

Unit 3

Number theory

Introduction

Number theory is a branch of mathematics concerned with properties of the integers,

$$\dots, -2, -1, 0, 1, 2, 3, \dots$$

The study of number theory goes back at least to the Ancient Greeks, who investigated the *prime numbers*,

$$2, 3, 5, 7, 11, 13, 17, \dots,$$

which are those integers greater than 1 with the property that each integer is divisible only by itself and 1.

The foundations of modern number theory were laid out by the eminent German mathematician Carl Friedrich Gauss, in his influential book *Disquisitiones Arithmeticae* (published in 1801). This text, which builds on the work of other number theorists such as Fermat, Euler, Lagrange and Legendre, was written when Gauss was only 21 years old!

Number theory continues to flourish today and it attracts popular attention through its many famous unsolved problems. Among these is *Goldbach's conjecture*, which asserts that every even integer greater than 2 can be written as the sum of two prime numbers. The German mathematician Christian Goldbach (1690–1764) made this conjecture in 1742, and yet it remains unproved today (although it has been verified by computer for all even integers up to 10^{14}).

Other famous conjectures in number theory have been proved in recent years, notably *Fermat's last theorem*, which says that it is impossible to find positive integers a , b and c that satisfy

$$a^n + b^n = c^n, \quad \text{where } n \text{ is an integer greater than } 2.$$

This assertion was made by the French lawyer and gifted amateur mathematician Pierre de Fermat. Fermat wrote in his copy of the classic Greek text *Arithmetica* that he had a truly wonderful proof of the assertion, but the margin was too narrow to contain it. After years of effort, with contributions by many mathematicians, the conjecture was finally proved in 1994, by the British mathematician Andrew Wiles (1953–). This proof is over 150 pages long and uses many new results so it seems highly unlikely that Fermat really did have a proof of his last theorem!

The early parts of Gauss's *Disquisitiones Arithmeticae* are about *congruences*, which are mathematical statements used to compare the remainders when two integers are each divided by another integer. Much of this unit is about congruences, and arithmetic involving congruences, which is known as *modular arithmetic*.

Modular arithmetic is sometimes described as 'clock arithmetic' because it is similar to the arithmetic you perform on a 12-hour clock. For example, if it is 9 o'clock now then in 5 hours' time it will be 2 o'clock, as illustrated



Carl Friedrich Gauss
(1777–1855)



Pierre de Fermat (c. 1601–65)

by the clocks in Figure 1 (in which the hour hands, but not the minute hands, are shown).

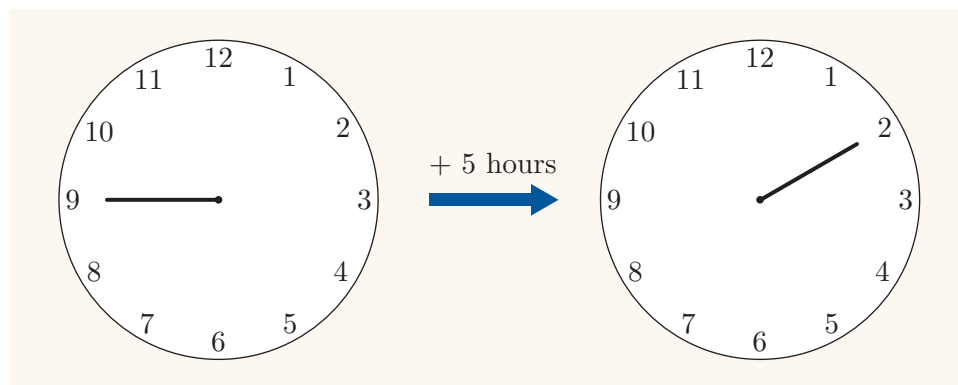


Figure 1 The left-hand clock shows 9 o'clock and the right-hand clock shows 5 hours later, 2 o'clock

The main goal of this unit is for you to become proficient at modular arithmetic, without the use of a calculator. In fact, you can put your calculator away, because you won't need it here at all.

There are many useful applications of modular arithmetic, and you'll see a selection of these later on. For instance, you'll learn about strategies using modular arithmetic for testing whether one integer is divisible by another. After reading about this, you'll be able to determine quickly whether the number

48 015 253 835 029

is divisible by 9.

You'll also find out how modular arithmetic is used to help prevent errors in identification numbers, such as the International Standard Book Number (ISBN) of a modern edition of *Disquisitiones Arithmeticae*, shown in Figure 2. The last digit of that ISBN, namely 6, is a 'check digit', which can be found from the other digits using modular arithmetic.

At the very end of the unit, you'll get a taste of how modular arithmetic is used to create secure means of disguising messages in the subject of *cryptography*. This subject is of particular importance in the modern era because of the large amount of sensitive data that is transferred electronically. You'll learn about a collection of processes for disguising information called *affine ciphers*, which, although relatively insecure, share many of the features of more complex processes in cryptography.



Figure 2 ISBN of *Disquisitiones Arithmeticae*

1 Euclid's algorithm and congruences

Central to this section is the observation that when you divide one integer by another, you are left with a remainder, which may be 0. You'll see how this observation is applied repeatedly in an important technique called *Euclid's algorithm*, which can be used to obtain the highest common factor of two integers. Towards the end of the section, you'll learn about an effective way of communicating properties of remainders using statements called *congruences*.

1.1 The division theorem

Let's begin by reminding ourselves of some terminology about numbers. The **integers** are the numbers

$$\dots, -2, -1, 0, 1, 2, 3, \dots,$$

and the **positive integers** or **natural numbers** are

$$1, 2, 3, \dots$$

It can be useful to represent the integers by equally spaced points on a straight line, as shown in Figure 3. This straight line is known as the **number line**. There are other points on the number line that don't correspond to integers, such as $1/2$, $\sqrt{3}$ or π , but in this unit we'll focus most of our attention on integers.

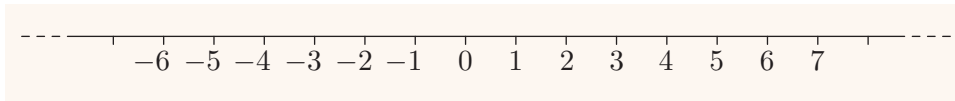


Figure 3 The integers on the number line

An integer a is said to be **divisible** by a positive integer n if there is a third integer k such that $a = nk$. We also say that a is a **multiple** of n , or n is a **factor** or **divisor** of a . For example, 84 is a multiple of 12; also 84 is divisible by 12, and 12 is a factor or divisor of 84. In fact, $84 = 12 \times 7$. Sometimes mathematicians write $n|a$ to mean that a is divisible by n , but that notation won't be used in this module.

Now consider the integers 38 and 5. Clearly, 38 is not a multiple of 5; in fact,

$$7 \times 5 < 38 < 8 \times 5,$$

or equivalently,

$$7 < \frac{38}{5} < 8.$$

We have 'trapped' $38/5$ between two consecutive integers 7 and 8. The integer 7 on the left is known as the *quotient* on dividing 38 by 5.

Since $7 \times 5 = 35$, we see that 38 is 3 more than a multiple of 5. The number 3 is known as the *remainder* on dividing 38 by 5. You can write

$$\begin{array}{ccc} 38 = 7 \times 5 + 3. \\ \uparrow \quad \quad \uparrow \\ \text{quotient} \quad \text{remainder} \end{array}$$

This equation is represented on the number line in Figure 4.

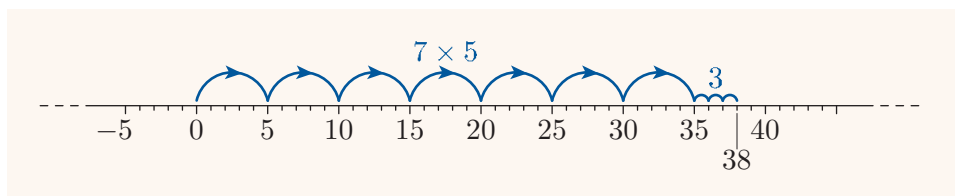


Figure 4 Dividing 38 by 5 on the number line

You obtain a quotient and remainder in this way whenever you divide one positive integer a by another positive integer n . The remainder is 0 if a is divisible by n , and otherwise it is a positive integer less than n .

Let's suppose now that a is *negative*. For example, suppose you wish to divide -38 by 5. You can trap $-38/5$ between two consecutive integers as follows:

$$-8 < -\frac{38}{5} < -7.$$

Once again, the quotient is the integer on the *left*, namely -8 . The remainder is then the difference between $-8 \times 5 = -40$ and -38 , namely 2. You can write

$$\begin{array}{ccc} -38 = (-8) \times 5 + 2. \\ \uparrow \quad \quad \uparrow \\ \text{quotient} \quad \text{remainder} \end{array}$$

This equation is represented on the number line in Figure 5.

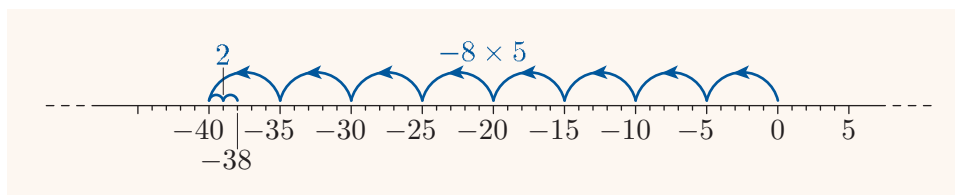


Figure 5 Dividing -38 by 5 on the number line

This time, the quotient is negative (the first eight jumps are to the left, rather than to the right), but it is chosen so that the remainder is still positive. The reason why we choose the quotient in this way to give a positive remainder is because this choice simplifies Euclid's algorithm, which you'll meet in the next subsection.

These observations about division can be summarised in **the division theorem**, sometimes known as **the division algorithm**, stated below. You can also find the division theorem and all the other important facts, definitions and techniques from this module in the MST125 *Handbook*.

The division theorem

Suppose that a is an integer and n is a positive integer. Then there are unique integers q and r such that

$$a = qn + r \quad \text{and} \quad 0 \leq r < n.$$

As you've learned already, the integer q is called the **quotient** of the division, and r is called the **remainder**. When $a = 29$ and $n = 7$, for example,

$$4 < \frac{29}{7} < 5,$$

so the quotient is 4. Or when $a = -29$ and $n = 7$, for example,

$$-5 < -\frac{29}{7} < -4,$$

so the quotient is -5 . Once you've found the quotient, you can then find the remainder by rearranging $a = qn + r$ to give $r = a - qn$. The remainder satisfies $0 \leq r < n$, so, in particular, it is always positive or 0. It is 0 when a is divisible by n .

**Example 1** *Finding quotients and remainders*

For each of the following numbers a and n , find the quotient q and the remainder r when you divide a by n , and write down the equation $a = qn + r$.

(a) $a = 32, \quad n = 9$ (b) $a = -32, \quad n = 9$

Solution

- (a) Observe that $3 < 32/9 < 4$. The quotient is the left-hand value.

$$q = 3,$$

- Find the remainder using $r = a - qn$.

$$r = 32 - 3 \times 9 = 5,$$

- Write down the equation $a = qn + r$.

and so

$$32 = 3 \times 9 + 5.$$

- (b) Observe that $-4 < -32/9 < -3$. The quotient is the left-hand value.

$$q = -4,$$

- Find the remainder using $r = a - qn$.

$$r = -32 - (-4) \times 9 = 4,$$

- Write down the equation $a = qn + r$.

and so

$$-32 = -4 \times 9 + 4.$$

Activity 1 *Finding quotients and remainders*

For each of the following numbers a and n , find the quotient and remainder when you divide a by n , and write down the equation $a = qn + r$.

- (a) $a = 59, \quad n = 7$ (b) $a = 84, \quad n = 12$ (c) $a = 100, \quad n = 9$
 (d) $a = 9, \quad n = 100$ (e) $a = 0, \quad n = 11$ (f) $a = -58, \quad n = 5$
 (g) $a = -100, \quad n = 9$ (h) $a = -96, \quad n = 12$ (i) $a = -4, \quad n = 5$

1.2 Euclid's algorithm

The **highest common factor** (HCF), or **greatest common divisor**, of two integers a and b is the greatest positive integer n that is a divisor of both a and b . For instance, the HCF of 18 and 30 is 6, because 6 is a divisor of both 18 and 30, and no integer greater than 6 is a divisor of both 18 and 30.

This subsection is about a procedure, known as Euclid's algorithm ('Euclid' is pronounced 'you-clid'), for finding the HCF of two integers. This important procedure is widely used in fields such as algebra, computer science and cryptography.

Euclid's Elements

Euclid was a Greek mathematician who worked in Alexandria around 300 BC. His most famous work was the influential textbook *Elements*, in which geometry is developed rigorously from a few foundational principles. *Elements* also contains some number theory, including observations about prime numbers and the procedure now known as Euclid's algorithm. The oldest complete text of *Elements* dates from the ninth century AD and is kept in the Bodleian library in Oxford.



A fragment of Euclid's *Elements*, dating from around 100 AD

An **algorithm** is a step-by-step procedure. One algorithm for finding the highest common factor of two integers involves finding the **prime factorisation** of each integer; that is, writing each integer as a product of prime numbers. Consider, for example, the two integers 252 and 120. Their prime factorisations are

$$252 = 2 \times 2 \times 3 \times 3 \times 7 \quad \text{and} \quad 120 = 2 \times 2 \times 2 \times 3 \times 5.$$

Now examine the prime factors of 252 and 120 one by one, and each time you find a factor that occurs in both factorisations place a circle round each of the matching factors, making sure that you ignore factors that are already circled. You obtain

$$252 = \textcircled{2} \times \textcircled{2} \times \textcircled{3} \times 3 \times 7 \quad \text{and} \quad 120 = \textcircled{2} \times \textcircled{2} \times 2 \times \textcircled{3} \times 5.$$

The product of the circled primes give the highest common factor, namely $2 \times 2 \times 3 = 12$. This method works well for small numbers like 252 and 120, but calculating prime factorisations of larger numbers can be a lengthy task. In fact, huge numbers with hundreds of digits often cannot be factorised into primes using even the most powerful computers in existence.

Euclid's algorithm is a much faster way of working out the highest common factor of two integers. In fact, if you apply the algorithm to the integers 252 and 120 then it produces the HCF so quickly that it's hard to get a good idea of how the method works! Here's a description of the algorithm for the pair of integers 207 and 60. The first step is to apply the

division theorem to write down an expression of the form $207 = q \times 60 + r$. You find that

$$207 = 3 \times 60 + 27.$$

Ignore the quotient 3 for now, and instead focus on 60 (the smaller of our original pair of integers), and the remainder 27. Apply the division theorem to these two integers to obtain

$$60 = 2 \times 27 + 6.$$

Again, ignore the quotient 2, and apply the division theorem to 27 and 6 to obtain

$$27 = 4 \times 6 + 3.$$

Then apply the division theorem to 6 and 3 to obtain

$$6 = 2 \times 3 + 0.$$

Now stop, because you have obtained a remainder 0. In practice, you should list the equations one under another:

$$\begin{array}{r} 207 = 3 \times 60 + 27 \\ 60 = 2 \times 27 + 6 \\ 27 = 4 \times 6 + 3 \\ 6 = 2 \times 3 + 0. \end{array}$$

With each step of Euclid's algorithm, the remainders decrease. This is because, for example, in the second step the remainder 6 is the remainder on dividing 60 by 27 and must therefore be less than 27 which is the remainder from the first step. It follows that there will eventually be a final step with remainder 0.

The remainder in the second-to-last step, which in this case is 3, is the highest common factor of our original integers 207 and 60 (as you'll see shortly).

You've now seen a description of how to apply Euclid's algorithm but haven't seen an explanation of why it works. In order to get a better understanding of why it works, first write down the pairs of integers used at each stage of the algorithm:

$$207, 60 \longrightarrow 60, 27 \longrightarrow 27, 6 \longrightarrow 6, 3.$$

The HCF of the pair 207, 60 is the same as the HCF of the pair 60, 27. To see why this is so, recall the first equation from Euclid's algorithm:

$$207 = 3 \times 60 + 27.$$

If 207 and 60 are both divisible by an integer n , then 3×60 is also divisible by n . This implies that $207 - 3 \times 60$ is divisible by n . So 27, which is equal to $207 - 3 \times 60$, is divisible by n as well. Therefore any factor of both 207 and 60 is also a factor of both 60 and 27. Using the same kind of argument you can see that any factor of both 60 and 27 is also a factor of both 207 and 60. It follows that the HCF of 207 and 60 is equal to the HCF of 60 and 27.

With similar reasoning, you find that each pair of integers in the chain of arrows has the same HCF. The HCF of the final pair is 3, which is the remainder obtained in the second-to-last step of Euclid's algorithm. Therefore this remainder 3 is the HCF of 207 and 60.

Strategy:

To find a highest common factor using Euclid's algorithm

Suppose that a and b are positive integers.

1. By applying the division theorem repeatedly, form a list of equations:

$$\begin{array}{rcl}
 a & = & q_1 b + r_1 \\
 b & = & q_2 r_1 + r_2 \\
 r_1 & = & q_3 r_2 + r_3 \\
 r_2 & = & q_4 r_3 + r_4 \\
 r_3 & = & q_5 r_4 + r_5 \\
 \vdots & & \vdots
 \end{array}$$

2. Stop when you obtain an equation in which the remainder is 0.
3. The highest common factor of a and b is the remainder in the second-to-last equation.


Example 2 *Using Euclid's algorithm to find an HCF*

Find the highest common factor of 209 and 78.

Solution

Apply the division theorem repeatedly until a remainder of 0 is obtained.

Euclid's algorithm gives

$$209 = 2 \times 78 + 53$$

$$78 = 1 \times 53 + 25$$

$$53 = 2 \times 25 + 3$$

$$25 = 8 \times 3 + 1$$

$$3 = 3 \times 1 + 0.$$

The highest common factor is the remainder found in the second-to-last equation.

So the highest common factor of 209 and 78 is 1.

In this example, we could have omitted the last equation as we know that the remainders decrease at each stage. So, once we obtain a remainder of 1, we know that the remainder at the next stage must be 0 and so the highest common factor must be 1.

Activity 2 *Using Euclid's algorithm to find HCFs*

Using Euclid's algorithm, find the highest common factor of each of the following pairs of integers.

- (a) 93 and 21 (b) 138 and 61 (c) 231 and 49

1.3 Bézout's identity

One of the many uses of Euclid's algorithm is to establish **Bézout's identity** ('Bézout' is pronounced 'beh-zoot').

Bézout's identity

Suppose that a and b are integers, not both 0, and let d be their highest common factor. Then there are integers v and w such that

$$av + bw = d.$$

For example, 2 is the highest common factor of 14 and 10, and

$$14 \times 3 + 10 \times (-4) = 2.$$

Like Euclid's algorithm, Bézout's identity is an extremely useful tool. You will need it later on when studying division in modular arithmetic.

Bézout's identity is named after the French mathematician Étienne Bézout. In fact, Bézout proved a more general result than the one given here, which was proved much earlier by another French mathematician, Claude Gaspard Bachet de Méziriac (1581–1638). Both Bachet's result and Bézout's more general result are usually referred to as Bézout's identity (or Bézout's lemma). As well as making important contributions to algebra, Bézout also wrote popular textbooks. Among these is the six-volume work *Cours complet de mathématiques*, published between 1770 and 1782. These books were used by students taking the entrance exams of the prestigious École Polytechnique in France, and they were also translated from French to English and employed by institutions such as Harvard University.



Étienne Bézout (1730–83)

Let's work out how to find the integers v and w in Bézout's identity for the pair of integers 207 and 60 considered earlier. The same method works whenever a and b are positive integers. Towards the end of this subsection you'll learn how to find v and w when a and b are not both positive.

We found that the HCF of 207 and 60 is 3, so we need v and w to satisfy

$$207v + 60w = 3.$$

First write down the steps of Euclid's algorithm again, omitting the final step, with remainder 0:

$$207 = 3 \times 60 + 27$$

$$60 = 2 \times 27 + 6$$

$$27 = 4 \times 6 + 3.$$

It is helpful to circle all the numbers apart from the quotients, like so:

$$\textcircled{207} = 3 \times \textcircled{60} + \textcircled{27}$$

$$\textcircled{60} = 2 \times \textcircled{27} + \textcircled{6}$$

$$\textcircled{27} = 4 \times \textcircled{6} + \textcircled{3}.$$

Now rearrange each of these three equations to make the remainders on the right the subjects of the equations:

$$\textcircled{27} = \textcircled{207} - 3 \times \textcircled{60}$$

$$\textcircled{6} = \textcircled{60} - 2 \times \textcircled{27}$$

$$\textcircled{3} = \textcircled{27} - 4 \times \textcircled{6}.$$

Next we use a process known as **backwards substitution**, in which we substitute into the bottom equation each of the expressions given on the right-hand side of this list of equations, working upwards one equation at a time. In doing this, we never combine the circled numbers with other numbers to simplify them: for example, we write $3 \times \textcircled{60}$ rather than 180, even though $3 \times 60 = 180$. The circles help you to remember not to simplify; think of a circled number as a variable.

Let's carry out backwards substitution. First substitute the expression for $\textcircled{6}$ from the second equation into the third equation:

$$\textcircled{3} = \textcircled{27} - 4 \times \left(\textcircled{60} - 2 \times \textcircled{27} \right).$$

This reduces to

$$\textcircled{3} = 9 \times \textcircled{27} - 4 \times \textcircled{60}.$$

Now substitute the expression for $\textcircled{27}$ from the first equation into this equation:

$$\textcircled{3} = 9 \times \left(\textcircled{207} - 3 \times \textcircled{60} \right) - 4 \times \textcircled{60}.$$

This reduces to

$$\textcircled{3} = 9 \times \textcircled{207} - 31 \times \textcircled{60}.$$

This equation is of the form described by Bézout's identity, namely,

$$207v + 60w = 3,$$

where $v = 9$ and $w = -31$.

(Check: $207 \times 9 + 60 \times (-31) = 1863 - 1860 = 3$.)

When calculating the integers v and w in Bézout's identity, you don't have to circle numbers as we have done here, although you may find that doing so avoids confusion.

Here's another example.

Example 3 *Finding integers v and w with $av + bw = d$ when a and b are both positive*

Find the highest common factor d of 185 and 49, and then find integers v and w such that $185v + 49w = d$.

Solution

 Apply Euclid's algorithm. 

Euclid's algorithm gives



$$185 = 3 \times 49 + 38$$

$$49 = 1 \times 38 + 11$$



$$38 = 3 \times 11 + 5$$

$$11 = 2 \times 5 + 1$$

$$5 = 5 \times 1 + 0.$$

 The highest common factor is the remainder found in the second-to-last step. 

So the highest common factor of 185 and 49 is 1.

 Rearrange all but the last equation to make the remainder the subject of each equation. 



Rearranging the equations gives

$$(38) = (185) - 3 \times (49)$$

$$(11) = (49) - 1 \times (38)$$

$$(5) = (38) - 3 \times (11)$$

$$(1) = (11) - 2 \times (5).$$

 Use backwards substitution to find integers v and w with $185v + 49w = 1$. First substitute the third equation into the fourth equation and simplify. 

Backwards substitution gives

$$\begin{aligned} (1) &= (11) - 2 \times ((38) - 3 \times (11)) \\ &= 7 \times (11) - 2 \times (38). \end{aligned}$$



Substitute the second equation into this expression and simplify.

$$\begin{aligned}
 &= 7 \times ((49) - 1 \times (38)) - 2 \times (38) \\
 &= 7 \times (49) - 9 \times (38)
 \end{aligned}$$

Substitute the first equation into this expression and simplify.

$$\begin{aligned}
 &= 7 \times (49) - 9 \times ((185) - 3 \times (49)) \\
 &= 34 \times (49) - 9 \times (185)
 \end{aligned}$$

So $185 \times (-9) + 49 \times 34 = 1$.

(Check: $185 \times (-9) + 49 \times 34 = -1665 + 1666 = 1$.)

Try the following activities, remembering to check your answers.

Activity 3 Finding integers v and w with $av + bw = d$ when a and b are both positive

- Find the highest common factor d of 93 and 42, and then find integers v and w such that $93v + 42w = d$.
- Find the highest common factor d of 70 and 29, and then find integers v and w such that $70v + 29w = d$.

So far in this subsection you've learned how to apply Euclid's algorithm and backwards substitution with *positive* integers a and b to obtain the equation $av + bw = d$ of Bézout's identity.

The next example shows you how to obtain the equation $av + bw = d$ when the integers a and b are not both positive.



Example 4 Finding integers v and w with $av + bw = d$ when a and b are not both positive

Find the highest common factor d of 126 and -33 , and then find integers v and w such that $126v - 33w = d$.

Solution

The HCF of 126 and -33 is the same as the HCF of the *positive* integers 126 and 33, which you can find using Euclid's algorithm.

Euclid's algorithm gives

$$126 = 3 \times 33 + 27$$

$$33 = 1 \times 27 + 6$$

$$27 = 4 \times 6 + 3$$

$$6 = 2 \times 3 + 0.$$

So the HCF of 126 and 33 is 3, and hence the HCF of 126 and -33 is also 3.

To find integers v and w such that $126v - 33w = d$, you should begin by finding integers v' and w' such that $126v' + 33w' = d$ in the usual way. First rearrange all but the last equation above to make the remainder the subject of each equation.

Rearranging the equations gives

$$(27) = (126) - 3 \times (33)$$

$$(6) = (33) - 1 \times (27)$$

$$(3) = (27) - 4 \times (6).$$

Apply backwards substitution.

Backwards substitution gives

$$\begin{aligned} (3) &= (27) - 4 \times ((33) - 1 \times (27)) \\ &= 5 \times (27) - 4 \times (33) \\ &= 5 \times ((126) - 3 \times (33)) - 4 \times (33) \\ &= 5 \times (126) - 19 \times (33). \end{aligned}$$

☁ Rearrange the equation obtained above into the form $126v - 33w = d$. ☁

So

$$126 \times 5 - 33 \times 19 = 3.$$

This is the equation $126v - 33w = d$ with $v = 5$ and $w = 19$.

(Check: $126 \times 5 - 33 \times 19 = 630 - 627 = 3$.)

Activity 4 Finding integers v and w with $av + bw = d$ when a and b are not both positive

- Find the highest common factor d of -112 and -91 , and then find integers v and w such that $-112v - 91w = d$.
- Find the highest common factor d of -105 and 39 , and then find integers v and w such that $-105v + 39w = d$.

Here's a puzzle that you might like to try to solve using Euclid's algorithm and backwards substitution.

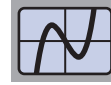
Activity 5 Using Euclid's algorithm and backwards substitution to solve a puzzle



Suppose you have two buckets of capacities 23 litres and 16 litres, and a cauldron, which has capacity over 200 litres. You are able to fill the buckets with water from a tap. By using these buckets, you can obtain certain quantities of water in the cauldron. For example, you could obtain 7 litres of water in the cauldron by filling the 23-litre bucket from the tap and pouring it into the cauldron, and then filling the 16-litre bucket from the cauldron and emptying it out.

Is it possible to use a similar method to obtain exactly 1 litre of water in the cauldron? If so, describe how you would do this.

When working through many of the activities in this section, you'll have carried out several calculations. In the next activity you'll see how you can use the computer algebra system to carry out such calculations more quickly. This can be especially helpful when you're working with large numbers.

Activity 6 Using the computer algebra system for number theory

Work through Section 4 of the *Computer algebra guide*.

1.4 Congruences

In this subsection you'll learn about a useful way of comparing the remainders of two integers, called a *congruence*. Later on, congruences will be used in *modular arithmetic*. This type of arithmetic is central to number theory, and it also has applications in other disciplines, as you'll see.

Before discussing the full definition of a congruence, let's first look at a special case.

Two integers a and b are said to be **congruent modulo 5** if they each have the same remainder on division by 5. For example, 7 and 22 are congruent modulo 5 because each has remainder 2 on division by 5. The integers 7 and 22 are marked on the number line in Figure 6. You can see that they are congruent modulo 5 because they each lie two places to the right of a multiple of 5.

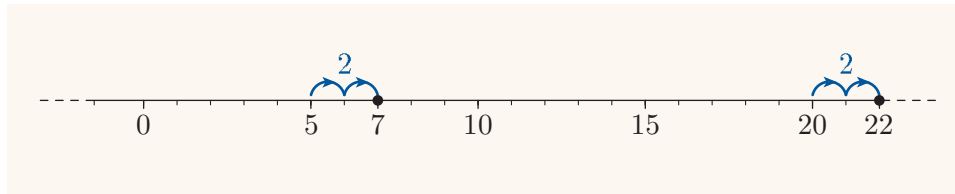


Figure 6 The integers 7 and 22 are congruent modulo 5

In contrast, the integers -12 and 6 are not congruent modulo 5 because -12 has remainder 3 on division by 5 whereas 6 has remainder 1 on division by 5. The integers -12 and 6 are marked on the number line in Figure 7. You can see that they are not congruent modulo 5 because -12 lies three places to the right of a multiple of 5 whereas 6 lies only one place to the right of a multiple of 5.

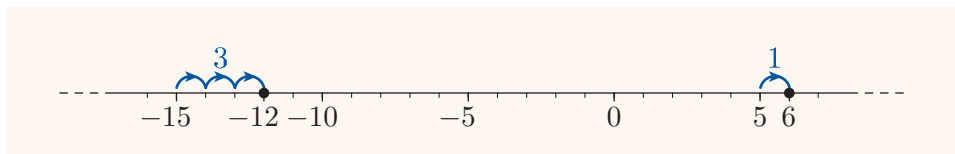


Figure 7 The integers -12 and 6 are not congruent modulo 5

The full definition of what it means to be congruent modulo n is similar to the definition of what it means to be congruent modulo 5, but with a positive integer n instead of 5.

Congruences

Let n be a positive integer. Two integers a and b are **congruent modulo n** if they each have the same remainder on division by n . If this is so then you write

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

Such a statement is called a **congruence**.

For example, 19 and 12 are congruent modulo 7; that is,

$$19 \equiv 12 \pmod{7},$$

because 19 and 12 each have remainder 5 on division by 7. Also, -8 and 10 are congruent modulo 6; that is,

$$-8 \equiv 10 \pmod{6},$$

because -8 and 10 each have remainder 4 on division by 6. The integers -8 and 10 are marked on the number line shown in Figure 8. You can see that they are congruent modulo 6 because they each lie four places to the right of a multiple of 6.

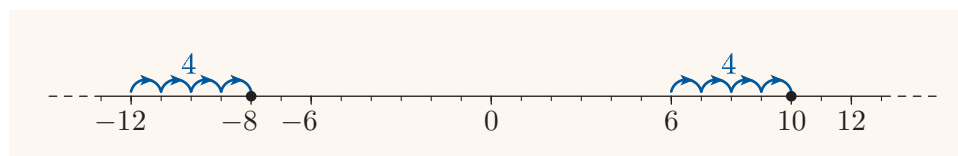


Figure 8 The integers -8 and 10 are congruent modulo 6

It is important to remember when working with congruences that to find the remainder of a negative integer such as -8 , on division by a positive integer n , you must find the multiple of n immediately to the *left* of -8 on the number line, and from this multiple of n count the number of places to the *right* you must move to get to -8 . You'll get plenty of practice at finding remainders of negative integers in the rest of this unit.

Activity 7 *Checking congruences*

Which of the following congruences are true?

- (a) $11 \equiv 26 \pmod{5}$ (b) $9 \equiv -9 \pmod{5}$
 (c) $28 \equiv 0 \pmod{7}$ (d) $-4 \equiv -18 \pmod{7}$
 (e) $-8 \equiv 5 \pmod{13}$ (f) $38 \equiv 0 \pmod{13}$

When working through this activity, you may have noticed that the congruence

$$a \equiv 0 \pmod{n},$$

which says that a has remainder 0 on division by n , is the same as the statement that a is divisible by n . For example,

$$24 \equiv 0 \pmod{6}$$

because 24 is divisible by 6.

The word ‘congruent’ means ‘in agreement’. The term makes its first appearance in modular arithmetic in Gauss’s *Disquisitiones Arithmeticae*, which features in the introduction to this unit, although it was used much earlier than this by geometers. Gauss chose the symbol \equiv because it is similar, but not identical, to the more familiar equals symbol $=$. Congruences share many properties with, but are not identical to, equations.

For the next activity, which is about congruences modulo 10, remember that the **digits** of an integer are the numbers $0, 1, 2, \dots, 9$ that make up that integer. The digits of 7238, for example, are 7, 2, 3 and 8.

Activity 8 *Understanding congruences modulo 10*

- (a) Suppose that a and b are *positive* integers. By comparing the final digits of a and b , can you determine whether they are congruent modulo 10?
- (b) Does the method suggested in (a) work if a is a positive integer but b is a negative integer?

In Activity 7, you checked whether two integers were congruent modulo n by finding their remainders modulo n . There is an alternative method for checking congruences, which is usually easier to apply.

Alternative method for checking congruences

The following statements are equivalent:

- a and b are congruent modulo n
- $a - b$ is divisible by n .

So to check whether two integers a and b are congruent modulo n you can check the second of these statements rather than the first.

For example, according to this alternative method, 27 and 12 are congruent modulo 5 because $27 - 12 = 15$, which is divisible by 5. In contrast, 9 and -4 are not congruent modulo 7 because $9 - (-4) = 13$, which is not divisible by 7. In fact, 27 and 12 both have remainder 2 on division by 5 so they are indeed congruent modulo 5. Also, 9 has remainder 2 and -4 has remainder 3 on division by 7, so it is true that 9 and -4 are not congruent modulo 7.

To understand why this alternative method works, you may find it is helpful to think of a number line.

If two integers a and b are congruent modulo n , then they have the same remainder modulo n . So the distance between a and b on the number line is an integer multiple of n . This distance is equal to $a - b$ when $a \geq b$, and to $b - a = -(a - b)$ when $b > a$. In either case, it follows that $a - b$ is divisible by n .

Similarly, if a and b are *not* congruent modulo n , then the distance between a and b is not an integer multiple of n ; that is, $a - b$ is *not* divisible by n .

You can practise using the alternative method in the next activity. It will help you to remember that you can either test whether $a - b$ is divisible by n , or test whether $b - a$ is divisible by n , because the two tests are equivalent.

Activity 9 Checking congruences using the alternative method

Which of the following congruences are true and which are false?

- (a) $63 \equiv 14 \pmod{7}$ (b) $-39 \equiv 39 \pmod{7}$
 (c) $63 \equiv 14 \pmod{12}$ (d) $-8 \equiv 16 \pmod{12}$
 (e) $-30 \equiv -17 \pmod{13}$ (f) $43 \equiv -87 \pmod{13}$

Another way of stating that $a - b$ is divisible by n is to state that there is an integer k (which may be negative) such that

$$a - b = kn;$$

that is,

$$a = b + kn.$$

This useful observation allows you to replace a congruence by an equation.

Writing a congruence as an equation

The congruence $a \equiv b \pmod{n}$ is equivalent to the statement that there is an integer k such that

$$a = b + nk.$$

For example, the congruence $7 \equiv 22 \pmod{5}$ is equivalent to the statement that there is an integer k such that

$$7 = 22 + 5k.$$

There certainly is such an integer k , namely $k = -3$.

You should use this technique to approach the next activity.

Activity 10 *Understanding congruences modulo 2*

Explain why every odd number is congruent to 1 modulo 2. Explain why every even number is congruent to 0 modulo 2.

Let's finish this subsection with three basic properties of congruences, some of which you may have assumed to hold already. You might have realised, for example, that it is equivalent to write

$$3 \equiv 7 \pmod{4} \quad \text{or} \quad 7 \equiv 3 \pmod{4}.$$

This follows from the second property in the next box.

Properties of congruences

- $a \equiv a \pmod{n}$
- if $a \equiv b \pmod{n}$ then $b \equiv a \pmod{n}$
- if $a \equiv b \pmod{n}$ and $b \equiv c \pmod{n}$, then $a \equiv c \pmod{n}$

The first property just says that a has the same remainder as itself on division by n . The second property is true because both congruences say that a and b have the same remainder on division by n . The final property says that if a and b have the same remainder on division by n , and b and c have the same remainder on division by n , then this is also true of a and c .

The three properties are known, in order, as **reflexivity**, **symmetry** and **transitivity** of congruences. You won't need these terms in this module, but they are important mathematical concepts which you may meet again in the future.

You'll find that you use these properties of congruences without explicitly thinking about them. The third property shows, for example, that instead of writing

$$9 \equiv 2 \pmod{7} \quad \text{and} \quad 2 \equiv -5 \pmod{7},$$

it makes sense to write

$$9 \equiv 2 \equiv -5 \pmod{7}.$$

You can join several congruences together in this way, and only include \pmod{n} at the very end.

Activity 11 *Checking congruences involving several integers*

Which of the following statements are true and which are false? (All of the congruences in a statement must be true in order for the whole statement to be true.)

- (a) $-7 \equiv 7 \equiv 17 \pmod{10}$ (b) $-17 \equiv 3 \equiv 31 \equiv 67 \pmod{2}$
 (c) $-84 \equiv 0 \equiv 108 \pmod{12}$

1.5 Residue classes

You have already seen that many integers have the same remainder on division by a positive integer n . For example, you saw that all the odd numbers are congruent to 1 modulo 2 and all the even numbers are congruent to 0 modulo 2. The odd integers are sometimes described as the *residue class* of 1 modulo 2. More generally, we have the following definition.

Residue class

Given any integer a , the collection of all integers congruent to a modulo n is known as the **residue class**, or **congruence class**, of a modulo n .

The word ‘residue’ means ‘remainder’. This term is used because the residue class of a modulo n is the class of those integers that have the same remainder on division by n as a does. For example, the residue class of 1 modulo 3 is shown on the number line in Figure 9.

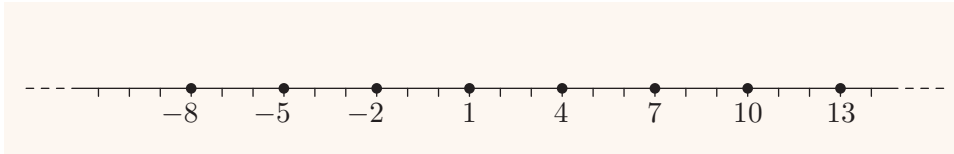


Figure 9 The residue class of 1 modulo 3

Because 1, 4 and -2 are all congruent modulo 3, you could also describe the class of integers marked in Figure 9 as the residue class of 4 modulo 3, or as the residue class of -2 modulo 3.

Figure 10 shows the residue class of 0 modulo 3. These are the integers that are divisible by 3.

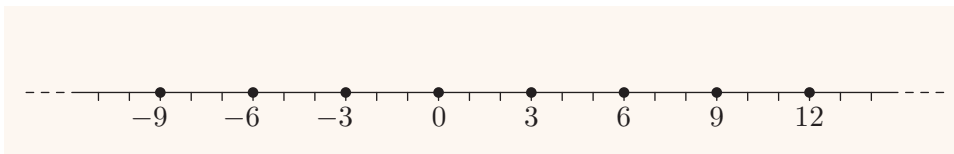


Figure 10 The residue class of 0 modulo 3

Activity 12 Plotting residue classes on a number line

- Plot the residue class of 2 modulo 3 on a number line.
- Plot the residue class of 1 modulo 4 on a number line.
- Plot the residue class of -1 modulo 4 on a number line.
- Plot the residue class of 0 modulo 5 on a number line.

You learned earlier (when you met the division theorem) that when you divide an integer a by a positive integer n , the remainder r satisfies

$$0 \leq r < n,$$

that is, r is one of the numbers $0, 1, \dots, n-1$. Since a and r each have the same remainder (namely r) when divided by n , it follows that

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

The remainder r is also known as the *least residue* of a modulo n , because it is the smallest number equal to or greater than 0 in the residue class of a modulo n . In the next section you'll learn about modular arithmetic, and there you'll find that a calculation involving an integer a can often be greatly simplified by performing the same calculation but using the least residue of a modulo n instead of a .

Least residues

The **least residue** of a modulo n is the remainder r that you obtain when you divide a by n .



The integer r is one of the numbers $0, 1, \dots, n-1$, and it satisfies

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

Example 5 *Finding the least residue*

Find the least residue of -33 modulo 7 .

Solution

 Find the quotient and remainder when you divide -33 by 7 . To do this, first notice that $-5 < -33/7 < -4$, so the quotient is -5 . The remainder is then given by $a - qn$. 

Since $-33 = 7 \times (-5) + 2$, the least residue is 2 .

Activity 13 *Finding least residues modulo 10*

Find the least residues of the following integers modulo 10 .

- (a) 17 (b) 50 (c) 6 (d) -1 (e) -38

Activity 14 *Finding least residues modulo 3*

Find the least residues of the following integers modulo 3 .

- (a) 17 (b) 9 (c) -2 (d) -10 (e) 3

Here's a puzzle that you might like to try to solve using residues.

Activity 15 *Finding the day of the week in 1000 days' time*

What day of the week will it be in 1000 days' time?

2 Modular arithmetic

Modular arithmetic is the application of the usual arithmetic operations – namely addition, subtraction, multiplication and division – for congruences. Addition, subtraction and multiplication are often simpler to carry out in modular arithmetic than they are normally, because you can use congruences to reduce large numbers to small numbers. For example, the multiplication 572×863 is difficult to calculate in your head, but working with congruences modulo 10 gives

$$572 \equiv 2 \pmod{10} \quad \text{and} \quad 863 \equiv 3 \pmod{10},$$

and you'll see later that this implies that

$$572 \times 863 \equiv 2 \times 3 \equiv 6 \pmod{10}.$$

You have to be more careful with division than the other arithmetic operations in modular arithmetic, so we leave division until the next section.

2.1 Addition and subtraction

Let's begin with two basic properties of congruences, which are useful for simplifying additions and subtractions.

Addition and subtraction rules for congruences

If $a \equiv b \pmod{n}$ and $c \equiv d \pmod{n}$, then

$$a + c \equiv b + d \pmod{n}$$

$$a - c \equiv b - d \pmod{n}.$$

To see why the first rule is true, remember that if $a \equiv b \pmod{n}$ and $c \equiv d \pmod{n}$, then both $a - b$ and $c - d$ are divisible by n . It follows that $(a - b) + (c - d)$ is divisible by n . But

$$(a - b) + (c - d) = (a + c) - (b + d),$$

so $(a + c) - (b + d)$ is divisible by n . Therefore $a + c \equiv b + d \pmod{n}$.

A similar argument can be used to establish the second rule.

With practice, you'll soon get used to applying these rules, without the need to refer back to them. You'll find them helpful, for instance, in simplifying long additions with check digits later in this section. Let's look at some examples that highlight how the rules can be applied effectively. Suppose, for instance, that you are asked to find the least residue of $19 + 37$ modulo 18. One way to solve this is to first add 19 and 37 to get 56, and then find the least residue of 56 modulo 18, which is 2. There is an alternative method though: you can find the least residues of 19 and 37 modulo 18 *before* you add them.

You find that

$$19 \equiv 1 \pmod{18} \quad \text{and} \quad 37 \equiv 1 \pmod{18},$$

so, by the addition rule,

$$19 + 37 \equiv 1 + 1 \equiv 2 \pmod{18}.$$



It is important to remember that the *least* residue of the sum of two integers isn't necessarily equal to the sum of the least residues of those integers. For example, the least residue of $19 + 18$ modulo 10 is 7 (since $19 + 18 = 37$). On the other hand, the least residues of 19 and 18 modulo 10 are 9 and 8, respectively, so the sum of these residues is 17. You need to carry out one further step and note that the least residue of 17 modulo 10 is equal to 7 in order to obtain the least residue of the sum.

It is not always simpler to find least residues modulo n before adding or subtracting. Suppose, for example, that you want to find the least residue of $85 - 84$ modulo 7. It is much easier to simply subtract 84 from 85 without first finding the least residues of each of these integers modulo 7. Sometimes there is scope for ingenuity in adding and subtracting in congruences, as the next example demonstrates.

Example 6 Adding and subtracting in modular arithmetic

Find the least residue of $171 + 169$ modulo 17.

Solution

 You could first find the least residues of 171 and 169 modulo 17, but in this case it's easier to notice that both 171 and 169 are within 1 of 170, a multiple of 17, so they are congruent to 1 or -1 modulo 17. 

$$171 \equiv 1 \pmod{17} \quad \text{and} \quad 169 \equiv -1 \pmod{17}$$

 Apply the addition rule for congruences. 

Therefore

$$171 + 169 \equiv 1 + (-1) \equiv 0 \pmod{17}.$$

So the least residue is 0.

You don't have to solve the problem in this way though. You could instead calculate $171 + 169 = 340$, and then observe that $340 \equiv 0 \pmod{17}$.

In the following activities you should try to find each least residue using as simple a method as you can. Your methods may differ from those of the solutions provided, because there are many ways to carry out modular arithmetic. There's no need to use a calculator here; in fact, you'll develop a better understanding of modular arithmetic if you approach the activity without one.

Activity 16 *Adding and subtracting modulo 6*

Find the least residues of the following integers modulo 6.

- (a) $7 + 3$ (b) $7 - 3$ (c) $23 - 24$
 (d) $-3 - 19$ (e) $67 + 68$ (f) $601 - 6001$

Activity 17 *Adding and subtracting modulo 10*

Find the least residues of the following integers modulo 10.

- (a) $6 + 4$ (b) $14 - 7$ (c) $13 - 15$
 (d) $-21 - 17$ (e) $101 + 11 + 1$ (f) $101 - 11 - 1$

2.2 Multiplication and powers

Multiplication in modular arithmetic is simpler than multiplication in normal arithmetic because you can often replace the integers to be multiplied with simpler numbers before you multiply them. This is because of the following rule.

Multiplication rule for congruences

If $a \equiv b \pmod{n}$ and $c \equiv d \pmod{n}$, then

$$ac \equiv bd \pmod{n}.$$

To see why this rule is true, first note that if both $a - b$ and $c - d$ are divisible by n , then $(a - b)c + (c - d)b$ is also divisible by n . But

$$(a - b)c + (c - d)b = ac - bd,$$

so $ac - bd$ is divisible by n . Hence $ac \equiv bd \pmod{n}$.

You'll soon become familiar with the rules for addition, subtraction and multiplication, so you needn't commit them to memory. Let's consider an example. Suppose you wish to find the least residue of 52×37 modulo 7. It is difficult to work out 52×37 in your head. Instead, observe that

$$52 \equiv 3 \pmod{7} \quad \text{and} \quad 37 \equiv 2 \pmod{7},$$

so, using the multiplication rule,

$$52 \times 37 \equiv 3 \times 2 \equiv 6 \pmod{7}.$$

We simplified this multiplication by working with the least residues of 52 and 37 modulo 7. Sometimes it is better to choose an integer in a residue class other than the least residue, as the following example demonstrates.



Example 7 *Multiplying in modular arithmetic*

Find the least residue of 17×14 modulo 19.

Solution

Find integers small in absolute value that are congruent to 17 and 14 modulo 19.

$$17 \equiv -2 \pmod{19} \quad \text{and} \quad 14 \equiv -5 \pmod{19}$$

Apply the multiplication rule for congruences.

Therefore

$$17 \times 14 \equiv (-2) \times (-5) \equiv 10 \pmod{19}.$$

So the least residue is 10.

Activity 18 *Multiplying modulo 7*

Find the least residues of the following integers modulo 7.

- (a) 3×6 (b) 22×29 (c) $(-5) \times 16$
 (d) 51×74 (e) $47 \times (-25)$ (f) $(-29) \times (-44)$

Activity 19 *Multiplying modulo 8*

Find the least residues of the following integers modulo 8.

- (a) 4×4 (b) 17×26 (c) $(-6) \times 34$
 (d) 16×457 (e) $47 \times (-25)$ (f) $(-61) \times (-46)$

If $a \equiv b \pmod{n}$ then the multiplication rule for congruences gives

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

You can now apply the multiplication rule to

$$a \equiv b \pmod{n} \quad \text{and} \quad a^2 \equiv b^2 \pmod{n}$$

to give

$$a^3 \equiv b^3 \pmod{n}.$$

Carrying on in this fashion, you obtain the power rule for congruences.

Power rule for congruences

If $a \equiv b \pmod{n}$, and m is a positive integer, then

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

For example, suppose you wish to find the least residue of 19^5 modulo 9. Since $19 \equiv 1 \pmod{9}$, it follows that

$$19^5 \equiv 1^5 \equiv 1 \pmod{9},$$

so the least residue is 1. This is a particularly simple application of the power rule. You'll usually need to do more working than this, as you'll see in the next example.

Example 8 *Raising to a power in modular arithmetic*

Find the least residue of 11^6 modulo 9.

Solution

 Use the power rule for congruences. 

Since

$$11 \equiv 2 \pmod{9},$$



it follows that

$$11^6 \equiv 2^6 \pmod{9}.$$

 Start calculating powers of 2. 

Calculating powers of 2 gives

$$2^2 = 4 \text{ and } 2^3 = 8.$$

 You could continue in this way to obtain $2^6 = 64$, and then find the least residue of 64 modulo 9. There is a quicker method though. Since $8 \equiv -1 \pmod{9}$, it follows that $2^3 \equiv -1 \pmod{9}$. You can then jump straight to $2^6 = 2^3 \times 2^3$. 

Since

$$2^3 \equiv -1 \pmod{9},$$

it follows that

$$2^6 \equiv 2^3 \times 2^3 \equiv (-1) \times (-1) \equiv 1 \pmod{9}.$$

So the least residue is 1.



Try the following activities. You may find that you use different methods to those given in the solutions.

Activity 20 *Raising to a power modulo 6*

Find the least residues of the following integers modulo 6.

- (a) 25^{25} (b) $(-9)^4$ (c) 20^6

Activity 21 *Raising to a power modulo 13*

Find the least residues of the following integers modulo 13.

- (a) 25^{25} (b) 54^4 (c) 16^9

2.3 Fermat's little theorem

Fermat's little theorem is a fundamental result in number theory that helps you to calculate powers modulo n when n is a prime number. Not only is Fermat's little theorem central to number theory, it also has numerous applications in disciplines that require numeric computations; perhaps most significantly, it plays an essential role in *RSA ciphers*, which are widely used systems for disguising sensitive information. At the end of this unit, you'll learn about some other, similar, methods called *affine ciphers* that are used for disguising information.

Fermat's little theorem was conceived by the French amateur mathematician Pierre de Fermat (referred to in the introduction) who in 1640 communicated the result in a letter to a friend along with the comment 'I'd send you the proof, but I fear that it is too long'. In fact, the earliest proof was published in 1736 by the Swiss mathematician Leonhard Euler (1707–83).

Before looking at Fermat's little theorem about powers modulo a general prime number, let's investigate the properties of powers modulo the prime number 5.

Activity 22 *Raising to the fourth power modulo 5*

Find the least residues of the following integers modulo 5.

- (a) 1^4 (b) 2^4 (c) 3^4 (d) 4^4 (e) 7^4

From parts (a) to (d) of this activity you should have found that

$$1^4 \equiv 2^4 \equiv 3^4 \equiv 4^4 \equiv 1 \pmod{5}.$$

Suppose now that a is any integer that is not a multiple of 5. We know that either

$$a \equiv 1 \pmod{5}, \quad a \equiv 2 \pmod{5}, \quad a \equiv 3 \pmod{5} \quad \text{or} \quad a \equiv 4 \pmod{5}.$$

Therefore the power rule for congruences, together with the result of Activity 22, tells us that

$$a^4 \equiv 1 \pmod{5}.$$

This observation about powers modulo 5 is a special case of Fermat's little theorem.

Fermat's little theorem

Let p be a prime number, and let a be an integer that is not a multiple of p . Then

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

Since 5 is a prime number, Fermat's little theorem tells us immediately that all the least residues in Activity 22 are 1. Also, for example, 13 is a prime number, so

$$6^{12} \equiv 1 \pmod{13} \quad \text{and} \quad (-15)^{12} \equiv 1 \pmod{13}.$$

When applying Fermat's little theorem, remember that the integer a must not be a multiple of p . After all, if a is a multiple of p , then $a \equiv 0 \pmod{p}$, so $a^{p-1} \equiv 0 \pmod{p}$.

In some other texts the congruence $a^{p-1} \equiv 1 \pmod{p}$ in Fermat's little theorem is replaced with the alternative congruence

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

You can obtain this congruence from $a^{p-1} \equiv 1 \pmod{p}$ by multiplying both sides by a . The theorem is less easy to apply in this alternative form but has the advantage that it is valid even if a is a multiple of p . This is because, if a is a multiple of p , then $a \equiv 0 \pmod{p}$, so

$$a^p \equiv a \equiv 0 \pmod{p}.$$

Carmichael numbers and the Hardy–Ramanujan number

Fermat's little theorem tells us that if n is a prime number, then

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

for any integer a . This congruence may fail if n is not a prime number; for example, if $n = 4$ and $a = 2$ then

$$2^4 \equiv 16 \equiv 0 \not\equiv 2 \pmod{4}.$$

There are, however, some positive integers n that are *not* prime numbers and yet have the property that the congruence $a^n \equiv a \pmod{n}$ is true for every integer a . These positive integers are known as **Carmichael numbers** after the American mathematician Robert Daniel Carmichael (1879–1967) who discovered the smallest such number, namely 561.

The next two Carmichael numbers are 1105 and 1729, and there are infinitely many more of them. The integer 1729 is also known as the **Hardy–Ramanujan number** after a famous anecdote by the distinguished British mathematician Godfrey Harold Hardy (1877–1947) about a conversation he had with his friend Srinivasa Ramanujan. Ramanujan was an Indian mathematician of extraordinary talent who was ill in hospital at the time of the incident. Hardy gave the following account of their exchange on page 147 of an article titled 'The Indian Mathematician Ramanujan' which was published in 1937 in *The American Mathematical Monthly* (vol. 44, no. 3, pp. 137–55):

I remember once going to see him when he was ill at Putney. I had ridden in taxi cab number 1729 and remarked that the number seemed to me rather a dull one, and that I hoped it was not an unfavorable omen. 'No,' he replied, 'it is a very interesting number; it is the smallest number expressible as the sum of two cubes in two different ways.'

In fact,

$$1729 = 1^3 + 12^3 = 9^3 + 10^3.$$



Srinivasa Ramanujan
(1887–1920)

Let's leave the justification of Fermat's little theorem for now – we'll return to it in a later unit – and instead consider an example of how the theorem can help us to calculate powers in modular arithmetic.

**Example 9** *Applying Fermat's little theorem*

Find the least residue of 4^{20} modulo 7.

Solution

As 7 is a prime number, we can apply Fermat's little theorem.

By Fermat's little theorem,

$$4^6 \equiv 1 \pmod{7}.$$

Therefore

$$4^{12} \equiv (4^6)^2 \equiv 1^2 \equiv 1 \pmod{7},$$

$$4^{18} \equiv (4^6)^3 \equiv 1^3 \equiv 1 \pmod{7},$$

and so forth; in fact, 4 to the power of *any* positive multiple of 6 is congruent to 1 modulo 7. In light of this, you can simplify the problem by writing 20 as a multiple of 6 plus a remainder term.

Since

$$20 = 3 \times 6 + 2,$$

we obtain

Recall the usual index laws for calculating powers, which tell us that $4^{3 \times 6 + 2} = 4^{3 \times 6} \times 4^2 = (4^6)^3 \times 4^2$.

$$\begin{aligned} 4^{20} &\equiv (4^6)^3 \times 4^2 \\ &\equiv 1^3 \times 4^2 \\ &\equiv 16 \\ &\equiv 2 \pmod{7}. \end{aligned}$$

So the least residue is 2.

Activity 23 *Applying Fermat's little theorem with $p = 7$*

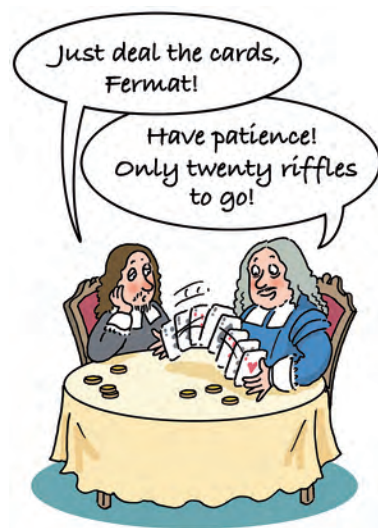
Find the least residues of the following integers modulo 7.

- (a) 5^6 (b) 18^{18} (c) $(-11)^{33}$

Activity 24 *Applying Fermat's little theorem with $p = 11$*

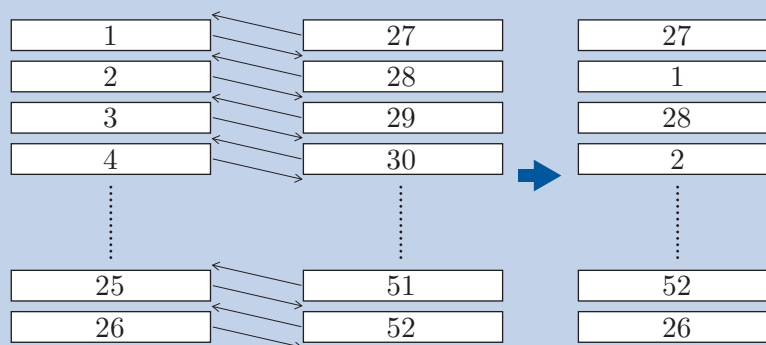
Find the least residues of the following integers modulo 11.

- (a) 7^{10} (b) $(-5)^{31}$ (c) 13^{85}



Riffling

Riffling is a process for shuffling a deck of cards whereby you split the deck into two piles and then combine the two piles in such a way that the cards are interleaved. In a perfect riffle of a 52-card deck, the two piles each have 26 cards, and they are combined alternately, as shown below.



The cards used here are numbered $1, 2, \dots, 52$ according to their position in the original deck, with 1 the original top card and 52 the original bottom card. The deck is split into two piles, $1, 2, \dots, 26$ and $27, 28, \dots, 52$, as shown on the left in Figure 2.3. After the riffle, the card originally at position x is moved to position a , where $a \equiv 2x \pmod{53}$. For example,

position 7 \longrightarrow position 14, and
position 27 \longrightarrow position 1

because $27 \times 2 = 54$ and $54 \equiv 1 \pmod{53}$. It follows that after two consecutive perfect riffles, the card originally at position x is moved to position b , where $b \equiv 2^2x \pmod{53}$. Similarly, after 52 perfect riffles, the card originally at position x is moved to position c , where $c \equiv 2^{52}x \pmod{53}$.

Fermat's little theorem tells us that

$$2^{52} \equiv 1 \pmod{53},$$

which implies that $c \equiv x \pmod{53}$. That is, after 52 perfect riffles, the cards are returned to their original order!

2.4 Divisibility tests

Let's take a break from developing the properties of modular arithmetic, to look at how it is used in divisibility tests. A **divisibility test** is a method for checking whether one integer is divisible by another. For example, an integer is divisible by 2 if its last digit is 0, 2, 4, 6 or 8. Here you'll learn how modular arithmetic can be used to give a method for checking whether an integer is divisible by 3. This method can be adapted to give a test for divisibility by 9, as you'll see at the end of the subsection.

Let's start by looking at the test for divisibility by 3, then later on you'll see an explanation for how it works, using modular arithmetic. The **digit sum** of an integer is the number you obtain by adding together the digits of that number. For example, the digit sum of 5847 is 24, because

$$5 + 8 + 4 + 7 = 24.$$

If the integer is negative, then you should ignore the minus sign when working out the digit sum. For example, the digit sum of -5847 is also 24. The divisibility by 3 test is based on the following observation.

Divisibility by 3

If an integer is divisible by 3, then its digit sum is divisible by 3, and vice versa.

For instance, 6847 is not divisible by 3 because its digit sum 25 is not divisible by 3, whereas 5847 is divisible by 3 because its digit sum 24 is divisible by 3. With large numbers it may be difficult to tell whether the digit sum itself is divisible by 3, in which case you may need to find another digit sum, as shown in the next example.

Example 10 Testing divisibility by 3

Is the number 8 675 038 695 divisible by 3?

Solution

 Find the digit sum of 8 675 038 695. 

The digit sum of 8 675 038 695 is

$$8 + 6 + 7 + 5 + 0 + 3 + 8 + 6 + 9 + 5 = 57$$

 To determine whether 57 is divisible by 3, you can now find *its* digit sum. 

and the digit sum of 57 is

$$5 + 7 = 12.$$

Since 12 is divisible by 3, so is 57, and hence so is 8 675 038 695.

Activity 25 *Testing divisibility by 3*

Which of the following numbers are divisible by 3?

- (a) 982 (b) 753 (c) 8364 (d) -9245
 (e) 98 285 385 335 (f) 10^{100}

Let's now see why the test for divisibility by 3 works. This explanation involves a four digit number; similar reasoning applies to a number with more (or fewer) digits. Any four digit number n can be written as $10^3a + 10^2b + 10c + d$, where a , b , c and d are the digits of the number.

For instance,

$$\underbrace{7263}_n = \underbrace{10^3 \times 7}_{10^3a} + \underbrace{10^2 \times 2}_{10^2b} + \underbrace{10 \times 6}_{10c} + \underbrace{3}_d.$$

Since

$$10 \equiv 1 \pmod{3},$$

it follows that, for any positive integer n ,

$$10^n \equiv 1^n \equiv 1 \pmod{3}.$$

Therefore

$$10^3a + 10^2b + 10c + d \equiv a + b + c + d \pmod{3}.$$

This shows that n and its digit sum $a + b + c + d$ both have the same remainder on division by 3, so one is divisible by 3 as long as the other is divisible by 3.

This argument also works with congruences modulo 9 instead of modulo 3, and so there is a similar test for divisibility by 9.

Divisibility by 9

If an integer is divisible by 9, then its digit sum is divisible by 9, and vice versa.

For instance, 5847 is not divisible by 9 because its digit sum is 24 which is not divisible by 9, whereas 5841 is divisible by 9 because its digit sum is 18 which is divisible by 9.

Activity 26 *Testing divisibility by 9*

Which of the following numbers are divisible by 9?

- (a) 8469 (b) 6172 (c) 7 989 989 897 979 897

Other divisibility tests

There are other tests that you can perform to test divisibility by numbers other than 3 and 9. Here are some of the simpler tests of this type.

To test whether an integer is divisible by 11, you should first find the *alternating digit sum* of the integer. The alternating digit sum is found by alternately adding and subtracting the digits of the integer, starting from the units digit, and working backwards through the other digits.

For example, the alternating digit sum of 673 148 is

$$8 - 4 + 1 - 3 + 7 - 6 = 3.$$

If the integer is divisible by 11, then its alternating digit sum is divisible by 11, and vice versa. Therefore 673 148 is not divisible by 11.

To test whether an integer is divisible by 4, you should first find the number formed from the final two digits of the original integer. For example, the final two digits of the integer 673 148 give the number 48. If the original integer is divisible by 4, then the number formed from the final two digits is divisible by 4, and vice versa. Therefore 673 148 is divisible by 4, as 48 is divisible by 4.

A similar divisibility test works for powers of 2 other than 4. For example, to test whether an integer is divisible by 8 (note that $8 = 2^3$), you just need to check whether the number formed from the final *three* digits of the integer is divisible by 8.

The correctness of these divisibility tests can be proved by using modular arithmetic.

2.5 Check digits

Groceries often have an identification number printed on them, accompanied by a barcode. The barcode is just a way of formatting the identification number so that it can easily be read by a scanner, and then identified from a database on a computer. Two barcodes are shown in Figure 11. On the left is an example of a Universal Product Code (UPC), which is a system of numbering used on many objects sold in the United Kingdom. On the right is an example of an International Standard Book Number (ISBN), which is a system of numbering used on books.



Figure 11 (a) A UPC (b) an ISBN

Sometimes errors may occur in communicating identification numbers; for example, a shop assistant may type an identification number incorrectly into a cash register. To help prevent such errors, the last digit is used as a check. It is known as a **check digit**. Here you'll learn how check digits work for ISBNs, using modular arithmetic. Check digits for other schemes work in a similar manner. Actually, you'll learn about 10-digit ISBNs, which were used before the introduction of 13-digit ISBNs in 2007. These 13-digit ISBNs also have check digits, but the explanation of how they work, although similar, is slightly more complicated.

Let's label the digits a_1, a_2, \dots, a_{10} of an ISBN in reverse order, so that a_1 is the check digit, as shown below for the ISBN of *Silent Spring*, by Rachel Carson.

a_{10}	a_9	a_8	a_7	a_6	a_5	a_4	a_3	a_2	a_1
0	1	4	1	3	9	1	5	2	9

check
digit

The digits a_2, a_3, \dots, a_{10} identify the language, publisher and title of the book. The check digit a_1 is then defined to be the integer from $\{0, 1, 2, \dots, 10\}$ that satisfies

$$a_1 \equiv -2a_2 - 3a_3 - 4a_4 - 5a_5 - 6a_6 - 7a_7 - 8a_8 - 9a_9 - 10a_{10} \pmod{11}.$$

Rearranging this congruence gives

$$a_1 + 2a_2 + 3a_3 + 4a_4 + 5a_5 + 6a_6 + 7a_7 + 8a_8 + 9a_9 + 10a_{10} \equiv 0 \pmod{11}.$$

An ISBN must satisfy this congruence in order to be valid. If the congruence is not satisfied, then there is an error and the number is not an ISBN. Let's check the ISBN of *Silent Spring*, using the symbol \cdot as a

shorthand for the multiplication symbol \times . The congruence check is satisfied because

$$\begin{aligned}
 & a_1 + 2a_2 + 3a_3 + 4a_4 + 5a_5 + 6a_6 + 7a_7 + 8a_8 + 9a_9 + 10a_{10} \\
 & \equiv 9 + 2 \cdot 2 + 3 \cdot 5 + 4 \cdot 1 + 5 \cdot 9 + 6 \cdot 3 + 7 \cdot 1 + 8 \cdot 4 + 9 \cdot 1 + 10 \cdot 0 \\
 & \equiv 9 + 4 + 15 + 4 + 45 + 18 + 7 + 32 + 9 + 0 \\
 & \equiv 9 + 4 + 4 + 4 + 1 + 7 + 7 + 10 + 9 \\
 & \equiv 55 \\
 & \equiv 0 \pmod{11}.
 \end{aligned}$$

The check digit a_1 is one of the integers $0, 1, 2, \dots, 10$. When a_1 is 10, it is denoted in the ISBN by an X (the Roman numeral for 10) to ensure that it is represented by a single symbol.

The two most common types of errors when communicating ISBNs are interchanging two adjacent digits in the ISBN (for example, typing 123**54**6789X instead of 123**45**6789X) or altering a single digit (for example, typing **7**23456789X instead of **1**23456789X). The 10-digit code fails the ISBN congruence check if one of these errors occurs. To see why this is so, let's consider a valid ISBN with digits a_1, a_2, \dots, a_{10} , in reverse order, which must satisfy the congruence check $S \equiv 0 \pmod{11}$, where

$$S = a_1 + 2a_2 + 3a_3 + 4a_4 + 5a_5 + 6a_6 + 7a_7 + 8a_8 + 9a_9 + 10a_{10}.$$

Suppose that in typing the ISBN you accidentally interchange a_6 and a_7 (but make no other errors). Your ISBN congruence check will now involve the sum

$$T = a_1 + 2a_2 + 3a_3 + 4a_4 + 5a_5 + \mathbf{6a_7} + \mathbf{7a_6} + 8a_8 + 9a_9 + 10a_{10}.$$

Unless $a_6 = a_7$ (in which case interchanging a_6 and a_7 won't matter) you obtain

$$T - S \equiv (6a_7 + 7a_6) - (6a_6 + 7a_7) \equiv a_6 - a_7 \not\equiv 0 \pmod{11}$$

(where $\not\equiv$ means 'is not congruent to'). Since $S \equiv 0 \pmod{11}$, it follows that $T \not\equiv 0 \pmod{11}$. Therefore your number fails the ISBN congruence check, so you know that you have made an error.

Next let's suppose instead that in typing the ISBN you accidentally change a_{10} to a different digit a'_{10} (but make no other errors). This time your congruence check will involve the sum

$$T = a_1 + 2a_2 + 3a_3 + 4a_4 + 5a_5 + 6a_6 + 7a_7 + 8a_8 + 9a_9 + \mathbf{10a'_{10}}.$$

Then

$$T - S \equiv 10a'_{10} - 10a_{10} \pmod{11}.$$

Remember that $10 \equiv -1 \pmod{11}$. Therefore

$$T - S \equiv (-1) \times a'_{10} - (-1) \times a_{10} \equiv a_{10} - a'_{10} \not\equiv 0 \pmod{11},$$

so again $T \not\equiv 0 \pmod{11}$. Since your number fails the ISBN congruence check, you know that you have made an error.

In this example of a single digit error we have assumed that a_{10} is the incorrect digit. If the error was in a different digit, then the argument to show that

$$T - S \not\equiv 0 \pmod{11}$$

is similar, but uses the idea of multiplicative inverses modulo 11, which you'll meet in the next section.



You've now seen that the congruence check will detect whether one of the two most common errors has occurred. However, it won't necessarily detect whether more than one of these errors has occurred, or if a different error has occurred.

Example 11 *Checking whether a 10-digit code could be an ISBN*

Does the following 10-digit code satisfy the ISBN congruence check?

0521683726

Solution

 Label the digits $a_1, a_2, a_3, \dots, a_{10}$ in reverse order, and evaluate $a_1 + 2a_2 + 3a_3 + 4a_4 + 5a_5 + 6a_6 + 7a_7 + 8a_8 + 9a_9 + 10a_{10}$ 

$$\begin{aligned} & a_1 + 2a_2 + 3a_3 + 4a_4 + 5a_5 + 6a_6 + 7a_7 + 8a_8 + 9a_9 + 10a_{10} \\ & \equiv 6 + 2 \cdot 2 + 3 \cdot 7 + 4 \cdot 3 + 5 \cdot 8 + 6 \cdot 6 + 7 \cdot 1 + 8 \cdot 2 + 9 \cdot 5 + 10 \cdot 0 \\ & \equiv 6 + 4 + 21 + 12 + 40 + 36 + 7 + 16 + 45 + 0 \end{aligned}$$

 Simplify modulo 11. 

$$\begin{aligned} & \equiv 6 + 4 + 10 + 1 + 7 + 3 + 7 + 5 + 1 \\ & \equiv 44 \\ & \equiv 0 \pmod{11} \end{aligned}$$

So 0521683726 satisfies the ISBN congruence check.

You may find it helpful in carrying out the ISBN congruence check to remember that

$$10 \equiv -1 \pmod{11}, \quad 9 \equiv -2 \pmod{11} \quad \text{and} \quad 8 \equiv -3 \pmod{11}.$$

Activity 27 *Checking whether 10-digit codes could be ISBNs*

Do the following 10-digit codes satisfy the ISBN congruence check?

- (a) 0412606100 (b) 020142278X (c) 0691118809

3 Multiplicative inverses and linear congruences

In this section you'll learn about *multiplicative inverses modulo n* , which give you a way of dividing in modular arithmetic. You'll use them to solve *linear congruences*; these are congruences such as

$$5x \equiv 2 \pmod{12},$$

where x is an unknown.

In the subject of cryptography, linear congruences are used in procedures for disguising information called *ciphers*. At the end of the section you'll learn how to unravel particular types of ciphers, called *affine ciphers*, by solving linear congruences.

3.1 Multiplicative inverses

You've seen how to add, subtract and multiply in modular arithmetic, and now you'll learn how to divide in modular arithmetic. Let's begin with an example which demonstrates that you cannot divide both sides of a congruence by an integer in the way you might expect. Consider the congruence

$$20 \equiv 8 \pmod{6}.$$

Even though 20 and 8 are each divisible by 4, with $20/4 = 5$ and $8/4 = 2$, you cannot divide both sides of the congruence by 4 because

$$5 \not\equiv 2 \pmod{6}.$$

We need a different concept of division in modular arithmetic. To motivate this new concept, recall that in normal arithmetic, dividing by the integer 4, for example, is the same as multiplying by the reciprocal of 4, namely $\frac{1}{4}$. The reciprocal $\frac{1}{4}$ satisfies

$$4 \times \frac{1}{4} = 1.$$

In modular arithmetic, the only numbers used are integers, so we cannot multiply by the fraction $\frac{1}{4}$. Instead we need numbers that perform the same role as reciprocals, called *multiplicative inverses modulo n* .

Multiplicative inverses modulo n

A **multiplicative inverse of a modulo n** is an integer v such that

$$av \equiv 1 \pmod{n}.$$

For example, 5 is a multiplicative inverse of 2 modulo 9 because

$$2 \times 5 \equiv 1 \pmod{9}.$$

Activity 28 Finding multiplicative inverses modulo 9

Find a multiplicative inverse modulo 9 of each of the following integers.

- (a) 1 (b) 5 (c) 7 (d) 16

For some integers a and positive integers n , there is no multiplicative inverse of a modulo n . For example, 3 doesn't have a multiplicative inverse modulo 9. To see this, suppose on the contrary that v is a multiplicative inverse of 3 modulo 9. Then

$$3v \equiv 1 \pmod{9}.$$

Let's now use the method explained near the end of Subsection 1.4 for writing a congruence as an equation. This method shows that our congruence is equivalent to the statement

$$3v = 1 + 9k,$$

for some integer k . However, the left-hand side of this equation is divisible by 3, but the right-hand side is not (because 3 is a factor of $9k$, so $1 + 9k$ is one more than a multiple of 3). This is impossible and so 3 doesn't have a multiplicative inverse modulo 9 after all.

Activity 29 Showing that some integers don't have a multiplicative inverse modulo 9

Show that each of the following integers doesn't have a multiplicative inverse modulo 9.

- (a) 0 (b) 6 (c) 18

What's special about the integer 3 and each of the integers in Activity 29 is that they each share a common factor (other than 1) with 9. For instance, 3 and 9 share a common factor of 3. With reasoning similar to that used to solve Activity 29, you can show that any integer that shares a common factor (other than 1) with 9 doesn't have a multiplicative inverse modulo 9.

In contrast, the integer 2 and each of the integers from Activity 28 share no common factors with 9 other than 1. In other words, the highest common factor of any one of these integers and 9 is 1. Two integers whose highest common factor is 1 are said to be **coprime**. If a and 9 are coprime integers, then a *does* have a multiplicative inverse modulo 9. To see why this is so, remember that Bézout's identity tells us that if the highest common factor of a and 9 is 1, then there are integers v and w such that

$$av + 9w = 1.$$

Therefore

$$av = 1 - 9w.$$

Using the method for writing a congruence as an equation, in reverse, we see that

$$av \equiv 1 \pmod{9}.$$

Therefore v is a multiplicative inverse of a modulo 9.

Arguing in a similar way but using modulo n rather than modulo 9, you can obtain the following rule for deciding whether an integer a has a multiplicative inverse modulo n .

Existence of multiplicative inverses modulo n

- If the integers a and n are coprime, then there is a multiplicative inverse of a modulo n .
- If a and n are not coprime, then there is not a multiplicative inverse of a modulo n .

You saw earlier that 5 is a multiplicative inverse of 2 modulo 9. It's not the only multiplicative inverse of 2 modulo 9 though; every integer that is congruent to 5 modulo 9 is a multiplicative inverse of 2 modulo 9. For example,

$$\begin{aligned} 14 &\equiv 5 \pmod{9}, & \text{so } 2 \times 14 &\equiv 2 \times 5 \equiv 1 \pmod{9}, \\ -4 &\equiv 5 \pmod{9}, & \text{so } 2 \times (-4) &\equiv 2 \times 5 \equiv 1 \pmod{9}, \end{aligned}$$

and so 14 and -4 are also multiplicative inverses of 2 modulo 9. Remember that the collection of integers congruent to 5 modulo 9 is called the residue class of 5 modulo 9. Among these integers is the least residue of 5 modulo 9, which is 5 itself. When you are asked to find a multiplicative inverse modulo n it is usually clearest to give the least residue.

So far, you've found multiplicative inverses modulo n by trying the values $1, 2, 3, \dots, n-1$ one by one. This method can, however, be very time consuming if n is large! In the next example, you'll see how to find multiplicative inverses by using Euclid's algorithm and backwards substitution.

In general, you can use whichever method you wish, although a helpful rule to follow is that you should use the first method when $n \leq 13$, and otherwise use the second method. The reason for the integer 13 is that in modular arithmetic modulo n , where $n \leq 13$, the only pairs of integers that you'll need to multiply together are those that fall within the familiar 1 to 12 multiplication tables (providing that each of your integers is a least residue modulo n).

Sometimes you'll be able to find a multiplicative inverse with an intelligent guess, without using either of these methods. For example, to find the multiplicative inverse of 29 modulo 30, you just need to observe that

$$29 \equiv -1 \pmod{30},$$

so

$$29 \times 29 \equiv (-1) \times (-1) \equiv 1 \pmod{30}.$$



Therefore 29 is its own multiplicative inverse modulo 30.

Example 12 *Finding multiplicative inverses modulo n*



For each of the following values of a and n , determine whether a multiplicative inverse of a modulo n exists and, if it does, find one.

- (a) $a = 5, n = 13$ (b) $a = 30, n = 73$

Solution

- (a)  To determine whether there is a multiplicative inverse, check whether 5 and 13 are coprime. They must be coprime, as they are both prime numbers. 



The integers 5 and 13 are coprime, so there is a multiplicative inverse of 5 modulo 13.



 Since $n \leq 13$, try the values 1, 2, 3, ... one by one until you find the multiplicative inverse modulo 13. You needn't necessarily check the integer 1, as clearly $5 \times 1 \not\equiv 1 \pmod{13}$. 

$$\begin{array}{ll} 5 \times 1 \equiv 5 \pmod{13} & 5 \times 2 \equiv 10 \pmod{13} \\ 5 \times 3 \equiv 15 \equiv 2 \pmod{13} & 5 \times 4 \equiv 20 \equiv 7 \pmod{13} \\ 5 \times 5 \equiv 25 \equiv 12 \pmod{13} & 5 \times 6 \equiv 30 \equiv 4 \pmod{13} \\ 5 \times 7 \equiv 35 \equiv 9 \pmod{13} & 5 \times 8 \equiv 40 \equiv 1 \pmod{13} \end{array}$$

 Stop, as you have found an integer v such that $5v \equiv 1 \pmod{13}$. 

So 8 is a multiplicative inverse of 5 modulo 13.



 You may have noticed a short cut that saves some calculations. You saw that $5 \times 5 \equiv 12 \equiv -1 \pmod{13}$, so $(-5) \times 5 \equiv -12 \equiv 1 \pmod{13}$. Since $-5 \equiv 8 \pmod{13}$, it follows that a multiplicative inverse of 5 modulo 13 is 8. 

- (b)  To determine whether there is a multiplicative inverse, check whether 30 and 73 are coprime. The numbers are quite large so use Euclid's algorithm to find the highest common factor. 

Euclid's algorithm gives

$$\begin{aligned} 73 &= 2 \times 30 + 13 \\ 30 &= 2 \times 13 + 4 \\ 13 &= 3 \times 4 + 1 \\ 4 &= 4 \times 1 + 0. \end{aligned}$$

Since the second-to-last remainder is 1, the integers 30 and 73 are coprime, so there is a multiplicative inverse of 30 modulo 73.

 Rearrange all but the last equation and then apply backwards substitution to find integers v and w with $30v + 73w = 1$. The integer v will be a multiplicative inverse of 30 modulo 73 since $30v = 1 - 73w$. 



Rearranging the equations gives

$$\textcircled{13} = \textcircled{73} - 2 \times \textcircled{30}$$



$$\textcircled{4} = \textcircled{30} - 2 \times \textcircled{13}$$

$$\textcircled{1} = \textcircled{13} - 3 \times \textcircled{4}.$$

Backwards substitution gives

$$\begin{aligned}\textcircled{1} &= \textcircled{13} - 3 \times (\textcircled{30} - 2 \times \textcircled{13}) \\ &= 7 \times \textcircled{13} - 3 \times \textcircled{30} \\ &= 7 \times (\textcircled{73} - 2 \times \textcircled{30}) - 3 \times \textcircled{30} \\ &= 7 \times \textcircled{73} - 17 \times \textcircled{30}.\end{aligned}$$

(Check: $7 \times 73 - 17 \times 30 = 511 - 510 = 1$.)

 Write the equation $7 \times 73 - 17 \times 30 = 1$ as a congruence modulo 73 to give the multiplicative inverse. 



Since

$$(-17) \times 30 = 1 - 7 \times 73,$$

we obtain

$$(-17) \times 30 \equiv 1 \pmod{73}.$$

So -17 is a multiplicative inverse of 30 modulo 73.

 The solution could end here, however, it is helpful to also find a multiplicative inverse that is a least residue modulo 73. 

Since

$$-17 \equiv 56 \pmod{73},$$

56 is also a multiplicative inverse of 30 modulo 73.

Activity 30 Finding multiplicative inverses modulo n

For each of the following values of a and n , determine whether a multiplicative inverse of a modulo n exists and, if it does, find one.

- (a) $a = 10, n = 13$ (b) $a = 12, n = 21$ (c) $a = 18, n = 19$
 (d) $a = 0, n = 11$ (e) $a = 7, n = 16$ (f) $a = 10, n = 57$
 (g) $a = 84, n = 217$ (h) $a = 43, n = 96$

Basketball circles

Suppose 7 basketball players stand in a circle, equally spaced. One player has a ball and she throws it to the player 3 places to her right. The receiver then throws the ball 3 places to his right, and so forth. Let's label the people 0, 1, 2, ..., 6 anticlockwise, starting with player 0 who begins with the ball. The path the ball follows is shown in Figure 12(a). After m throws, the ball is with the player congruent to

$$\underbrace{3 + 3 + \cdots + 3}_{m \text{ copies of } 3} = 3m$$

modulo 7. For example, after 7 throws, player 0 has the ball again, because $3 \times 7 \equiv 0 \pmod{7}$. After 5 throws, player 1 has the ball, because $3 \times 5 \equiv 1 \pmod{7}$.

Now suppose there are n basketball players (rather than 7) and each player throws the ball a places (rather than 3) to his or her right. After m throws, the ball is with the player congruent to am modulo n . Therefore player 1 receives the ball when m is a multiplicative inverse of a modulo n . If a and n are *not* coprime, then player 1 never receives the ball, as is the case in Figure 12(b).

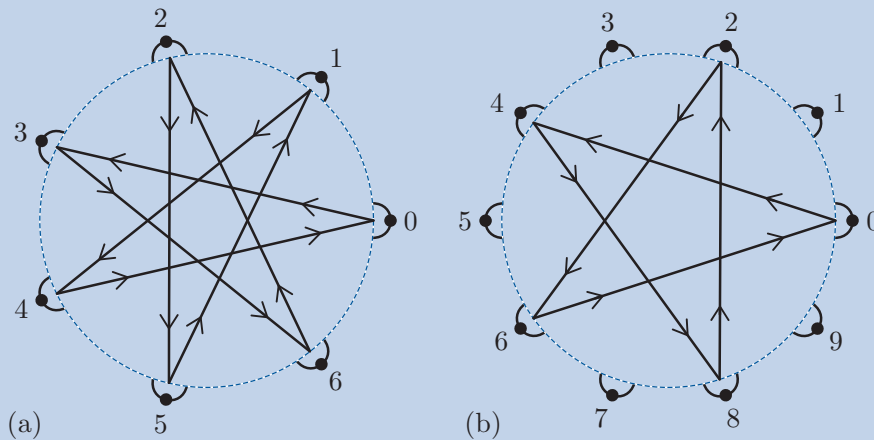


Figure 12 (a) A basketball circle with 7 players and throws of 3 places to the right (b) a basketball circle with 10 players and throws of 4 places to the right

3.2 Linear congruences

Congruences such as

$$5x \equiv 2 \pmod{12},$$

in which there is an unknown x , are called *linear congruences*.

Linear congruences

A **linear congruence** is a congruence of the form

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

where a and b are known, and x is unknown.

The process of finding the values of x for which a linear congruence is true is called **solving** the linear congruence. Any number x for which the linear congruence is true is a *solution* of the linear congruence. If x is a solution of a linear congruence, then any number in the same residue class as x modulo n is also a solution. So the solutions are given by linear congruences of the form

$$x \equiv c \pmod{n}.$$

In this subsection, you'll learn how to solve linear congruences in which a and n are coprime. You'll learn about linear congruences in which a and n are *not* coprime in the next subsection. You'll see that some linear congruences have *no* solutions.

You saw earlier that, if a and n are coprime, then a has a multiplicative inverse modulo n . In fact, you saw that a has many multiplicative inverses modulo n . You'll now see how a multiplicative inverse v of a modulo n can be used to solve the linear congruence $ax \equiv b \pmod{n}$. First, multiply both sides of the linear congruence by v :

$$vax \equiv vb \pmod{n}.$$

Since $va \equiv 1 \pmod{n}$, it follows that the solutions of the linear congruence $ax \equiv b \pmod{n}$ are given by

$$x \equiv vb \pmod{n}.$$

Solving linear congruences when a and n are coprime

If a and n are coprime, then the linear congruence $ax \equiv b \pmod{n}$ has solutions. The solutions are given by

$$x \equiv vb \pmod{n},$$

where v is any multiplicative inverse of a modulo n .

For example, consider the linear congruence

$$5x \equiv 6 \pmod{9}.$$

You saw earlier that 2 is a multiplicative inverse of 5 modulo 9 because

$$2 \times 5 \equiv 10 \equiv 1 \pmod{9}$$

and so the solutions of the linear congruence are given by

$$x \equiv 2 \times 6 \equiv 12 \equiv 3 \pmod{9};$$

that is,

$$x \equiv 3 \pmod{9}.$$

In other words, the solutions of the linear congruence consist of those integers congruent to 3 modulo 9 (such as $\dots, -15, -6, 3, 12, 21, \dots$). You can check this by substituting $x = 3$ back in to the original linear congruence:

$$5 \times 3 \equiv 15 \equiv 6 \pmod{9}.$$

In fact, for this particular linear congruence, it would be quicker simply to try out the values $1, 2, 3, \dots$ one by one until you find a solution. We suggest that you apply this direct method for solving a linear congruence whenever $n \leq 13$. Let's consider some examples of linear congruences of this type, and return to linear congruences with $n > 13$ later on.


Example 13 *Solving a linear congruence when a and n are coprime and $n \leq 13$*

Solve the linear congruence

$$11x \equiv 7 \pmod{8}.$$

Solution

Simplify the linear congruence by replacing 11 with the least residue of 11 modulo 8.

Since $11 \equiv 3 \pmod{8}$, an equivalent linear congruence is

$$3x \equiv 7 \pmod{8}.$$

Check that this linear congruence has solutions.

As 3 and 8 are coprime, this linear congruence has solutions.

Try the values 1, 2, 3, ... one by one until you find a solution.

Trying the values 1, 2, 3, ... one by one, we find that

$$\begin{array}{ll} 3 \times 1 \equiv 3 \pmod{8} & 3 \times 2 \equiv 6 \pmod{8} \\ 3 \times 3 \equiv 9 \equiv 1 \pmod{8} & 3 \times 4 \equiv 12 \equiv 4 \pmod{8} \\ 3 \times 5 \equiv 15 \equiv 7 \pmod{8}. \end{array}$$

So the solutions are given by

$$x \equiv 5 \pmod{8}.$$

Activity 31 *Solving linear congruences when a and n are coprime and $n \leq 13$*

Solve the following linear congruences.

$$(a) \ 2x \equiv 5 \pmod{7} \quad (b) \ 7x \equiv 8 \pmod{10} \quad (c) \ 15x \equiv -13 \pmod{11}$$

For large values of n , it is quicker to solve a linear congruence $ax \equiv b \pmod{n}$ by using the result you saw earlier. This states that the solutions are given by

$$x \equiv vb \pmod{n},$$

where v is a multiplicative inverse of a modulo n .



Example 14 *Solving a linear congruence when a and n are coprime and $n > 13$*

Solve the linear congruence

$$7x \equiv 13 \pmod{24}.$$

Solution

☁ Check that the linear congruence has solutions. ☁

As 7 and 24 are coprime, the linear congruence has solutions.

☁ Since 24 is a large integer, use a multiplicative inverse of 7 modulo 24 to find the solutions. ☁

The solutions are given by

$$x \equiv 13v \pmod{24},$$

where v is a multiplicative inverse of 7 modulo 24.

☁ Use Euclid's algorithm and backwards substitution to find v . ☁

Euclid's algorithm gives

$$24 = 3 \times 7 + 3$$

$$7 = 2 \times 3 + 1.$$

☁ There is no need to write down the next equation given by Euclid's algorithm since this equation has remainder 1. Apply backwards substitution to find integers v and w with $7v + 24w = 1$. There are only two equations, so you may choose not to rearrange them first. ☁

Backwards substitution gives

$$\begin{aligned} 1 &= 7 - 2 \times 3 \\ &= 7 - 2(24 - 3 \times 7) \\ &= 7 \times 7 - 2 \times 24. \end{aligned}$$

So

$$7 \times 7 \equiv 1 \pmod{24},$$

and hence 7 is a multiplicative inverse of 7 modulo 24. So the solutions are given by

$$x \equiv 13 \times 7 \equiv 91 \equiv 19 \pmod{24}.$$

☁ Remember to check your answer. That is, check that if $x \equiv 19 \pmod{24}$ then $7x \equiv 13 \pmod{24}$. To do this, it helps to use the congruence $19 \equiv -5 \pmod{24}$. ☁

(Check: $7 \times 19 \equiv 7 \times (-5) \equiv -35 \equiv 13 \pmod{24}$.)

Activity 32 *Solving linear congruences when a and n are coprime and $n > 13$*

Solve the following linear congruences.

(a) $7x \equiv 8 \pmod{20}$ (b) $3x \equiv -26 \pmod{17}$

(c) $13x \equiv 3 \pmod{30}$

Here's a puzzle that you might like to try to solve using linear congruences.

Activity 33 *Using linear congruences to solve a puzzle*


10 pirates discover a treasure chest containing no more than 100 gold coins. They share the coins out equally, but find there are 6 left over. In frustration they throw 3 of their comrades overboard, and share the coins out equally again among the remaining 7. This time the coins can be distributed equally, with none left over. How many coins are there?

Hint: let N be the number of gold coins. When the 10 pirates first share the N coins out, they find there are 6 left over. Write this observation as a congruence modulo 10. After 3 pirates are thrown overboard, the remaining 7 pirates succeed in sharing out the N coins equally among themselves. Use this fact to write down an expression for N that you can substitute into the congruence that you wrote down earlier to give you a linear congruence.

3.3 More linear congruences

In this subsection you'll learn about linear congruences $ax \equiv b \pmod{n}$ for which a and n are *not* coprime. This is a bit more complicated than the case when a and n are coprime.

Let's begin with an example, the linear congruence

$$6x \equiv 4 \pmod{15}.$$

This is unlike any of the linear congruences you met earlier because the integers a and n (6 and 15) are not coprime: their highest common factor is 3. If x is a solution of this linear congruence, then you can write

$$6x = 4 + 15k,$$

for some integer k . Subtracting $15k$ from both sides gives

$$6x - 15k = 4.$$

However, the left-hand side of this equation is divisible by 3 but the right-hand side is not. This contradiction shows that there are *no* solutions of the linear congruence $6x \equiv 4 \pmod{15}$.

Similar arguments can be used to obtain the following more general result.

Linear congruences without solutions

Let d be the highest common factor of the integers a and n , where $n > 1$. The linear congruence

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

has no solutions if b is not divisible by d .

For example, the linear congruence

$$-15x \equiv 8 \pmod{20}$$

has no solutions, because the highest common factor of -15 and 20 is 5 , and 8 is not divisible by 5 .

Activity 34 *Showing that some linear congruences have no solutions*

Show that the following linear congruences have no solutions.

(a) $4x \equiv 5 \pmod{10}$ (b) $-12x \equiv 8 \pmod{42}$

(c) $48x \equiv 70 \pmod{111}$

So far you've learned how to solve the linear congruence

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

when a and n are coprime, and you've seen that the linear congruence has no solutions when b is not divisible by the highest common factor of a and n . Let's suppose now that the linear congruence doesn't fall into either of these categories: so the highest common factor of a and n is not 1 , but it is a divisor of b . For example, consider the linear congruence

$$9x \equiv 21 \pmod{24}.$$

The highest common factor of 9 and 24 is 3 , and 3 is a divisor of 21 . The linear congruence is equivalent to the statement that

$$9x = 21 + 24k, \quad \text{for some integer } k.$$

If we divide each side of this equation by 3 , the highest common factor of 9 and 24 , then we obtain

$$3x = 7 + 8k, \quad \text{for some integer } k.$$

Expressed as a linear congruence, this statement says that

$$3x \equiv 7 \pmod{8}.$$

This new linear congruence is equivalent to the original one, $9x \equiv 21 \pmod{24}$. However, the new linear congruence is of the form $ax \equiv b \pmod{n}$, where a and n are coprime, so you can solve it using the

methods of the previous subsection. In fact, you saw how to solve it in Example 13; the solutions are given by

$$x \equiv 5 \pmod{8}.$$

Notice that the original linear congruence was a congruence modulo 24 whereas the solutions are given by a congruence modulo 8.

This method works with other linear congruences of a similar type. It is summarised as follows.

Linear congruences with solutions

Let d be the highest common factor of the integers a and n , where $n > 1$. The linear congruence

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

has solutions if b is divisible by d . The solutions are given by the solutions of the equivalent linear congruence

$$\frac{a}{d}x \equiv \frac{b}{d} \pmod{\frac{n}{d}}.$$

It's worth emphasising here that if b is divisible by d then the numbers a/d , b/d and n/d are all integers. (You should not write down a congruence involving a number that is not an integer.) What is more, after dividing a and n by their highest common factor d , you are left with integers a/d and n/d with no common factors (other than 1). That is, a/d and n/d are coprime, so you can solve the linear congruence

$$\frac{a}{d}x \equiv \frac{b}{d} \pmod{\frac{n}{d}}$$

using the techniques of the previous subsection.

Notice that the statement in the box is true even if $d = 1$ (that is, even if a and n are coprime) although in that case it doesn't tell you anything useful because if $d = 1$ then the two linear congruences

$$ax \equiv b \pmod{n} \quad \text{and} \quad \frac{a}{d}x \equiv \frac{b}{d} \pmod{\frac{n}{d}}$$

are identical.



Example 15 *Solving a linear congruence when a and n are not coprime*

Solve the linear congruence $12x \equiv 16 \pmod{20}$.

Solution

☁ Check that the linear congruence has solutions. ☁

The highest common factor of 12 and 20 is 4. Since 16 is divisible by 4, the linear congruence has solutions.

☁ Divide each of the integers 12, 16 and 20 in the linear congruence $12x \equiv 16 \pmod{20}$ by 4 to obtain an equivalent linear congruence. ☁

and is equivalent to

$$3x \equiv 4 \pmod{5}.$$

☁ Since the numbers involved are small, try the values 1, 2, 3, ... one by one until you find a solution. ☁

Trying the values 1, 2, 3, ... one by one, we find that

$$3 \times 1 \equiv 3 \pmod{5} \quad 3 \times 2 \equiv 6 \equiv 1 \pmod{5}$$

$$3 \times 3 \equiv 9 \equiv 4 \pmod{5}.$$

So the solutions are given by

$$x \equiv 3 \pmod{5}.$$

Activity 35 *Solving linear congruences when a and n are not coprime*

Solve the following linear congruences.

(a) $12x \equiv 6 \pmod{15}$ (b) $-25x \equiv 10 \pmod{40}$

(c) $18x \equiv 6 \pmod{98}$

You now know how to determine whether a linear congruence has solutions and, if so, how to find the solutions. The results that you've met are summarised as follows.

Solving the linear congruence $ax \equiv b \pmod{n}$

Let d be the highest common factor of a and n .

- If $d = 1$, then the linear congruence has solutions. The solutions are given by

$$x \equiv vb \pmod{n},$$

where v is any multiplicative inverse of a modulo n .

- If b is not divisible by d , then the linear congruence has no solutions.
- If b is divisible by d , then the linear congruence has solutions and the solutions are given by the solutions of the equivalent linear congruence

$$\frac{a}{d}x \equiv \frac{b}{d} \pmod{\frac{n}{d}}.$$

You may also find the decision tree in Figure 13 helpful.

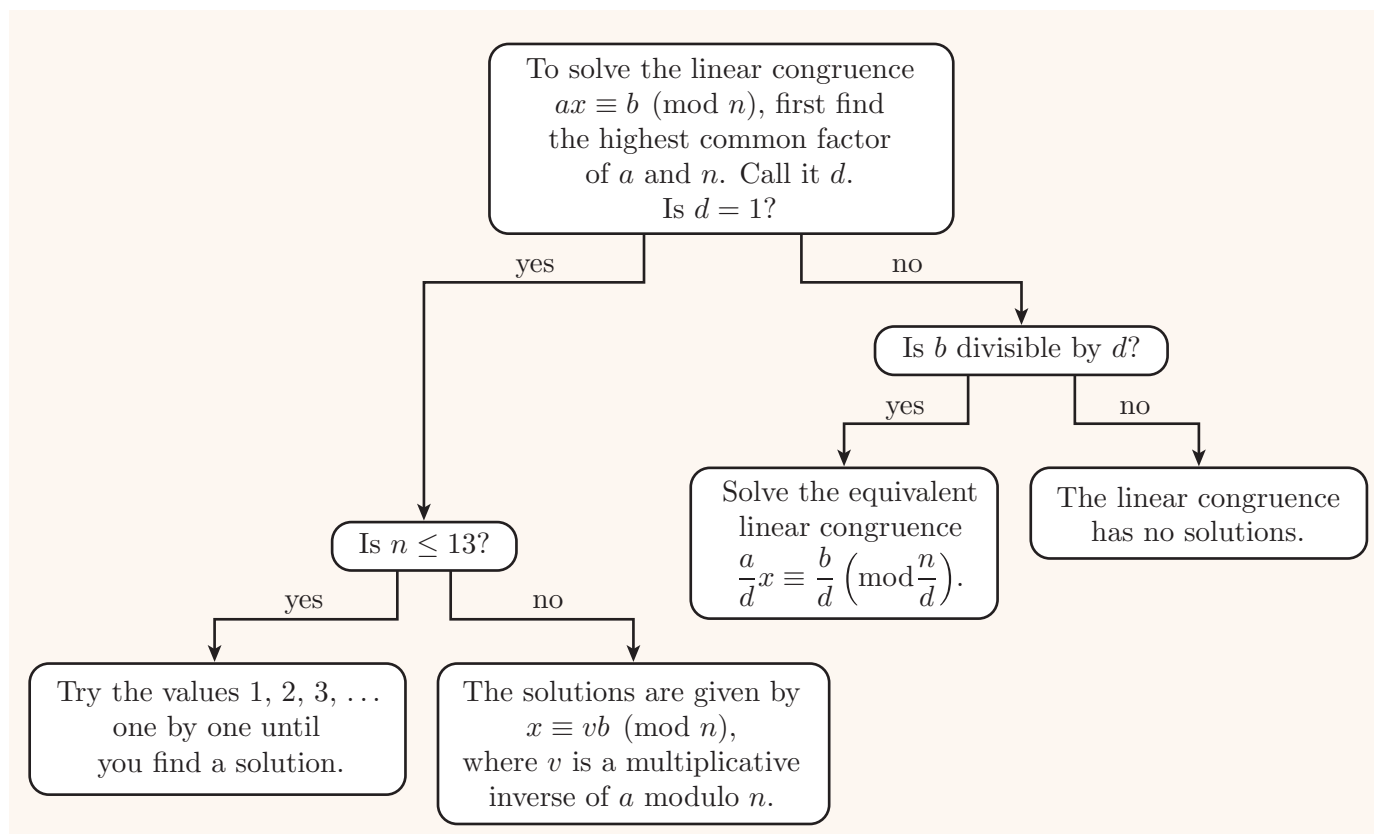


Figure 13 A decision tree for solving a linear congruence

Activity 36 *Solving a variety of linear congruences*

Solve the following linear congruences.

- (a) $5x \equiv 21 \pmod{9}$ (b) $11x \equiv 6 \pmod{38}$
 (c) $21x \equiv 14 \pmod{30}$ (d) $-48x \equiv 24 \pmod{28}$

3.4 Affine ciphers

Usually, when a sensitive message is transmitted, it is first transformed to disguise it from all but the intended recipients. The algorithm used to transform a message is called a **cipher**, and the design of ciphers is called **cryptography**. Ciphers have been used throughout history for military and diplomatic communications and, in recent years, they have been increasingly used to protect the electronic transfer of confidential information and money.

Here you'll learn about one particular type of cipher, called an *affine cipher*, which uses some of the theory of linear congruences developed earlier. Although it is too basic a cipher to be used for sensitive information, many of the features of affine ciphers are shared by more sophisticated ciphers.

Before you can apply an affine cipher, or a cipher of a similar type, you must first replace the letters of the message you wish to transmit by numbers. Throughout this subsection we use Table 1 to switch between letters and numbers.

Table 1 A conversion table for letters and numbers

A	B	C	D	E	F	G	H	I	J	K	L	M
0	1	2	3	4	5	6	7	8	9	10	11	12
N	O	P	Q	R	S	T	U	V	W	X	Y	Z
13	14	15	16	17	18	19	20	21	22	23	24	25

For example, using Table 1 you can write the message

HULLABALOO

as

7, 20, 11, 11, 0, 1, 0, 11, 14, 14.

Now suppose that we wish to apply a cipher to this message; this process is called **enciphering**. Many simple ciphers consist of a rule for reordering the integers $0, 1, 2, \dots, 25$ to disguise the message. For instance, you may have a rule that says you should replace the integer x with the integer $E(x)$ from $0, 1, 2, \dots, 25$ that satisfies

$$E(x) \equiv 5x + 23 \pmod{26}.$$

Using this rule,

$$\begin{aligned} E(0) &= 23, & \text{as } 5 \times 0 + 23 &\equiv 23 \pmod{26}, \\ E(1) &= 2, & \text{as } 5 \times 1 + 23 &\equiv 28 \equiv 2 \pmod{26}, \\ E(2) &= 7, & \text{as } 5 \times 2 + 23 &\equiv 33 \equiv 7 \pmod{26}, \end{aligned}$$

and so on. Our message 7, 20, 11, 11, 0, 1, 0, 11, 14, 14 becomes

$$\begin{array}{cccccccccc} 7, & 20, & 11, & 11, & 0, & 1, & 0, & 11, & 14, & 14 \\ \downarrow & \downarrow & \downarrow & \downarrow & \downarrow & \downarrow & \downarrow & \downarrow & \downarrow & \downarrow \\ 6, & 19, & 0, & 0, & 23, & 2, & 23, & 0, & 15, & 15. \end{array}$$

You can check this yourself. To do so, it may help you to notice that $23 \equiv -3 \pmod{26}$, so the rule for enciphering the message can be rewritten as

$$E(x) \equiv 5x - 3 \pmod{26}.$$

This cipher is an example of an affine cipher.

Affine ciphers

An **affine cipher** modulo 26 is a rule E for reordering the integers $0, 1, 2, \dots, 25$ given by

$$E(x) \equiv ax + b \pmod{26},$$

where a and b are integers, and a and 26 are coprime.

This definition only allows affine ciphers modulo 26, because the only ciphers you'll meet here are those that use the 26 letters of the alphabet represented by integers in Table 1. To encipher a message that uses a different set of characters you can use an affine cipher of the form $E(x) \equiv ax + b \pmod{n}$, where n is the number of characters you wish to choose from, and a and n are coprime.

The integers a and 26 must be coprime so that a has a multiplicative inverse modulo 26. The significance of this will be made clear shortly. For now, you may like to practise enciphering a message using an affine cipher.

Activity 37 *Enciphering a message with an affine cipher*

Using Table 1 and the affine cipher

$$E(x) \equiv 3x + 14 \pmod{26},$$

encipher the message BROUHAHA.

The process of recovering the original message from an enciphered message is called **deciphering**. With affine ciphers, it's possible to decipher a message if you know the particular affine cipher used to encipher the message. For example, suppose that you receive the message

$$6, 19, 0, 0, 23, 2, 23, 0, 15, 15,$$

which you know has been created using the affine cipher

$E(x) \equiv 5x + 23 \pmod{26}$ considered earlier. To decipher the first integer from this message, namely 6, you must find the integer x from $0, 1, 2, \dots, 25$ that satisfies $E(x) = 6$. That is, you must solve the congruence

$$5x + 23 \equiv 6 \pmod{26}.$$

To find x , first subtract 23 from both sides of the congruence.

Since $6 - 23 \equiv -17 \equiv 9 \pmod{26}$, you obtain

$$5x \equiv 9 \pmod{26}.$$

This is a linear congruence. It follows from the results in the previous subsection that this can be solved, since 5 and 26 are coprime, and the solutions are given by

$$x \equiv 9v \pmod{26},$$

where v is a multiplicative inverse of 5 modulo 26. The simplest way to find a value for v is to observe that

$$5 \times 5 \equiv 25 \equiv -1 \pmod{26},$$

so

$$(-5) \times 5 \equiv 1 \pmod{26}$$

and hence -5 is a multiplicative inverse of 5 modulo 26.

(Since $21 \equiv -5 \pmod{26}$, the integer 21 is also a multiplicative inverse of 5 modulo 26; however, it's easier to use -5 .) So the solutions are given by

$$x \equiv (-5) \times 9 \equiv -45 \equiv 7 \pmod{26}$$

and hence x is the integer 7.

You could decipher each of the integers of the enciphered message in this way to recover the original message. If you were to do so, then you would find that you perform a similar set of operations each time. A quicker method to decipher the whole message is to obtain a ‘deciphering rule’ D that undoes the enciphering rule E . Let’s explain how to find D . Suppose that you wish to decipher the integer y . (You’ve just seen how to decipher the integer 6.) You must find the integer x that satisfies $E(x) = y$. That is, you must solve the congruence

$$5x + 23 \equiv y \pmod{26}.$$

Subtracting 23 from both sides gives

$$5x \equiv y - 23 \pmod{26}.$$

Multiplying both sides by -5 , which as you’ve seen is a multiplicative inverse of 5 modulo 26, gives

$$x \equiv -5(y - 23) \pmod{26}.$$

So the rule D that undoes the transformation E is given by

$$D(y) \equiv -5(y - 23) \pmod{26}.$$

This strategy for obtaining a deciphering rule works for *any* affine cipher.

Deciphering rule for affine ciphers

The rule D for deciphering the affine cipher $E(x) \equiv ax + b \pmod{26}$ is given by

$$D(y) \equiv v(y - b) \pmod{26},$$

where v is any multiplicative inverse of a modulo 26.

In the terminology of sets and functions, E is a one-to-one function and D is the inverse function of E .



Example 16 *Deciphering a message that has been enciphered using an affine cipher*

Suppose you receive the enciphered message 3, 17, 18, 7, which you know has been created using the affine cipher

$$E(x) \equiv 9x + 21 \pmod{26}.$$

What does the message say?

Solution

Write down a rule for deciphering the message.

A rule D for deciphering the message is given by

$$D(y) \equiv v(y - 21) \pmod{26},$$

where v is a multiplicative inverse of 9 modulo 26.

Find a multiplicative inverse of 9 modulo 26. You could apply Euclid's algorithm and backwards substitution, but it's quicker to notice that $3 \times 9 = 27$.

Since

$$3 \times 9 \equiv 27 \equiv 1 \pmod{26},$$

we see that 3 is a multiplicative inverse of 9 modulo 26. So

$$D(y) \equiv 3(y - 21) \equiv 3(y + 5) \pmod{26}.$$

Use the deciphering rule to decipher the message.

Hence

$$D(3) \equiv 3(3 + 5) \equiv 24 \pmod{26},$$

$$D(17) \equiv 3(17 + 5) \equiv 66 \equiv 14 \pmod{26},$$

$$D(18) \equiv 3(18 + 5) \equiv 69 \equiv 17 \pmod{26},$$

$$D(7) \equiv 3(7 + 5) \equiv 36 \equiv 10 \pmod{26}.$$

So the deciphered message is

$$24, 14, 17, 10,$$

which, by Table 1, says

YORK.

Activity 38 *Deciphering messages that have been enciphered using affine ciphers*

Suppose you receive the following two messages that have been enciphered using the specified affine cipher E . What do the messages say?

- (a) 14, 10, 6, 22, 22, using $E(x) \equiv 5x + 10 \pmod{26}$
 (b) 22, 8, 11, 22, 9, using $E(x) \equiv -9x + 6 \pmod{26}$

The ciphers that you have met in this section have all been very simple and you could have cracked them without using modular arithmetic. The ideas that you have met, however, are used in the construction of more sophisticated ciphers.

The RSA factorising challenge

RSA ciphers are widely used in computing, business and military communication. They are named after Ron Rivest, Adi Shamir and Leonard Adleman who developed the algorithm in 1977. Modular arithmetic is a fundamental tool in RSA ciphers, as it is in many ciphers.

To encipher a message using the RSA algorithm, you must first choose two large prime numbers p and q , and form their product $n = pq$. The integer n can be made public, but p and q must remain secret. If p and q are discovered, then the cipher can be cracked. If p and q are sufficiently large, then it is extremely difficult to find them even if you know the value of n . In 1991, RSA Laboratories published a list of around fifty integers n , each a product of two primes, with a challenge to factorise them. Cash prizes were offered for factorising some of the larger numbers.

The smallest number in the list is known as RSA-100 because it has 100 digits. It is

15226050279225333605356183781326374297180681149613
 80688657908494580122963258952897654000350692006139.

Within a month of the challenge opening, RSA-100 had been factorised into two primes:

37975227936943673922808872755445627854565536638199
 \times 40094690950920881030683735292761468389214899724061.

By 2007, when the challenge finished, fewer than half the numbers in the list had been factorised.

Learning outcomes

After studying this unit, you should be able to:

- find quotients and remainders from integer division
- apply Euclid's algorithm and backwards substitution
- understand the definitions of congruences, residue classes and least residues
- add and subtract integers modulo n
- multiply integers and calculate powers modulo n
- understand and apply Fermat's little theorem
- test whether an integer is divisible by 3 or 9
- check whether 10-digit ISBNs are valid
- determine multiplicative inverses modulo n
- solve linear congruences
- encipher and decipher messages using affine ciphers.

Solutions to activities

Solution to Activity 1

- (a) The quotient $q = 8$ and the remainder $r = 3$.
So the equation $a = qn + r$ is

$$59 = 8 \times 7 + 3.$$

- (b) $q = 7$, $r = 0$, and so $84 = 7 \times 12 + 0$.
 (c) $q = 11$, $r = 1$, and so $100 = 11 \times 9 + 1$.
 (d) $q = 0$, $r = 9$, and so $9 = 0 \times 100 + 9$.
 (e) $q = 0$, $r = 0$, and so $0 = 0 \times 11 + 0$.
 (f) $q = -12$, $r = 2$, and so $-58 = -12 \times 5 + 2$.
 (g) $q = -12$, $r = 8$, and so $-100 = -12 \times 9 + 8$.
 (h) $q = -8$, $r = 0$, and so $-96 = -8 \times 12 + 0$.
 (i) $q = -1$, $r = 1$, and so $-4 = -1 \times 5 + 1$.

Solution to Activity 2

- (a) Euclid's algorithm gives

$$93 = 4 \times 21 + 9$$

$$21 = 2 \times 9 + 3$$

$$9 = 3 \times 3 + 0.$$

So the highest common factor of 93 and 21 is 3.

- (b) Euclid's algorithm gives

$$138 = 2 \times 61 + 16$$

$$61 = 3 \times 16 + 13$$

$$16 = 1 \times 13 + 3$$

$$13 = 4 \times 3 + 1$$

$$3 = 3 \times 1 + 0.$$

So the highest common factor of 138 and 61 is 1.

- (c) Euclid's algorithm gives

$$231 = 4 \times 49 + 35$$

$$49 = 1 \times 35 + 14$$

$$35 = 2 \times 14 + 7$$

$$14 = 2 \times 7 + 0.$$

So the highest common factor of 231 and 49 is 7.

Solution to Activity 3

- (a) Euclid's algorithm gives

$$93 = 2 \times 42 + 9$$

$$42 = 4 \times 9 + 6$$

$$9 = 1 \times 6 + 3$$

$$6 = 2 \times 3 + 0.$$

So the highest common factor of 93 and 42 is 3.

Rearranging the equations gives

$$\textcircled{9} = \textcircled{93} - 2 \times \textcircled{42}$$

$$\textcircled{6} = \textcircled{42} - 4 \times \textcircled{9}$$

$$\textcircled{3} = \textcircled{9} - 1 \times \textcircled{6}.$$

Backwards substitution gives

$$\begin{aligned} \textcircled{3} &= \textcircled{9} - \left(\textcircled{42} - 4 \times \textcircled{9} \right) \\ &= 5 \times \textcircled{9} - \textcircled{42} \\ &= 5 \times \left(\textcircled{93} - 2 \times \textcircled{42} \right) - \textcircled{42} \\ &= 5 \times \textcircled{93} - 11 \times \textcircled{42}. \end{aligned}$$

So $93 \times 5 + 42 \times (-11) = 3$. This is the equation $93v + 42w = d$ with $v = 5$ and $w = -11$.

(Check: $93 \times 5 + 42 \times (-11) = 465 - 462 = 3$.)

- (b) Euclid's algorithm gives

$$70 = 2 \times 29 + 12$$

$$29 = 2 \times 12 + 5$$

$$12 = 2 \times 5 + 2$$

$$5 = 2 \times 2 + 1$$

$$2 = 2 \times 1 + 0.$$

The highest common factor of 70 and 29 is 1.

Rearranging the equations gives

$$\textcircled{12} = \textcircled{70} - 2 \times \textcircled{29}$$

$$\textcircled{5} = \textcircled{29} - 2 \times \textcircled{12}$$

$$\textcircled{2} = \textcircled{12} - 2 \times \textcircled{5}$$

$$\textcircled{1} = \textcircled{5} - 2 \times \textcircled{2}.$$

Backwards substitution gives

$$\begin{aligned} \textcircled{1} &= \textcircled{5} - 2 \times \left(\textcircled{12} - 2 \times \textcircled{5} \right) \\ &= 5 \times \textcircled{5} - 2 \times \textcircled{12} \\ &= 5 \times \left(\textcircled{29} - 2 \times \textcircled{12} \right) - 2 \times \textcircled{12} \\ &= 5 \times \textcircled{29} - 12 \times \textcircled{12} \\ &= 5 \times \textcircled{29} - 12 \times \left(\textcircled{70} - 2 \times \textcircled{29} \right) \\ &= 29 \times \textcircled{29} - 12 \times \textcircled{70}. \end{aligned}$$

So $70 \times (-12) + 29 \times 29 = 1$. This is the equation $70v + 29w = d$ with $v = -12$ and $w = 29$.

(Check:

$$70 \times (-12) + 29 \times 29 = -840 + 841 = 1.)$$

Solution to Activity 4

(a) Euclid's algorithm gives

$$112 = 1 \times 91 + 21$$

$$91 = 4 \times 21 + 7$$

$$21 = 3 \times 7 + 0.$$

So the HCF of 112 and 91 is 7, and hence the HCF of -112 and -91 is also 7.

Rearranging the equations gives

$$(21) = (112) - 1 \times (91)$$

$$(7) = (91) - 4 \times (21).$$

Backwards substitution gives

$$\begin{aligned} (7) &= (91) - 4 \times ((112) - 1 \times (91)) \\ &= 5 \times (91) - 4 \times (112). \end{aligned}$$

So

$$-112 \times 4 - 91 \times (-5) = 7.$$

This is the equation $-112v - 91w = d$ with $v = 4$ and $w = -5$.

(Check:

$$-112 \times 4 - 91 \times (-5) = -448 + 455 = 7.)$$

(b) Euclid's algorithm gives

$$105 = 2 \times 39 + 27$$

$$39 = 1 \times 27 + 12$$

$$27 = 2 \times 12 + 3$$

$$12 = 4 \times 3 + 0.$$

So the HCF of 105 and 39 is 3, and hence the HCF of -105 and 39 is also 3. Rearranging the equations gives

$$(27) = (105) - 2 \times (39)$$

$$(12) = (39) - 1 \times (27)$$

$$(3) = (27) - 2 \times (12).$$

Backwards substitution gives

$$\begin{aligned} (3) &= (27) - 2 \times ((39) - 1 \times (27)) \\ &= 3 \times (27) - 2 \times (39) \\ &= 3 \times ((105) - 2 \times (39)) - 2 \times (39) \\ &= 3 \times (105) - 8 \times (39). \end{aligned}$$

So

$$-105 \times (-3) + 39 \times (-8) = 3.$$

This is the equation $-105v + 39w = d$ with $v = -3$ and $w = -8$.

(Check:

$$-105 \times (-3) + 39 \times (-8) = 315 - 312 = 3.)$$

Solution to Activity 5

In order to obtain 1 litre of water in the cauldron in this way, we would need to find integers v and w such that

$$23v + 16w = 1.$$

It is easy to see that the highest common factor of the integers 23 and 16 is 1 and so the existence of such integers v and w follows from Bézout's identity. So it is possible to obtain 1 litre of water in the cauldron in this way.

In order to describe how to do this, we find the integers v and w in the usual way. Euclid's algorithm gives

$$23 = 1 \times 16 + 7$$

$$16 = 2 \times 7 + 2$$

$$7 = 3 \times 2 + 1$$

$$2 = 2 \times 1 + 0.$$

Rearranging the equations gives

$$(7) = (23) - 1 \times (16)$$

$$(2) = (16) - 2 \times (7)$$

$$(1) = (7) - 3 \times (2).$$

Backwards substitution gives

$$\begin{aligned} (1) &= (7) - 3 \times ((16) - 2 \times (7)) \\ &= 7 \times (7) - 3 \times (16) \\ &= 7 \times ((23) - 1 \times (16)) - 3 \times (16) \\ &= 7 \times (23) - 10 \times (16). \end{aligned}$$

So

$$23 \times 7 + 16 \times (-10) = 1.$$

So if we fill the 23-litre bucket from the tap and pour it into the cauldron 7 times, then fill the 16-litre bucket from the cauldron and empty it out 10 times, we will be left with 1 litre of water in the cauldron.

Solution to Activity 7

- (a) True: 11 and 26 each have remainder 1 on division by 5.
- (b) False: 9 has remainder 4 on division by 5 and -9 has remainder 1 on division by 5.
- (c) True: 28 and 0 each have remainder 0 on division by 7.
- (d) True: -4 and -18 each have remainder 3 on division by 7.
- (e) True: -8 and 5 each have remainder 5 on division by 13.
- (f) False: 38 is not divisible by 13.

Solution to Activity 8

- (a) The final digit of a positive integer is the remainder that we obtain when we divide that integer by 10. It follows that to check whether two positive integers are congruent modulo 10, we just need to check whether their final digits are equal.
- (b) The method described in (a) doesn't work when we compare a positive integer with a negative integer. For example, -17 and 27 both have final digit 7, but they are not congruent modulo 10, because -17 has remainder 3 (not 7) when divided by 10.

Solution to Activity 9

- (a) True: $63 - 14 = 49$, which is divisible by 7.
- (b) False: $-39 - 39 = -78$, which is not divisible by 7.
- (c) False: $63 - 14 = 49$, which is not divisible by 12.
- (d) True: $-8 - 16 = -24$, which is divisible by 12.
- (e) True: $-30 - (-17) = -13$, which is divisible by 13.
- (f) True: $43 - (-87) = 130$, which is divisible by 13.

Solution to Activity 10

If a is an odd number, then we can write $a = 1 + 2k$ for some integer k . This means that $a \equiv 1 \pmod{2}$.

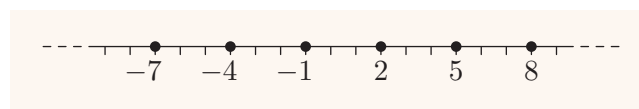
If a is an even number, then we can write $a = 2k$, or $a = 0 + 2k$, for some integer k . This means that $a \equiv 0 \pmod{2}$.

Solution to Activity 11

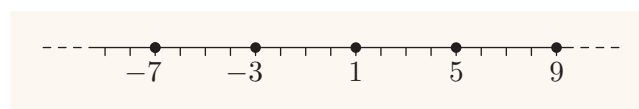
- (a) False: -7 and 7 are not congruent modulo 10, because $7 - (-7) = 14$, and 14 is not divisible by 10.
- (b) True: -17 , 3 , 31 and 67 are all odd integers, so each has a remainder 1 when divided by 2.
- (c) True: -84 , 0 and 108 each have a remainder 0 when divided by 12.

Solution to Activity 12

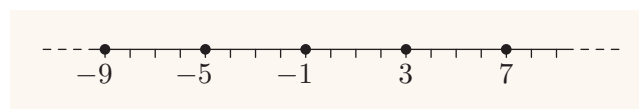
(a)



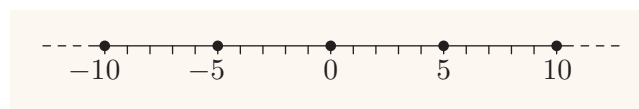
(b)



(c)



(d)



Solution to Activity 13

- (a) Since $17 = 1 \times 10 + 7$, the least residue is 7.
- (b) Since $50 = 5 \times 10 + 0$, the least residue is 0.
- (c) Since $6 = 0 \times 10 + 6$, the least residue is 6.
- (d) Since $-1 = (-1) \times 10 + 9$, the least residue is 9.
- (e) Since $-38 = (-4) \times 10 + 2$, the least residue is 2.

Solution to Activity 14

- (a) Since $17 = 5 \times 3 + 2$, the least residue is 2.
 (b) Since $9 = 3 \times 3 + 0$, the least residue is 0.
 (c) Since $-2 = (-1) \times 3 + 1$, the least residue is 1.
 (d) Since $-10 = (-4) \times 3 + 2$, the least residue is 2.
 (e) Since $3 = 1 \times 3 + 0$, the least residue is 0.

Solution to Activity 15

There are 7 days in a week and so, in 1000 days' time, the day will be the same as it is today plus the remainder that you obtain when you divide 1000 by 7 (that is, the least residue of 1000 modulo 7). When you divide 1000 by 7 you obtain a remainder of 6. Therefore $1000 \equiv 6 \pmod{7}$. Since $6 \equiv -1 \pmod{7}$, it follows that in 1000 days' time it will be the same day as yesterday!

Solution to Activity 16

- (a) $7 + 3 \equiv 10 \equiv 4 \pmod{6}$

So the least residue is 4.

(The statement 'So the least residue is ...' is omitted in solutions to subsequent parts of this activity. We follow a similar convention in later activities.)

- (b) $7 - 3 \equiv 4 \pmod{6}$
 (c) $23 - 24 \equiv -1 \equiv 5 \pmod{6}$
 (d) $-3 - 19 \equiv 3 - 1 \equiv 2 \pmod{6}$
 (e) $67 + 68 \equiv 1 + 2 \equiv 3 \pmod{6}$
 (f) $601 - 6001 \equiv 1 - 1 \equiv 0 \pmod{6}$

Solution to Activity 17

- (a) $6 + 4 \equiv 10 \equiv 0 \pmod{10}$
 (b) $14 - 7 \equiv 7 \pmod{10}$
 (c) $13 - 15 \equiv -2 \equiv 8 \pmod{10}$
 (d) $-21 - 17 \equiv -1 - 7 \equiv -8 \equiv 2 \pmod{10}$
 (e) $101 + 11 + 1 \equiv 1 + 1 + 1 \equiv 3 \pmod{10}$
 (f) $101 - 11 - 1 \equiv 1 - 1 - 1 \equiv -1 \equiv 9 \pmod{10}$

Solution to Activity 18

- (a) $3 \times 6 \equiv 18 \equiv 4 \pmod{7}$

So the least residue is 4.

Here is an alternative solution.

$$3 \times 6 \equiv 3 \times (-1) \equiv -3 \equiv 4 \pmod{7}$$

Again, we see that the least residue is 4.

There are many other solutions to this problem, as there are to the other parts of this activity. Your solutions may differ from those that are given.

- (b) $22 \times 29 \equiv 1 \times 1 \equiv 1 \pmod{7}$
 (c) $(-5) \times 16 \equiv 2 \times 2 \equiv 4 \pmod{7}$
 (d) $51 \times 74 \equiv 2 \times 4 \equiv 8 \equiv 1 \pmod{7}$
 (e) $47 \times (-25) \equiv (-2) \times 3 \equiv -6 \equiv 1 \pmod{7}$
 (f) $(-29) \times (-44) \equiv 29 \times 44 \equiv 1 \times 2 \equiv 2 \pmod{7}$

Solution to Activity 19

- (a) $4 \times 4 \equiv 16 \equiv 0 \pmod{8}$
 (b) $17 \times 26 \equiv 1 \times 2 \equiv 2 \pmod{8}$
 (c) $(-6) \times 34 \equiv 2 \times 2 \equiv 4 \pmod{8}$
 (d) $16 \times 457 \equiv 0 \times 457 \equiv 0 \pmod{8}$
 (e) $47 \times (-25) \equiv (-1) \times (-1) \equiv 1 \pmod{8}$
 (f) $(-61) \times (-46) \equiv 61 \times 46$
 $\quad \quad \quad \equiv (-3) \times (-2)$
 $\quad \quad \quad \equiv 6 \pmod{8}$

Solution to Activity 20

- (a) Since
- $25 \equiv 1 \pmod{6}$
- , it follows that

$$25^{25} \equiv 1^{25} \equiv 1 \pmod{6}.$$

So the least residue is 1.

- (b) Since
- $-9 \equiv 3 \pmod{6}$
- , it follows that

$$(-9)^4 \equiv 3^4 \pmod{6}.$$

Calculating powers of 3 gives

$$3^2 = 9$$

and so

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

Therefore

$$3^4 \equiv 3^2 \times 3^2 \equiv 3 \times 3 \equiv 9 \equiv 3 \pmod{6}.$$

In summary,

$$(-9)^4 \equiv 3 \pmod{6}.$$

So the least residue is 3.

- (c) Since
- $20 \equiv 2 \pmod{6}$
- , it follows that

$$20^6 \equiv 2^6 \pmod{6}.$$

Calculating powers of 2 gives

$$2^2 = 4 \text{ and } 2^3 = 8$$

and so

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

Therefore

$$2^6 \equiv 2^3 \times 2^3 \equiv 2 \times 2 \equiv 4 \pmod{6}.$$

In summary,

$$20^6 \equiv 4 \pmod{6}.$$

So the least residue is 4.

Solution to Activity 21

- (a) Since
- $25 \equiv -1 \pmod{13}$
- , it follows that

$$25^{25} \equiv (-1)^{25} \equiv -1 \equiv 12 \pmod{13}.$$

So the least residue is 12.

- (b) Since
- $54 \equiv 2 \pmod{13}$
- , it follows that

$$54^4 \equiv 2^4 \equiv 16 \equiv 3 \pmod{13}.$$

So the least residue is 3.

- (c) Since
- $16 \equiv 3 \pmod{13}$
- , it follows that

$$16^9 \equiv 3^9 \pmod{13}.$$

Calculating powers of 3 gives

$$3^2 = 9 \text{ and } 3^3 = 27$$

and so

$$3^3 \equiv 1 \pmod{13}.$$

Therefore

$$3^9 \equiv 3^3 \times 3^3 \times 3^3 \equiv 1^3 \equiv 1 \pmod{13}.$$

In summary,

$$16^9 \equiv 1 \pmod{13}.$$

So the least residue is 1.

Solution to Activity 22

- (a) Since
- $1^4 = 1$
- , the least residue is 1.

- (b) Since

$$2^4 \equiv 16 \equiv 1 \pmod{5},$$

the least residue is 1.

- (c) Since

$$3^4 \equiv (-2)^4 \equiv 16 \equiv 1 \pmod{5},$$

the least residue is 1.

(Alternatively, since

$$3^4 \equiv 81 \equiv 1 \pmod{5},$$

the least residue is 1.)

- (d) Since

$$4^4 \equiv (-1)^4 \equiv 1 \pmod{5},$$

the least residue is 1.

- (e) Since
- $7 \equiv 2 \pmod{5}$
- it follows from part (b) that

$$7^4 \equiv 2^4 \equiv 1 \pmod{5}.$$

So the least residue is 1.

Solution to Activity 23

- (a) By Fermat's little theorem,
 $5^6 \equiv 1 \pmod{7}$.

So the least residue is 1.

- (b) First, $18 \equiv 4 \pmod{7}$ so
 $18^{18} \equiv 4^{18} \pmod{7}$.

By Fermat's little theorem,
 $4^6 \equiv 1 \pmod{7}$.

Since $18 = 3 \times 6$, we obtain

$$\begin{aligned} 4^{18} &\equiv (4^6)^3 \\ &\equiv 1^3 \\ &\equiv 1 \pmod{7}. \end{aligned}$$

So the least residue is 1.

- (c) First, $-11 \equiv 3 \pmod{7}$ so
 $(-11)^{33} \equiv 3^{33} \pmod{7}$.

By Fermat's little theorem,
 $3^6 \equiv 1 \pmod{7}$.

Since $33 = 5 \times 6 + 3$, we obtain

$$\begin{aligned} 3^{33} &\equiv (3^6)^5 \times 3^3 \\ &\equiv 1^5 \times 3^3 \\ &\equiv 27 \\ &\equiv 6 \pmod{7}. \end{aligned}$$

So the least residue is 6.

Solution to Activity 24

- (a) By Fermat's little theorem,
 $7^{10} \equiv 1 \pmod{11}$.

So the least residue is 1.

- (b) First, $-5 \equiv 6 \pmod{11}$ so
 $(-5)^{31} \equiv 6^{31} \pmod{11}$.

By Fermat's little theorem,
 $6^{10} \equiv 1 \pmod{11}$.

Since $31 = 3 \times 10 + 1$, we obtain

$$\begin{aligned} 6^{31} &\equiv (6^{10})^3 \times 6^1 \\ &\equiv 1^3 \times 6 \\ &\equiv 6 \pmod{11}. \end{aligned}$$

So the least residue is 6.

- (c) First, $13 \equiv 2 \pmod{11}$ so

$$13^{85} \equiv 2^{85} \pmod{11}.$$

By Fermat's little theorem,

$$2^{10} \equiv 1 \pmod{11}.$$

Since $85 = 8 \times 10 + 5$, we obtain

$$\begin{aligned} 2^{85} &\equiv (2^{10})^8 \times 2^5 \\ &\equiv 1^8 \times 2^5 \\ &\equiv 32 \\ &\equiv 10 \pmod{11}. \end{aligned}$$

So the least residue is 10.

Solution to Activity 25

- (a) The digit sum of 982 is $9 + 8 + 2 = 19$. This is not divisible by 3, so 982 is not divisible by 3.

- (b) The digit sum of 753 is $7 + 5 + 3 = 15$. This is divisible by 3, so 753 is divisible by 3.

- (c) The digit sum of 8364 is

$$8 + 3 + 6 + 4 = 21.$$

This is divisible by 3, so 8364 is divisible by 3.

- (d) The digit sum of -9245 is

$$9 + 2 + 4 + 5 = 20.$$

This is not divisible by 3, so -9245 is not divisible by 3.

- (e) The digit sum of 98 285 385 335 is

$$9 + 8 + 2 + 8 + 5 + 3 + 8 + 5 + 3 + 3 + 5 = 59.$$

The digit sum of 59 is $5 + 9 = 14$. This is not divisible by 3, so 59 is not divisible by 3, and hence 98 285 385 335 is not divisible by 3.

- (f) The digits of 10^{100} consist of a single 1 and one hundred 0s. Therefore 10^{100} has digit sum 1, which is not divisible by 3, so 10^{100} is not divisible by 3.

Solution to Activity 26

(a) The digit sum of 8469 is $8 + 4 + 6 + 9 = 27$.
This is divisible by 9, so 8469 is divisible by 9.

(b) The digit sum of 6172 is $6 + 1 + 7 + 2 = 16$.
This is not divisible by 9, so 6172 is not divisible by 9.

(c) The digit sum of 7 989 989 897 979 897 is

$$7 + 9 + 8 + 9 + 9 + 8 + 9 + 8 \\ + 9 + 7 + 9 + 7 + 9 + 8 + 9 + 7 = 132.$$

The digit sum of 132 is $1 + 3 + 2 = 6$. This is not divisible by 9, therefore 132 is not divisible by 9, and nor is 7 989 989 897 979 897.

Solution to Activity 27

$$\begin{aligned} \text{(a)} \quad & 0 + 2 \cdot 0 + 3 \cdot 1 + 4 \cdot 6 + 5 \cdot 0 \\ & + 6 \cdot 6 + 7 \cdot 2 + 8 \cdot 1 + 9 \cdot 4 + 10 \cdot 0 \\ & \equiv 0 + 0 + 3 + 24 + 0 + 36 + 14 + 8 + 36 + 0 \\ & \equiv 0 + 0 + 3 + 2 + 0 + 3 + 3 + 8 + 3 + 0 \\ & \equiv 22 \\ & \equiv 0 \pmod{11} \end{aligned}$$

So 0412606100 satisfies the ISBN congruence check.

$$\begin{aligned} \text{(b)} \quad & 10 + 2 \cdot 8 + 3 \cdot 7 + 4 \cdot 2 + 5 \cdot 2 \\ & + 6 \cdot 4 + 7 \cdot 1 + 8 \cdot 0 + 9 \cdot 2 + 10 \cdot 0 \\ & \equiv 10 + 16 + 21 + 8 + 10 + 24 + 7 + 0 + 18 + 0 \\ & \equiv 10 + 5 + 10 + 8 + 10 + 2 + 7 + 0 + 7 + 0 \\ & \equiv 59 \\ & \not\equiv 0 \pmod{11} \end{aligned}$$

So 020142278X does not satisfy the ISBN congruence check.

$$\begin{aligned} \text{(c)} \quad & 9 + 2 \cdot 0 + 3 \cdot 8 + 4 \cdot 8 + 5 \cdot 1 \\ & + 6 \cdot 1 + 7 \cdot 1 + 8 \cdot 9 + 9 \cdot 6 + 10 \cdot 0 \\ & \equiv 9 + 0 + 24 + 32 + 5 + 6 + 7 + 72 + 54 + 0 \\ & \equiv 9 + 0 + 2 + 10 + 5 + 6 + 7 + 6 + 10 + 0 \\ & \equiv 55 \\ & \equiv 0 \pmod{11} \end{aligned}$$

So 0691118809 satisfies the ISBN congruence check.

(Alternatively, the solutions to parts (a), (b) and (c) can be shortened by using congruences such as

$$10 \equiv -1 \pmod{11},$$

$$9 \equiv -2 \pmod{11},$$

$$8 \equiv -3 \pmod{11}.$$

For example, the congruences in (a) can be written as

$$\begin{aligned} & 0 + 2 \cdot 0 + 3 \cdot 1 + 4 \cdot 6 + 5 \cdot 0 \\ & - 5 \cdot 6 - 4 \cdot 2 - 3 \cdot 1 - 2 \cdot 4 - 1 \cdot 0 \\ & \equiv 0 + 0 + 3 + 24 + 0 - 30 - 8 - 3 - 8 + 0 \\ & \equiv -22 \\ & \equiv 0 \pmod{11}. \end{aligned}$$

Solution to Activity 28

(a) Since

$$1 \times 1 \equiv 1 \pmod{9},$$

1 is itself a multiplicative inverse of 1 modulo 9.

(b) Since

$$5 \times 2 \equiv 1 \pmod{9},$$

2 is a multiplicative inverse of 5 modulo 9.

(c) Trying the values 1, 2, 3, ... one by one, we find that

$$7 \times 4 \equiv 28 \equiv 1 \pmod{9},$$

so 4 is a multiplicative inverse of 7 modulo 9.

(d) Since

$$16 \equiv 7 \pmod{9},$$

16 has the same multiplicative inverse modulo 9 as 7, namely 4 (as you saw in part (c)), because

$$16 \times 4 \equiv 7 \times 4 \equiv 1 \pmod{9}.$$

Solution to Activity 29

- (a) The integer 0 doesn't have a multiplicative inverse modulo 9 because

$$0 \times v \equiv 0 \pmod{9}$$

for any integer v .

- (b) The congruence

$$6v \equiv 1 \pmod{9}$$

is equivalent to the statement that

$$6v = 1 + 9k,$$

for some integer k . In this equation, the left-hand side is divisible by 3, but the right-hand side is not. This is impossible, so 6 does not have a multiplicative inverse modulo 9.

(Alternatively, suppose that v is a multiplicative inverse of 6 modulo 9. Then $2v$ is a multiplicative inverse of 3 modulo 9 because

$$3 \times 2v \equiv 6v \equiv 1 \pmod{9}.$$

However, we've seen already that 3 does *not* have a multiplicative inverse modulo 9, so in fact there is no such integer v . That is, 6 doesn't have a multiplicative inverse modulo 9 after all.)

- (c) The integer 18 doesn't have a multiplicative inverse modulo 9 because $18 \equiv 0 \pmod{9}$, so

$$18v \equiv 0 \times v \equiv 0 \pmod{9}$$

for any integer v .

Solution to Activity 30

- (a) The integers 10 and 13 are coprime, so there is a multiplicative inverse of 10 modulo 13. Trying the values 2, 3, 4, ... one by one, we find that

$$4 \times 10 \equiv 40 \equiv 1 \pmod{13},$$

so 4 is a multiplicative inverse of 10 modulo 13.

- (b) The integers 12 and 21 are not coprime (since both are divisible by 3), so there is no multiplicative inverse of 12 modulo 21.
- (c) The integers 18 and 19 are coprime, so there is a multiplicative inverse of 18 modulo 19. Since $18 \equiv -1 \pmod{19}$ it follows that

$$18 \times 18 \equiv (-1) \times (-1) \equiv 1 \pmod{19}.$$

Therefore 18 is a multiplicative inverse of 18 modulo 19.

- (d) The integers 0 and 11 are not coprime (since both are divisible by 11), so there is no multiplicative inverse of 0 modulo 11.

(Alternatively, since $0 \times v \equiv 0 \pmod{11}$, for any integer v , there is no multiplicative inverse of 0 modulo 11. Reasoning in the same way you see that 0 doesn't have a multiplicative inverse modulo n , for any integer n .)

- (e) The integers 7 and 16 are coprime, so there is a multiplicative inverse of 7 modulo 16. Trying the values 2, 3, 4, ... one by one, we find that

$$7 \times 7 \equiv 49 \equiv 1 \pmod{16},$$

so 7 is a multiplicative inverse of 7 modulo 16.

- (f) Euclid's algorithm gives

$$57 = 5 \times 10 + 7$$

$$10 = 1 \times 7 + 3$$

$$7 = 2 \times 3 + 1$$

$$3 = 3 \times 1 + 0.$$

A remainder 1 is obtained, so 10 and 57 are coprime, and hence 10 has a multiplicative inverse modulo 57. Rearranging the equations gives

$$\textcircled{7} = \textcircled{57} - 5 \times \textcircled{10}$$

$$\textcircled{3} = \textcircled{10} - 1 \times \textcircled{7}$$

$$\textcircled{1} = \textcircled{7} - 2 \times \textcircled{3}.$$

Backwards substitution gives

$$\begin{aligned} \textcircled{1} &= \textcircled{7} - 2 \times (\textcircled{10} - 1 \times \textcircled{7}) \\ &= 3 \times \textcircled{7} - 2 \times \textcircled{10} \\ &= 3 \times (\textcircled{57} - 5 \times \textcircled{10}) - 2 \times \textcircled{10} \\ &= 3 \times \textcircled{57} - 17 \times \textcircled{10}. \end{aligned}$$

(Check: $3 \times 57 - 17 \times 10 = 171 - 170 = 1$.)

Hence

$$(-17) \times 10 \equiv 1 \pmod{57}$$

and so -17 is a multiplicative inverse of 10 modulo 57. Since

$$-17 \equiv 40 \pmod{57},$$

40 is also a multiplicative inverse of 10 modulo 57.

(g) Euclid's algorithm gives

$$217 = 2 \times 84 + 49$$

$$84 = 1 \times 49 + 35$$

$$49 = 1 \times 35 + 14$$

$$35 = 2 \times 14 + 7$$

$$14 = 2 \times 7 + 0.$$

So 7 is a factor of both 84 and 217, and hence there is no multiplicative inverse of 84 modulo 217.

(h) Euclid's algorithm gives

$$96 = 2 \times 43 + 10$$

$$43 = 4 \times 10 + 3$$

$$10 = 3 \times 3 + 1$$

$$3 = 3 \times 1 + 0.$$

A remainder 1 is obtained, so 43 and 96 are coprime, and hence 43 has a multiplicative inverse modulo 96. Rearranging the equations gives

$$\textcircled{10} = \textcircled{96} - 2 \times \textcircled{43}$$

$$\textcircled{3} = \textcircled{43} - 4 \times \textcircled{10}$$

$$\textcircled{1} = \textcircled{10} - 3 \times \textcircled{3}.$$

Backwards substitution gives

$$\textcircled{1} = \textcircled{10} - 3 \times (\textcircled{43} - 4 \times \textcircled{10})$$

$$= 13 \times \textcircled{10} - 3 \times \textcircled{43}$$

$$= 13 \times (\textcircled{96} - 2 \times \textcircled{43}) - 3 \times \textcircled{43}$$

$$= 13 \times \textcircled{96} - 29 \times \textcircled{43}.$$

(Check: $13 \times 96 - 29 \times 43 = 1248 - 1247 = 1$.)

Hence

$$(-29) \times 43 \equiv 1 \pmod{96},$$

and so -29 is a multiplicative inverse of 43 modulo 96. Since

$$-29 \equiv 67 \pmod{96},$$

67 is also a multiplicative inverse of 43 modulo 96.

Solution to Activity 31

(a) As 2 and 7 are coprime, the linear congruence has solutions. Trying the values 1, 2, 3, ... one by one, we find that

$$2 \times 6 \equiv 12 \equiv 5 \pmod{7},$$

and so the solutions are given by

$$x \equiv 6 \pmod{7}.$$

(There is a clever alternative way of solving this linear congruence. Notice that

$$5 \equiv -2 \pmod{7},$$

and so the linear congruence is equivalent to

$$2x \equiv -2 \pmod{7}.$$

Thus the solutions are given by

$$x \equiv -1 \equiv 6 \pmod{7}.)$$

(b) As 7 and 10 are coprime, the linear congruence has solutions. Trying the values 1, 2, 3, ... one by one, we find that

$$7 \times 4 \equiv 28 \equiv 8 \pmod{10},$$

and so the solutions are given by

$$x \equiv 4 \pmod{10}.$$

(c) Since

$$15 \equiv 4 \pmod{11} \quad \text{and} \quad -13 \equiv 9 \pmod{11},$$

the linear congruence is equivalent to

$$4x \equiv 9 \pmod{11}.$$

As 4 and 11 are coprime, this linear congruence has solutions. Trying the values 1, 2, 3, ... one by one, we find that

$$4 \times 5 \equiv 20 \equiv 9 \pmod{11},$$

and so the solutions are given by

$$x \equiv 5 \pmod{11}.$$

Solution to Activity 32

- (a) As 7 and 20 are coprime, the linear congruence has solutions. The solutions are given by

$$x \equiv 8v \pmod{20},$$

where v is a multiplicative inverse of 7 modulo 20.

Since

$$3 \times 7 \equiv 21 \equiv 1 \pmod{20},$$

we see that 3 is a multiplicative inverse of 7 modulo 20. So the solutions are given by

$$x \equiv 8 \times 3 \equiv 24 \equiv 4 \pmod{20}.$$

(Check: $7 \times 4 \equiv 28 \equiv 8 \pmod{20}$.)

(If you don't guess the value 3 of a multiplicative inverse of 7 modulo 20, then you can calculate a multiplicative inverse using Euclid's algorithm and backwards substitution. This method is used to calculate multiplicative inverses in the remaining parts of this activity.)

- (b) Since $-26 \equiv 8 \pmod{17}$, we can rewrite the linear congruence as

$$3x \equiv 8 \pmod{17}.$$

As 3 and 17 are coprime, the linear congruence has solutions. The solutions are given by

$$x \equiv 8v \pmod{17},$$

where v is a multiplicative inverse of 3 modulo 17.

Euclid's algorithm gives

$$17 = 5 \times 3 + 2$$

$$3 = 1 \times 2 + 1.$$

Backwards substitution gives

$$1 = 3 - 2 = 3 - (17 - 5 \times 3) = 6 \times 3 - 17.$$

So

$$6 \times 3 \equiv 1 \pmod{17}$$

and hence 6 is a multiplicative inverse of 3 modulo 17. So the solutions are given by

$$x \equiv 8 \times 6 \equiv 48 \equiv 14 \pmod{17}.$$

(Check: $3 \times 14 \equiv 3 \times (-3) \equiv -9 \equiv 8 \pmod{17}$.)

- (c) As 13 and 30 are coprime, the linear congruence has solutions. The solutions are given by

$$x \equiv 3v \pmod{30},$$

where v is a multiplicative inverse of 13 modulo 30.

Euclid's algorithm gives

$$30 = 2 \times 13 + 4$$

$$13 = 3 \times 4 + 1.$$

Backwards substitution gives

$$1 = 13 - 3 \times 4$$

$$= 13 - 3 \times (30 - 2 \times 13)$$

$$= 7 \times 13 - 3 \times 30.$$

So

$$7 \times 13 \equiv 1 \pmod{30}$$

and hence 7 is a multiplicative inverse of 13 modulo 30. So the solutions are given by

$$x \equiv 3 \times 7 \equiv 21 \pmod{30}.$$

(Check:

$$13 \times 21 \equiv 13 \times (-9) \equiv -117 \equiv 3 \pmod{30}.)$$

Solution to Activity 33

Let N be the total number of coins. There are 6 coins left over when the N coins are first shared out among the 10 pirates, so

$$N \equiv 6 \pmod{10}.$$

The second time the N coins are shared out, among the remaining 7 pirates, there are no coins left over, so $N = 7x$, for some positive integer x . Substituting $N = 7x$ into the first congruence gives

$$7x \equiv 6 \pmod{10}.$$

Trying the values 1, 2, 3, ... one by one, we find that

$$7 \times 8 \equiv 56 \equiv 6 \pmod{10}$$

and so the possible solutions are given by

$$x \equiv 8 \pmod{10}.$$

Since the total number of coins $N = 7x$ is no more than 100, the only possibility is that $N = 7 \times 8 = 56$.

Solution to Activity 34

- (a) The highest common factor of 4 and 10 is 2. Since 5 is not divisible by 2, the linear congruence has no solutions.
- (b) The highest common factor of -12 and 42 is 6. Since 8 is not divisible by 6, the linear congruence has no solutions.
- (c) To find the highest common factor of 48 and 111, we apply Euclid's algorithm:

$$111 = 2 \times 48 + 15$$

$$48 = 3 \times 15 + 3$$

$$15 = 5 \times 3 + 0.$$

Therefore the highest common factor is 3. Since 70 is not divisible by 3, the linear congruence has no solutions.

Solution to Activity 35

- (a) The highest common factor of 12 and 15 is 3. Since 6 is also divisible by 3, the linear congruence can be solved and is equivalent to

$$4x \equiv 2 \pmod{5}.$$

Trying the values 1, 2, 3, ... one by one, we find that

$$4 \times 3 \equiv 12 \equiv 2 \pmod{5}.$$

So the solutions are given by

$$x \equiv 3 \pmod{5}.$$

(Check: $4 \times 3 \equiv 12 \equiv 2 \pmod{5}$.)

(Alternatively, proceed as before to obtain the linear congruence

$$4x \equiv 2 \pmod{5}.$$

Since $4 \equiv -1 \pmod{5}$, this linear congruence is equivalent to

$$-x \equiv 2 \pmod{5}.$$

Hence the solutions are given by

$$x \equiv -2 \equiv 3 \pmod{5}.)$$

- (b) Since $-25 \equiv 15 \pmod{40}$, the linear congruence can be rewritten as

$$15x \equiv 10 \pmod{40}.$$

The highest common factor of 15 and 40 is 5. Since 10 is also divisible by 5, this linear congruence has solutions and is equivalent to

$$3x \equiv 2 \pmod{8}.$$

Trying the values 1, 2, 3, ... one by one, we find that

$$3 \times 6 \equiv 18 \equiv 2 \pmod{8}.$$

So the solutions are given by

$$x \equiv 6 \pmod{8}.$$

(Check: $3 \times 6 \equiv 18 \equiv 2 \pmod{8}$.)

- (c) To find the highest common factor of 18 and 98, you could apply Euclid's algorithm, but it's probably easier to express each number as a product of prime factors: $18 = 2 \times 3^2$ and $98 = 2 \times 7^2$. You can see that the highest common factor is 2. Since 6 is divisible by 2, the linear congruence has solutions and is equivalent to

$$9x \equiv 3 \pmod{49}.$$

The solutions of this linear congruence are given by

$$x \equiv 3v \pmod{49},$$

where v is a multiplicative inverse of 9 modulo 49.

Euclid's algorithm gives

$$49 = 5 \times 9 + 4$$

$$9 = 2 \times 4 + 1.$$

Backwards substitution gives

$$1 = 9 - 2 \times 4$$

$$= 9 - 2(49 - 5 \times 9)$$

$$= 11 \times 9 - 2 \times 49.$$

So

$$11 \times 9 \equiv 1 \pmod{49},$$

and hence 11 is a multiplicative inverse of 9 modulo 49. So the solutions are given by

$$x \equiv 3 \times 11 \equiv 33 \pmod{49}.$$

(Check:

$$9 \times 33 \equiv 9 \times (-16) \equiv -144 \equiv 3 \pmod{49}.)$$

Solution to Activity 36

- (a) Since $21 \equiv 3 \pmod{9}$, we can rewrite the linear congruence as

$$5x \equiv 3 \pmod{9}.$$

As 5 and 9 are coprime, the linear congruence has solutions. Trying the values 1, 2, 3, ... one by one, we find that

$$5 \times 6 \equiv 30 \equiv 3 \pmod{9}.$$

So the solutions are given by

$$x \equiv 6 \pmod{9}.$$

- (b) As 11 and 38 are coprime, the linear congruence has solutions. The solutions are given by

$$x \equiv 6v \pmod{38},$$

where v is a multiplicative inverse of 11 modulo 38.

Euclid's algorithm gives

$$38 = 3 \times 11 + 5$$

$$11 = 2 \times 5 + 1.$$

Backwards substitution gives

$$1 = 11 - 2 \times 5$$

$$= 11 - 2(38 - 3 \times 11)$$

$$= 7 \times 11 - 2 \times 38.$$

So

$$7 \times 11 \equiv 1 \pmod{38}$$

and hence 7 is a multiplicative inverse of 11 modulo 38. So the solutions are given by

$$x \equiv 6 \times 7 \equiv 42 \equiv 4 \pmod{38}.$$

(Check: $11 \times 4 \equiv 44 \equiv 6 \pmod{38}$.)

- (c) The highest common factor of 21 and 30 is 3. Since 14 is not divisible by 3, the linear congruence has no solutions.
- (d) Since $-48 \equiv 8 \pmod{28}$, the linear congruence can be rewritten as
- $$8x \equiv 24 \pmod{28}.$$
- The highest common factor of 8 and 28 is 4. Since 24 is also divisible by 4, this linear congruence has solutions and is equivalent to
- $$2x \equiv 6 \pmod{7}.$$
- Trying the values 1, 2, 3, ... one by one, we find that
- $$2 \times 3 \equiv 6 \pmod{7}.$$

So the solutions are given by

$$x \equiv 3 \pmod{7}.$$

(Check: $2 \times 3 \equiv 6 \pmod{7}$.)

Solution to Activity 37

Using Table 1, the message BROUHAHA becomes

1, 17, 14, 20, 7, 0, 7, 0.

Next, applying the affine cipher

$$E(x) \equiv 3x + 14 \pmod{26},$$

we find that

$$E(1) \equiv 3 \times 1 + 14 \equiv 17 \pmod{26},$$

$$E(17) \equiv 3 \times 17 + 14 \equiv 65 \equiv 13 \pmod{26},$$

$$E(14) \equiv 3 \times 14 + 14 \equiv 56 \equiv 4 \pmod{26},$$

$$E(20) \equiv 3 \times 20 + 14 \equiv 74 \equiv 22 \pmod{26},$$

$$E(7) \equiv 3 \times 7 + 14 \equiv 35 \equiv 9 \pmod{26},$$

$$E(0) \equiv 3 \times 0 + 14 \equiv 14 \pmod{26}.$$

Therefore the enciphered message is

17, 13, 4, 22, 9, 14, 9, 14.

Solution to Activity 38

- (a) A rule D for deciphering the message is given by

$$D(y) \equiv v(y - 10) \pmod{26},$$

where v is a multiplicative inverse of 5 modulo 26.

Since

$$(-5) \times 5 \equiv -25 \equiv 1 \pmod{26},$$

we see that -5 is a multiplicative inverse of 5 modulo 26. (You can also use Euclid's algorithm and backwards substitution to find a multiplicative inverse of 5 modulo 26.) So

$$D(y) \equiv -5(y - 10) \pmod{26}.$$

Hence

$$D(14) \equiv -5(14 - 10) \equiv -20 \equiv 6 \pmod{26},$$

$$D(10) \equiv -5(10 - 10) \equiv 0 \pmod{26},$$

$$D(6) \equiv -5(6 - 10) \equiv 20 \pmod{26},$$

$$D(22) \equiv -5(22 - 10) \equiv -60 \equiv 18 \pmod{26}.$$

So the deciphered message is

6, 0, 20, 18, 18,

which, using Table 1, says

GAUSS.

(b) A rule D for deciphering the message is given by

$$D(y) \equiv v(y - 6) \pmod{26},$$

where v is a multiplicative inverse of -9 modulo 26.

Since

$$(-3) \times (-9) \equiv 27 \equiv 1 \pmod{26},$$

we see that -3 is a multiplicative inverse of -9 modulo 26. (You can also use Euclid's algorithm and backwards substitution to find a multiplicative inverse of -9 modulo 26.) So

$$D(y) \equiv -3(y - 6) \pmod{26}.$$

Hence

$$D(22) \equiv -3(22 - 6) \equiv -48 \equiv 4 \pmod{26},$$

$$D(8) \equiv -3(8 - 6) \equiv -6 \equiv 20 \pmod{26},$$

$$D(11) \equiv -3(11 - 6) \equiv -15 \equiv 11 \pmod{26},$$

$$D(9) \equiv -3(9 - 6) \equiv -9 \equiv 17 \pmod{26}.$$

So the deciphered message is

4, 20, 11, 4, 17,

which, using Table 1, says

EULER.

Acknowledgements

Grateful acknowledgement is made to the following sources:

Page 154: Srinivasa Ramanujan: Konrad Jacobs /
http://en.wikipedia.org/wiki/File:Srinivasa_Ramanujan_-_OPC_-_1.jpg.
This file is licensed under the Creative Commons Attribution-Share Alike
Licence <http://creativecommons.org/licenses/by-sa/3.0>

Every effort has been made to contact copyright holders. If any have been inadvertently overlooked the publishers will be pleased to make the necessary arrangements at the first opportunity.