8. Choose a value of n and count the number of elements in G_n. Try this with various values of n. Can you discover any rules governing the relation between n and the number of elements in G_n? [In Section 1.6 below we give rules for computing the number of elements in G_n directly from n.]
9. The observation that $10 \equiv 1 \bmod 9$ is the basis for the procedure of 'casting out nines'. The method is as follows.
   Given an integer X written in base 10 (as is usual), compute the sum of the digits of X: call the result the **digit sum** of X. If the digit sum is greater than 9, we form the digit sum again. Continue in this way to obtain the **iterated digit sum** which is at most 9. (Thus 5734 has digit sum 19 which has digit sum 10 which has digit sum 1, so the iterated digit sum of 5734 is 1.)
   Now suppose that we have a calculation which we want to check by hand: say, for example, someone claims that

$$873\,985 \times 79\,041 = 69\,069\,967\,565.$$

   Compute the iterated digit sums of 873 985 and 79 041 (these are 4 and 3 respectively), multiply these together (to get 12), and form the iterated digit sum of the product (which is 3). Then the result should equal the iterated digit sum of 69 069 967 565 (which is 5). Since it does not, the 'equality' is incorrect. If the results had been equal then all we could say would be that no error was detected.
   (i) Using the method of casting out nines what can you say about the following computations?

$$56\,563 \times 9961 = 563\,454\,043;$$
$$1234 \times 5678 \times 901 = 6\,213\,993\,452;$$
$$333 \times 666 \times 999 = 221\,556\,222.$$

   (ii) The following equation is false but you are told that only the underlined digit is in error. What is the correct value for that digit?

$$674\,532 \times 9764 = 6\,586\,140\,448.$$

   (iii) Justify the method of casting out nines.

1.5 Solving linear congruences

A **linear congruence** is an 'equation' of the form

$$ax \equiv b \bmod n$$

where x is an integer variable. Written in terms of congruence classes this

becomes the equation

$$[a]_n X = [b]_n$$

where a solution X is now to be a congruence class.

Such an equation may have

(i) no solution (as, for example, $2x \equiv 1 \bmod 4$),
(ii) exactly one solution (for example $2x \equiv 1 \bmod 5$), or
(iii) more than one solution (for example the congruence $2x \equiv 0 \bmod 4$ discussed at the beginning of Section 1.4).

The first result shows how to distinguish between these cases and how to find all solutions for such a congruence (if there are any). This result was first given by Brahmagupta (c. 628). Of course he did not express it as we have done: rather he gave the criterion for solvability of, and the general solution of, $ak + nt = b$, where a, n, b are fixed integers and k and t are integer unknowns. (Note that if we have solved $ax \equiv b \bmod n$ then if k is a solution for x we have that n divides $ak - b$, that is, $ak - b = ns$ for some integer s so, writing t for $-s$, we have $ak + nt = b$. Since a, k, n and b are known we compute t from this equation. Therefore solving $ak + nt = b$ for k and t is equivalent to solving the congruence $ax \equiv b \bmod n$ for x.) An equation of the form $ak + nt = b$ is 'indeterminate' in the sense that, since it is just one equation with two unknowns, it has infinitely many solutions if it has any at all. One sees, however, that the solutions form themselves into complete congruence classes.

Theorem 1.5.1 *The linear congruence*

$$ax \equiv b \bmod n$$

has solutions if and only if the greatest common divisor, d, of a and n divides b. If d does divide b there are d solutions up to congruence modulo n, and these solutions are all congruent modulo n/d.

Proof Suppose that there is a solution, c say, to

$$ax \equiv b \bmod n.$$

Then, since

$$ac \equiv b \bmod n,$$

we have that n divides $ac - b$; say

$$ac - b = nk.$$

Rearrange this to obtain

$$b = ac - nk.$$

The greatest common divisor d of a and n divides both terms on the right-hand side of this equation, and hence we deduce that d divides b, as claimed.

Conversely, suppose d divides b, say $b = de$. Write d as a linear combination of a and n; say

$$d = ak + nt.$$

Multiply this by e to obtain

$$b = ake + nte.$$

This gives

$$a(ke) \equiv b \bmod n,$$

and so the congruence has a solution, ke, as required. Therefore the first assertion of the theorem has been proved.

Suppose now that c is a solution of

$$ax \equiv b \bmod n.$$

So as before we have

$$ac = b + nk$$

for some integer k. By the above, d divides b and hence we may divide this equation by d to get the equation in integers

$$(a/d)\,c = b/d + (n/d)k.$$

Thus

$$(a/d)\,c \equiv b/d \bmod (n/d).$$

That is, every solution of the original congruence is also a solution of the congruence

$$(a/d)\,x \equiv b/d \bmod (n/d).$$

Conversely it is easy to see (by reversing the steps) that every solution to this second congruence is also a solution to the original one. So the solution is really a congruence class modulo n/d. Such a congruence class splits into d distinct congruence classes modulo n. Namely if c is a solution then the congruence classes of

$$c,\ c + (n/d),\ c + 2\,(n/d),\ c + 3\,(n/d),\ \ldots,\ c + (d-1)\,(n/d)$$

are distinct solutions modulo n, and are all the solutions modulo n. □

Comment We strongly suggest working through the above proof with particular values for a, b and n (say, the values from Example 3 (or 4) below). Try running the proof with particular numbers parallel to the proof with letters to see how the general and special cases relate to each other.

This yields the following method for solving a linear congruence.

To find all solutions of the linear congruence $ax \equiv b \bmod n$.

1. Calculate $d = (a, n)$.
2. Test whether d divides b.
   (a) If d does not divide b then there is no solution.
   (b) If d divides b then there are d solutions mod n.
3. To find the solutions in case (b), 'divide the congruence throughout by d' to get
$$(a/d)x \equiv (b/d) \bmod (n/d).$$
Notice that since a/d and n/d have greatest common divisor 1, this congruence will have a unique solution.
4. Calculate the inverse $[e]_{n/d}$ of $[a/d]_{n/d}$ (by inspection or by the matrix method).
5. Multiply to get
$$[x]_{n/d} = [e]_{n/d}[b/d]_{n/d}$$
and calculate a solution, c, for x.
6. The solutions to the original congruence will be the classes modulo n of
$$c, c + (n/d), \ldots, c + (d-1)(n/d).$$

Example 1 Solve the congruence
$$6x \equiv 5 \bmod 17.$$
Since $(6, 17) = 1$ and 1 divides 5 there is, by Theorem 1.5.1, a unique solution modulo 17. It is found by calculating $[6]_{17}^{-1}$ (found by inspection to be $[3]_{17}$) and multiplying both sides by this inverse. We obtain
$$x \equiv 3 \times 5 \equiv 15 \bmod 17$$
as the solution (unique up to congruence mod 17). (Therefore the values of x which are solutions are $\ldots, -19, -2, 15, 32, \ldots$.)

Example 2 To solve
$$6x \equiv 5 \bmod 15$$
note that $(6, 15) = 3$ and 3 does not divide 5, so by 1.5.1 there is no solution.

Example 3 In the congruence

$$6x \equiv 9 \bmod 15,$$

$(6, 15) = 3$ and 3 divides 9, so by 1.5.1 there are three solutions up to congruence modulo 15.

To find these we find the solutions up to congruence modulo 5 ($5 = 15/3$), and we do this by dividing the whole congruence by the greatest common divisor of 6 and 15. This gives

$$2x \equiv 3 \bmod 5.$$

Now, $(2, 5) = 1$ so there is a unique solution (this is the point of dividing through by the gcd). One quickly sees that

$$x \equiv 4 \bmod 5$$

is the unique solution mod 5. The proof of 1.5.1 shows that the solutions of the original congruence are therefore the members of the congruence class $[4]_5$. In order to describe the solutions in terms of congruence classes modulo 15, we note that $[4]_5$ splits up as

$$[4]_{15}, [4 + 5]_{15}, [4 + 10]_{15}$$

that is, as

$$[4]_{15}, [9]_{15}, [14]_{15}.$$

Example 4 Solve the congruence

$$432x \equiv 12 \bmod 546.$$

The first task is to calculate the greatest common divisor of 432 and 546. Since we do not need to express this as a linear combination of 432 and 546 it is not necessary to use the matrix method: it is enough to factorise these numbers. We have that 432 is 6 times 72 while 546 is 6 times 91: since 91 is 7×13 and 72 is 8×9 one sees that 432 and 546 have no common factor greater than 6. Dividing the congruence by 6 gives

$$72x \equiv 2 \bmod 91.$$

The next task is to find the inverse of 72 modulo 91, and unless the reader is unusually gifted at arithmetic calculations, this is best done using the matrix method:

$$\left(\begin{array}{cc|c} 1 & 0 & 91 \\ 0 & 1 & 72 \end{array}\right) \to \left(\begin{array}{cc|c} 1 & -1 & 19 \\ 0 & 1 & 72 \end{array}\right) \to \left(\begin{array}{cc|c} 1 & -1 & 19 \\ -3 & 4 & 15 \end{array}\right) \to \left(\begin{array}{cc|c} 4 & -5 & 4 \\ -3 & 4 & 15 \end{array}\right)$$

$$\to \left(\begin{array}{cc|c} 4 & -5 & 4 \\ -15 & 19 & 3 \end{array}\right) \to \left(\begin{array}{cc|c} 19 & -24 & 1 \\ -15 & 19 & 3 \end{array}\right).$$

The top line of this matrix corresponds to the equation $19 \cdot 91 - 24 \cdot 72 = 1$ so it follows that the inverse of 72 modulo 91 is -24, or 67. So multiply both sides of the congruence by 67 to obtain

$$\begin{aligned} x &\equiv 2 \times 67 \bmod 91 \\ &\equiv 134 \bmod 91 \\ &\equiv 43 \bmod 91. \end{aligned}$$

Finally, to describe the solutions in terms of congruence classes modulo 546, we have that $[43]_{91}$ splits into six congruence classes modulo 546, namely

$$[43]_{546}, [134]_{546}, [225]_{546}, [316]_{546}, [407]_{546}, [498]_{546}.$$

Next we consider how to solve systems of linear congruences.

Suppose that we wish to find an integer which, when divided by 7 has a remainder of 3, and when divided by 25 has a remainder of 6. Is there such an integer? and if so how does one find it?

This question may be formulated in terms of congruences as:
find an integer x that satisfies

$$x \equiv 3 \bmod 7 \text{ and } x \equiv 6 \bmod 25.$$

The next theorem implies that there is a simultaneous solution to these congruences, and its proof tells us how to find a solution.

The theorem may have been known to the eighth century Buddhist monk Yi Xing. Certainly it appears in Qín Jiǔsháo's *Shù shū jiǔ zhāng* (*Mathematical Treatise in Nine Sections*) of 1247.

Theorem 1.5.2 (Chinese Remainder Theorem) *Suppose that $m \geq 2$ and $n \geq 2$ are relatively prime integers and that a and b are any integers. Then there is a simultaneous solution to the congruences*

$$\begin{aligned} x &\equiv a \bmod m, \\ x &\equiv b \bmod n. \end{aligned}$$

The solution is unique up to congruence mod mn.

Proof Since m and n are relatively prime, there exist integers k and t such that

$$mk + nt = 1. \qquad (*)$$

Then it is easily checked that $c = bmk + ant$ is a simultaneous solution for the congruences. For,

$$c \equiv ant \bmod m$$

and, from equation (*)

$$nt \equiv 1 \bmod m.$$

Hence

$$c \equiv a \times 1 = a \bmod m.$$

The proof that c is congruent to b modulo n is similar.

To show that the solution is unique up to congruence modulo mn, suppose that each of c, d is a solution to both congruences. Then

$$c \equiv a \bmod m \text{ and } d \equiv a \bmod m.$$

Hence

$$c - d \equiv 0 \bmod m.$$

Similarly

$$c - d \equiv 0 \bmod n.$$

That is, $c - d$ is divisible by both m and n. Since m and n are relatively prime it follows by Theorem 1.1.6(ii) that $c - d$ is divisible by mn, and hence c and d lie in the same congruence class mod mn.

Conversely, if c is a solution to both congruences and if

$$d \equiv c \bmod mn$$

then d is of the form $c + kmn$, and so the remainder when d is divided by m or n is the same as the remainder when c is divided by m or n. So d solves both congruences, as required. □

Comment For the first part of the proof (existence of a solution) notice that the equation $mk + nt = 1$, when reduced modulo n, becomes $[mk]_n = [1]_n$ so, if we multiply both sides by $[b]_n$ we obtain $[bmk]_n = [b]_n$. That is where the term bmk in $c = bmk + ant$ comes from, similarly (reducing mod m) for the other term.

Example Consider the problem, posed before the statement of Theorem 1.5.2, of finding a solution to the congruences

$$x \equiv 3 \bmod 7 \text{ and } x \equiv 6 \bmod 25.$$

First, find a combination of 7 and 25 which is 1: one such combination is

$$7(-7) + 25 \times 2 = 1.$$

Then we multiply these two terms by 6 and 3 respectively. (Note the 'swop over'!) This gives us

$$6 \cdot 7 \cdot (-7) + 3 \cdot 25 \cdot 2 = -144.$$

So the solution is $[-144]_{175}$ ($175 = 7 \cdot 25$). We should put this in standard form by adding a suitable multiple of 175: we obtain that the solution is $[31]_{175}$.

Alternatively, there is a method for solving this type of problem which does not involve having to remember how to construct the solution. We repeat the above example to illustrate this method.

A solution of the first congruence is of the form

$$x = 3 + 7k,$$

so if x satisfies the second congruence, we have

$$3 + 7k \equiv 6 \bmod 25.$$

Now solve this congruence for k: we have

$$7k \equiv 3 \bmod 25.$$

The inverse of 7 modulo 25 is 18 (by inspection), so

$$\begin{aligned} k &\equiv 3 \times 18 \bmod 25 \\ &\equiv 4 \bmod 25. \end{aligned}$$

Thus, for some integer r,

$$\begin{aligned} x &= 3 + 7(4 + 25r) \\ &= 3 + 28 + 175r \\ &= 31 + 175r \end{aligned}$$

as before.

Each of these methods allows us to solve systems of more than two congruences, so long as the 'moduli' are pairwise relatively prime, by solving two congruences at a time. Actually in the *Mathematical Treatise in Nine Sections* there are examples to show that the idea behind the method may sometimes be applied even if the moduli are not all pairwise relatively prime (see [Needham, Section 19 (i) (4)] or [Li Yan and Du Shiran, p. 165]).

Example Solve the simultaneous congruences

$$\begin{aligned} x &\equiv 2 \bmod 7 \\ x &\equiv 0 \bmod 9 \\ 2x &\equiv 6 \bmod 8. \end{aligned}$$

Observe that the third congruence is not in an immediately usable form, so we first solve it to obtain the two (since $(2, 8) = 2$) solutions:

$$x \equiv 3 \bmod 8 \text{ and } x \equiv 7 \bmod 8.$$

So now we have two sets of three congruences to solve, and we could treat these as entirely separate problems, only combining the solutions at the end. We may note, however, that there is no need to separate the solution for the third congruence into two solutions modulo 8, since the solution is really just the congruence class $[3]_4$. Thus we reduce to solving the simultaneous congruences

$$x \equiv 2 \bmod 7$$
$$x \equiv 0 \bmod 9$$
$$x \equiv 3 \bmod 4.$$

Since $(7, 9) = 1 = (7, 4) = (9, 4)$ we will be able to apply 1.5.2. Take (say) the first two congruences to solve together. We have

$$7 \cdot (-5) + 9 \cdot 4 = 1,$$

so a solution to the first two is:

$$0 \cdot 7(-5) + 2 \cdot 9 \cdot 4 = 72 \bmod 7 \cdot 9.$$

This simplifies to 9 mod 63. So now the problem has been reduced to solving

$$x \equiv 9 \bmod 63$$
$$x \equiv 3 \bmod 4.$$

We have

$$16 \cdot 4 - 1 \cdot 63 = 1.$$

This gives

$$9 \cdot 16 \cdot 4 - 3 \cdot 1 \cdot 63 \bmod 63 \cdot 4$$

as the solution. This simplifies to 135 mod 252.

Finally, in this section, we briefly consider solving non-linear congruences. There are many deep and difficult problems here and to give a reasonable account would take us very far afield. So we content ourselves with merely indicating a few points (below, and in the exercises).

Example Consider the quadratic equation

$$x^2 + 1 \equiv 0 \bmod n.$$

The existence of solutions, as well as the number of solutions, depends on n. For example, when n is 3, we can substitute the three congruence classes $[0]_3$, $[1]_3$ and $[2]_3$ into the equation to see that $x^2 + 1$ is never $[0]_3$. When n is 5, it can be seen that $[2]_5$ and $[3]_5$ are solutions. If n is 65, it can be checked that $[8]_{65}$, $[-8]_{65}$, $[18]_{65}$ and $[-18]_{65}$ are all solutions, and this leads to the (different) factorisations

$$\begin{aligned} x^2 + 1 &\equiv (x + 8)(x - 8) \bmod 65 \\ &\equiv (x + 18)(x - 18) \bmod 65. \end{aligned}$$

When n is a prime, however, to the extent that a polynomial can be factorised, the factorisation is unique.

Example Consider the polynomial $x^3 - x^2 + x + 1$: does it have any integer roots? Suppose that it had an integer root k: then we would have $k^3 - k^2 + k + 1 = 0$. Let n be any integer greater than 1, and reduce this equation modulo n to obtain

$$[k]_n^3 - [k]_n^2 + [k]_n + [1]_n = [0]_n.$$

So we would have that the polynomial $X^3 - X^2 + X + [1]_n$ with coefficients from $\mathbb{Z}_n$ has a root in $\mathbb{Z}_n$. This would be true for *every* n.

Let us take $n = 2$: so reducing $x^3 - x^2 + x + 1 = 0$ modulo 2 gives $X^3 - X^2 + X + [1]_2$. It is straightforward to check whether or not this equation has a solution in $\mathbb{Z}_2$: all we have to do is to substitute $[0]_2$ and $[1]_2$ in turn. Doing this, we find that $[1]_2$ is a root. This tells us nothing about whether or not the original polynomial has a root.

So we try taking $n = 3$: reduced modulo 3, the polynomial becomes $X^3 - X^2 + X + [1]_3$. Let us see whether this has a root in $\mathbb{Z}_3$. Substituting in turn $[0]_3$, $[1]_3$ and $[2]_3$ for X we get the values $[1]_3$, $[2]_3$ and $[1]_3$ for the polynomial. In particular none of these is zero, so the polynomial has no root modulo 3. Therefore the original polynomial has no integer root (for by the argument above, if it did, then it would also have to have a root modulo 3). In Chapter 6 we look again at polynomials with coefficients which are congruence classes.

Exercises 1.5

1. Find all the solutions (when there are any) of the following linear congruences:
   (i) $3x \equiv 1 \bmod 12$;
   (ii) $3x \equiv 1 \bmod 11$;
   (iii) $64x \equiv 32 \bmod 84$;

(iv) $15x \equiv 5 \bmod 17$;
(v) $15x \equiv 5 \bmod 18$;
(vi) $15x \equiv 5 \bmod 100$;
(vii) $23x \equiv 16 \bmod 107$.

2. Solve the following sets of simultaneous linear congruences:
(i) $x \equiv 4 \bmod 24$ and $x = 7 \bmod 11$;
(ii) $3x \equiv 1 \bmod 5$ and $2x \equiv 6 \bmod 8$;
(iii) $x \equiv 3 \bmod 5$, $2x \equiv 1 \bmod 7$ and $x \equiv 3 \bmod 8$.

3. Find the smallest positive integer whose remainder when divided by 11 is 8, which has last digit 4 and is divisible by 27.

4. (i) Show that the polynomial $x^4 + x^2 + 1$ has no integer roots, but that it has a root modulo 3, and factorise it over $\mathbb{Z}_3$.
(ii) Show that the equation $7x^3 - 6x^2 + 2x - 1 = 0$ has no integer solutions.

5. A hoard of gold pieces 'comes into the possession of' a band of 15 pirates. When they come to divide up the coins, they find that three are left over. Their discussion of what to do with these extra coins becomes animated, and by the time some semblance of order returns there remain only 7 pirates capable of making an effective claim on the hoard. When, however, the hoard is divided between these seven it is found that two pieces are left over. There ensues an unfortunate repetition of the earlier disagreement, but this does at least have the consequence that the four pirates who remain are able to divide up the hoard evenly between them. What is the minimum number of gold pieces which could have been in the hoard?

1.6 Euler's Theorem and public key codes

Suppose that we are interested in the behaviour of integers modulo 20. Fix an integer a and then form the successive powers of its congruence class:

$$[a]_{20}, [a]_{20}^2, [a]_{20}^3, \ldots, [a]_{20}^n, \ldots$$

What can happen? Let us try some examples (write '[3]' for '$[3]_{20}$' etc.). Taking $a = 3$ we obtain

$$[3]^1 = [3],\ [3]^2 = [9],\ [3]^3 = [27] = [7],$$
$$[3]^4 = [3]^3[3] = [7][3] = [21] = [1],\ [3]^5 = [3]^4[3] = [1][3] = [3],$$
$$[3]^6 = [3]^2 = [9],\ [3]^7 = [3]^3 = [7],\ [3]^8 = [1],\ [3]^9 = [3], \ldots$$

Observe that the successive powers are different until we reach [1] and then the pattern starts to repeat.