M 2 4 6

Number Theory

Workbook 1 (without solutions)

Congruences, Congruence Arithmetic and Diophantine Equations

Summer 2013

(originally written and devised by
Trevor Hawkes and Alyson Stibbard;
revised in 2010 by John Cremona)

Aims of these workbooks:

(a) To encourage you to teach yourself mathematics from written material,

(b) To help you develop the art of independent study — working either alone, or cooperatively with other students,

(c) To help you learn a mathematical topic, in this case Number Theory, through calculation and problem-solving.

Copies of this workbook, both with and without solutions, can be found on Mathstuff.

In this course you will constantly get your hands dirty and, we hope, your brain engaged. You will be expected to calculate, to experiment, and to explore, in order to uncover some of the secrets of the counting numbers 1,2,3,.. that have fascinated our ancestors since the dawn of history.

Note: You will need a pocket calculator for some of the questions in the workbooks, and are encouraged to use one for this purpose and to experiment with results and ideas in the course. Calculators are NOT needed and are NOT allowed in tests or in the examination.

Are You Ready?

To understand the material and do the problems in each section of this workbook, you will need to be on good terms with:

Section 1:
- division with remainder (see Workbook 0)
- equivalence relations and equivalence classes
- group axioms

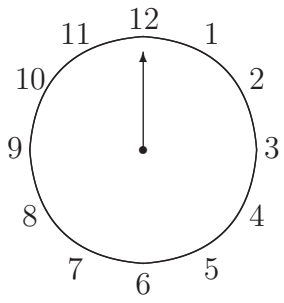
Section 4:
- the Euclidean Algorithm

These workbooks were orginally written and devised by *Trevor Hawkes and and Alyson Stibbard*. *Ben Carr* designed the LaTeX template and *Rob Reid* converted their drafts into elegant print. Over the years, other lecturers and students have corrected a number of typos, mistakes and other infelicities. In 2010 *John Cremona* made some substantial revisions.

Send corrections, ask questions or make comments at the module forum. You can join the MA246 forum by going to `http://forums.warwick.ac.uk/wf/misc/welcome.jsp` and signing in, clicking the *browse* tab, and then following the path: Departments > Maths > Modules > MA2xx modules > MA246 Number Theory.

1 Finite Arithmetic

"The world is a circle without a beginning"
— Lost Horizon



As the hand of the clock sweeps round, the hours keep repeating themselves. In a thousand hours it will still be no more than 12 o'clock (what time will it be?) In this workbook we will think in circles as we apply our minds to finite ("clock") arithmetic.

Some History:
In 1801, when he was only 24 years old, Karl Friedrich Gauss (1777-1855) published a very influential book called *Disquisitiones Arithmeticae* (Latin was still the common language for scientific and scholarly communication in those days). In this book, Gauss lays the foundations of modern number theory. One of many remarkable achievements to be found there is a fully-fledged mathematical framework for the "arithmetic of remainders" (or the "theory of congruences", as it is known today). Gauss was the first to understand and exploit the power of this idea and, importantly, the first to devise a good notation for working with it.

Three Practical Projects for Motivation

(a) Starting only with knowledge of

- today's date and day of the week, and
- your date of birth,

work out on which day of the week you were born. (Answer at the end of this section)

(b) A team of twelve frisbee players stand in a circle looking inwards. They fix a number $a > 0$ and agree always to throw the frisbee to the player a places further round in the circle in the clockwise direction. Thus, when $a = 1$, the frisbee is thrown to the next person on the left.

(i) For which values of a do *all* the players get a turn?

(ii) For the other values of a, which of the players handle the frisbee?

(Answer at the end of Section 2)

(c) Draw a straight line L in the plane $\mathbb{R}^2$.

(i) Does L pass through any "lattice points", i.e. points with integer coordinates?

(ii) How many lattice points does L pass through: just one, finitely many or infinitely many?

(Answer at the end of Section 3)

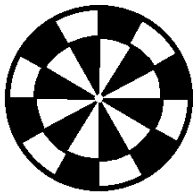
Section Targets

(a) To describe three of the four operations of finite arithmetic:

> *addition*, *subtraction* and *multiplication* modulo n,

where n is some fixed natural number.

(b) To understand the trickier, but more interesting, operation of *division* modulo n.



Parity

The *parity* of an integer is its oddness or evenness. Thus -3 and 10^0 have odd parity, while 0 and 10^6 have even parity.

(1.1) Questions about odd and even integers

(a) Write down two odd integers and note the parity of their sum and their product.

(b) Give a precise definition of an even number and an odd number. Suppose m is even and n is odd. Use your definition to show that $m+n$ is odd and mn is even.

(c) Complete the following addition and multiplication tables:

$+$	even	odd
even		
odd		

$\times$	even	odd
even		
odd		

Answers to (1.1)

(a)

(b)

continued...

(c)

(1.2) Definition Let n be a natural number ($n \in \mathbb{Z}$ and $n > 0$). We say two integers a and b are *congruent modulo* n, and write

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

if n divides $a - b$, or, equivalently, if $a = b + kn$ for some $k \in \mathbb{Z}$.

Examples

$$\begin{aligned} 11 &\equiv 5 \pmod{2} \text{ since } 11 = 5 + 3 \times 2 \\ -5 &\equiv 3 \pmod{4} \text{ since } -5 = 3 + (-2) \times 4 \end{aligned}$$

(1.3) Questions on Congruences

(a) Show that $10^6 \equiv 1 \pmod{7}$ and $-37 \equiv -2 \pmod{5}$.

(b) For the given pairs (x, n) below, find a number r satisfying $x \equiv r \pmod{n}$ and $0 \leq r < n$:

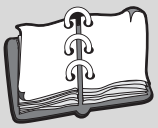
$$(102, 3), \quad (25, 4), \quad (1001, 101), \quad (10^{12}, 9)$$

(Section 2 of Workbook 0 will help.)

(c) For the same pairs (x, n), find an r satisfying

$$\begin{cases} x \equiv r \pmod{n} \\ -n < r \leq 0 \end{cases}$$

(d) Explain how 'division with remainder' shows that each integer is congruent modulo n to one and only one of the integers $0, 1, \ldots, n-1$



Equivalence Relations
Look up the section "Clock Arithmetic"in your *Foundations* (*Sets and Groups*) lecture notes and read the proof that 'congruence modulo n' is an equivalence relation. (Alternatively, just prove it for yourself bearing in mind that an equivalence relation is reflexive, symmetric and transitive.)

Notice that $0 \leq r < n$ iff $0 \leq r \leq n - 1$ since r and n are both integers.

(1.4) Continued...

(e) Find an integer m satisfying $n \leq m \leq n+11$ and $m \equiv 7 \pmod{12}$ in each of the following cases:

(i) $n = 100$

(ii) $n = 10^6$

(iii) $n = -999$

Answers to (1.4)

Division With Remainder
Make sure you have looked at this section in Workbook 0. Given integers a and b you need to know how to find q and r such that $a = qb + r$ and $0 \leq r < b$.

(1.5) Helpful Notation Let n be a fixed natural number and m be an integer. We define

$$n\mathbb{Z} + m = \{nk + m : k \in \mathbb{Z}\}$$

E.g. $2\mathbb{Z} + 1 = \{2k + 1 : k \in \mathbb{Z}\} = \{\pm 1, \pm 3, \pm 5 \ldots\}$ is the set of odd numbers, $10\mathbb{Z} = \{10k : k \in \mathbb{Z}\} = \{0, \pm 10, \pm 20, \ldots\}$ is the set of integers that are divisible by 10.

Note: We write $10\mathbb{Z}$ instead of $10\mathbb{Z} + 0$, and $3\mathbb{Z} - 2$ instead of $3\mathbb{Z} + (-2)$
What's in a name? Two seemingly different expressions can represent the same set, e.g. $2\mathbb{Z}+1$ and $2\mathbb{Z}-1$ both represent the odd numbers, so $2\mathbb{Z} + 1 = 2\mathbb{Z} - 1$.

(1.6) Questions about this notation

(a) Write down two elements from each of the congruence classes $2\mathbb{Z} - 1, 4\mathbb{Z} + 3$ and $7\mathbb{Z}$.

(b) Prove that $m \in n\mathbb{Z} + m$.

(c) Find 3 different values of m such that $4\mathbb{Z} + 3 = 4\mathbb{Z} + m$.

(d) Prove that $n\mathbb{Z} + a = n\mathbb{Z} + b$ iff $a \in n\mathbb{Z} + b$.

(e) Hence show that $n\mathbb{Z} + a = n\mathbb{Z} + b$ iff $a \equiv b \pmod{n}$.

Given a set $n\mathbb{Z} + m$, result (e) tells you that any integer congruent to m can be used to represent it. Equivalently, (d) says that any integer contained in $n\mathbb{Z} + m$ can be used to represent it, so you know at once that $2\mathbb{Z} + 1 = 2\mathbb{Z} + 5297$, since 5297 is odd.

Division with Remainder rides again

The set $n\mathbb{Z}+r$, $(0 \leq r < n)$, is the set of all integers that leave a remainder of r when divided by n.

Answers to (1.6)

The sets $\mathbb{Z}/n\mathbb{Z}$

For a given n, we define the set $\mathbb{Z}/n\mathbb{Z}$ by

$$\mathbb{Z}/n\mathbb{Z} = \{n\mathbb{Z}+m : m \in \mathbb{Z}\}$$

$\mathbb{Z}/n\mathbb{Z}$ is not as big as you might think! Many distinct m determine the same set $n\mathbb{Z}+m$. For instance, once you collapse it down,

$$\mathbb{Z}/4\mathbb{Z} = \{4\mathbb{Z}, 4\mathbb{Z}+1, 4\mathbb{Z}+2, 4\mathbb{Z}+3\}$$

which has only four elements.

(1.7) Further Questions about $n\mathbb{Z}+m$

(a) In each case, find an r satisfying $0 \leq r < 10$ such that $10\mathbb{Z}+111 = 10\mathbb{Z}+r, 10\mathbb{Z}-2 = 10\mathbb{Z}+r$ and $10\mathbb{Z}+10^9 = 10\mathbb{Z}+r$.

(b) Prove that $n\mathbb{Z}+m$ contains a *unique* integer r satisfying $0 \leq r < n$ such that $n\mathbb{Z}+m = n\mathbb{Z}+r$.

(c) For a given n, how many distinct sets of the form $n\mathbb{Z}+m$ are there? What are they? List them for $n = 2$.

(d) Prove that $a \equiv b \pmod{n}$ iff $a, b \in n\mathbb{Z}+r$ for some r satisfying $0 \leq r < n$.

The notation $\mathbb{Z}/n\mathbb{Z}$

N.B. Some people use the notation $\mathbb{Z}_n$ for $\mathbb{Z}/n\mathbb{Z}$, but Number Theorists never do! Other notations used are $\mathbb{Z}/(n)$ or even $\mathbb{Z}/n$. We will use $\mathbb{Z}/n\mathbb{Z}$ in these workbooks.

Answers to (1.7)

Equivalence Classes
If the first sentence in (1.8) makes no sense, return to your Foundations (Sets and Groups) notes and re-read the section on equivalence classes.

(1.8) Congruence Classes The equivalence relation 'congruent modulo n' partitions the set $\mathbb{Z}$ of integers into a set of equivalence classes, called the *congruence classes modulo* n. Each congruence class contains all those integers that are congruent to each other modulo n. From (1.7)(d) we can see that each congruence class is of the form $n\mathbb{Z}+r(0 \leq r < n)$ and that $\mathbb{Z}/n\mathbb{Z} = \{n\mathbb{Z}, n\mathbb{Z}+1, \ldots, n\mathbb{Z}+(n-1)\}$ gives the complete set of congruence classes modulo n.

Example: $\mathbb{Z}/3\mathbb{Z}$
The three congruence classes modulo 3 are

$$3\mathbb{Z} = \{0, \pm 3, \pm 6, \pm 9 \ldots\}$$
$$3\mathbb{Z}+1 = \{\ldots, -2, 1, 4, 7, \ldots\}$$
$$3\mathbb{Z}+2 = \{\ldots, -1, 2, 5, 8, \ldots\}$$

Notice that these sets partition $\mathbb{Z}$.

(1.9) Questions on Congruence Classes

(a) List the congruence classes modulo 4.

(b) Choose an element a from $4\mathbb{Z}+1$ and an element b from $4\mathbb{Z}+3$. Identify the congruence classes modulo 4 containing $a+b, a-b$ and ab.

(c) Now choose new elements α from $4\mathbb{Z}+1$ and β from $4\mathbb{Z}+3$. Identify the congruence classes modulo 4 containing $\alpha+\beta, \alpha-\beta$ and $\alpha\beta$. Compare your answers with (b). What do you notice?

(d) If $a \equiv \alpha \pmod{n}$ and $b \equiv \beta \pmod{n}$, prove that $a+b \equiv \alpha+\beta \pmod{n}, a-b \equiv \alpha-\beta \pmod{n}$ and $ab \equiv \alpha\beta \pmod{n}$.

Hint for (d):
By definition,

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

means $a = \alpha + kn$ for some $k \in \mathbb{Z}$

Answers to (1.9)

'Finite' Arithmetic
We are now in a position to do arithmetic with congruence classes.

(1.10) Adding, subtracting and multiplying congruence classes We now define three binary operations on the set $\mathbb{Z}/n\mathbb{Z}$:

- Addition: $(n\mathbb{Z}+a)+(n\mathbb{Z}+b)=n\mathbb{Z}+(a+b)$
- Subtraction: $(n\mathbb{Z}+a)-(n\mathbb{Z}+b)=n\mathbb{Z}+(a-b)$
- Multiplication: $(n\mathbb{Z}+a)(n\mathbb{Z}+b)=n\mathbb{Z}+ab$

Warning: We can write the congruence class $n\mathbb{Z}+m$ in many ways, e.g. $4\mathbb{Z}+3=4\mathbb{Z}+11=4\mathbb{Z}-9$ and any one of the infinitely many elements in $n\mathbb{Z}+m$ can play the role of the representative m. Since we have used particular representatives to define addition, subtraction and multiplication, we had better check that we get the same answers when any other representatives are used.

Why it Works
The equations here show that the definitions of addition, subtraction and multiplication do not depend on how we represent the congruence classes involved. This is what we mean by saying that the operations are *well-defined*.

(1.11) Questions to show that addition, subtraction, and multiplication are well-defined Assume that a, b, α and β are integers such that

$$\begin{aligned} n\mathbb{Z}+a &= n\mathbb{Z}+\alpha \\ n\mathbb{Z}+b &= n\mathbb{Z}+\beta \end{aligned}$$

Use (1.9)(d) and (1.6)(d) to prove that

- $n\mathbb{Z}+(a+b)=n\mathbb{Z}+(\alpha+\beta)$
- $n\mathbb{Z}+(a-b)=n\mathbb{Z}+(\alpha-\beta)$
- $n\mathbb{Z}+ab=n\mathbb{Z}+\alpha\beta$

Reminder
In (1.6)(e) we proved that

$$n\mathbb{Z}+a=n\mathbb{Z}+b$$

$$\Longleftrightarrow$$

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

Answers to (1.11)

The group structure of $(\mathbb{Z}/n\mathbb{Z}, +)$ depends crucially on the group structure of $(\mathbb{Z}, +)$.

(1.12) Remarks about group structure

(a) We proved in Foundations/Sets and Groups that $(\mathbb{Z}/n\mathbb{Z}, +)$ is a commutative group, with $n\mathbb{Z}$ as the neutral element 0 and $n\mathbb{Z} + (-r)$ the inverse of $n\mathbb{Z} + r$.

(b) Multiplication is a binary operation on $\mathbb{Z}/n\mathbb{Z}$ which satisfies the commutative and associative laws and has a neutral element.

(c) However, when $n > 1$, $\mathbb{Z}/n\mathbb{Z}$ is not a group with respect to multiplication because $n\mathbb{Z}$, the neutral element, does not have an inverse.

(d) The set $(\mathbb{Z}/n\mathbb{Z})^* = \mathbb{Z}/n\mathbb{Z} \setminus \{n\mathbb{Z}\}$ of non-zero classes is a group under multiplication if and only if n is prime. (This fact will be justified later.)

Warning
The symbol r now has two meanings: its usual meaning as the integer r and its new meaning as the congruence class $n\mathbb{Z} + r$ of $\mathbb{Z}/n\mathbb{Z}$.

(1.13) A new notation for the elements of $\mathbb{Z}/n\mathbb{Z}$
We saw in (1.6) that each element $n\mathbb{Z} + m$ of $\mathbb{Z}/n\mathbb{Z}$ contains a unique integer r such that $n\mathbb{Z}+m = n\mathbb{Z}+r$ and $0 \leq r < n$. We now denote the congruence class $n\mathbb{Z} + r$ simply by r, so that

$$\mathbb{Z}/n\mathbb{Z} = \{0, 1, \ldots, n-1\}$$

To avoid ambiguity we need new symbols $+_n$ and $\times_n$ to denote the binary operations of addition and multiplication in $\mathbb{Z}/n\mathbb{Z}$. Thus,

$$\begin{aligned} r +_n s &= n\mathbb{Z} + (r + s) \\ r \times_n s &= n\mathbb{Z} + rs \end{aligned}$$

(1.14) Example

$$\begin{aligned} 12\mathbb{Z} - 3 &= 12\mathbb{Z} + 9 = 9 \\ 12\mathbb{Z} + 20 &= 12\mathbb{Z} + 8 = 8 \\ 9 +_{12} 8 &= 12\mathbb{Z} + 17 = 12\mathbb{Z} + 5 = 5 \\ 9 \times_{12} 8 &= 12\mathbb{Z} + 72 = 12\mathbb{Z} + 0 = 0 \end{aligned}$$

Reminder
In Part (g) of (1.14) the notation $(\mathbb{Z}/5\mathbb{Z})^*$ means the set of four non-zero elements of $\mathbb{Z}/5\mathbb{Z}$.

(1.15) Questions on the new labels $\{0, 1, \ldots, n-1\}$ for the elements of $\mathbb{Z}/n\mathbb{Z}$

(a) Write down the "new labels" for $4\mathbb{Z}+2, 4\mathbb{Z}+3, 4\mathbb{Z}+5$ and $4\mathbb{Z}+6$.

(b) Find the unique r in $(4\mathbb{Z}+2)+(4\mathbb{Z}+3)$ satisfying $0 \leq r \leq 3$.

(c) What is $2 +_4 3$ and $2 \times_4 3$?

(d) Which elements of $\mathbb{Z}/6\mathbb{Z} = \{0, 1, \ldots, 5\}$ represent $1 +_6 2 +_6 \ldots +_6 5$ and $1 \times_6 2 \times_6 \ldots \times_6 5$?

(e) Quickly work out $99 \times_{100} 99 \times_{100} \ldots \times_{100} 99$ (99 terms) in $\mathbb{Z}/100\mathbb{Z}$.

(f) In $\mathbb{Z}/n\mathbb{Z}$, show that $r +_n s$ is either $r+s$ or $r+s-n$.

(g) Using the notation of (1.13), construct the addition table for $(\mathbb{Z}/5\mathbb{Z}, +_5)$ and the multiplication table for $((\mathbb{Z}/5\mathbb{Z})^*, \times_5)$.

Answers to (1.15)

(1.16) We have looked at the arithmetic of congruences from two different viewpoints. The first focused on the congruence classes modulo n as the *objects* to be added, subtracted, multiplied (and later on, divided). The second emphasised a set of labels for the congruence classes $0, 1, \ldots, (n-1)$ which we manipulated according to the standard rule:

Calculate in $\mathbb{Z}$ and reduce modulo n.

The first approach contains an idea of dramatic importance, capable of powerful generalisation throughout mathematics (the idea of a quotient structure). The second approach is just a conventional practical notation for carrying out the calculations implied by the first.

Summary of Section 1

Let n be a natural number.

- The congruence class $n\mathbb{Z}+m$ consists of the (infinitely many) integers that are congruent to m modulo n.
- $n\mathbb{Z} + m = n\mathbb{Z} + s$ for all $s \in n\mathbb{Z} + m$.
- $n\mathbb{Z} + m$ contains a unique integer r satisfying $0 \leq r < m$. Every integer in $n\mathbb{Z} + m$ leaves a remainder r when divided by n.
- The sum of two congruence classes $(n\mathbb{Z} + a) + (n\mathbb{Z} + b)$ is defined to be the congruence class containing $a + b$, namely $n\mathbb{Z} + (a + b)$. The definition does not depend on the choice of the representatives a and b. The same applies to the difference and product.
- If we denote $n\mathbb{Z} + r$ simply by r when $0 \leq r < n$, then $\mathbb{Z}/n\mathbb{Z} = \{0, 1, \ldots, n-1\}$. Furthermore, the sum (difference, product) of two congruence classes described this way is denoted by $+_n$ $(-_n, \times_n)$ to distinguish it from the usual sum (difference, product) of two integers. Thus, for instance,
$$s -_n t = n\mathbb{Z} + (s - t)$$
where s and t on the left hand side of the equation denote elements of $\mathbb{Z}/n\mathbb{Z}$ and on the right-hand side denote ordinary integers.
- In practice, the sum/difference/product of two elements s, t of $\mathbb{Z}/n\mathbb{Z}$ is the remainder when the sum/difference/product of the *integers* s and t is divided by n.

A solution to the birthday problem (by Trevor Hawkes)
I (TOH) will illustrate the solution with my own birthday. I am writing this on Tuesday, 17th March, 1998. I was born on 24th October, 1936. Let's label the days of the week $0, \ldots, 6$ starting with Monday as 0, and suppose that I was born on day d ($0 \leq d \leq 6$). If m days have passed since my birthday, then $m + d \equiv 1 \pmod 7$ since today (Tuesday) is day 1. I need only calculate m modulo 7. Between my birthday and 24th October, 1997 some 61 years have elapsed. The number of days in a normal year is $365 \equiv 1 \pmod 7$ and in a leap year $366 \equiv 2 \pmod 7$. Since 15 of the 61 years were leap years, the number of days from 24/10/36 to 24/10/97 is congruent to

$$15 \times 2 + (61 - 15) = 76 \equiv 6 \pmod 7$$

The number of days from 24/10/97 to today is congruent to 7(for Oct) +2(for Nov) +3(for Dec) +3(for Jan) +0(for Feb) +17(for Mar) $= 32 \equiv 4 \pmod 7$. Putting these two calculations together gives

$$m \equiv 6 + 4 \equiv 3 \pmod 7$$

and so $1 \equiv m + d \equiv 3 + d \pmod 7$. Hence, $d \equiv 1 - 3 = -2 \equiv 5 \pmod 7$, and therefore I was born on day 5 of the week, that is to say a Saturday. (I knew this anyway, because my mother told me that I was "Saturday's child" that "works hard for a living". But using modular arithmetic is less hard work than counting the days on your fingers!)

Exercise Work out the day of the week on which you were born. (Leap years are the ones that are divisible by 4 excepting those divisible by 100 but including those divisible by 400. The year 2000 was a leap year!)

2 Solving Linear Congruences

Motivation: Return to the second project at the start of Section 1. Assign the numbers $0, 1, \ldots, 11$ to the twelve frisbee players, counting in a clockwise direction. Assume that the frisbee starts with player 0 and is always thrown to the player a places to the left (assuming the players are facing inwards). After x turns, the frisbee has moved ax places beyond its starting point and has therefore reached the player whose number is congruent to ax modulo 12. To ensure that every player gets a turn we must be able to solve the congruence

$$ax \equiv b \pmod{12} \tag{2.a}$$

for all values of b between 0 and 11

Section Targets To investigate solutions of the linear congruence

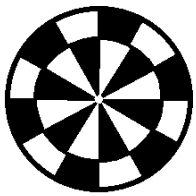
$$ax \equiv b \pmod{n} \tag{2.b}$$

where n is a natural number. (By a *solution* we mean an integral value of x satisfying this congruence for given integers a and b.) Specifically, we will do these things:

(a) Decide for what values of a and n there is a solution for *all* possible values of b. (In frisbee terms, this amounts to deciding for what number of players and what length of throw we are guaranteed that each player will get a turn.)

(b) Given a, b and n, decide *whether or not* there is a solution x. (This amounts to deciding whether a *particular* player in a given frisbee game will get a turn.)

(c) Given a, b and n, determine *how many* solutions there are. (This amounts to determining *how many turns* a given player will get.)



Note: If $r \equiv s \pmod{n}$, then $rx \equiv sx \pmod{n}$. Hence, for instance, $71x \equiv x \pmod{7}$.

(2.1) Questions on some special cases of (2.b)

(a) By trial and error or simple cunning, find a solution to the following congruences whenever a solutions exists.

(i) $2x \equiv 3 \pmod{5}$

(ii) $2x \equiv 3 \pmod{6}$

(iii) $771x \equiv 71 \pmod{7}$

(iv) $22x \equiv 1 \pmod{23}$

(b) If x_0 is the solution you found to congruence (i), check whether x_0+5 and x_0-5 are also solutions. Deduce that (i) has infinitely many solutions.

(c) Describe *all* the solutions to congruence (iv) in part (a).

Observe that the congruence

$$x \equiv y \pmod{n}$$

is equivalent to

$$-x \equiv -y \pmod{n}.$$

Answers to (2.1)

(a)(i)

(ii)

(iii)

(iv)

(b)

(c)

(2.2) Questions on linear congruences with no solution

(a) Find values of b for which the following linear congruences have *no* solutions;

(i) $3x \equiv b \pmod 6$

(ii) $14x \equiv b \pmod 7$

(iii) $4x \equiv b \pmod 8$

(iv) $10x \equiv b \pmod{30}$

(b) Now find all values of b for which the four congruences in (a) *do* have solutions.

Answers to (2.2)

A pattern is emerging here. Try to formulate a necessary and sufficient condition for the congruence $ax \equiv b \pmod n$ to have a solution.

The following idea will give us a useful way of looking at the congruence $ax \equiv b \pmod n$:

A *residue* is an old-fashioned word for a 'remainder'.

(2.3) Definition Let n be a natural number. A *complete set of residues modulo* n is a subset S of $\mathbb{Z}$ containing exactly one element from each of the distinct congruence classes,

$$n\mathbb{Z}, n\mathbb{Z}+1, \ldots, n\mathbb{Z}+n-1$$

Evidently $S = \{0, 1, \ldots, n-1\}$ is a complete set of residues modulo n.

Hint for (c)
Suppose $a \in \mathbb{Z}$. Then

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

for some $0 \leq r < n$. It follows from (1.9)(d) that $a^2 = r^2$ for some $0 \leq r < n$.

(2.4) Questions on complete sets of residues

(a) Which of the following sets form a complete set of residues modulo 5?

(i) $\{-5, -4, -3, -2, -1\}$

(ii) $\{11, 22, 33, 44, 55\}$

(iii) $\{0, -1, 2, -3, 4\}$

(iv) $\{1^2, 2^2, 3^2, 4^2, 5^2\}$

(b) Find a complete set of residues modulo 6

(i) lying in the range $(-110, -101)$,

(ii) consisting of integers differing from each other by at least 100, and

(iii) lying in an arithmetic progression with common difference 7.

(c) Is there a complete set of residues modulo p consisting of perfect squares

(i) when $p = 7$?

(ii) for any prime p?

Answers to (2.4)

(a)(i)

(ii)

(iii)

(iv)

(b)(i)

(ii)

(iii)

(c)(i)

(ii)

(2.5) Question characterising a complete set of residues (CSR) Let $n \in \mathbb{N}$ and $S \subseteq \mathbb{Z}$. Prove that the following two conditions are together necessary and sufficient for S to be a CSR modulo n.

(a) $|S| = n$ and

(b) no two elements of S are congruent modulo n.

Answer to (2.5)

Something to note:
If $b \equiv \beta \pmod{n}$ then $ax \equiv \beta \pmod{n}$ iff $ax \equiv b \pmod{n}$. Furthermore, if $a \equiv \alpha \pmod{n}$ and $x \equiv y \pmod{n}$ then $ax \equiv \alpha y$ by 1.7. It follows that $ax \equiv b \pmod{n}$ iff $\alpha y \equiv b \pmod{n}$.

Given a, b and n, we wish to decide whether the linear congruence

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

has solutions. A key step in working this out is to first decide for what values of a and n the congruence

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

has a solution x for *all* b. To make life easier, we notice that the problem does not change if a, b and x are replaced with congruent values (mod n). (For a justification of this statement, see the box on the left.) When convenient, we can assume without loss of generality that a, b or x all lie in the set $S_n = \{0, 1, 2, \ldots, n-1\}$, i.e. that $0 \leq a, b, x \leq n-1$.

Now back to the problem of deciding when $ax \equiv b \pmod{n}$ has a solution for all b. First notice that if we multiply the elements of $S_n = \{0, 1, 2, \ldots, n-1\}$ by a we get a new set,

$$aS_n = \{0, a, 2a, \ldots, (n-1)a\}$$

and so there will be solutions $x \in S_n$ for *all* choices of $b \in S_n$ iff aS_n contains elements congruent to each element of S_n, in other words iff aS_n is a complete set of residues modulo n.

A matter of terminology
The **h**ighest **c**ommon **f**actor (hcf) is also known as the **g**reatest **c**ommon **d**ivisor (gcd):

$\text{hcf}\{a, b\} = \text{hcf}(a, b) = \gcd(a, b)$.

(2.6) Questions on when aS_n is a complete set of residues Let $n \in \mathbb{N}$ and let $S_n = \{0, 1, \ldots, n-1\}$ denote the *basic set of residues modulo* n.

(a) For each of the following values of n compute the set

$$aS_n = \{0, a, 2a, \ldots, (n-1)a\}$$

for each $a \in S_n$ and find all values of a for which aS_n is a complete set of residues modulo n.

(i) $n = 4$ (ii) $n = 5$ (iii) $n = 6$

(b) Use your calculations to decide whether the following equations have a solution for all $b \in S_n$ and to find the value of x corresponding to each b when a such solution exists.

(i) $3x \equiv b \pmod 4$

(ii) $3x \equiv b \pmod 5$

(iii) $3x \equiv b \pmod 6$

(c) For $n = 4, 5, 6$ calculate $\text{hcf}\{a, n\}$ for the values of a where,

(i) aS_n is a complete set of residues (CSR)

(ii) aS_n is *not* a CSR.

(d) Make a conjecture for a condition on a and n that ensures the congruence $ax \equiv b \pmod n$ has a solution for all $b \in S_n$.

Note our use of the notation $\{0, 2, 4, 8\} \equiv \{0, 2\}$ to mean that the elements of the first set are all congruent modulo $n = 4$ to the elements in the second set.
To save space, let's agree to write,

$$x \equiv y \ (n)$$

instead of

$$x \equiv y \pmod n$$

in future.

Answers to (2.6)

(a)(i)

continued. . .

(a)(ii)

(iii)

(b)(i)

(ii)

(iii)

continued...

(c)

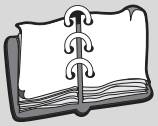
(d)

We now want to prove the following:

Be careful!
The hypothesis that $\text{hcf}\{a, n\} = 1$ is essential! Try $a = b = 2$ and $n = 4$.

(2.7) Lemma *Let a and n be integers with $\text{hcf}\{a, n\} = 1$. Then*

n divides ab if and only if n divides b.



Euclidean Algorithm
This gives you a procedure for finding the highest common factor of two numbers. You can read about it in your Foundations notes. One consequence of the Euclidean algorithm is that if a and b are integers, then there exist integers u and v such that

$$\text{hcf}\{a, b\} = ua + vb$$

At the end of this workbook we will revisit the Euclidean Algorithm and give an efficient way of carrying it out.

We could appeal to the Fundamental Theorem of Arithmetic (FTA), factorising a and b in products of prime powers and observing that the condition $\text{hcf}\{a, n\} = 1$ implies that the primes involved in n are distinct from those involved in a. Then uniqueness of factorisation in the equation,

$$mn = ab$$

forces the prime powers in a to appear as prime powers in m. But we are using a sledgehammer to crack a nut. A better approach (because it is both shorter and more basic) is to use the following consequence of the Euclidean algorithm (which is also used in a standard proof of the FTA):

There exist integers u and v such that

$$ua + vn = \text{hcf}\{a, n\} = 1 \qquad (2.c)$$

Hint: If n divides ab, then n divides $uab + vnb$.

(2.8) Question Prove Lemma 2.7

Answer to (2.8)

We are now ready to prove the following theorem:

(2.9) Theorem *Let $n \in \mathbb{N}$ and let $a, b \in \mathbb{Z}$. The linear congruence,*

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

has a solution for all values of b if and only if $\text{hcf}\{a, n\} = 1$.

By a contrapositive argument, Step 1 shows that if $ax \equiv b \pmod{n}$ has a solution *for all* b, then $\text{hcf}\{a, b\} = 1$.

(2.10) Question leading to a proof of Theorem 2.9 Fill in the details of the following proof:
Step 1: If $d = \text{hcf}\{a, n\} > 1$ then d does not divide $ax - 1$ and so $ax \equiv 1(n)$ has no solution.
Step 2: If $\text{hcf}\{a, n\} = 1$, then the elements of $aS_n = \{0, a, 2a, \ldots, (n-1)a\}$ are pairwise incongruent modulo n.
Step 3: Hence the set aS_n is a complete set of residues.
Step 4: Therefore $ax \equiv b \pmod{n}$ has a solution for each $b \in \mathbb{Z}$.

Answers to (2.10)

We can now give the complete answer to the question, "when does the linear congruence $ax \equiv b \pmod{n}$ have a solution?"

(2.11) Theorem *Let $n \in \mathbb{N}$ and let $a, b \in \mathbb{Z}$. The linear congruence*

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

has a solution if and only if

$$\text{hcf}\{a, n\} \text{ divides } b \tag{2.d}$$

(2.12) Question leading to a proof of Theorem 2.11 Fill in the details of the following proof: Let $d = \text{hcf}\{a, n\}$ and write $a = da_0$ and $n = dn_0$, observing that $\text{hcf}\{a_0, n_0\} = 1$ (convince yourself of this).
Step 1: If $ax \equiv b(n)$ for some $x \in \mathbb{Z}$, show that d divides ax and $ax - b$ and hence that d divides b.
Step 2: Now suppose that d divides b and write $b = db_0$. Show that $ax \equiv b(n)$ if and only if

$$a_0 x \equiv b_0(n_0) \tag{2.e}$$

Step 3: Use Theorem 2.9 to conclude the proof.

Answers to (2.12)

Summary of Section 2

During the section, we worked steadily towards a necessary and sufficient condition for the linear congruence

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

to have a solution $x \in \mathbb{Z}$, and came up with the answer: There exists a solution iff

$$\text{hcf}\{a, n\} \text{ divides } b$$

We also discovered that $ax \equiv b \pmod{n}$ has a solution *for all* b iff $\text{hcf}\{a, n\} = 1$. On the way we introduced and explored the fruitful idea of a Complete Set of Residues (CSR) modulo n. We also used a consequence of the Euclidean algorithm to prove that if n divides ab and $\text{hcf}\{a, n\} = 1$, then n divides b.

Solution to the Frisbee Problem
We can now answer the question formulated at the beginning of this section in relation to Project (b). Every player gets a turn iff the congruence,

$$ax \equiv b \pmod{12}$$

has a solution for all $b \in \{0, 1, \ldots, 11\}$. By Theorem 2.9, this happens when $\text{hcf}\{a, 12\} = 1$, i.e. for all a that are coprime with 12. These are precisely the integers in the congruence classes

$$12\mathbb{Z} + 1, \quad 12\mathbb{Z} + 5, \quad 12\mathbb{Z} + 7, \quad 12\mathbb{Z} + 11.$$

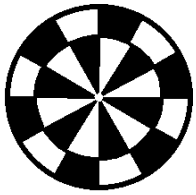
Thus, everyone gets a turn if and only if the frisbee is consistently thrown either $1, 5, 7$ or 11 places round the circle (in either direction).
Now decide, for the remaining values of a, which players get a turn.

3 Solving Linear Diophantine Equations

Motivation: In this section we shift our focus from solving a *linear congruence* of the form $ax \equiv b \pmod{n}$ to solving a *Linear Diophantine Equation* of the form

$$ax + by = c. \tag{3.a}$$

Here "Diophantine" just means that we are seeking solutions which are *integers*.



Section Targets To investigate solutions of the linear Diophantine equation

$$ax + by = c$$

where a, b, c are given integers, and only *integral* solutions x, y are of interest.

Specifically, we will do two things:

(a) Decide for what values of a, b and c there is a solution.

(b) Given a, b and c, describe the general solution.

The task of actually finding the solutions when they exist will be left to the final section.

(3.1) Question on passing between congruences and equations

(a) The congruence $3x \equiv 7 \pmod{11}$ has the solutions $x = 6$. Write down a solution (x, y) to the equation $3x + 11y = 7$ in which $x = 6$.

(b) The equation $3x + 11y = 7$ also has the solution $(x, y) = (-5, 2)$. What is the corresponding solution to the congruence $3x \equiv 7 \pmod{11}$?

(c) Show that for every $k \in \mathbb{Z}$, $(x, y) = (-5+11k, 2-3k)$ is a solution to the equation $3x + 11y = 7$. Which k gives the solution in (a)?

(d) Do all solutions to the equation have this form? If so, prove it.

Answers to (3.1)

(a)

(b)

(c)

(d)

The following theorem should now be obvious:

(3.2) Theorem *Let $n \in \mathbb{N}$ and let $a, b \in \mathbb{Z}$. There is a bijection between*

(a) *The set of solutions $x \in \mathbb{Z}$ to the linear congruence $ax \equiv b \pmod{n}$; and*

(b) *The set of solutions $(x, y) \in \mathbb{Z}^2$ to the linear equation $ax + ny = b$.*

With this new viewpoint we can reinterpret the main theorem of the previous section (Theorem 2.11), changing notation slightly:

(3.3) Theorem *Let $a, b, c \in \mathbb{Z}$. The equation*

$$ax + by = c$$

has a solution $(x, y) \in \mathbb{Z}^2$ if and only if $\mathrm{hcf}(a, b) \mid c$.

Easy facts about hcf**:**
$\mathrm{hcf}(\pm a, \pm b) = \mathrm{hcf}(a, b)$.
$\mathrm{hcf}(\pm a, 0) = |a|$.
$\mathrm{hcf}(a, b) = \mathrm{hcf}(b, a)$.
$\mathrm{hcf}(0, 0) = 0$.

Proof If $b = 0$ this just says that $ax = c$ has a solution if and only if $a \mid c$, which is obvious by definition. Otherwise, let $n = |b| \in \mathbb{N}$; every solution (x, y) gives $x \in \mathbb{Z}$ satisfying $ax \equiv c \pmod{n}$, so $\mathrm{hcf}(a, b) = \mathrm{hcf}(a, n) \mid c$ (by Theorem 2.11), and conversely by Theorem 3.2.

We now turn to the question of *uniqueness* of solutions. A congruence such as $ax \equiv b \pmod{n}$ will *never* have a unique integer solution (or even finitely many) since if x is a solution then so is $x + kn$ for all $k \in \mathbb{Z}$. When counting solutions to a congruence, therefore, we only count as distinct solutions which are *incongruent* modulo the modulus. (Equivalently, we only count solutions x satisfying $0 \leq x < n$ where n is the modulus.)

We could alternatively describe the general solution to (a) by $x \equiv 4 \pmod{5}$, since $4 + 5\mathbb{Z}$ is the union of $4 + 10\mathbb{Z}$ and $9 + 10\mathbb{Z}$. This is more concise, but hides the fact that the original congruence was modulo 10 and that there are *two* solutions modulo 10.

Examples

(a) Consider $4x \equiv 6 \pmod{10}$. The solutions x with $0 \leq x < 10$ are $x = 4$ and $x = 9$, so x is a solution if and only if $x \equiv 4 \pmod{10}$ or $x \equiv 9 \pmod{10}$. The number of solutions is 2.

(b) Consider $17x \equiv 37 \pmod{101}$. This has *one* solution: since $\mathrm{hcf}(17, 101) = 1$ (both 17 and 101 are prime!), $\{17x \mid 0 \leq x < 101\}$ is a CSR modulo 101, so $17x \equiv b \pmod{101}$ has a unique solution for every b.

The last example is the simplest situation. As in Theorem 2.11, when $\mathrm{hcf}(a, n) = 1$ there is always a solution to $ax \equiv b \pmod{n}$, and the proof of Theorem 2.11 shows that it is unique.

(3.4) Theorem *Let $n \in \mathbb{N}$ and let $a \in \mathbb{Z}$ with* $\mathrm{hcf}(a, n) = 1$. *Then for all $b \in \mathbb{Z}$ the congruence $ax \equiv b \pmod{n}$ has a* unique *solution modulo n.*

(3.5) Let $n = 9$.

(a) Fill in the following table: all entries should be in the range $0 \ldots 8$.

x (mod 9)	0	1	2	3	4	5	6	7	8
$4x \equiv$	0	4				2			
$6x \equiv$	0	6				3			

(b) What property does the map $x \mapsto 4x$ from $\mathbb{Z}/9\mathbb{Z}$ to itself have, which the map $x \mapsto 6x$ does not have?

(c) Use your table to solve $4x \equiv b \pmod 9$ for $b = 5, 6$ and 7.

(d) Use your table to solve $6x \equiv 3 \pmod 9$.

Answer to (3.5)

(a)

(b)

(c)

(d)

An equivalent way of stating Theorem 3.4 is to say that when $\mathrm{hcf}(a, n) = 1$, then for each $b \in \mathbb{Z}$:

(a) there exists a solution x_0 to $ax \equiv b \pmod n$;

(b) the general solution is $x = x_0 + kn$ for $k \in \mathbb{Z}$, in the sense that $x_0 + kn$ is a solution for all k and every solution has this form.

Converting this to a statement about linear equations gives the following:

(3.6) Theorem *Let $a, b \in \mathbb{Z}$ be coprime. Then for all $c \in \mathbb{Z}$ the equation $ax + by = c$ has a solution $(x, y) \in \mathbb{Z}^2$. If (x_0, y_0) is any one solution then the general solution is $(x, y) = (x_0 + kb, y_0 - ka) = (x_0, y_0) + k(b, -a)$ for $k \in \mathbb{Z}$.*

(3.7) Illustrations of Theorem 3.6

(a) Write down one solution (x_0, y_0) to $5x + 7y = -3$.

(b) Now write down the general solution.

(c) Repeat parts (a) and (b) with the equation $6x - 11y = 2$.

Answer to (3.7)

(a)

(b)

(c)

Does every line in $\mathbb{R}^2$ have such an equation with $a, b, c \in \mathbb{Z}$? with $a, b, c \in \mathbb{Q}$? If not, try to give conditions on L which ensure that it does have such an equation. [Thinking about the slope of L might help.]

Geometric interpretation: The equation $ax+by = c$ is the equation of a straight line L in the plane $\mathbb{R}^2$ (provided that a and b are not both 0). Since we want *integer* solutions for x and y, we are asking whether L passes through any of the *integer points* (also called *lattice points*) $(x, y) \in \mathbb{Z}^2 \subset \mathbb{R}^2$.
There may be none: for example the line $2x + 4y = 5$ can have no integer points [why?]. Theorem 3.3 says that the obvious *necessary* condition that $\text{hcf}(a, b) \mid c$ is also sufficient for integer solutions to exist. Theorem 3.6 says that when a, b are coprime then there are always infinitely many integer points on the line L, which are evenly spaced along it: from any one such point (x_0, y_0) one can get to all others by taking "steps" along the vector $(b, -a)$ (or in the reverse direction).

Theorems 3.4 and 3.6 only cover the simplest case, but the general case easily reduces to this.

(3.8)

(a) Consider the congruence $6x \equiv 3 \pmod{15}$.

1. Find $\text{hcf}(6, 15)$.
2. Deduce that solutions exist.
3. Find one solution.
4. Find *all* solutions x with $0 \leq x < 15$. How many are there? What was $\text{hcf}(6, 15)$ again?

(b) Repeat part (a) with the congruence $15x \equiv 10 \pmod{20}$.

Answer to (3.8)

(a)

(b)

(3.9) Theorem *Let $n \in \mathbb{N}$ and let $a, b \in \mathbb{Z}$. Set $h = \text{hcf}(a, n)$, and assume that $h \mid b$. Then the congruence $ax \equiv b \pmod{n}$ has precisely h solutions (only counting as distinct solutions which are incongruent modulo n). Moreover, if x_0 is any one solution then the complete set of solutions is $\{x_0 + kn/h \mid 0 \leq k < h\}$.*

Make sure you understand this.

Proof Write $a = ha_0$, $n = hn_0$, $b = hb_0$. Then $ax \equiv b \pmod{n} \Leftrightarrow a_0 x \equiv b_0 \pmod{n_0}$. Since $\text{hcf}(a_0, n_0) = 1$, there is a unique solution modulo n_0 by Theorem 3.4. If x_0 is a solution then the general solution has the form $x = x_0 + kn_0$; taking $0 \leq k < h$ gives the distinct solutions modulo n.

(3.10) In each case give the number of solutions, and list the solutions with $0 \leq x < n$ in each case, where n is the modulus):

(a) $4x \equiv 8 \pmod{12}$.

(b) $15x \equiv 3 \pmod{18}$.

Answer to (3.10)

(a)

(b)

(3.11) Theorem *Let $a, b, c \in \mathbb{Z}$, with a, b not both zero. Set $h = \mathrm{hcf}(a, b)$, and assume that $h \mid c$, so that the equation $ax + by = c$ has a solution $(x_0, y_0) \in \mathbb{Z}^2$ by Theorem 3.3. Then the general solution is $(x, y) = (x_0 + kb/h, y_0 - ka/h) = (x_0, y_0) + k(b/h, -a/h)$ for $k \in \mathbb{Z}$.*

Proof Write $a = ha_0$, $b = hb_0$, $c = hc_0$. Then $ax + by = c \Leftrightarrow a_0x + b_0y = c_0$, and the general solution to this is $(x_0 + kb_0, y_0 - ka_0)$ by Theorem 3.6

(3.12) In each case give the general solution, using the particular solution given:

(a) $12x + 18y = 66$; $(4, 1)$.

(b) $26x + 91y = 39$; $(-2, 1)$.

Answer to (3.12)

(a)

(b)

In the final section we will see how to find the particular solution in an efficient and straightforward way.

Summary of Section 3

In this section, we saw that there was a precise correspondence between solutions of a linear congruence

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

and solutions of a linear Diophantine Equation

$$ax + by = c.$$

Using this and the results of the previous sections we proved that the equation has a solution if and only if

$$\text{hcf}\{a, b\} \text{ divides } c,$$

and we found the general solution when this condition is satisfied.
We also gave a geometric interpretation of this result in terms of lattice points lying on a straight line in the plane.

4 Numerical techniques

Section Targets In this section we turn from the theory of linear congruences and linear Diophantine Equations to how one actually solves them in practice. The key is the (extended) Euclidean Algorithm, which you met before in Foundations (Sections 3 and 4.1 of the Foundations lecture notes).
Specifically, we will first show how, given integers a and b, to:

(a) use the *Euclidean Algorithm* (EA) to compute $h = \text{hcf}(a, b)$ (also called $\gcd(a, b)$);

(b) use the *Extended Euclidean Algorithm* (EEA) to also compute x, y such that

$$ax + by = h = \text{hcf}(a, b).$$

Then we show how to find one solution to either a linear congruence $ax \equiv b \pmod{n}$ or a linear Diophantine equation $ax + by = c$, and also find the general solution. Specifically, we will develop general methods for the following problems:

(c) Given a, b and n:

(i) determine whether or not the linear congruence $ax \equiv b \pmod{n}$ has a solution;

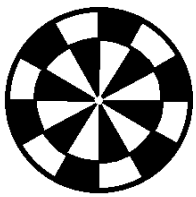
(ii) if so, find one solution, and the general solution.

(d) Given a, b and c:

(i) determine whether or not the linear Diophantine equation $ax + by = c$ has a solution (x, y);

(ii) if so, find one solution, and the general solution.

The techniques developed here will also be useful in Workbooks 4 and 5.



We may as well assume that $a, b > 0$ since $\mathrm{hcf}(\pm a, \pm b) = \mathrm{hcf}(a, b)$ and $\mathrm{hcf}(\pm a, 0) = |a|$.

The standard layout for the Euclidean Algorithm is usually shown like this:

$$\begin{array}{rcll} a & = & q_0 b + r_1 & 0 \leq r_1 < b \\ b & = & q_1 r_1 + r_2 & 0 \leq r_2 < r_1 \\ r_1 & = & q_2 r_2 + r_3 & 0 \leq r_3 < r_2 \\ \vdots & \vdots & \vdots \; \vdots \; \vdots & \vdots \; \vdots \\ r_{t-2} & = & q_{t-1} r_{t-1} + r_t & 0 \leq r_t < r_{t-1} \\ r_{t-1} & = & q_t r_t & \end{array}$$

For example, when $a = 89$ and $b = 49$ this looks like

$$\begin{aligned} 89 &= 1 \times 49 + 40 \\ 49 &= 1 \times 40 + 9 \\ 40 &= 4 \times 9 + 4 \\ 9 &= 2 \times 4 + 1 \\ 4 &= 4 \times 1. \end{aligned}$$

There is a lot of repetition in writing this out. A more concise form is just to write two columns:

$$\begin{array}{cc} a & q_0 \\ b & q_1 \\ r_1 & q_2 \\ \vdots & \vdots \\ r_{t-2} & q_{t-1} \\ r_{t-1} & q_t \\ r_t & \end{array}$$

The left column is the *remainder sequence* (r), starting with a, b and ending with the last non-zero remainder r_t which is $\mathrm{hcf}(a, b)$. The right column is the *quotient sequence* (q), which you do not even need to write down if all you want is the value of $\mathrm{hcf}(a, b)$. (We will need the quotients for the Extended Euclidean Algorithm, EEA.) In the example this looks like this:

$$\begin{array}{cc} (r) & (q) \\ 89 & 1 \\ 49 & 1 \\ 40 & 4 \\ 9 & 2 \\ 4 & 4 \\ 1 & \end{array}$$

At each step you divide one number in the left column by the one below it, write the quotient to its right and the remainder underneath; then move down one row. Stop when the remainder is 0, which you do not need to write down, but you should write down the last quotient (which is 4 in this case).

This is already enough to find $\mathrm{hcf}(a, b)$: it is the last entry in the left column. In our example, $\mathrm{hcf}(89, 49) = 1$.

(r)	(q)
78	0
123	1
78	1
45	1
33	2
12	1
9	3
3	

(4.1) Here is another example, with $a = 78$ and $b = 123$, where the hcf is not 1, and the first quotient is 0 (since $a < b$): So $\text{hcf}(78, 123) = 3$.

(4.2) Use the concise layout to compute $\text{hcf}(123, 456)$.

Answer to (4.2)

Now we come to the EEA. While the EA allows us to decide on the existence of solutions to linear congruences and equations, the EEA will allow us to actually find solutions when they exist. There are also many further applications, which we will see in later workbooks.

What we do is this. To the columns of remainders and quotients in the EA layout we add two more columns, labelled u and v. For example:

(r)	(q)	(u)	(v)	$(au - bv)$
		1	0	89
89	1	0	1	-49
49	1	1	1	40
40	4	1	2	-9
9	2	5	9	4
4	4	11	20	-1
1		49	89	0

Here we have also included a 5th column labelled $au - bv$ which will help up keep track of what is happening, but which we do not need to include in practice. Notice that this 5th column is the same as the r column but with alternating signs and shifted one row.

What is the rule for producing the u and v sequences? For u, we start with $1, 0$ and

then repeatedly use the general formula

$$u_n = q_n u_{n-1} + u_{n-2}.$$

For the v sequence we start with $0, 1$ and use the same recurrence:

$$v_n = q_n v_{n-1} + v_{n-2}.$$

This is simpler in practice than it sounds: start the u and v columns off with $\begin{matrix} 1 & 0 \\ 0 & 1 \end{matrix}$ (looking like a 2×2 identity matrix), with the bottom row aligned with the first row of r, q values. To get each row from the previous ones, use the recurrence relations: multiply each u value by the q next to it, add to the u above; this gives the next u. Do exactly the same for the vs. For example, the entry 9 in the v column comes from $9 = 4 \times 2 + 1$ using the preceding values $v = 2$ and $v = 1$ and the value $q = 4$ next to $v = 2$.

Note that the u and v columns only depend on the qs and not the rs. To see that the values of $au - bv$ are the same as the r values but with alternating sign, note that this is obviously true for the first two rows; and an induction proof can be used to show that it remains true. As a consequence, in the last but one row we have $au - bv = \pm h$ since $h = \text{hcf}(a, b)$ is the final r value. (Also, in the very last row we have $au - bv = 0$, which can be useful as a check.)

So to solve $ax + by = h = \text{hcf}(a, b)$ we simple put $(x, y) = (u, -v)$ or $(x, y) = (-u, v)$ depending on the parity of the number of rows used.

Here is another example:

EEA for $a = 78$, $b = 123$:

(r)	(q)	(u)	(v)
		1	0
78	0	0	1
123	1	1	0
78	1	1	1
45	1	2	1
33	2	3	2
12	1	8	5
9	3	11	7
3		41	26

(4.3) From the table we take $(u, v) = (11, 7)$ and find $au - bv = 78 \cdot 11 - 123 \cdot 7 = -3$, so $h = 3 = ax + by$ with $(x, y) = (-u, v) = (-11, 7)$.
The very last row in the u, v columns is not needed, but serves as a check since the values here satisfy $au - bv = 0$: in fact $u = b/h$ and $v = a/h$. (The reduced form of the fraction 78/123 is therefore 26/41.)

(4.4) Practice with the EEA Use this method to solve

(a) $16x + 83y = 1$;

(b) $355x + 113y = 1$;

(c) $377x + 233y = 1$.

What does (b) have to do with π?
What does (c) have to do with rabbits?

Answer to (4.4)

(a)

(b)

(c)

We now put everything together into a general method for solving either $ax \equiv b \pmod{n}$ or $ax + by = c$.

(4.5) To solve $ax \equiv b \pmod{n}$

(a) Compute $h = \text{hcf}(a, n)$ using EA.

(b) Test whether $h \mid b$; no solutions if not. If $h \mid b$:

(c) Write $h = ax_0 + ny_0$ using EEA.

(d) One solution is $x_1 = x_0 b/h$; the general solution is $x \equiv x_1 \pmod{n/h}$, and the h solutions modulo n are $x = x_1 + kn/h$ for $0 \leq k < h$.

Note that once you have checked $h \mid b$ it is probably easier to divide through by h and solve $(a/h)x \equiv (b/h) \pmod{n/h}$ since the numbers are smaller.

(4.6) Practice solving linear congruences Use this method to solve

(a) $19x \equiv 30 \pmod{40}$;

(b) $9x \equiv 5 \pmod{25}$;

(c) $103x \equiv 444 \pmod{999}$;

(d) $980x \equiv 1500 \pmod{1600}$.

Answer to (4.6)

(a)

(b)

(c)

continued. . .

(d)

(4.7) To solve $ax + by = c$

(a) Compute $h = \text{hcf}(a, b)$ using EA.

(b) Test whether $h \mid c$; no solutions if not. If $h \mid c$:

(c) Write $h = ax_0 + by_0$ using EEA.

(d) One solution is $(x_1, y_1) = (x_0c/h, y_0c/h)$; the general solution is

$$(x, y) = (x_1, y_1) + k(b/h, -a/h).$$

The general solution may also be written as

$$x = (cx_0 + kb)/h, \qquad y = (cy_0 - ka)/h.$$

Note that once you have checked $h \mid c$ it is probably easier to divide through by h and solve $(a/h)x + (b/h)y = (c/h)$ since the numbers are smaller.

(4.8) Practice solving linear Diophantine Equations Use this method to solve

(a) $2x + 5y = 11$;

(b) $17x + 13y = 100$;

(c) $21x + 14y = 147$;

(d) $60x + 18y = 97$;

(e) $1402x + 1969y = 1$.

In each case it is fine to divide out by any common factors you notice, and to use an obvious base solution if you spot one. The general method is there to help in hard cases, not to make easy cases harder!

Answers to (4.8)

(a)

(b)

(c)

(d)

continued...

(e)

Summary of Section 4

In this section, we reviewed the Euclidean Algorithm (EA), and the Extended Euclidean Algorithm (EEA), showing a simple concise way to set these out for computation.
We then showed how to use the EA to determine whether both linear congruences

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

and linear Diophantine Equations

$$ax + by = c$$

have solutions, and how to use the EEA to find their solutions (including the general solution) when solutions exist.