
k	$1 + \cdots + (2k - 1)$	k^2
$\vdots$	$\vdots$	$\vdots$

We shall prove this in Example 3.2 below.

Proof by induction: the idea.

Recall that the **natural numbers** are the positive integers, $0, 1, 2, \cdots$. These have the property that if we begin at 1 and keep adding 1 then we eventually form a list which contains **every** natural number.

$$1 \overset{+1}{\rightarrow} 2 \overset{+1}{\rightarrow} 3 \overset{+1}{\rightarrow} 4 \overset{+1}{\rightarrow} \cdots \overset{+1}{\rightarrow} k \overset{+1}{\rightarrow} k+1 \overset{+1}{\rightarrow} \cdots$$

Therefore if we have a sequence of statements, one corresponding to each natural number, and

1. we can prove the first one is true (the case $n = 1$) and
2. we can show that if the kth one is true then the $k + 1$st is also true (for any $k \geq 1$)

then all the statements must be true.

Example 3.1. Prove by induction that $3|(n^3 - n)$, for all $n \geq 1$.

Solution.
First we need to prove the statement holds in the case $n = 1$. This is easy as when $n = 0$ we have $n^3 - n = 0$ and $3|0$.

Now we need to show that if the kth statement holds then so does the $k + 1$st. For clarity write out what we are assuming and what it is we have to prove, namely:

We assume that $3|k^3 - k$, as this is the case $n = k$ of our statements.

We shall show that in this case $3|(k+1)^3 - (k+1)$, which is the case $n = k+1$.

We can do this as follows.

We may now conclude, using induction, that $3|n^3 - n$, for all $n \geq 1$.

To describe proof by induction more formally suppose that we have a sequence of statements $P(1)$, $P(2)$, $P(3)$, ..., $P(n)$, ... one for each positive integer n. For example $P(n)$ might be "$3|n^3 - n$" as in the first example above, or it could be "the sum of the first n odd positive integers equals n^2", as in the second example. With this notation we can say the **Principle of Induction** is as follows. Given the sequence of statements $P(n)$ suppose that we can show both that

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

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

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

Example 3.2. Prove by induction that $1 + 3 + 5 + \cdots + (2n-1) = n^2$, for all $n \geq 1$.
Solution. In the above notation $P(n)$ is the statement $1 + 3 + 5 + \cdots + (2n-1) = n^2$, so statements $P(1)$, $P(2)$, ... , $P(5)$, $P(100)$ and $P(k)$ appear in the table on page 53. Proof by induction takes the following form.

Basis Show that $P(1)$ is true. This is the case $n = 1$. In this example when $n = 1$ we have the statement $1 = 1^2$, obtained by replacing each occurrence of n in $P(n)$ with 1. Since this is true the first part of the proof is complete.

The inductive hypothesis (IH) Now we assume the statement holds in the case $n = k$: that is we assume that $P(k)$ is true, which in our example means we assume that

$$1 + 3 + \cdots + (2k-1) = k^2,$$

where $k \geq 1$. Note that we obtain this by replacing every occurence of n in $P(n)$ with k.

The inductive step Next we must show that the statement holds in the case where $n = k + 1$. That is we must show that $P(k+1)$ holds, which in our case means that we must prove that

$$1 + 3 + \cdots + (2(k+1) - 1) = (k+1)^2.$$

(Again we obtain $P(k+1)$ by replacing n with $k+1$ throughout $P(n)$.)

Remarks.

- In proof by induction we make the assumption that $P(k)$ holds for some $k \geq 1$ and then prove that $P(k+1)$ also holds. For the proof to be correct we must be sure this works for **all possible** values of k. If it fails for just one value of k then the proof does not work.
- Often there is more than one way of proving a statement, or sequence of statements. For instance Examples 1.13 and 3.1 both prove the same thing (almost). In this case the original proof seems better as it gives more insight into why the statement is true.

Example 3.3. Use induction to prove

$$\frac{1}{1\times 2}+\frac{1}{2\times 3}+\frac{1}{3\times 4}+\cdots+\frac{1}{n(n+1)}=1-\frac{1}{n+1},$$

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

Here $P(n)$ is the statement

$$\frac{1}{1\times 2}+\frac{1}{2\times 3}+\frac{1}{3\times 4}+\cdots+\frac{1}{n(n+1)}=1-\frac{1}{n+1}$$

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

Note that it would save space and effort to use summation notation for this problem. That is we could write

$$\frac{1}{1\times 2}+\frac{1}{2\times 3}+\frac{1}{3\times 4}+\cdots+\frac{1}{n(n+1)}=\sum_{j=1}^{n}\frac{1}{j\times(j+1)}$$

in which case $P(n)$ would appear as

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

This requires care when writing out $P(k)$ and $P(k+1)$. As j is just a dummy variable it remains untouched and the rule is exactly as before: to obtain $P(k)$ replace n with k throughout $P(n)$. Thus $P(k)$ appears as

$$\sum_{j=1}^{k}\frac{1}{j\times(j+1)}=1-\frac{1}{k+1}$$

as in the worked solution to the problem. The same applies to $P(k+1)$.
This notation will be used in problem class and assignment exercises.

3.2 Change of basis

We don't need to start an induction proof with the case $n=1$. We can modify (1) and (2) on page 55 in an obvious way so that we can start with any other integer. That is 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 3.4 (Bernoulli's Inequality)**.** Prove that

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

Example 3.5. 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 $n = 9$. In fact, for any positive integer t and sufficiently large n we have $2^n > n^t$. In our proof $t = 3$ and we show exactly what "sufficiently large" means in this case.

3.3 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 the Fibonacci numbers (after doing the problem class exercises).

3.4 Exercises

3.1 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 $n \in \mathbb{N}$.

3.2 Prove by induction that

$$\sum_{r=1}^{n} r(r!) = (n+1)! - 1$$

for all integers $n \geq 1$.

3.3 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 $x \in \mathbb{R}, x \geq 0$.

3.4 Prove by induction that:

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

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

3.5 (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.

(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 2.2.)

3.6 A *geometric progression* is a sequence of the form

$$a, ar, ar^2, ar^3, \ldots$$

where $a, r \in \mathbb{R}$ and $r \neq 1$. What is the sum of the first n terms of this geometric progression?

3.7 Sum the geometric progression with $a = 1$ and $r = x$ ($\neq 1$) and so find an expression for $x^n - 1$. Write out explicit formulae for $x^2 - 1$, $x^3 - 1$ and $x^4 - 1$. Now sum the geometric progression with $a = 1$, $r = -x$ ($x \neq -1$) and $n = 2m + 1$, for some $m \in \mathbb{N}$. Hence find an expression for $x^{2m+1} + 1$. Write out explicit formulae for $x^3 + 1$, $x^5 + 1$ and $x^7 + 1$.

3.8 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) $24|2 \cdot 7^n + 3 \cdot 5^n - 5$.

3.9 *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 $n \geq 1$.

There must be something wrong here but what is it? If it's not immediately obvious try thinking about the following situation. Suppose that you are given a bag of $n \geq 2$ smarties and that it turns out that whichever 2 of the smarties you choose they have the same colour. It seems pretty clear that they're all the same colour. Are you sure? What makes this different from the geography example above?

3.10 The Fibonacci numbers are the elements of the sequence $f_1, f_2, f_3, \ldots$ generated by the rules

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

Thus the first few Fibonacci numbers are

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

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

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

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

3.11 Prove that every 5th Fibonacci number is divisible by 5, that is $5|f_{5n}$, for all $n \geq 1$.

3.12 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 4

Prime Numbers

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. It may seem surprising then that, in spite of several hundred years effort and many thousands of pages of mathematics, it is commonly accepted that most of the theory of prime numbers is yet to be discovered. If you Google "Ulam Spiral" for example you'll see examples of behaviour of prime numbers that, as far as I know, we have as yet no idea how to explain.

Here we shall make a start: 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.

4.1 Definition of Prime and Composite 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 4.1. A positive integer $p > 1$ is called a **prime** if the only positive divisors of p are 1 and p. An integer greater than 1 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 4.2 (The prime divisor property)**.** *If p is a prime and $p|ab$ then $p|a$ or $p|b$.*

Example 4.3. 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 4.4. *If p is prime and $p|a_1 \cdots a_n$ then $p|a_i$, for some i.*

4.2 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: see Section 4.3 below and 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

$$2 \cdot 5 \cdot 2 \cdot 7,$$
$$2 \cdot 7 \cdot 2 \cdot 5,$$
$$7 \cdot 2 \cdot 2 \cdot 5$$

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 4.5. By definition primes cannot have any factorisation other than the obvious one: e.g. 7 cannot be written as a product of primes other than by writing it as ... well ... 7. If it could be then it wouldn't be prime!

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 4.6 (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.

□

4.3 Rational numbers and polynomials

Before continuing we shall pause to see that this theorem really did need proving: that it is not a universal truth that holds in all situations where we can do arithmetic. To begin with consider the rational numbers $\mathbb{Q}$. We can factor 2 as

$$2 = 4 \cdot (1/2) = 8 \cdot (1/4) = \cdots = 2^n \cdot (1/2^{n-1}) = \cdots =$$

and in general as $2q \cdot (1/q)$, for any non-zero element $q \in \mathbb{Q}$. Therefore there is no hope of anything like Theorem 4.6 holding in $\mathbb{Q}$.

To see how the uniqueness part of the Theorem might fail, even when we can factorise elements into products of primes, we could investigate arithmetic with polynomials, but we shall not go into that here.

4.4 Collected prime factorisation

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 4.7. *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 $a_i \geq 1$.

4.5 The square root of 2

If n is a positive integer and has collected prime factorisation $n = p_1^{\alpha_1} \cdots p_k^{\alpha_k}$ then $n^2 = (p_1^{\alpha_1} \cdots p_k^{\alpha_k})(p_1^{\alpha_1} \cdots p_k^{\alpha_k})$ so has collected prime factorisation

What this shows is that an integer m is of the form n^2, for some integer n, if and only if every prime in the prime factorisation of m has even exponent. i.e.

We can use this fact to prove the following result, as a corollary of the Fundamental Theorem of Arithmetic. Recall that a rational number is one which can be written as a fraction and that we denote the set of all rational numbers by $\mathbb{Q}$.

Corollary 4.8. *There is no rational number r such that $r^2 = 2$. That is $\sqrt{2} \notin \mathbb{Q}$.*

The same argument applies if we replace 2 by any other prime number so there are lots of numbers which are not rational. A real number which is not rational is called **irrational**. It turns out that there are also infinitely many irrational numbers, such as π and e, which are not roots of primes.

4.6 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 4.9. *An integer $n > 1$ is composite if and only if it has a prime divisor p such that $p \leq \sqrt{n}$.*

Proof.

□

Example 4.10. 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.

4.7 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 4.11. *There are infinitely many primes.*

Proof. The proof is by contradiction.

□

4.8 Objectives

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

(i) define prime and composite numbers;

(ii) recall the prime divisor property, Theorem 4.2, and understand its proof;

(iii) recall the Fundamental Theorem of Arithmetic, Theorem 4.6, and understand its proof;

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

(v) use the sieve of Eratosthenes;

(vi) recall the statement of Theorem 4.11 and understand its proof.

4.9 Exercises

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

4.2 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.

4.3 (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.

4.4 (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.

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

Chapter 5

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.

5.1 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 5.1 (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 5.2. Cast out Nines from 215763401.

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

Example 5.3. Check the computation

$$215763401 \times 51422218 = 11095032642643428.$$

Such 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.

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.

5.2 The “Odd & Even” Number System

5.3 Red, white and blue arithmetic

5.4 Congruence

In the Red, White and Blue number system we collected together all integers which left remainder 0, 1, or 2 after attempting division by 3, and called them white, red or blue, respectively. We saw that 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 5.4. 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

$$a = nq + r \text{ and } b = np + r, \text{ where } 0 \leq r < n \tag{5.1}$$

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 $b-a = np$, for some p. In this case if $a = nq + r$, with $0 \leq r < n$, then $b = np + a = n(p+q) + r$ and (5.1) holds.

Example 5.5. Congruence modulo 2 gives rise to the Odd and Even number system.

Example 5.6. Congruence modulo 3 gives rise to the Red, White and Blue number system.

Example 5.7. 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.

5.5 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 5.8. *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 5.9. *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 $0 \leq r < n$. 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 $0 \leq r < n$ and $0 \leq s < n$. Assuming that $r > s$ then $n|r - s$ and $n > r \geq r - s$, contradicting Lemma 1.20.3. Thus a is congruent to only one integer in the list. □

Example 5.10. 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

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

5.6 Modular exponentiation

In coding and cryptography it's often necessary to compute powers of numbers modulo n; that is $x^m \pmod n$, where x, m and n may be integers with hundreds of digits. To see what's involved consider say $m = 10^{100}$, which is a 1 followed by 100 zeroes (this number is called a *googol*). Now if $x = 10$ then x^m is a 1 followed by 10^{100} zeros (and is called a *googolplex*). It's estimated that there are around 10^{80} elementary particles in the universe, so even if each of these could be used as a zero it would be impossible to write down this number. This shows that if x and m have over 100 digits then no computer, in the lifetime of the known universe, can possibly compute $x^m \pmod n$ by first computing x^m and then reducing modulo n. However, Maple can (using the command "`x&^m mod n;`") compute, for example, $x^m \pmod n$ when

$$\begin{aligned}
x &= 584872422111233465340456456429056847639246235844999349393999453003003003030202734324234237689473423423\\
m &= 895857774764666430996883476132354068564353545785698694543332456457643234523452344433423273478237645634\\
n &= 887846566785886898996958463521645786903466534564564532899045672585898456756221110403977207340340300332234234;
\end{aligned}$$

giving the answer

$$x^m \pmod n = 887846566785886898996958463521645786903466534564564532899045672585898456756221110403977207340340300332234234$$

To see how this can be done consider the following computation of $7^{183} \pmod{257}$.

$$\begin{aligned}
7^2 &\equiv 49 \pmod{257}\\
7^4 &\equiv 49^2 \equiv 2401 \equiv 88 \pmod{257}\\
7^8 &\equiv 88^2 \equiv 7744 \equiv 34 \pmod{257}\\
7^{16} &\equiv 34^2 \equiv 1156 \equiv 128 \pmod{257}\\
7^{32} &\equiv 128^2 \equiv 16384 \equiv 193 \pmod{257}\\
7^{64} &\equiv 193^2 \equiv 37249 \equiv 241 \pmod{257}\\
7^{128} &\equiv 241^2 \equiv 58081 \equiv 256 \pmod{257}.
\end{aligned}$$

It turns out that these powers of 7 can be combined to give 7^{329}. This follows from the observation that $128 = 2^7$ is the largest power of 2 which is less than (or equal to) 183. In fact we can write 183 as a sum of powers of 2:

$$\begin{aligned}
183 &= 128 + 55\\
&= 128 + 32 + 23\\
&= 128 + 32 + 16 + 7\\
&= 128 + 32 + 16 + 4 + 3\\
&= 128 + 32 + 16 + 4 + 2 + 1\\
&= 2^7 + 2^5 + 2^4 + 2^2 + 2^1 + 2^0.
\end{aligned}$$

(This is essentially an algorithm for finding the binary expansion of 183.) Therefore

$$\begin{aligned} 7^{183} &\equiv 7^{128+32+16+4+2+1} \pmod{257} \\ &\equiv 7^{128}7^{32}7^{16}7^{4}7^{2}7 \pmod{257} \\ &\equiv 256 \cdot 193 \cdot 128 \cdot 88 \cdot 49 \cdot 7 \pmod{257} \\ &\equiv 190890377216 \pmod{257} \\ &\equiv 175 \pmod{257}. \end{aligned}$$

All these computations are possible on a standard calculator but 7^{183} itself has over 150 digits.

Computation of $x^m \pmod n$ by repeated squaring

1. Find the largest power of 2 less than or equal m: say $2^k \leq m < 2^{k+1}$.
2. Compute $x^2 \pmod n$, ..., $x^{2^k} \pmod n$, reducing modulo n each time.
3. Express m as a sum of powers of 2.
4. Compute $x^m \pmod n$ using the values $x^{2^i} \pmod n$.

Example 5.11. Find the value of $11^{231} \pmod{391}$ (giving an answer between 0 and 390) .

Solution.

1. The largest power of 2 which is no greater than 231 is $2^7 = 128$.

2. Repeatedly squaring 11 and reducing modulo 391 we obtain

3. Writing $231 = 128 + 103 = 128 + 64 + 39 = 128 + 64 + 32 + 7 = 128 + 64 + 32 + 4 + 2 + 1$ we have $11^{231} = 11^{128+64+32+4+2+1}$.

4. Combining the above

5.7 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

$$a_m a_{m-1} \cdots a_1 a_0 \equiv a_m + a_{m-1} + \cdots + a_1 + a_0 \pmod 9. \tag{5.2}$$

Now consider Casting out Nines, Procedure 5.1. 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 (5.2), the result is an integer congruent to m modulo 9. In Step 2 we add the digits and again, from (5.2), 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 $0 \leq r < 9$ 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 $0 \leq r < 9$. 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 (5.2).

Lemma 5.12. *An integer is divisible by* 9 *if and only if the sum of its digits is divisible by* 9.

Example 5.13. Are either of 215763401 or 215743401 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

$$\begin{aligned} &939756564890843577455655687386 75 = \\ &(939756564890843577455655687386 \times 100) + 75 \equiv 75 \pmod 4. \end{aligned}$$

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 5.14. Does 4 divide 937475900345 or 80345003732?

5.8 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 5.15. Try to find the inverse of 2 modulo 6.

Example 5.16. Do either 3 or 7 have inverses modulo 10?

Example 5.17. Which numbers have inverses modulo 8?

Lemma 5.18. *An integer a has an inverse modulo n if and only if* $\gcd(a, n) = 1$.

Proof.

□

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 5.19. 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.

5.9 Solving Congruences

Example 5.20. Find all integers x such that

$$6x \equiv 4 \pmod{8}. \tag{5.3}$$

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 use part of the multiplication table (see Example 5.17:

From the table we see that the only solutions are $x = 2$ and $x = 6$. Notice

From this example we see that

cancellation does not always work when solving congruences.

The method of the example certainly works but it requires alot of effort. A more efficient method is to use the results of Section 2.4. Suppose we wish to find solutions to the congruence

$$ax \equiv b \pmod{n}. \tag{5.4}$$

By definition of congruence x is a solution to (5.4) 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 2.4 and we know from Theorem 2.5 that it has a solution if and only if $\gcd(a,n)|b$. If $\gcd(a,n)|b$ then, as in Section 2.4, 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

$$x = u - (n/d)t$$

and

$$y = v - (a/d)t,$$

for $t \in \mathbb{Z}$. Therefore,

the congruence $ax \equiv b \pmod{n}$ has solutions if and only if $d = \gcd(a,n)$. Moreover, if this congruence has a particular solution $x = u$ then the list of solutions consists of the integers of the form

$$u - (n/d)t,$$

where t runs through the integers $\mathbb{Z}$.

Applying this to congruence (5.3) of Example 5.20,

In the general case (of congruence (5.4)) the only remaining question is which of the solutions we have found are congruent?

We summarise our findings in a Theorem.

Theorem 5.21. *Let a, b and n be integers with $n > 0$ and let $d = \gcd(a, n)$. Then the congruence $ax \equiv b \pmod{n}$ has a solution if and only if $d|b$. If $d|b$ then both the following hold.*

(i) There are exactly d pairwise incongruent solutions. (That is, solutions no two of which are congruent to each other.)

(ii) If x_0 is one solution then the complete list of (pairwise incongruent) solutions is

$$x_0,\ x_0 + (n/d),\ x_0 + (2n/d), \cdots, x_0 + ([d-1]n/d).$$

That is, the solutions are precisely $x_0 + (tn/d)$, for $0 \leq t \leq d - 1$.

Example 5.22. Find all solutions to the congruence

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

Example 5.23. Find all solutions to the congruence $6x \equiv 9 \pmod{15}$.

Example 5.24. Compare the solutions to the congruences

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

5.10 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 5.25. 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 5.26. *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.

5.11 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 5.8 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.

5.12 Exercises

5.1 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) $(6+5) \cdot (5+7)$.

5.2 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) $(4+5) \cdot (6+7)$.

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

5.4 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?

5.5 Construct tables, similar to those in Question 5.4, for addition and multiplication in modulo 9. Which integers have inverse modulo 9?

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

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

5.7 Use repeated squaring to compute the following.
(i) $11^{127} \pmod{351}$;
(ii) $16^{200} \pmod{351}$.

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

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

5.9 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) $-63x \equiv 0 \pmod{99}$.

5.10 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

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

5.11 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.

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

(a) $\begin{array}{rcl} 7x + 10 & \equiv & 2 \\ 3x + 9 & \equiv & 4 \end{array}$;

(b) $\begin{array}{rcl} 2x + 3y & \equiv & 8 \\ 5x + 4y & \equiv & 8 \end{array}$;

(c) $\begin{array}{rcl} 4x + 15y & \equiv & 3 \\ 3x + 2y & \equiv & 5 \end{array}$;

(d) $\begin{array}{rcl} 5x + 3y & \equiv & 7 \\ 7x + 2y & \equiv & 1 \end{array}$.

5.13 Let $n = a_m a_{m-1} \cdots a_1 a_0$ be an integer written in base 10.

(a) Show n is divisible by 8 if and only if $a_2 a_1 a_0$ is divisible by 8.

(b) Devise a similar test for divisibility by 2^k, for $k \geq 1$.

(c) Show that n is divisible by 5 if and only if a_0 divisible by 5.

(d) Devise a test for divisibility by 5^k, for $k \geq 1$.

(e) Test 13451, 800832, 23422345, 234221375 and 2987090 for divisibility by 8 and 125.

(f) What can you say about the last 3 digits of a number that is divisible by both 8 and 125?

5.14 Use induction on k to prove Theorem 5.26.

Chapter 6

In Course Assessment Exercises

Show all working.
Unless you are explicitly asked not to, you may use all results from the notes, but you should say what you are using and make clear how it is used.
Marks are given for clearly reasoned explanations of answers, not for the answers themselves.
Answers should be written legibly and, as far as possible in sentences.
Up to 10% of the marks may be deducted for illegible handwriting, and/or badly structured solutions.

6.1 Assignment 1

6.1.1 **No help will be given with this question.**

(a) Write out in full the definition of a *divides* b, for integers a and b.

(b) Carefully state the Division Algorithm (making sure to include all conditions on a, q and r).

(c) Show that n^3 has the form $8k$, $8k+1$, $8k+3$, $8k+5$ or $8k+7$, for all integers n. Use your working to show that $n^3 - n$ is divisible by 8, for all odd integers n.

6.1.2

(a) Find the greatest common divisor of 28028 and 21294.

(b) Find integers x and y such that

$$28028x + 21294y = \gcd(28028, 21294).$$

(c) Which of the following equations have integer solutions? Justify your answers but do not find solutions.
(i) $28028u+21294v = -545$; (ii) $28028u+21294v = 546$; (iii) $28028u+21294v = 1$;

(d) Find integers u and v such that

$$28028u + 21294v = 364.$$

(e) Find the general form of the integer solutions to the equation of part 1(d).

(f) Find all solutions u, v to the equation of part 1(d) such that

(i) $u < 200$ and $v < 200$.

(ii) $u < 200$ and $v < -200$;

(iii) $u < 200$ and $v > 200$.

6.1.3 Let a, b, c, r, s, t, u and v be integers.

(a) Prove from the definition of division that if $a|b$ and $b|c$ then $a|c$.

(b) Prove that if $r|s$ and $r|t$ then $r|sx + ty$, for all integers x and y.

(c) Show that an integer c is a common divisor of u and v if and only if c is a common divisor of u and $v - u$. (The previous part of the question should help.) Use this to show that $\gcd(u, v) = \gcd(u, v - u)$.

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

6.1.5 Let a and d be (fixed) real numbers. Prove by induction that:

$$\sum_{i=0}^{n} a + id = \frac{(n+1)}{2}(2a + nd),$$

for all integers $n \geq 0$.

6.1.6 Prove that every 6th Fibonacci number is divisible by 4, that is $4|f_{6n}$, for all $n \geq 1$.

6.2 Assignment 2

6.2.1 Let $f(x) = x^n + a_{n-1} + \cdots + a_1 x + a_0$ be a polynomial of degree n (with leading coefficient 1). A *root* of f is a real number w such that $f(w) = 0$. In this question you will show that if $a_0, \ldots, a_{n-1}$ are all integers then every root of f is either an integer or an irrational number. Suppose then that $a_0, \ldots, a_n$ are all integers and that w is a root of f.

(a) Show, by using an appropriate result from the notes, that if p is a prime number and u and m are integers, with $m > 0$, such that $p|u^m$ then $p|u$.

(b) Suppose that w is *not* irrational. Then w must be rational: that is $w = a/b$, where a and b are integers, $b \neq 0$ and $\gcd(a, b) = 1$. The result will follow if it can be shown that $b = \pm 1$. (For then we'll have shown that either w is irrational or $w = \pm a$; an integer.)

To do this perform the following.

Replace w with a/b throughout the equation $f(w) = 0$.

Multiply both sides of the resulting equation by b^n.

Simplify the resulting expression. If this is done correctly all denominators will cancel and

you will obtain an equation which involves only integers.

(c) Solve the resulting equation for a^n and show that

$$a^n = bg,$$

where g is an integer. [Hint: $-a_{n-1}a^{n-1} - \cdots - a_1ab^{n-2} - a_0b^{n-1}$ is an integer.]

(d) Assume that $b \neq \pm 1$ and quote a result from the notes which implies that in this case b has a prime divisor, p say.

(e) Show, using the expression for a^n above and the first part of the question, that $p|a$.

(f) Why does this give a contradiction? What was the assumption that gave rise to this contradiction? What is the conclusion?

6.2.2 This question applies the result of the previous question to show some numbers are irrational. Say that a real number a is *not an mth power of an integer* if $a \neq r^n$, for all integers r. In this case $\sqrt[m]{a}$ is not an integer.

(a) Let a be an integer which is not an mth power of an integer. By considering roots of $x^m - a$ show that $\sqrt[m]{a}$ is irrational.

(b) Show that $\sqrt[4]{5}$, $\sqrt[2]{15}$, $\sqrt[3]{9}$ are irrational.

6.2.3 In this question you will give a proof that there are infinitely many primes which are congruent to 5 modulo 6.

(a) Find prime numbers p and q, with $q \neq 5$, such that $p \equiv 1 \pmod 6$ and $q \equiv 5 \pmod 6$.

(b) Show that 2 is the only prime number congruent to 2 modulo 6.

Show that 3 is the only prime number congruent to 3 modulo 6.

(c) Show that there is no prime congruent to 4 modulo 6.

(d) Now show that there are infinitely many primes congruent to 5 modulo 6, as follows. Assume that there are finitely many primes congruent to 5 modulo 6 and let the complete list of them be $5, p_1, \ldots, p_r$. (Note that $p_i \neq 5$, for all $i = 1, \ldots, r$.) Define $N = 6p_1 \cdots p_r + 5$.

i. Show that $2 \nmid N$, $3 \nmid N$ and that $p_i \nmid N$, for $i = 1, \ldots, r$.

ii. Show that $5 \nmid N$.

iii. Show that there is a prime q such that $q \equiv 5 \pmod 6$ and $q|N$.

iv. Combine the above to show that there are infinitely many primes congruent to 5 modulo 6.

6.2.4 Calculate 7^2, 7^3 and 7^4 and 8^2, 8^3 and 8^4 modulo 12 (giving your answers as integers between 0 and 11).

Write down the values of $7^{251} \pmod{12}$ and $8^{1350} \pmod{12}$.

Calculate 6^2, 6^3 and 6^4 modulo 12.

Write down the value of $6^n \pmod{12}$, for any $n \geq 4$.

6.2.5 Use repeated squaring to compute the value of $13^{123} \pmod{261}$. (Give an answer between 0 and 260.)

6.2.6 **No help will be given with this question.**

(a) Let a, b and n be integers with $n > 0$. State a theorem from the course which describes when the congruence

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

has a solution and, when it does, how many pairwise incongruent solutions there are.

(b) State how many pairwise incongruent solutions there are to the following congruences. Briefly justify your answers using the previous part of the question.

i. $15x \equiv 6 \pmod{18}$;

ii. $15x \equiv 10 \pmod{18}$.

(c) Find all solutions to each congruence in part (b) which has a solution.

6.2.7 This question proves a result known as Fermat's little theorem.

(a) Show that working modulo 5 the set of integers $\{1, 2, 3, 4\}$ is the same as the set of integers $\{3, 6, 9, 12\}$.

(b) The result of the previous part of the question works in general. If p is prime and $1 \leq a \leq p-1$ then the integers $a, 2a, 3a, \ldots, (p-1)a$ are congruent modulo p to the integers $1, 2, 3, \ldots, p-1$, in some order. To prove this do the following.

Let r and s be integers with $0 \leq r < s \leq p-1$.

Show that $p \nmid s - r$.

Now show that $ar \not\equiv as \pmod{p}$, for all such r, s. [Hint: use the fact that every integer not congruent to zero has an inverse modulo p.]

Use the particular case $r = 0$ to show that $as \not\equiv 0 \pmod{p}$.

Combinine these facts to show that, in some order, the integers

$$a, 2a, \ldots, (p-1)a$$

are congruent to the integers

$$1, 2, \ldots, (p-1)$$

modulo p.

(c) Show that

$$1 \cdot 2 \cdot \cdots \cdot (p-1) \equiv a \cdot 2a \cdot \cdots \cdot (p-1)a \pmod{p}.$$

Use this to show that

$$a^{p-1} \equiv 1 \pmod{p}.$$

(d) By considering separately the cases $p \nmid b$ and $p|b$ show that

$$b^p \equiv b \pmod{p},$$

for all integers b.

Appendix A

Set Theory

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.

A.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 A.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 1.7 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 1.7 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 1.10 in Section 1.2.)

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.

A.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/).

A.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 ... 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

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

A.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

$$\{78, 69, 45, 32\} \not\supset \{78, 31, 64, 49\}.$$

A.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).

A.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?)

A.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 "$\ldots$", 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

$$\{n \in \mathbb{N} \,|\, n \text{ is a multiple of } 10\} = \{10, 20, 30, \ldots\},$$
$$\{n \in \mathbb{N} \,|\, n \text{ is a multiple of } 10 \text{ and of } 3\} = \{30, 60, 90, \ldots\},$$
$$\{n \in \mathbb{N} \,|\, n \text{ is a multiple of } 3 \text{ and } n+1 \text{ is a multiple of } 7\} = \{6, 27, 48, \ldots\}.$$

A.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 $S \backslash T = \{A, B, C\}$.

A.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.

A.10 Exercises

You can use these questions to test your set theory. There are similar questions on the computer, some of which are assesed. If you can't do them you should read the Chapter or use the "Reveal" function on the computer assesments.

A.1 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 $n < 30\}$;

A.2 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 $\}$;

A.3 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 $x^3 < 343\}$.

A.4 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$\}$

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 $\mid$	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
$\{x \in S : x$ 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)
$a \mid b$	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
$\lvert x \rvert$	the modulus (or absolute value) of x
$\gcd(a, b)$	greatest common divisor of a and b
$\mathrm{hcf}(a, b)$	highest common factor of a and b ($\gcd(a, b) = \mathrm{hcf}(a, b)$)
$\sum_{j=1}^{n} a_j$	$a_1 + \cdots + a_n$
$a \equiv b \pmod{n}$	a is congruent to b modulo n

NEWCASTLE UNIVERSITY

SCHOOL OF MATHEMATICS & STATISTICS

SEMESTER 1 MOCK EXAM

MAS1241

Number Systems

Time allowed: 1 hour 30 minutes

Candidates should attempt all questions. Marks for each question are indicated. However you are advised that marks indicate the relative weight of individual questions, they do not correspond directly to marks on the University scale.

There are EIGHT questions on this paper.

Write your answers on the exam paper, in the spaces provided.
Write rough work on the reverse of the pages.
State carefully where you use any results from the course.
(Unlike the mock exam the real exam paper will have a write on format with spaces for answers.)

1. (a) Find the greatest common divisor of 1400 and 37730.

(b) Find integers x and y such that

$$1400x + 37730y = \gcd(1400, 37730).$$

(c) Which of the following equations have integer solutions? In each case either find integer solutions u and v or explain (briefly) why no solution exists.

(i) $1400u + 37730v = 210$;

(ii) $1400u + 37730v = 102$.

(d) Find the general solution for those equations in part (c) above which have a solution.

(e) Find all solutions with $x > -1000$ and $y > 0$.

[25 marks]

2. (a) Let a, b, c and d be integers such that $a|b$ and $c|d$. Prove that $ac|bd$.

(b) Show that

$$5n^2|(5n^2 + 3)^2 - 9,$$

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

[5 marks]

3. Let a, b and c be non-zero integers such that $\gcd(a, b) = \gcd(a, c) = 1$. Show that $\gcd(a, bc) = 1$.

[5 marks]

4. (a) Show that n^2 has the form $5k$, $5k + 1$ or $5k + 4$, with $k \in \mathbb{Z}$, for all integers n.

(b) Show, using the first part of the question, that if $5|n^2$ then $5|n$.

[15 marks]

5. Prove by induction that:

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

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

[10 marks]

6. 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 marks]

7. (a) Complete the table below for multiplication modulo 8 using only the integers $0, 1, 2, \ldots, 7$.

$\times$	0	1	2	3	4	5	6	7
0	0	0	0	0	0	0	0	0
1	0	1	2	3	4	5	6	7
2	0	2	4					
3	0							
4								
5								
6								
7								

(b) Which integers have inverses modulo 8?

(c) Compute $13^{23} \pmod 8$.

(d) State how many incongruent solutions there are to the following congruences. Justify your answers. Then find all solutions.

(i) $10x \equiv 6 \pmod{18}$;

(ii) $10x \equiv 9 \pmod{18}$.

[20 marks]

8. (a) Let a, b and c be integers such that $a|b$ and $a|c$. Show that $a|b-c$.

(b) Let n be a positive integer and let $S = n! + 1$. Show that if p is a prime divisor of S then $p > n$.

(c) Use the first part of the question to show that there are infinitely many primes. [**Hint:** If there are finitely many primes then set n in the previous part of the question equal to the largest prime.]

[15 marks]

THE END

MAS2241 Number Systems

Semester 1: Mock Exam

This is the same as the MAS1241 exam except that there is an additional ninth question and also the marks for the first eight questions are different. The marks are: Q1 22; Q2 4; Q3 4; Q4 12; Q5 8; Q6 4; Q7 18; Q8 12; Q9 16. The extra question is the following.

9. (a) Let a and b be coprime integers and assume that $a|c$ and $b|c$, for some integer c. Show that $ab|c$.

(b) Let m and n be non-zero integers and let $d = \gcd(m, n)$. Assume $m = ud$ and $n = vd$, where $u, v \in \mathbb{Z}$.

(i) Show that u and v are coprime.

(ii) Let $k = mn/d$. Show that $k = uvd$. Show that if $m|w$ and $n|w$, for some integer w, then $k|w$. [**Hint.** Show that u and v both divide w/d and use part (a).]

(iii) Suppose that r, s are integers such that $r \equiv s \pmod{m}$ and $r \equiv s \pmod{n}$. Show that $r \equiv s \pmod{k}$.

MAS1241: Semester 1 Mock Exam Solutions

1. (a)

$$\begin{aligned} 37730 &= 1400 \cdot 26 + 1330 \\ 1400 &= 1330 \cdot 1 + 70 \\ 1330 &= 70 \cdot 19. \end{aligned}$$

$\gcd(37730, 1400) = 70$.

(b)

$$\begin{aligned} 70 &= 1400 - 1330 \\ &= 1400 - (37730 - 1400 \cdot 26) \\ &= 37730 \cdot (-1) + 1400 \cdot 27. \end{aligned}$$

$x = 27$, $y = -1$.

(c) (i) $70|210$ so there are solutions. $210 = 70 \cdot 3$ so $u = 81$, $v = -3$ is a solution.
(ii) $70 \nmid 102$ so there are no solutions.

(d) The general solution to (i) has the form $x = u+(37730/70)t$ and $y = v-(1400/70)t$, with $u = 81$ and $v = -3$. That is $x = 81 + 539t$ and $y = -3 - 20t$.

(e) We consider only equation (i). For $x > -1000$ we require $81 + 539t > -1000$ that is $539t > -1081$, so $t > -1081/539$. Thus $x > -1000$ if $t \geq -2$. For $y > 0$ we require $-3 - 20t > 0$ that is $-20t > 3$ so $t < -3/20$. Thus $x > 0$ if $t \leq -1$. Therefore we restrict t so that $-2 \leq t \leq 1$ and obtain solutions $x = -458, y = 17$ and $x = -997, y = 37$.

2. (a) $a|b$ so $b = ap$, for some $p \in \mathbb{Z}$. $c|d$ so $d = cq$, for some $q \in \mathbb{Z}$. Therefore $bd = apcq = ac(pq)$ which implies $ac|bd$.

(b)

$$\begin{aligned} (5n^2 + 3)^2 - 9 &= (5n^2)^2 + 6 \cdot 5n^2 + 9 - 9 \\ &= 5n^2(5n^2 + 6). \end{aligned}$$

Therefore $5n^2|(5n^2 + 3)^2 - 9$, for all $n \in \mathbb{Z}$.

3. If $\gcd(a, b) = \gcd(a, c) = 1$ then there exist integers u, v and x, y such that $au + bv = 1$ and $ax + cy = 1$. Then

$$(au + bv)(ax + cy) = 1,$$

so

$$au(ax + cy) + abvx + bcxy = 1$$

and we have $ak+bcl = 1$, with $k = u(ax+cy)+bvx$ and $l = xy$. Therefore $\gcd(a, bc) = 1$, as required.

4. (a) From the Division Algorithm it follows that $n = 5q + r$, with $0 \leq r < 4$. Therefore

$$n^2 = (5q + r)^2 = 25q^2 + 10qr + r^2 = 5K + r^2,$$

for some $r, K \in \mathbb{Z}$ with $0 \leq r < 4$.
If $r = 0$ or 1 then $n^2 = 5K$ or $5K + 1$, respectively.
If $r = 2$ then $n^2 = 5K + 4$.
If $r = 3$ then $n^2 = 5K + 9 = 5(K + 1) + 4$.
If $r = 4$ then $n^2 = 5K + 16 = 5(K + 3) + 1$.
Thus n^2 has the form $5k$, $5k + 1$ or $5k + 4$, for some $k \in \mathbb{Z}$, as required.

(b) If $5|n^2$ then n^2 has the form $5k$, for some $k \in \mathbb{Z}$. From the above, if $n = 5q + r$, with $r \neq 0$ then $n^2 = 5k + s$, with $s = 1$ or 4. Hence $n = 5q + r$ with $r = 0$, that is $5|n$.

5. $P(n)$ is

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

Basis: The left hand side of $P(1)$ is

$$\sum_{k=1}^{1} k(k + 1) = 1 \times (1 + 1) = 2.$$

The right hand side of $P(1)$ is

$$\frac{1}{3}(1 + 1)(1 + 2) = 2.$$

Therefore $P(1)$ holds.

Inductive hypothesis: Assume $P(m)$ holds for some $m \geq 1$.

Inductive step: Then

$$\begin{aligned} \textstyle\sum_{k=1}^{m+1} k(k + 1) &= \textstyle\sum_{k=1}^{m} k(k + 1) + (m + 1)(m + 1 + 1) \\ &= \tfrac{1}{3} m(m + 1)(m + 2) + (m + 1)(m + 2), \text{ using } P(m), \\ &= \tfrac{1}{3}(m + 1)(m + 2)(m + 3) \\ &= \tfrac{1}{3}[m + 1]([m + 1] + 1)([m + 1] + 2), \end{aligned}$$

which is $P(m + 1)$. Therefore $P(n)$ is true for all $n \geq 1$.

6. item The odd numbers from 3 to 100 are
3, 5, 7, 9, 11, 13, 15, 17, 19, 21, 23, 25, 27, 29, 31, 33, 35, 37, 39, 41, 43, 45, 47, 49, 51,

53, 55, 57, 59, 61, 63, 65, 67, 69, 71, 73, 75, 77, 79, 81, 83, 85, 87, 89, 91, 93, 95, 97, 99.
Crossing out multiples of 3 reduces the list to
3, 5, 7, 11, 13, 17, 19, 23, 25, 29, 31, 35, 37, 41, 43, 47, 49, 53, 55, 59, 61, 65, 67, 71, 73, 77, 79, 83, 85, 89, 91, 95, 97.
Crossing out multiples of 5 leaves
3, 5, 7, 11, 13, 17, 19, 23, 29, 31, 37, 41, 43, 47, 49, 53, 59, 61, 67, 71, 73, 77, 79, 83, 89, 91, 97.
Finally, crossing out multiples of 7 we have a complete list of primes less than 100:
2, 3, 5, 7, 11, 13, 17, 19, 23, 29, 31, 37, 41, 43, 47, 53, 59, 61, 67, 71, 73, 79, 83, 89, 97.

7. (a)

$\times$	0	1	2	3	4	5	6	7
0	0	0	0	0	0	0	0	0
1	0	1	2	3	4	5	6	7
2	0	2	4	6	0	2	4	6
3	0	3	6	1	4	7	2	5
4	0	4	0	4	0	4	0	4
5	0	5	2	7	4	1	6	3
6	0	6	4	2	0	6	4	2
7	0	7	6	5	4	3	2	1

(b) $1, 3, 5$ and 7.

(c) $13 \equiv 5 \pmod 8$ so $13^2 \equiv 25 \equiv 1 \pmod 8$. Therefore $13^{22} \equiv (13^2)^{11} \equiv 1^{11} \equiv 1 \pmod 8$. Finally $13^{23} \equiv 13 \times 13^{22} \equiv 5 \times 1 \equiv 5 \pmod 8$.

(d) We have $\gcd(10, 18) = 2$ and $2|6$ but $2 \nmid 9$, so (i) has solutions and (ii) does not. There are 2 pairwise incongruent solutions to (i) (using Theorem 5.23). By trial and error we can see that $x = 6$ is a solution to (i). Solutions differ by $18/2 = 9$ so $x = 15$ is the second solution.

8. (a) As $a|b$ and $a|c$ we have $b = au$ and $c = av$, for some $u, v \in \mathbb{Z}$. Therefore $b - c = au - av = a(u - v)$ and so $a|b - c$.

(b) Suppose p is a prime divisor of S. If $p \leq n$ then $p|n!$ (as $n! = 1 \cdots (p-1)p(p+1) \cdots n$). Therefore, from (a) $p|S - n! = 1$. From Lemma 1.18 it follows that $p \leq 1$, which is a contradiction since all primes are greater than 1. Hence all prime divisors p of S satisfy $p > n$.

(c) Suppose there are finitely many primes and let q be the largest. Then let $S = q!+1$. As $S > 1$ it must have a prime divisor p, say. From part (b) we have $p > q$, but this is a contradiction since q is the largest prime. Therefore there are infinitely many primes.

MAS2241: Semester 1 Mock Exam Solutions

9. (a) As a and b divide c we have $c = ax = by$, for some integers x and y. Therefore $a|by$ and as a and b are coprime Euclid's lemma implies that $a|y$. Therefore $y = az$, for some integer z, and we have $c = abz$: that is $ab|c$.

(b) (i) There are integers p and q such that $mp+nq = d$ and substituting for m, n with ud an vd, respectively, gives $udp + vdq = d$. Cancelling d we have $up + vq = 1$, so $\gcd(u, v) = 1$, as required.

(ii) $k = mn/d = (udvd)/d = uvd$. As $m|w$ and $n|w$ we have $w = mg = nh$, for some $h, g \in \mathbb{Z}$, so $w = udg = vdh$. Therefore $w/d = ug = vh$ and so both u and v divide w/d. From part (a) we see that uv divides w/d, so $w/d = uvf$, for some $f \in \mathbb{Z}$. Multiplying through by d we obtain $w = uvdf = kf$, so $k|w$.

(iii) If $r \equiv s \pmod{m}$ and $r \equiv s \pmod{n}$ then $m|s - r$ and $n|s - r$, so $k|s - r$, from part (b)(ii). Therefore $r \equiv s \pmod{k}$.